aws

Entwicklerhandbuch

OpenSearch Amazon-Dienst



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

OpenSearch Amazon-Dienst: Entwicklerhandbuch

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, Kunden irrezuführen oder Amazon in irgendeiner Weise herabzusetzen oder zu diskreditieren. Alle anderen Handelsmarken, die nicht Eigentum von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise zu Amazon gehören oder nicht, mit Amazon verbunden sind oder von Amazon gesponsert werden.

Table of Contents

Was ist Amazon OpenSearch Service? 1
Funktionen von Amazon OpenSearch Service 2
Wann sollte dies verwendet werden? 3
Unterstützte Versionen von Elasticsearch und OpenSearch 4
Standard- und verlängerter Support 4
Unterstützte Standardversionen und erweiterte Versionen 7
Berechnung der Gebühren für verlängerten Support 7
Preisgestaltung 9
Zugehörige Services 9
Einrichtung 11
Erteilen Sie Berechtigungen 11
Erteilen programmgesteuerten Zugriffs 11
Richten Sie das ein AWS CLI 13
Öffnen Sie die -Konsole 14
Erste Schritte 15
Domain erstellen 16
Daten für die Indizierung hochladen 17
Option 1: Hochladen eines einzelnen Dokuments 18
Option 2: Hochladen mehrerer Dokumente 18
Dokumente suchen 19
So suchen Sie Dokumente über die Befehlszeile 19
So suchen Sie Dokumente mit OpenSearch Dashboards 21
Domäne löschen 22
OpenSearch Einnahme durch Amazon 23
Die wichtigsten Konzepte 23
Vorteile 25
Einschränkungen 26
Unterstützte Data Prepper-Versionen 26
Skalierung von Pipelines 27
Preisgestaltung 29
Unterstützt AWS-Regionen 29
Rollen und Benutzer einrichten 29
Rolle „Pipeline“ 31
Rolle „Aufnahme“ 34

Pipelines Zugriff auf Domains gewähren ... 36
Pipelines Zugriff auf Sammlungen gewähren ... 40
Erste Schritte mit Ingestion OpenSearch ... 46
Tutorial: Daten in eine Domain aufnehmen ... 46
Tutorial: Daten in eine Sammlung aufnehmen ... 55
Funktionen der Pipeline ... 62
Dauerhafte Pufferung ... 63
Aufteilen ... 65
Verkettung ... 66
Warteschlangen für unzustellbare Nachrichten ... 67
Indexverwaltung ... 69
End-to-end Bestätigung ... 73
Gegendruck an der Quelle ... 73
Pipelines erstellen ... 74
Voraussetzungen und erforderliche IAM-Rolle ... 75
Erforderliche IAM-Berechtigungen ... 75
Angabe der Pipeline-Version ... 77
Angeben des Aufnahmepfads ... 78
Pipelines erstellen ... 79
Den Status der Pipeline-Erstellung verfolgen ... 84
Mit Blueprints arbeiten ... 85
Pipelines anzeigen ... 87
Pipelines aktualisieren ... 90
Überlegungen ... 90
Erforderliche Berechtigungen ... 91
Pipelines werden aktualisiert ... 92
Blaue/grüne Bereitstellungen für Pipeline-Updates ... 93
Verwalten von Pipelinekosten ... 93
Stoppen einer Pipeline ... 94
Starten einer Pipeline ... 95
Löschen von Pipelines ... 96
Unterstützte Plugins und Optionen ... 97
Unterstützte Plugins ... 98
Stateless versus statusbehaftete Prozessoren ... 100
Konfigurationsanforderungen und Einschränkungen ... 101
Integration von Pipelines ... 106

Aufbau des Aufnahmeendpunkts ... 106
Eine Aufnahmerolle erstellen ... 107
Atlassian-Dienste ... 109
Amazon-DynamoDB ... 127
Amazon DocumentDB ... 144
Confluent Cloud Kafka ... 163
Amazon MSK ... 173
Amazon S3 ... 181
Amazon Security Lake ... 191
Fluent Bit ... 196
Fluentd ... 198
OpenTelemetry Kollektor ... 200
Selbstverwaltetes Kafka ... 202
Selbstverwaltete Cluster OpenSearch ... 210
Amazon Kinesis Data Streams ... 218
Nächste Schritte ... 224
AWS Lambda ... 224
Daten zwischen Domains und Sammlungen migrieren ... 227
Einschränkungen ... 228
OpenSearch Dienst als Quelle ... 229
Angabe mehrerer OpenSearch Service-Domain-Senken ... 231
Migrieren von Daten zu einer OpenSearch serverlosen VPC-Sammlung ... 232
Verwaltung von Pipelines mit dem AWS SDKs ... 232
Python ... 233
Sicherheit bei der Datenaufnahme OpenSearch ... 237
Konfigurieren des VPC-Zugriffs für Pipelines ... 238
Identitäts- und Zugriffsverwaltung ... 243
Überwachung mit CloudTrail ... 252
Markieren von Pipelines ... 256
Erforderliche Berechtigungen ... 257
Arbeiten mit Tags (Konsole) ... 257
Arbeiten mit Tags (AWS CLI) ... 258
Protokollierung und Überwachung ... 259
Überwachen der Pipeline-Protokolle ... 259
Überwachen der Pipeline ... 261
Bewährte Methoden ... 294

Allgemeine bewährte Methoden ... 295
Empfohlene CloudWatch Alarme ... 295
Amazon OpenSearch Serverlos ... 302
Vorteile ... 302
Was ist Amazon OpenSearch Serverless? ... 303
Anwendungsfälle für Serverless OpenSearch ... 304
Funktionsweise ... 304
Auswahl eines Sammlungstyps ... 306
Preisgestaltung ... 307
Unterstützt AWS-Regionen ... 308
Einschränkungen ... 308
Vergleich von OpenSearch Service und Serverless OpenSearch ... 309
Tutorial: Erste Schritte mit Serverless OpenSearch ... 313
Schritt 1: Konfigurieren von Berechtigungen ... 314
Schritt 2: Erstellen einer Sammlung ... 315
Schritt 3: Daten hochladen und suchen ... 316
Schritt 4: Sammlung löschen ... 317
Nächste Schritte ... 318
Erstellen und Verwalten von Sammlungen ... 318
Verwalten von Sammlungen ... 319
Arbeiten mit Sammlungen für die Vektorsuche ... 328
Verwenden von Datenlebenszyklus-Richtlinien ... 337
Verwaltung von Sammlungen mit dem AWS SDKs ... 346
Sammlungen erstellen mit CloudFormation ... 357
Verwalten von Kapazitätsgrenzen ... 359
Konfigurieren von Kapazitätseinstellungen ... 362
Maximale Kapazitätsgrenzen ... 362
Überwachung der Kapazitätsnutzung ... 363
Erfassung von Daten in Sammlungen ... 363
Erforderliche Mindestberechtigungen ... 364
OpenSearch Verschlucken ... 365
Fluent Bit ... 365
Amazon Data Firehose ... 366
Go ... 366
Java ... 369
JavaScript ... 370

Logstash ... 373
Python ... 375
Ruby ... 377
Andere Kunden ... 378
Sicherheit bei Serverless OpenSearch ... 379
Verschlüsselungsrichtlinien ... 381
Netzwerkrichtlinien ... 382
Daten-Zugriffsrichtlinien ... 383
IAM und SAML-Authentifizierung ... 384
Sicherheit der Infrastruktur ... 384
Erste Schritte mit Sicherheit ... 385
Identitäts- und Zugriffsverwaltung ... 400
Verschlüsselung ... 419
Netzwerkzugriff ... 430
Datenzugriffskontrolle ... 442
VPC-Endpunkte ... 453
SAML-Authentifizierung ... 465
Compliance-Validierung ... 475
Markieren von Sammlungen ... 476
Erforderliche Berechtigungen ... 477
Markieren von Sammlungen (Konsole) ... 477
Sammlungen taggen ()AWS CLI ... 478
Unterstützte Vorgänge und Plugins ... 478
Unterstützte OpenSearch API-Operationen und -Berechtigungen ... 478
Unterstützte OpenSearch Plugins ... 484
Überwachen von OpenSearch Serverless-Management ... 485
Überwachung mit CloudWatch ... 486
Überwachung mit CloudTrail ... 492
Überwachung mit EventBridge ... 495
Erstellen und Verwalten von Domains ... 499
OpenSearch Dienstdomänen erstellen ... 499
OpenSearch Dienstdomänen erstellen (Konsole) ... 499
OpenSearch Dienstdomänen erstellen (AWS CLI) ... 506
OpenSearch Dienstdomänen erstellen (AWS SDKs) ... 508
OpenSearch Dienstdomänen erstellen (AWS CloudFormation) ... 508
Konfigurieren von Zugriffsrichtlinien ... 508

Erweiterte Clustereinstellungen ... 509
Konfigurationsänderungen ... 510
Änderungen, die normalerweise zu Bereitstellungen führen blue/green ... 510
Änderungen, die normalerweise nicht zu blue/green Bereitstellungen führen ... 511
Feststellen, ob eine Änderung eine Blau/Grün-Bereitstellung verursacht ... 512
Verfolgen einer Konfigurationsänderung ... 517
Stufen einer Konfigurationsänderung ... 519
Auswirkungen von blauen/grünen Bereitstellungen auf die Leistung ... 522
Gebühren für Konfigurationsänderungen ... 523
Beheben von Validierungsfehlern ... 523
Service-Software-Updates ... 529
Optionale und erforderliche Updates ... 530
Patch-Updates ... 531
Überlegungen ... 531
Starten eines Updates ... 532
Zeitfenster außerhalb der Spitzenzeiten ... 535
Überwachung von Updates ... 536
Wenn Domains nicht für ein Update in Frage kommen ... 537
Zeitfenster außerhalb der Spitzenzeiten ... 538
Softwareupdates für den Service außerhalb der Spitzenzeiten ... 539
Auto-Tune-Optimierungen außerhalb der Spitzenzeiten ... 539
Aktivierung des Zeitfensters außerhalb der Spitzenzeiten ... 540
Konfiguration eines benutzerdefinierten Zeitfensters außerhalb der Spitzenzeiten ... 541
Geplante Aktionen anzeigen ... 542
So verschieben Sie den Termin ... 543
Migration von Auto-Tune-Wartungsfenstern ... 545
Benachrichtigungen ... 547
Einstieg in die Verwendung von Benachrichtigungen ... 547
Schweregrad ... 548
Beispiel für ein Ereignis EventBridge ... 549
Konfigurieren einer Multi-AZ-Domain ... 550
Multi-AZ mit Standby ... 550
Multi-AZ ohne Standby ... 552
Unterbrechungen bei Availability Zones ... 556
VPC-Unterstützung ... 558
VPC im Vergleich zu öffentlichen Domänen ... 558

Einschränkungen ... 559
Architektur ... 559
Erstellen von Index-Snapshots ... 567
Voraussetzungen ... 568
Registrieren eines manuellen Snapshot-Repositorys ... 572
Manuelle Snapshots erstellen ... 577
Wiederherstellen von Snapshots ... 578
Löschen von manuellen Snapshots ... 581
Automatisieren von Snapshots mit Snapshot Management ... 581
Automatisieren von Snapshots mit Index-Statusmanagement ... 583
Verwenden von Curator für Snapshots ... 584
Aktualisieren von Domains ... 584
Unterstützte Upgrade-Pfade ... 585
Aktualisierung einer Domain (Konsole) ... 588
Aktualisierung einer Domain (CLI) ... 588
Aktualisierung einer Domain (SDK) ... 589
Beheben von Validierungsfehlern ... 591
Fehlerbehebung bei einem Upgrade ... 591
Verwenden eines Snapshots zum Migrieren von Daten ... 594
Erstellen eines benutzerdefinierten Endpunkts ... 602
Benutzerdefinierte Endpunkte für neue Domänen ... 603
Benutzerdefinierte Endpunkte für vorhandene Domänen ... 604
CNAME-Zuordnung ... 604
Automatische Optimierung ... 605
Änderungsarten ... 605
Aktivieren oder Deaktivieren der automatischen Optimierung ... 607
Automatische Optimierung ... 608
Automatische Optimierung ... 609
Markieren von Domänen ... 609
Tag-Beispiel ... 610
Markierung von Domänen (Konsole) ... 611
Domains taggen ()AWS CLI ... 611
Domains taggen ()AWS SDKs ... 613
Ausführen von administrativen Aktionen ... 614
Den OpenSearch Prozess auf einem Datenknoten neu starten ... 615
Einen Datenknoten neu starten ... 615

Der Dashboard-Prozess wird neu gestartet ... 616
Einschränkungen ... 617
Arbeiten mit Direktanfragen ... 618
Preisgestaltung ... 618
Einschränkungen ... 619
Allgemeine Einschränkungen ... 619
Einschränkungen für Amazon S3 ... 619
Einschränkungen für Amazon CloudWatch Logs ... 620
Einschränkungen für Amazon Security Lake ... 620
Empfehlungen ... 621
Allgemeine Empfehlungen ... 621
Amazon S3 S3-Empfehlungen ... 622
CloudWatch Protokolliert Empfehlungen ... 623
Empfehlungen von Security Lake ... 623
Kontingente ... 624
Kontingente für Amazon S3 ... 624
Kontingente für Protokolle CloudWatch ... 625
Kontingente für Security Lake ... 626
Unterstützt AWS-Regionen ... 627
Verfügbar AWS-Regionen für Amazon S3 ... 628
Verfügbar AWS-Regionen für CloudWatch Protokolle ... 628
Verfügbar AWS-Regionen für Security Lake ... 629
Direkte Abfragen in S3 ... 629
Eine S3-Datenquelle erstellen ... 630
Konfiguration einer S3-Datenquelle ... 638
Direkte Abfragen in Logs CloudWatch ... 641
Eine CloudWatch Logs-Datenquelle erstellen ... 642
Konfiguration einer CloudWatch Logs-Datenquelle ... 648
Direkte Abfragen in Security Lake ... 650
Eine Security Lake-Datenquelle erstellen ... 650
Konfiguration einer Security Lake-Datenquelle ... 657
Verwaltung einer Datenquelle ... 660
Überwachung mit CloudWatch Metrik-Datenquellen ... 660
Datenquellen aktivieren und deaktivieren ... 664
Überwachung mit Budget AWS ... 664
Löschen einer Datenquelle ... 665

Optimieren der Abfrageleistung ... 666
Indizes überspringen ... 666
Materialisierte Ansichten ... 667
Erläuterung von Indizes ... 667
Unterstützte SQL- und PPL-Befehle ... 668
Unterstützte SQL-Befehle ... 669
Unterstützte PPL-Befehle ... 883
Domänen überwachen ... 1068
Überwachen von Cluster-Metriken ... 1069
Metriken anzeigen in CloudWatch ... 1070
OpenSearch Integritäts-Interpretations-Diagrammen ... 1071
Cluster-Metriken ... 1071
Dedizierte Hauptknoten-Metriken ... 1080
Dedizierte Statistiken für Koordinator-Knoten ... 1081
EBS-Volume-Metriken ... 1082
Instance-Metriken ... 1085
UltraWarm Metriken ... 1098
Cold-Storage-Metriken ... 1104
OR1 Metriken ... 1105
Warnungsmetriken ... 1106
Metriken zur Anomalieerkennung ... 1107
Asynchrone Suchmetriken ... 1109
Automatische Optimierung ... 1111
Multi-AZ mit Standby-Metriken ... 1112
Point-in-Time-Metriken ... 1115
SQL-Metriken ... 1115
k-NN-Metriken ... 1116
Metriken für Cluster-übergreifende Suchen ... 1119
Cluster-übergreifende Replikationsmetriken ... 1120
Learning-to-Rank-Metriken ... 1122
Metriken für Piped Processing Language ... 1123
Überwachen von Protokollen ... 1123
Aktivieren der Veröffentlichung von Protokollen (Konsole) ... 1125
Aktivieren der Veröffentlichung von Protokollen (AWS CLI) ... 1127
Aktivieren der Protokollveröffentlichung ()AWS SDKs ... 1130
Aktivieren der Veröffentlichung von Protokollen (CloudFormation) ... 1130

Schwellenwerte für langsame Protokollierung von Suchanfragen festlegen 1132
Schwellenwerte für Shard Slow Log festlegen 1133
Langsame Protokolle testen 1133
Anzeigen von -Protokollen 1134
Überwachen der Prüfprotokolle 1134
Einschränkungen 1135
Aktivieren von Prüfprotokollen 1136
Aktivieren Sie die Auditprotokollierung mit dem AWS CLI 1138
Aktivieren der Prüfungsprotokollierung über die Konfigurations-API 1138
Protokollebenen und -Kategorien prüfen 1138
Prüfprotokolleinstellungen 1141
Prüfungsprotokollbeispiel 1145
Konfigurieren von Prüfungsprotokollen mit der REST-API 1148
Überwachung von Ereignissen 1149
Aktualisieren der Software 1150
Automatische Optimierung von Ereignissen 1157
Ereignisse zum Cluster-Zustand 1162
VPC-Endpunktereignisse 1175
Ausmusterung von Knoten 1178
Ereignisse, bei denen der Knoten heruntergefahren ist 1180
Ereignisse für Domain-Fehler 1182
Tutorial: Überwachung von OpenSearch Service-Ereignissen 1184
Tutorial: Senden von SNS-Warnungen für verfügbare Updates 1187
Überwachung mit CloudTrail 1188
Amazon OpenSearch Service-Informationen in CloudTrail 492
Grundlegendes zu Amazon OpenSearch Service-Protokolldateieinträgen 493
Sicherheit 1193
Datenschutz 1194
Verschlüsselung im Ruhezustand 1195
Node-to-node Verschlüsselung 1199
Identitäts- und Zugriffsverwaltung 1200
Arten von Richtlinien 1201
OpenSearch Serviceanfragen stellen und signieren 1210
Konflikte in Richtlinien 1212
Richtlinienelementreferenz 1213
Erweiterte Optionen und Überlegungen zur API 1219

Konfigurieren von Zugriffsrichtlinien ... 1223
Zusätzliche Beispielrichtlinien ... 1223
Referenz für API-Berechtigungen ... 1223
AWS verwaltete Richtlinien ... 1224
Serviceübergreifende Confused-Deputy-Prävention ... 1235
Differenzierte Zugriffskontrolle ... 1237
Das Gesamtbild: detaillierte Zugriffskontrolle und Servicesicherheit OpenSearch ... 1238
Die wichtigsten Konzepte ... 1241
Über den Masterbenutzer ... 1242
Aktivieren der differenzierten Zugriffskontrolle ... 1243
Als Masterbenutzer auf OpenSearch Dashboards zugreifen ... 1247
Verwalten von Berechtigungen ... 1249
Empfohlene Konfigurationen ... 1255
Einschränkungen ... 1258
Hauptbenutzer ändern ... 1260
Zusätzliche Hauptbenutzer ... 1260
Manuelle Snapshots ... 1262
Integrationen ... 1262
REST-API-Unterschiede ... 1263
Tutorial: Detaillierte Zugriffskontrolle mit Cognito-Authentifizierung ... 1265
Tutorial: Interne Benutzerdatenbank mit einfacher Authentifizierung ... 1270
Compliance-Validierung ... 1273
Ausfallsicherheit ... 1275
JSON-Web-Tokens ... 1275
Überlegungen ... 1276
Ändern der Domainzugriffsrichtlinie ... 1276
Konfiguration der JWT-Authentifizierung und -Autorisierung ... 1277
Verwenden eines JWT zum Senden einer Testanfrage ... 1277
Sicherheit der Infrastruktur ... 1279
Arbeiten mit von OpenSearch Service verwalteten VPC-Endpunkten ... 1280
SAML-Authentifizierung für Dashboards OpenSearch ... 1285
SAML-Konfigurationsübersicht ... 1285
Überlegungen ... 1286
SAML-Authentifizierung für VPC-Domains ... 1287
Ändern der Domainzugriffsrichtlinie ... 1287
Konfigurieren der SP- oder IDP-initiierten Authentifizierung ... 1289

Konfigurieren der SP- und der IDP-initiierten Authentifizierung ... 1295
Konfigurieren der SAML-Authentifizierung (AWS CLI) ... 1296
Konfigurieren der SAML-Authentifizierung (Konfigurations-API) ... 1296
SAML-Fehlerbehebung ... 1297
Deaktivieren der SAML-Authentifizierung ... 1300
IAM Identity Center-Unterstützung für Amazon Service OpenSearch ... 1301
Amazon Cognito Cognito-Authentifizierung für Dashboards OpenSearch ... 1304
Voraussetzungen ... 1305
Konfigurieren einer Domain zur Verwendung der Amazon-Cognito-Authentifizierung ... 1309
Zulassen der authentifizierten Rolle ... 1313
Konfigurieren von Identitätsanbietern ... 1314
(Optional) Konfigurieren von individuell festgelegtem Zugriff ... 1315
(Optional) Anpassen der Anmeldeseite ... 1316
(Optional) Konfiguration der erweiterten Sicherheit ... 1316
Testen ... 1317
Kontingente ... 1317
Häufige Konfigurationsprobleme ... 1317
Amazon Cognito Cognito-Authentifizierung für Dashboards deaktivieren OpenSearch ... 1322
Löschen von Domains, die die Amazon Cognito Cognito-Authentifizierung für OpenSearch Dashboards verwenden ... 1322
Verwenden von serviceverknüpften Rollen ... 1323
Rolle zur Erstellung von VPC-Domänen und Datenquellen ... 1323
Rolle bei der Sammlungserstellung ... 1327
Rolle bei der Pipeline-Erstellung ... 1330
Beispiel-Code ... 1334
Elasticsearch-Client-Kompatibilität ... 1334
Komprimieren von HTTP-Anforderungen ... 1335
Aktivieren der gzip-Komprimierung ... 1335
Erforderliche Header ... 1336
Beispiel-Code (Python 3) ... 1336
Mit dem AWS SDKs ... 1338
Java ... 1338
Python ... 1349
Knoten ... 1352
Indizierung von Daten ... 1355
Namensbeschränkungen bei Indizes ... 1355

Reduzierung der Antwortgröße ... 1356
Indexcodecs ... 1358
Streaming-Daten werden in den OpenSearch Service geladen ... 1358
Streaming-Daten aus Ingestion werden geladen OpenSearch ... 1359
So laden Sie Streaming-Daten aus Amazon S3 ... 1359
So laden Sie Streaming-Daten aus Amazon Kinesis Data Streams ... 1365
So laden Sie Streaming-Daten aus Amazon DynamoDB ... 1369
Streaming-Daten von Amazon Data Firehose laden ... 1374
Streaming-Daten von Amazon laden CloudWatch ... 1374
Streaming-Daten werden geladen von AWS IoT ... 1374
Laden von Daten mit Logstash ... 1374
Konfiguration ... 1375
Suchen von Daten ... 1378
URI-Suchanfragen ... 1379
Anforderungstextsuchen ... 1380
Boosten der Felder ... 1382
Hervorheben der Suchergebnisse ... 1382
Count-API ... 1384
Paginieren der Suchergebnisse ... 1385
Zeitpunkt ... 1385
Die `size` Parameter `from` und ... 1385
Abfragesprache für Dashboards ... 1386
Pakete ... 1388
Erforderliche Berechtigungen ... 1389
Hochladen von Paketen nach Amazon S3 ... 1389
Importieren und Zuordnen von Paketen ... 1390
Pakete verwenden mit OpenSearch ... 1391
Aktualisieren von Paketen ... 1396
Manuelles Aktualisieren von Indizes mit einem neuen Wörterbuch ... 1399
Trennen und Entfernen von Paketen ... 1401
Benutzerdefinierte Plugins ... 1402
Plugins von Drittanbietern ... 1421
SQL-Unterstützung ... 1425
Beispielaufruf ... 1427
Hinweise und Unterschiede ... 1427
SQL Workbench ... 1428

SQL CLI ... 1278
JDBC-Treiber ... 1428
ODBC-Treiber ... 1428
k-NN-Suche ... 1428
Erste Schritte mit k-NN ... 1429
k-NN-Unterschiede, -Optimierung und -Einschränkungen ... 1432
Cluster-übergreifende Suche ... 1432
Einschränkungen ... 1433
Voraussetzungen für die Cluster-übergreifende Suche ... 1434
Cluster-übergreifende Suche – Preise ... 1434
Einrichten einer Verbindung ... 1434
Entfernen einer Verbindung ... 1436
Einrichten von Sicherheit und Beispiel-Walkthrough-Anleitungen ... 1436
OpenSearch Dashboards ... 1443
Learning to Rank ... 1443
Erste Schritte mit Learning to Rank ... 1444
Learning-to-Rank-API ... 1465
Asynchrone Suche ... 1472
Beispiele für Suchaufrufe ... 1472
Asynchrone Suchberechtigungen ... 1474
Asynchrone Sucheinstellungen ... 1475
Cluster-übergreifende Suche ... 1475
UltraWarm ... 1477
Zeitpunkt ... 1477
Überlegungen ... 1478
Erstellen eines PIT ... 1478
Zeitpunktberechtigungen ... 1480
PIT-Einstellungen ... 1481
Cluster-übergreifende Suche ... 1481
UltraWarm ... 1481
Semantische Suche ... 1482
Gleichzeitige Segmentsuche ... 1482
Generierung von Abfragen in natürlicher Sprache ... 1483
Voraussetzungen ... 1483
Erste Schritte ... 1484
Konfigurieren von Berechtigungen ... 1484

Automatisierung der Konfiguration ... 1485
OpenSearch Dashboards ... 1486
Steuern des Zugriffs auf Dashboards ... 1487
Verwenden eines Proxys für den Zugriff auf den Service über Dashboards OpenSearch ... 1487
Konfiguration von Dashboards für die Verwendung eines WMS-Kartenservers ... 1491
Einen lokalen Dashboards-Server mit dem Service verbinden OpenSearch ... 1492
Indizes in Dashboards verwalten ... 1494
Weitere Features ... 1494
OpenSearch Benutzeroberfläche ... 1496
Versionsverlauf ... 1497
Erste Schritte ... 1499
Erforderliche Berechtigungen für die Erstellung von Amazon OpenSearch Service-Anwendungen ... 1499
Erstellen einer Anwendung ... 1503
Verwaltung von Anwendungsadministratoren ... 1511
Aktivieren des SAML-Verbunds mit IAM ... 1515
Schritt 1: Richten Sie die Identitätsanbieter-Anwendung (Okta) ein ... 1516
Schritt 2: Richten Sie die AWS Konfiguration für Okta ein ... 1520
Schritt 3: Erstellen Sie die Amazon OpenSearch Service-Zugriffsrichtlinie in IAM ... 1522
Schritt 4: Überprüfen Sie das vom Identitätsanbieter initiierte Single Sign-On-Erlebnis mit SAML ... 1525
Verwaltung von Datenquellenzuordnungen und VPC-Zugriffsberechtigungen ... 1529
Zuordnen einer Datenquelle zu einer UI-Anwendung OpenSearch ... 1529
Verwaltung des Zugriffs auf Domänen in einer VPC ... 1530
Konfiguration des Zugriffs auf OpenSearch serverlose Sammlungen in einer VPC ... 1531
Amazon OpenSearch Service-Workspaces verwenden ... 1535
Arbeitsbereiche für OpenSearch UI-Anwendungen erstellen ... 1535
Datenschutz im Workspace und Mitarbeiter ... 1536
Typen von Arbeitsbereichen ... 1537
Regions- und kontoübergreifender Datenzugriff mit clusterübergreifender Suche ... 1538
Einrichtung von Zugriffsberechtigungen für den region- und kontoübergreifenden Datenzugriff mit clusterübergreifender Suche ... 1540
Eine Verbindung zwischen Domänen herstellen ... 1543
Testen Sie Ihre Sicherheitseinstellungen für den region- und kontoübergreifenden Datenzugriff mit clusterübergreifender Suche ... 1545
Löschen einer Verbindung ... 1548

Verwaltung des Zugriffs auf die OpenSearch Benutzeroberfläche von einem VPC-Endpunkt aus ... 1549
Erstellen einer privaten Verbindung zwischen einer VPC und OpenSearch einer Benutzeroberfläche ... 1549
Aktualisierung der VPC-Endpunktrichtlinie, um den Zugriff auf die OpenSearch UI-Anwendung zu ermöglichen ... 1551
Widerrufen des Zugriffs auf die OpenSearch Benutzeroberfläche in einer VPC-Endpunktrichtlinie ... 1551
Verwalten von Indexen ... 1553
UltraWarm Speicher ... 1553
Voraussetzungen ... 1554
UltraWarm Speicheranforderungen und Leistungsüberlegungen ... 1556
UltraWarm Preisgestaltung ... 1557
Aktiviert UltraWarm ... 1557
Migration von Indizes auf Speicher UltraWarm ... 1560
Automatisieren von Migrationen ... 1563
Migrationsoptimierung ... 1563
Abbrechen von Migrationen ... 1564
Auflisten von Hot- und Warm-Indizes ... 1564
Warm-Indizes in den Hot Storage zurückbringen ... 1564
Wiederherstellen von Warm-Indizes aus Snapshots ... 1565
Manuelle Snapshots von Warm-Indizes ... 1566
Migration Warm-Indizes in Cold Storage ... 1567
Bewährte Methoden für KNN-Indizes ... 1568
Deaktivierung UltraWarm ... 1569
Cold Storage ... 1569
Voraussetzungen ... 1570
Cold-Speicheranforderungen und Leistungsüberlegungen ... 1572
Preise für Cold-Speicherung ... 1572
Aktivieren von Cold-Speicherung ... 1572
Verwaltung von Cold-Indizes in Dashboards OpenSearch ... 1574
Migration von Indizes auf Cold-Speicher ... 1574
Automatisierung von Migrationen zum Cold-Speicher ... 1576
Abbruch von Migrationen zum Cold-Speicher ... 1576
Auflisten der Cold-Indizes ... 1577
Migrieren von Cold-Indizes zum Warm-Speicher ... 1581

Wiederherstellen von Cold-Indizes aus Snapshots ... 1582
Abbruch von Migrationen von Cold- zu Warm-Speicher ... 1583
Cold-Index-Metadaten aktualisieren ... 1583
Cold-Indizes löschen ... 1584
Deaktivieren von Cold-Speicherung ... 1584
OpenSearch optimierte Speicherkosten ... 1584
Einschränkungen ... 1585
Optimierung für einen besseren Aufnahmedurchsatz ... 1585
Wie sich OpenSearch optimierte Instances von anderen Instances unterscheiden ... 1586
Wie OR1 unterscheidet es sich vom UltraWarm Speicher ... 1586
Provisioning einer Domain mit Instanzen OR1 ... 1587
Indexstatusmanagement ... 1588
Erstellen einer ISM-Richtlinie ... 1589
Beispielrichtlinien ... 1590
ISM-Vorlagen ... 1594
Unterschiede ... 1595
Tutorial: Automatisierung von ISM-Prozessen ... 1596
Index-Rollups ... 1601
Erstellen eines Index-Rollup-Auftrags ... 1601
Indextransformationen ... 1603
Erstellen eines Indextransformationsauftrags ... 1603
Cluster-übergreifende Replikation ... 1605
Einschränkungen ... 1606
Voraussetzungen ... 1607
Berechtigungsanforderungen ... 1607
Einrichten einer clusterübergreifenden Verbindung ... 1608
So starten Sie eine Replikation ... 1610
Replikation bestätigen ... 1610
Replikation pausieren und Fortsetzen ... 1612
Replikation beenden ... 1612
Automatisches Folgen ... 1613
Aktualisierung verbundener Domänen ... 1614
Remote-Neuindexierung ... 1615
Voraussetzungen ... 1616
Daten zwischen OpenSearch Service-Internetdomänen neu indizieren ... 1616
Daten neu indizieren, wenn sich die Remote-Domain in einer VPC befindet ... 1618

Indizieren Sie Daten zwischen OpenSearch Nicht-Servicedomänen neu ... 1623
Große Datensätze neu indizieren ... 1623
Remote-Neuindexierungseinstellungen ... 1625
Datenströme ... 1626
Erste Schritte mit Datenströmen ... 1626
Überwachen von Daten ... 1630
Warnfunktion ... 1630
Warnungsberechtigungen ... 1631
Erste Schritte mit Warnungen ... 1631
Benachrichtigungen ... 1632
Unterschiede ... 1633
Anomalie-Erkennung ... 1634
... 1635
Tutorial: Erkennen hoher CPU-Auslastung mit Anomalieerkennung ... 1639
Amazon-Q-Unterstützung ... 1643
Unterstützt AWS-Regionen ... 1644
Einrichten von Amazon Q Developer OpenSearch Service Service Service Service Service Service Service ... 1644
Generieren Sie Visualisierungen in natürlicher Sprache ... 1645
Zusammenfassungen und Einblicke in Benachrichtigungen anzeigen ... 1646
Bevor Sie beginnen ... 1649
Zusammenfassungen und Einblicke in Warnmeldungen anzeigen ... 1650
Sehen Sie sich die von Amazon Q generierten Zusammenfassungen der Abfrageergebnisse auf der Discover-Seite an ... 1651
Anomaliedetektoren beschreiben beschreiben. ... 1653
Greifen Sie auf den Amazon Q-Chat für OpenSearch Servicefragen zu ... 1654
Machine Learning ... 1658
Anschlüsse für AWS-Services ... 1658
Voraussetzungen ... 1658
Erstellen Sie einen OpenSearch Service-Connector ... 1662
Anschlüsse für externe Plattformen ... 1664
Voraussetzungen ... 1665
Erstellen Sie einen OpenSearch Service-Connector ... 1668
CloudFormation Vorlagen-Integrationen ... 1670
Voraussetzungen ... 1671
Amazon SageMaker AI Vorlagen ... 1672

Amazon Bedrock-Vorlagen ... 1673
ML Commons-Einstellungen werden nicht unterstützt ... 1674
Flow-Framework-Plugin ... 1675
ML-Konnektoren im Service erstellen OpenSearch ... 1676
Konfigurieren von Berechtigungen ... 1683
Sicherheitsanalysen ... 1685
Komponenten und Konzepte der Sicherheitsanalyse ... 1685
Typen von Protokollen ... 1686
Detektoren ... 1686
Regeln ... 1686
Funde ... 1687
Benachrichtigungen ... 1687
Erkunden von Sicherheitsanalysen ... 1687
Konfigurieren von Berechtigungen ... 1689
Fehlerbehebung ... 1691
Kein solcher Indexfehler ... 1691
Beobachtbarkeit ... 1692
Erkunden Ihrer Daten mit Ereignisanalytik ... 1692
Erstellen von Visualisierungen ... 1695
Detaillierter Einblick in Trace Analytics ... 1696
Trace Analytics ... 1696
Voraussetzungen ... 1697
OpenTelemetry Collector-Probenkonfiguration ... 1698
OpenSearch Beispielkonfiguration für die Aufnahme ... 1699
Spurendaten untersuchen ... 1700
Piped Processing Language ... 1701
... 1702
Bewährte Methoden ... 1704
Überwachen und Warnen ... 1704
CloudWatch Alarme konfigurieren ... 1704
Aktivieren der Protokollveröffentlichung ... 1705
Shard-Strategie ... 1705
Ermitteln der Anzahl der Shards und Datenknoten ... 1706
Vermeiden von Speicherversatz ... 1707
Stabilität ... 1707
Bleiben Sie auf dem Laufenden mit OpenSearch ... 1707

Verbessern Sie die Snapshot- ... 1708
Dedizierte Hauptknoten aktivieren ... 1708
Bereitstellen über mehrere Availability Zones hinweg ... 1709
Steuern von Erfassungsablauf und Pufferung ... 1709
Erstellen von Zuordnungen für Such-Workloads ... 1710
Verwenden von Indexvorlagen ... 1710
Indizes mit Indexstatusmanagement verwalten ... 1712
Entferne nicht verwendete Indizes ... 1712
Verwenden mehrerer Domains für hohe Verfügbarkeit ... 1712
Leistung ... 1713
Größe und Komprimierung von Massenanfragen optimieren ... 1713
Größe der Antworten auf Massenanfragen reduzieren ... 1713
Aktualisierungsintervalle optimieren ... 1714
Automatische Optimierung aktivieren ... 1714
Sicherheit ... 1714
Differenzierte Zugriffskontrolle aktivieren ... 1714
Bereitstellen von Domains innerhalb einer VPC ... 1715
Anwenden einer restriktiven Zugriffsrichtlinie ... 1715
Verschlüsselung im Ruhezustand aktivieren ... 1715
Aktivieren Sie die Verschlüsselung node-to-node ... 1716
Überwachen Sie mit AWS Security Hub ... 1716
Kostenoptimierung ... 1716
Instance-Typen der neuesten Generation verwenden ... 1716
Verwenden Sie die neuesten Amazon-EBS-gp3-Volumes ... 1717
Verwendung UltraWarm und Cold Storage für Zeitreihen-Protokolldaten ... 1717
Empfehlungen für Reserved Instances überprüfen ... 1718
Größenanpassung von Domains ... 1718
Berechnung der Speicheranforderungen ... 1718
Auswahl der Anzahl der Shards ... 1720
Auswählen von Instance-Typen und Tests ... 1722
Petabyte-Größe ... 1724
Dedizierte Koordinatorknoten ... 1726
Wann sollten dedizierte Koordinatorknoten verwendet werden ... 1726
Architektur und Verhalten ... 1726
Anforderungen und Einschränkungen ... 1727
Bereitstellung dedizierter Koordinatorknoten ... 1727

Bewährte Methoden ... 1728
Dedizierte Hauptknoten ... 1729
Anzahl der dedizierten Hauptknoten auswählen ... 1731
Auswählen von Instance-Typen für dedizierte Hauptknoten ... 1732
Empfohlene CloudWatch Alarme ... 1733
Allgemeine Hinweise ... 1742
Unterstützte Instance-Typen ... 1742
Instance-Typen der aktuellen Generation ... 1742
Instance-Typen der vorherigen Generation ... 1761
Funktionen nach Engine-Version ... 1765
Plug-ins nach Engine-Version ... 1771
Optionale Plug-ins ... 1775
Unterstützte Vorgänge ... 1776
Erwähnenswerte API-Unterschiede ... 1776
Kontingente ... 1832
UltraWarm Speicherkontingente ... 1833
Anzahl der Datenknoten pro AZ ... 1732
Gesamtzahl der Knoten pro Instanzfamilie ... 1833
EBS-Volume-Größenkontigente ... 1834
Netzwerk-Kontingente ... 1844
Kontingente für die Größe von Shards ... 1852
Anzahl der Kontingente ... 1852
Java-Prozess-Kontingente ... 1853
Domain-Richtlinien-Kontingente ... 1853
Reserved Instances ... 1853
Erwerben von Reserved Instances (Konsole) ... 1854
Erwerben von Reserved Instances (AWS CLI) ... 1855
Erwerben von Reserved Instances (AWS SDKs) ... 1857
Untersuchen der Kosten ... 1859
Andere unterstützte Ressourcen ... 1859
Tutorials ... 1861
Erstellen und Suchen von Dokumenten ... 1861
Voraussetzungen ... 1861
Hinzufügen eines Dokuments zu einem Index ... 1862
Erstellen automatisch generierter IDs ... 1863
Aktualisieren eines Dokuments mit einem POST-Befehl ... 1864

Ausführen von Massenaktionen ... 1865
Suchen nach Dokumenten ... 1866
Zugehörige Ressourcen ... 1868
Migration zum Service OpenSearch ... 1868
Snapshot erstellen und hochladen ... 1869
Domain erstellen ... 1870
Erteilen Sie Berechtigungen für den Zugriff auf den S3-Bucket ... 1871
Stellen Sie den Snapshot wieder her ... 1874
Erstellen einer Suchanwendung ... 1876
Voraussetzungen ... 1877
Schritt 1: Indizieren von Beispieldaten ... 1877
Schritt 2: Lambda-Funktion erstellen und bereitstellen ... 1878
Schritt 3: Erstellen Sie die API in API Gateway ... 1881
Schritt 4: (Optional) Ändern der Domain-Zugriffsrichtlinie ... 1884
Zuordnen der Lambda-Rolle (bei Verwendung einer differenzierten Zugriffskontrolle) ... 1887
Schritt 5: Testen der Webanwendung ... 1887
Nächste Schritte ... 1890
Visualisieren von Support-Aufrufen ... 1891
Schritt 1: Konfigurieren der Voraussetzungen ... 1892
Schritt 2: Kopieren des Beispiel-Codes ... 1893
(Optional) Schritt 3: Indizieren von Beispieldaten ... 1897
Schritt 4: Analysieren und Visualisieren Sie Ihre Daten ... 1899
Schritt 5: Bereinigen Sie Ressourcen und nächste Schritte ... 1903
Umbenennung von Amazon OpenSearch Service ... 1905
Neue API-Version ... 1905
Umbenannte Instance-Typen ... 1906
Änderungen der Zugriffsrichtlinie ... 1906
IAM-Richtlinien ... 1906
SCP-Richtlinien ... 1906
Neue Ressourcentypen ... 1907
Kibana wurde in Dashboards OpenSearch umbenannt ... 1908
Umbenannte CloudWatch Kennzahlen ... 1909
Änderungen Fakturierung und Kostenmanagement ... 1910
Neues Ereignisformat ... 1911
Was bleibt gleich? ... 1911
Erste Schritte: Aktualisieren Sie Ihre Domains auf OpenSearch 1.x ... 1911

Fehlerbehebung ... 1913
Ich kann nicht auf OpenSearch Dashboards zugreifen ... 1913
Zugriff auf VPC-Domain nicht möglich ... 1913
Cluster im schreibgeschützten Zustand ... 1913
Roter Cluster-Status ... 1915
Automatische Behebung von roten Clustern ... 1916
Wiederherstellung nach einem kontinuierlich starken Workload ... 1917
Gelber Cluster-Status ... 1919
ClusterBlockException ... 1920
Zu wenig verfügbarer Speicherplatz ... 1920
Hoher JVM-Speicherdruck ... 1920
Fehler bei der Migration zu Multi-AZ mit Standby ... 1921
Erstellen eines Indexes, einer Indexvorlage oder einer ISM-Richtlinie während der Migration von Domänen ohne Standby zu Domänen mit Standby ... 1691
Falsche Anzahl von Datenkopien ... 1922
JVM OutOfMemoryError ... 1922
Fehlgeschlagene Cluster-Knoten ... 1923
Maximales Shard-Limit überschritten ... 1924
Domain bleibt im Bearbeitungsstatus hängen ... 1924
Niedrige EBS-Burst-Balance ... 1924
Die EBS-Metrik nimmt bei der Größenänderung des Volumens zu ... 1925
Prüfungsprotokolle können nicht aktiviert werden ... 1925
Schließen des Indexes nicht möglich ... 1926
Prüfungen für Client-Lizenz ... 1926
Drosselung anfordern ... 1926
SSH im Knoten nicht möglich ... 1926
Snapshot-Fehler „Nicht gültig für die Speicherklasse des Objekts“ ... 1927
Ungültiger Host-Header ... 1927
Ungültiger M3-Instance-Typ ... 1927
Hot Queries funktionieren nach der Aktivierung nicht mehr UltraWarm ... 1928
Nach einem Upgrade ist kein Downgrade möglich ... 1928
Erforderliche Zusammenfassung der Domains für alle AWS-Regionen ... 1928
Browserfehler bei der Verwendung von OpenSearch Dashboards ... 1929
Knoten-Shard und Speicherversatz ... 1929
Index-Shard und Speicherversatz ... 1930
Unautorisierte Operation nach dem Auswählen des VPC-Zugriffs ... 1931

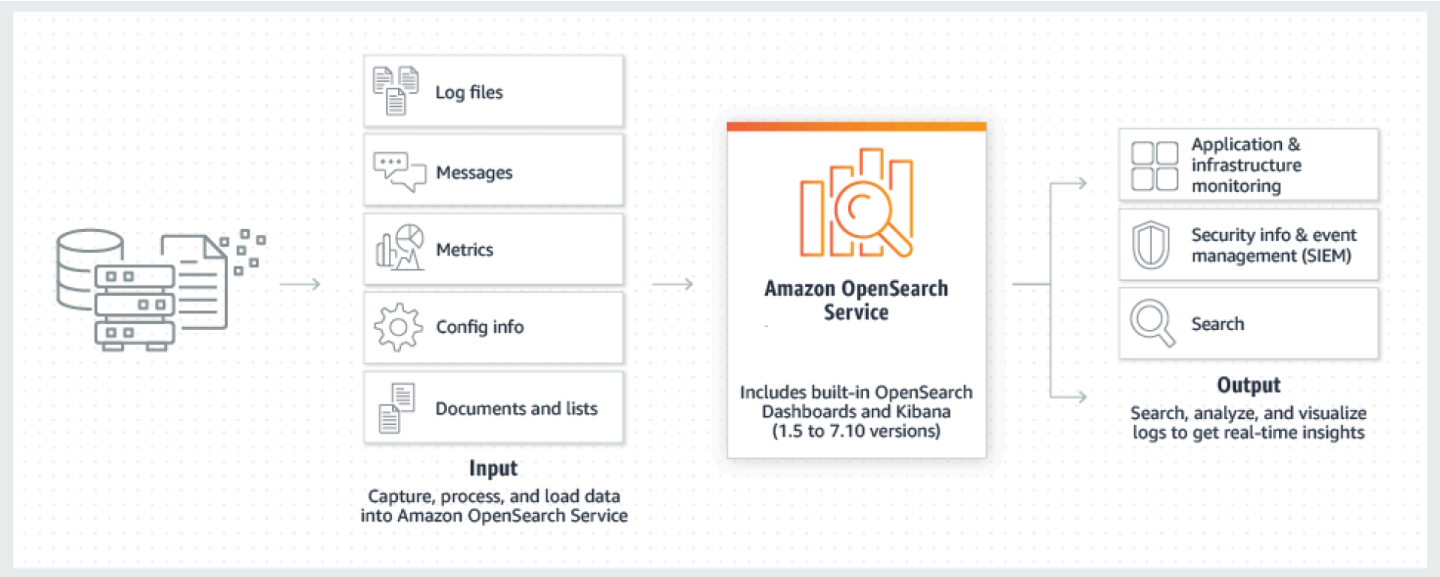
Hängenbleiben im Status "Loading" nach dem Erstellen von VPC-Domains 1931
Abgelehnte Anfragen an die API OpenSearch 1932
Verbindung von Alpine Linux kann nicht hergestellt werden 1933
Zu viele Anfragen für Search Backpressure 1933
Zertifikatsfehler bei der Verwendung von SDKs 1933
Die Installation eines benutzerdefinierten Plugins schlägt aufgrund der Versionskompatibilität fehl 1935
Dokumentverlauf 1937
Frühere Aktualisierungen 1993
AWS Glossar 1996
..... mcmxcvii

Was ist Amazon OpenSearch Service?

Amazon OpenSearch Service ist ein verwalteter Service, der das Bereitstellen, Betreiben und Skalieren von OpenSearch Clustern in der AWS -Cloud einfach macht. Eine OpenSearch Service-Domain ist ein Synonym für einen OpenSearch Cluster. Domains sind Cluster mit den Einstellungen, Instance-Typen, Instance-Anzahl und Speicherressourcen, die Sie angeben. Amazon OpenSearch Service unterstützt OpenSearch ältere Elasticsearch OSS (bis zu 7.10, der letzten Open-Source-Version der Software). Wenn Sie eine Domain erstellen, haben Sie die Option, die Suchmaschine zu verwenden.

OpenSearchist ein vollständiges Open-Source-Such- und Analysemodul für die Protokollanalyse, Echtzeitüberwachung von Anwendungen, Clickstream-Analyse und ähnliche Anwendungsfälle. Weitere Informationen finden Sie in der OpenSearch -Dokumentation.

Amazon OpenSearch Service stellt alle Ressourcen für Ihren OpenSearch Cluster bereit und startet ihn. Es erkennt und ersetzt auch automatisch ausgefallene OpenSearch Service-Knoten. Dadurch wird der Verwaltungsaufwand im Zusammenhang mit selbstverwalteten Infrastrukturen verringert. Sie können Ihren Cluster mit einem einzigen API-Aufruf oder wenigen Klicks in der Konsole skalieren.



Um mit der Nutzung von OpenSearch Service zu beginnen, erstellen Sie eine OpenSearch Dienstdomäne, die einem OpenSearch Cluster entspricht. Jede EC2 Instance im Cluster fungiert als ein OpenSearch Service-Knoten.

Sie können über die OpenSearch Service-Konsole eine Domain innerhalb weniger Minuten einrichten und konfigurieren. Wenn Sie den programmatischen Zugriff bevorzugen, können Sie den AWS CLIAWS SDKs, oder Terraform verwenden.

Funktionen von Amazon OpenSearch Service

OpenSearch Dieser Service umfasst die folgenden Funktionen:

Skalieren

- Zahlreiche Konfigurationen von CPU, Arbeitsspeicher und Speicherkapazität, bekannt als Instance-Typen, einschließlich kostengünstiger Graviton-Instances
- Unterstützt bis zu 1002 Datenknoten
- Bis zu 25 PB angeschlossener Speicher
- UltraWarmKostengünstiger Kaltspeicher für schreibgeschützte Daten

Sicherheit

- AWS Identity and Access Management (IAM) -Zugriffskontrolle
- Einfache Integration mit Amazon VPC und VPC-Sicherheitsgruppen
- Verschlüsselung von Data-at-Rest und node-to-node Verschlüsselung
- Amazon Cognito-, HTTP Basic- oder SAML-Authentifizierung für Dashboards OpenSearch
- Sicherheit auf Index-Ebene, Dokumentebene und Feldebene
- Prüfungsprotokolle
- Dashboards-Multi-Tenancy

Stabilität

- Mehrere geografische Standorte für Ihre Ressourcen, bezeichnet als Regionen und Availability Zones
- Knotenzuweisung über zwei oder drei Availability Zones in derselben AWS -Region hinweg, wird als Multi-AZ bezeichnet
- Dedizierte Hauptknoten für die Auslagerung von Cluster-Management-Aufgaben
- Automatisierte Snapshots für die Sicherung und Wiederherstellung von OpenSearch Service-Domains

Flexibilität

- SQL-Unterstützung für die Integration mit Business-Intelligence-(BI-)Anwendungen
- Benutzerdefinierte Pakete zur Verbesserung der Suchergebnisse

Integration in beliebte Services

- Datenvisualisierung mit OpenSearch Dashboards
- Integration mit Amazon CloudWatch für die Überwachung von OpenSearch Service-Domänenmetriken und die Einrichtung von Alarmen
- Integration mit AWS CloudTrail zur Prüfung der Konfigurations-API-Aufrufe an OpenSearch Service-Domains
- Integration mit Amazon S3, Amazon Kinesis und Amazon DynamoDB für das Laden von Streaming-Daten in Service OpenSearch
- Warnungen von Amazon SNS, wenn Ihre Daten bestimmte Schwellenwerte überschreiten

Wann sollte ich den Service OpenSearch im Vergleich zu Amazon OpenSearch Service verwenden

Anhand der folgenden Tabelle können Sie entscheiden, ob der bereitgestellte Amazon OpenSearch Service oder der selbstverwaltete Service die richtige Wahl für Sie OpenSearch ist.

OpenSearch	OpenSearch Amazon-Dienst
• Ihr Unternehmen ist bereit, selbst bereitgestellte Cluster manuell zu überwachen und zu verwalten, und verfügt über Mitarbeiter mit den entsprechenden Fähigkeiten. • Sie möchten die vollständige Kontrolle über Ihren Code auf Kompilierebene haben. • Ihr Unternehmen bevorzugt Open-Source-Software oder verwendet ausschließlich Open-Source-Software.	• Sie möchten Ihre Infrastruktur nicht manuell verwalten, überwachen und warten. • Sie suchen einfache Möglichkeiten, die steigenden Analysekosten zu bewältigen, indem Sie Ihre Daten auf mehrere Speicherebenen verteilen und dabei die Stabilität und die niedrigen Kosten von Amazon S3 nutzen. • Sie möchten die Vorteile von Integrationen mit anderen Anbietern AWS-Services wie DynamoDB, Amazon DocumentDB (mit MongoDB-Kompatibilität), IAM und nutzen. CloudWatch CloudFormation

OpenSearch	OpenSearch Amazon-Dienst
• Sie verfolgen eine Multi-Cloud-Strategie, die Technologien erfordert, die nicht anbieterspezifisch sind. • Ihr Team ist in der Lage, alle kritischen Produktionsprobleme zu lösen. • Sie möchten die Flexibilität haben, das Produkt nach Ihren Wünschen zu verwenden, zu modifizieren und zu erweitern. • Sie möchten sofort auf neue Funktionen zugreifen können, sobald sie veröffentlicht werden.	• Sie möchten bei präventiver Wartung und bei Produktionsproblemen einfach auf Support Unterstützung zugreifen können. • Sie möchten Funktionen wie Selbstheilung, proaktive Wartung, Ausfallsicherheit und Backups nutzen.

Unterstützte Versionen von Elasticsearch und OpenSearch

OpenSearch Der Service unterstützt die folgenden Versionen von OpenSearch:

- 2.19, 2.17, 2.15, 2.13, 2.11, 2.9, 2.7, 2.5, 2.3, 1.3, 1.2, 1.1 und 1.0

OpenSearch Der Service unterstützt die folgenden Versionen von Legacy-Elasticsearch:

- 7.10, 7.9, 7.8, 7.7, 7.4, 7.1, 6.8, 6.7, 6.5, 6.4, 6.3, 6.2, 6.0, 5.6, 5.5, 5.3, 5.1, 2.3 und 1.5

Wir empfehlen, auf die neueste verfügbare OpenSearch Version zu aktualisieren, um den OpenSearch Service in Bezug auf Preis-Leistungs-Verhältnis, Funktionsvielfalt und Sicherheitsverbesserungen optimal nutzen zu können.

Standard- und verlängerter Support

AWS bietet Bugfixes und Sicherheitsupdates für Versionen, die unter Standardunterstützung fallen. AWS Bietet kritische Sicherheitsfixes für Versionen mit erweitertem Support für mindestens 12 Monate nach Ablauf des Standard-Supports zu einer Pauschalgebühr pro Normalized Instance Hour (NIH). NIH basiert auf der Instanzgröße und den Nutzungsstunden.

Gebühren für erweiterten Support fallen automatisch an, wenn auf einer Domain eine Version ausgeführt wird, für die der Standardsupport nicht mehr verfügbar ist. Um diese Gebühren zu vermeiden, führen Sie ein Upgrade auf eine unterstützte Version durch.

Die folgenden Tabellen zeigen das Ende des Supports für Elasticsearch-Versionen OpenSearch und ältere Elasticsearch-Versionen.

OpenSearch Der Service unterstützt mehrere Versionen von OpenSearch und ältere Open-Source-Versionen von Elasticsearch. Für einige Versionen haben wir bereits die Termine für das Ende des Standard-Supports und die Verlängerung des Supports veröffentlicht. Wir empfehlen Ihnen, auf die neueste verfügbare OpenSearch Version zu aktualisieren, um den OpenSearch Service in Bezug auf Preis-Leistungs-Verhältnis, Funktionsvielfalt und Sicherheitsverbesserungen optimal nutzen zu können. Die folgenden Tabellen enthalten Listen von Elasticsearch und deren OpenSearch Versionen sowie deren Support-Zeitpläne.

Der Zeitplan für das Ende des Supports für Elasticsearch-Versionen sieht wie folgt aus:

Softwareversion	Ende des Standard-Supports	Ende des verlängerten Support
Elasticsearch Versionen 1.5 und 2.3	7. November 2025	7. November 2026
Elasticsearch-Versionen 5.1 bis 5.5	7. November 2025	7. November 2026
Elasticsearch Versionen 5.6	7. November 2025	7. November 2028
Elasticsearch-Versionen 6.0 bis 6.7	7. November 2025	7. November 2026

Softwarev ersion	Ende des Standard-Supports	Ende des verlängerten Support
Elasticse arch Versionen 6.8	Nicht angekündigt	Nicht angekündigt
Elasticse arch-Vers ionen 7.1 bis 7.8	7. November 2025	7. November 2026
Elasticse arch Versionen 7.9	Nicht angekündigt	Nicht angekündigt
Elasticse arch Versionen 7.10	Nicht angekündigt	Nicht angekündigt

Der Zeitplan für das Ende des Supports für OpenSearch Versionen sieht wie folgt aus:

Version der Software	Ende des Standard-Supports	Ende des verlängerten Support
OpenSearc h Versionen 1.0 bis 1.2	7. November 2025	7. November 2026
OpenSearc h Versionen 1.3	Nicht angekündigt	Nicht angekündigt

Version der Software	Ende des Standard-Supports	Ende des verlängerten Support
OpenSearch Versionen 2.3 bis 2.9	7. November 2025	7. November 2026
OpenSearch Versionen 2.11 und höhere Versionen	Nicht angekündigt	Nicht angekündigt

Standardsupport und erweiterter Support für Elasticsearch OpenSearch

AWS bietet regelmäßige Bugfixes und Sicherheitsupdates für Versionen, die unter den Standard-Support fallen. AWS Stellt für Versionen mit erweitertem Support kritische Sicherheitsupdates für einen Zeitraum von mindestens 12 Monaten nach Ende des Standard-Supports gegen eine zusätzliche Pauschalgebühr für jede Normalized Instance Hour (NIH) bereit. NIH wird als Faktor der Instance-Größe (z. B. mittel, groß) und der Anzahl der Instance-Stunden berechnet (ein Beispiel finden Sie im Abschnitt „Berechnung der Gebühren für erweiterten Support“ weiter unten). Gebühren für erweiterten Support werden automatisch berechnet, wenn auf einer Domain eine Version ausgeführt wird, für die der Standardsupport abgelaufen ist. Sie können ein Upgrade auf eine aktuelle Version durchführen, für die weiterhin der Standardsupport gilt, um Gebühren für erweiterten Support zu vermeiden. Weitere Informationen zu den Gebühren für erweiterten Support finden Sie auf der Seite mit den Preisen. Allgemeine Informationen zum erweiterten Support finden Sie in den häufig gestellten Fragen zum erweiterten Support.

Berechnung der Gebühren für verlängerten Support

Für Domains, für die Versionen mit erweitertem Support ausgeführt werden, wird ein pauschaler Aufpreis berechnetfee/Normalized Instance Hour (NIH), for example, $0.0065 in the US East (North Virginia) Region. NIH is computed as a factor of the instance size (e.g., medium, large), and the number of instance hours. For example, if you are running an m7g.medium.search instance for 24 hours in the US East (North Virginia) Region, which is priced at $0.068/Instance hour (on-

demand), you will typically pay $1.632 ($0.068x24). If you are running a version that is in extended support, you will pay an additional $0.0065/NIH, der als 0,0065$ x 24 (Anzahl der Instanzstunden) x 2 (Größennormalisierungsfaktor; 2 für mittelgroße Instances) berechnet wird, was 0,312$ für erweiterten Support für 24 Stunden entspricht. Der Gesamtbetrag, den Sie für 24 Stunden zahlen, setzt sich aus den Kosten für die Nutzung der Standard-Instance und den Kosten für den erweiterten Support zusammen, die sich auf 1,944 USD (1,632 USD+0,312 USD) belaufen. Die folgende Tabelle zeigt den Normalisierungsfaktor für verschiedene Instance-Größen in Service. OpenSearch

Instance-Größe	Normalisierungsfaktor
Nano	0,25
Micro	0,5
small	1
Medium	2
large	4
xlarge	8
2xlarge	16
4xlarge	32
8xlarge	64
9xlarge	72
10xlarge	80
12xlarge	96
16xlarge	128
18xlarge	144
24xlarge	192
32xlarge	256

Preise für Amazon OpenSearch Service

Für OpenSearch Service bezahlen Sie für jede Nutzungsstunde einer EC2 Instance und für die Gesamtgröße aller EBS-Speicher-Volumes, die an Ihre Instances angefügt sind. Es fallen auch AWS die üblichen Datenübertragungsgebühren an.

Es gibt jedoch einige wichtige Datenübertragungsausnahmen. Wenn eine Domain mehrere Availability Zones verwendet, stellt OpenSearch Service den Datenverkehr zwischen den Availability Zones nicht in Rechnung. Die während der Zuweisung und dem Rebalancing von Shards innerhalb einer Domain auftretende Datenübertragung ist beachtlich. OpenSearch Warten Sie für diesen Verkehr weder Zähler noch Rechnungen. Ebenso stellt OpenSearch Service keine Datenübertragung zwischen UltraWarmKalt -Knoten und Amazon S3 in Rechnung.

Ausführliche Preisinformationen finden Sie unter Amazon OpenSearch Service Preise. Weitere Informationen zu den Kosten bei Konfigurationsänderungen finden Sie unter the section called “Gebühren für Konfigurationsänderungen”.

Zugehörige Services

OpenSearch Dieser Service wird häufig mit folgenden Services verwendet:

Amazon CloudWatch

OpenSearch Service-Domains senden Metriken automatisch an, CloudWatch sodass Sie den Zustand und die Leistung von Domains überwachen können. Weitere Informationen finden Sie unter Überwachung von OpenSearch Cluster-Metriken mit Amazon CloudWatch.

CloudWatch Logs ist auch zu einem Richtungswechsel fähig. Sie könnten CloudWatch Logs konfigurieren, um Daten an OpenSearch Service zu streamen. Weitere Informationen hierzu finden Sie unter the section called “Streaming-Daten von Amazon laden CloudWatch”.

AWS CloudTrail

Verwenden Sie AWS CloudTrail , um einen Verlauf der OpenSearch Service-Konfigurations-API-Aufrufe und verwandter Ereignisse für Ihr Konto abzurufen. Weitere Informationen finden Sie unter Überwachung von Amazon OpenSearch Service API-Aufrufen mit AWS CloudTrail.

Amazon Kinesis

Kinesis ist ein vollständig verwalteter Service für die Verarbeitung riesiger Streaming-Datenmengen in Echtzeit. Weitere Informationen erhalten Sie unter the section called “So laden

Sie Streaming-Daten aus Amazon Kinesis Data Streams" und the section called "Streaming-Daten von Amazon Data Firehose laden".

Amazon S3

Amazon Simple Storage Service (Amazon S3) bietet Speicher für das Internet. Dieser Leitfaden bietet Lambda-Beispiel-Code für die Integration mit Amazon S3. Weitere Informationen finden Sie unter the section called "So laden Sie Streaming-Daten aus Amazon S3".

AWS IAM

AWS Identity and Access Management (IAM) ist ein Webservice, den Sie verwenden können, um den Zugriff auf Ihre OpenSearch Service-Domains zu verwalten. Weitere Informationen finden Sie unter the section called "Identitäts- und Zugriffsverwaltung".

AWS Lambda

AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Dieser Leitfaden bietet Lambda-Beispiel-Code für das Streamen von Daten aus DynamoDB, Amazon S3 und Kinesis. Weitere Informationen finden Sie unter the section called "Streaming-Daten werden in den OpenSearch Service geladen".

Amazon-DynamoDB

Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbank-Service, der schnelle und planbare Leistung mit nahtloser Skalierbarkeit bereitstellt. Weitere Informationen zum Streaming von Daten an OpenSearch Service finden Sie unterthe section called "So laden Sie Streaming-Daten aus Amazon DynamoDB".

Amazon QuickSight

Sie können Daten aus OpenSearch Service mithilfe von QuickSight Dashboards visualisieren. Weitere Informationen finden Sie unter Verwenden von Amazon OpenSearch Service mit QuickSight im QuickSight Benutzerhandbuch.

> **Note**
>
> OpenSearch enthält einen bestimmten Apache-lizenzierten Elasticsearch-Code von Elasticsearch B.V. und anderen Quellcode. Elasticsearch B.V. ist nicht die Quelle dieses anderen Quellcodes. ELASTICSEARCH ist eine eingetragene Marke von Elasticsearch B.V.

Amazon OpenSearch Service einrichten

Erteilen Sie Berechtigungen

In Produktionsumgebungen empfehlen wir Ihnen, detailliertere Richtlinien zu verwenden. Weitere Informationen zur Zugriffsverwaltung finden Sie unter Zugriffsverwaltung für AWS Ressourcen im IAM-Benutzerhandbuch.

Um Zugriff zu gewähren, fügen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzu:

- Benutzer und Gruppen in AWS IAM Identity Center:

  Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter Erstellen eines Berechtigungssatzes im AWS IAM Identity Center -Benutzerhandbuch.
- Benutzer, die in IAM über einen Identitätsanbieter verwaltet werden:

  Erstellen Sie eine Rolle für den Identitätsverbund. Befolgen Sie die Anleitung unter Eine Rolle für einen externen Identitätsanbieter (Verbund) erstellen im IAM-Benutzerhandbuch.
- IAM-Benutzer:
  - Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Befolgen Sie die Anleitung unter Eine Rolle für einen IAM-Benutzer erstellen im IAM-Benutzerhandbuch.
  - (Nicht empfohlen) Weisen Sie einem Benutzer eine Richtlinie direkt zu oder fügen Sie einen Benutzer zu einer Benutzergruppe hinzu. Befolgen Sie die Anweisungen unter Hinzufügen von Berechtigungen zu einem Benutzer (Konsole) im IAM-Benutzerhandbuch.

Erteilen programmgesteuerten Zugriffs

Benutzer benötigen programmgesteuerten Zugriff, wenn sie AWS außerhalb der AWS Management Console mit interagieren möchten. Die Vorgehensweise, um programmgesteuerten Zugriff zu gewähren, hängt davon ab, welcher Benutzertyp auf zugreift AWS.

Um Benutzern programmgesteuerten Zugriff zu gewähren, wählen Sie eine der folgenden Optionen.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
Mitarbeiteridentität (Benutzer, die in IAM Identity Center verwaltet werden)	Verwenden Sie temporäre Anmeldeinformationen, um programmatische Anfragen an das AWS CLI AWS SDKs, oder zu signieren. AWS APIs	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten. • Informationen zu den AWS CLI finden Sie unter Konfiguration der AWS CLI zur Verwendung AWS IAM Identity Center im AWS Command Line Interface Benutzerhandbuch. • Informationen zu AWS SDKs Tools und AWS APIs finden Sie unter IAM Identity Center-Authentifizierung im Referenzhandbuch AWS SDKs und im Tools-Ref erenzhandbuch.
IAM	Verwenden Sie temporäre Anmeldeinformationen, um programmatische Anfragen an das AWS CLI AWS SDKs, oder zu signieren. AWS APIs	Folgen Sie den Anweisungen unter Verwenden temporäre r Anmeldeinformationen mit AWS Ressourcen im IAM-Benutzerhandbuch.
IAM	(Nicht empfohlen) Verwenden Sie langfristige Anmeldeinformationen, um programmatische Anfragen an das AWS CLI AWS SDKs, oder zu signieren. AWS APIs	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten. • Informationen dazu AWS CLI finden Sie unter Authentifizierung mithilfe von IAM-Benutzeranmeld einformationen im AWS

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
		Command Line Interface Benutzerhandbuch. • Informationen zu AWS SDKs und Tools finden Sie unter Authentifizieren mit langfristigen Anmeldeinformationen im Referenzhandbuch AWS SDKs und im Tools-Referenzhandbuch. • Weitere Informationen finden Sie unter Verwaltung von Zugriffsschlüsseln für IAM-Benutzer im IAM-Benutzerhandbuch. AWS APIs

Installieren und konfigurieren Sie AWS CLI

Wenn Sie OpenSearch Service verwenden möchten APIs, müssen Sie die neueste Version von AWS Command Line Interface (AWS CLI) installieren. Sie AWS CLI müssen den OpenSearch Service nicht von der Konsole aus verwenden, und Sie können auch ohne die CLI loslegen, indem Sie die Schritte unter befolgenErste Schritte mit Amazon OpenSearch Service.

Um das einzurichten AWS CLI

1. Informationen zum Installieren der neuesten Version der AWS CLI für macOS, Linux oder Windows finden Sie unter Installieren oder Aktualisieren der AWS CLI.
2. Informationen zur Konfiguration AWS CLI und sicheren Einrichtung Ihres Zugriffs, einschließlich OpenSearch Service AWS-Services, finden Sie unter Schnellkonfiguration mit `aws configure`.
3. Geben Sie den folgenden DataBrew Befehl in die Befehlszeile ein, um die Einrichtung zu überprüfen.

```
aws opensearch help
```

AWS CLI Befehle verwenden den Standard AWS-Region aus Ihrer Konfiguration, sofern Sie ihn nicht mit einem Parameter oder einem Profil festlegen. Um Ihren AWS-Region mit einem Parameter festzulegen, können Sie den `--region` Parameter zu jedem Befehl hinzufügen.

Um Ihr AWS-Region Profil festzulegen, fügen Sie zunächst ein benanntes Profil in die `~/.aws/config` Datei oder die `%UserProfile%/.aws/config` Datei ein (für Microsoft Windows). Folgen Sie den Schritten unter Benannte Profile für AWS CLI. Legen Sie als Nächstes Ihre AWS-Region und andere Einstellungen mit einem Befehl fest, der dem im folgenden Beispiel ähnelt.

```
[profile opensearch]
aws_access_key_id = ACCESS-KEY-ID-OF-IAM-USER
aws_secret_access_key = SECRET-ACCESS-KEY-ID-OF-IAM-USER
region = us-east-1
output = text
```

Öffnen Sie die -Konsole

Die meisten konsolenorientierten Themen in diesem Abschnitt beginnen mit der OpenSearch Servicekonsole. Wenn Sie noch nicht bei Ihrem angemeldet sind AWS-Konto, melden Sie sich an, öffnen Sie dann die OpenSearch Servicekonsole und fahren Sie mit dem nächsten Abschnitt fort, um mit OpenSearch Service zu beginnen.

Erste Schritte mit Amazon OpenSearch Service

Melden Sie sich zunächst für ein AWS-Konto an, falls Sie noch keines haben. Nachdem Sie über ein Konto verfügen, schließen Sie das Erste Schritte -Tutorial für Amazon OpenSearch Service ab. Lesen Sie die folgenden einführenden Themen, wenn Sie weitere Informationen benötigen, während Sie sich Wissen über den Service aneignen:

- Erstellen Sie eine Domain.
- Festlegen der Domain-Größe entsprechend Ihrer Workload.
- Steuern Sie den Zugriff auf Ihre Domäne mithilfe einer Domainszugriffsrichtlinie oder einer differenzierten Zugriffssteuerung.
- Indizieren Sie Daten manuell oder von anderen AWS Diensten.
- Verwenden Sie OpenSearch Dashboards, um Ihre Daten zu durchsuchen und Visualisierungen zu erstellen.
- Erfahren Sie mehr über erweiterte Optionen zum Erstellen einer Domäne. Weitere Informationen finden Sie unter Erstellen und Verwalten von Domains.
- Erfahren Sie, wie Sie die Indizes in Ihrer Domain verwalten. Weitere Informationen finden Sie unter Verwalten von Indexen.
- Probieren Sie eines der Tutorials für die Arbeit mit Amazon OpenSearch Service aus. Weitere Informationen finden Sie unter Tutorials.

Informationen zur Migration von einem selbstverwalteten OpenSearch Cluster zu OpenSearch Service finden Sie unter. the section called “Migration zum Service OpenSearch ”

Weitere detaillierte Informationen finden Sie unter Erstellen und Verwalten von Domains und in anderen Themen in diesem Handbuch. Weitere Informationen zum Migrieren zu OpenSearch Service von einem selbstverwalteten OpenSearch Cluster finden Sie unter. the section called “Migration zum Service OpenSearch ”

Sie können die folgenden Schritte mithilfe der OpenSearch Servicekonsole AWS CLI, der oder der AWS SDK ausführen. Weitere Informationen zum Installieren und Einrichten der AWS CLI finden Sie im AWS Command Line Interface -Benutzerhandbuch.

Erstellen Sie eine Amazon OpenSearch Service-Domain

> **Important**
>
> Dies ist eine kurze Anleitung zum Konfigurieren einer Test -Domäne für Amazon OpenSearch Service. Verwenden Sie diesen Prozess nicht zum Erstellen von Produktionsdomänen. Eine ausführliche Beschreibung des Verfahrens erhalten Sie unter Erstellen und Verwalten von Domains.

Eine OpenSearch Service-Domäne ist ein Synonym für einen OpenSearch Cluster. Domains sind Cluster mit den Einstellungen, Instance-Typen, Instance-Anzahl und Speicherressourcen, die Sie angeben. Sie können eine OpenSearch Dienstdomäne erstellen, indem Sie die Konsole AWS CLI, den oder den AWS SDKs verwenden.

So erstellen Sie eine OpenSearch Dienstdomäne mithilfe der Konsole

1. Gehen Sie zu https://aws.amazon.comund wählen Sie In der Konsole anmelden.
2. Wählen Sie unter Analytics Amazon OpenSearch Service aus.
3. Wählen Sie Domäne erstellen aus.
4. Geben Sie einen Namen für die Domäne an. In den Beispielen in diesem Tutorial wird der Name Filme verwendet.
5. Wählen Sie für die Methode zur Domainerstellung die Option Standard create aus.

   > **Note**
   >
   > Um schnell eine Produktionsdomäne mit bewährten Methoden zu konfigurieren, können Sie Easy Create wählen. Für die Entwicklungs- und Testzwecke dieses Tutorials verwenden wir Standard Create.

6. Wählen Sie für Vorlagen Dev/Test.
7. Wählen Sie für die Bereitstellungsoption Domain with Standby.
8. Wählen Sie für Version die neueste Version aus.
9. Ignorieren Sie vorerst die Abschnitte Datenknoten, Warm- und Kaltdatenspeicher, Dedizierte Masterknoten, Snapshot-Konfiguration und Benutzerdefinierte Endpunkte.

10. Aus Gründen der Einfachheit nutzen Sie in diesem Tutorial eine Domäne mit öffentlichem Zugriff. Wählen Sie unter Netzwerk die Option Öffentlicher Zugriff aus.
11. Lassen Sie in den Einstellungen für differenzierte Zugriffssteuerung das Kontrollkästchen Differenzierte -Zugriffskontrolle aktivieren aktiviert. Wählen Sie Masterbenutzer erstellen aus und geben Sie einen Benutzernamen und ein Passwort ein.
12. Ignorieren Sie vorerst die Abschnitte SAML-Authentifizierung und Amazon-Cognito-Authentifizierung.
13. Wählen Sie für Zugriffsrichtlinie die Option Nur differenzierte Zugriffssteuerung verwenden aus. In diesem Tutorial ist die differenzierte Zugriffskontrolle für die Authentifizierung zuständig, nicht die Domänenzugriffsrichtlinie.
14. Ignorieren Sie die restlichen Einstellungen und wählen Sie Erstellen. Die Initialisierung neuer Domänen dauert in der Regel 15–30 Minuten, kann jedoch je nach Konfiguration auch länger dauern. Wählen Sie sie nach der Initialisierung der Domäne aus, um den Konfigurationsbereich zu öffnen. Beachten Sie den Domänenendpunkt unter Allgemeine Informationen (z. B. `https://search-my-domain.us-east-1.es.amazonaws.com`), den Sie im nächsten Schritt verwenden.

Weiter: Laden Sie Daten zur Indizierung in eine OpenSearch Dienstdomäne hoch

Daten aus Amazon OpenSearch Service zur Indizierung uploaden

> **Important**
>
> Dies ist eine kurze Anleitung zum Hochladen einer kleinen Menge von Testdaten auf Amazon OpenSearch Service. Weitere Informationen zum Hochladen von Daten in einer Produktionsdomäne finden Sie unter Indizierung von Daten.

Sie können Daten über die Befehlszeile oder die meisten Programmiersprachen in eine OpenSearch Service-Domäne hochladen.

Die folgenden Beispielanforderungen nutzen der Einfachheit halber und aus Gründen der Übersichtlichkeit curl, einen häufig verwendeten HTTP-Client. Clients wie curl können das Signieren von Anforderungen, das erforderlich ist, wenn Ihre Zugriffsrichtlinien IAM-Benutzer und -Rollen angeben, nicht durchführen. Um diesen Vorgang erfolgreich abzuschließen, müssen Sie eine

differenzierte Zugriffskontrolle mit einem primären Benutzernamen und Kennwort verwenden, wie Sie in Schritt 1 konfiguriert haben.

Sie können curl unter Windows installieren und an der Eingabeaufforderung verwenden, stattdessen wird aber ein Tool wie Cygwin oder das Windows-Subsystem für Linux empfohlen. In macOS und den meisten Linux-Verteilungen ist curl vorinstalliert.

Option 1: Hochladen eines einzelnen Dokuments

Führen Sie den folgenden Befehl aus, um ein einzelnes Dokument zur Domäne movies (Filme) hinzuzufügen:

```
curl -XPUT -u 'master-user:master-user-password' 'domain-endpoint/movies/_doc/1' -d
 '{"director": "Burton, Tim", "genre": ["Comedy","Sci-Fi"], "year": 1996, "actor":
 ["Jack Nicholson","Pierce Brosnan","Sarah Jessica Parker"], "title": "Mars Attacks!"}'
 -H 'Content-Type: application/json'
```

Geben Sie im Befehl den Benutzernamen und das von Ihnen in Schritt 1 erstellte Passwort bereit.

Eine detaillierte Erläuterung dieses Befehls und Informationen zum Erstellen signierter Anforderungen an OpenSearch Service finden Sie unterIndizierung von Daten.

Option 2: Hochladen mehrerer Dokumente

So laden Sie eine JSON-Datei mit mehreren Dokumenten in eine OpenSearch Dienstdomäne hoch

1. Erstellen Sie eine Datei mit dem Namen `bulk_movies.json`. Fügen Sie den folgenden Inhalt in die Datei ein und fügen Sie einen nachstehenden Zeilenumbruch hinzu:

   ```
   { "index" : { "_index": "movies", "_id" : "2" } }
   {"director": "Frankenheimer, John", "genre": ["Drama", "Mystery", "Thriller",
    "Crime"], "year": 1962, "actor": ["Lansbury, Angela", "Sinatra, Frank", "Leigh,
    Janet", "Harvey, Laurence", "Silva, Henry", "Frees, Paul", "Gregory, James",
    "Bissell, Whit", "McGiver, John", "Parrish, Leslie", "Edwards, James", "Flowers,
    Bess", "Dhiegh, Khigh", "Payne, Julie", "Kleeb, Helen", "Gray, Joe", "Nalder,
    Reggie", "Stevens, Bert", "Masters, Michael", "Lowell, Tom"], "title": "The
    Manchurian Candidate"}
   { "index" : { "_index": "movies", "_id" : "3" } }
   {"director": "Baird, Stuart", "genre": ["Action", "Crime", "Thriller"], "year":
    1998, "actor": ["Downey Jr., Robert", "Jones, Tommy Lee", "Snipes, Wesley",
    "Pantoliano, Joe", "Jacob, Ir\u00e8ne", "Nelligan, Kate", "Roebuck, Daniel",
   ```

```
 "Malahide, Patrick", "Richardson, LaTanya", "Wood, Tom", "Kosik, Thomas",
 "Stellate, Nick", "Minkoff, Robert", "Brown, Spitfire", "Foster, Reese",
 "Spielbauer, Bruce", "Mukherji, Kevin", "Cray, Ed", "Fordham, David", "Jett,
 Charlie"], "title": "U.S. Marshals"}
{ "index" : { "_index": "movies", "_id" : "4" } }
{"director": "Ray, Nicholas", "genre": ["Drama", "Romance"], "year": 1955, "actor":
 ["Hopper, Dennis", "Wood, Natalie", "Dean, James", "Mineo, Sal", "Backus, Jim",
 "Platt, Edward", "Ray, Nicholas", "Hopper, William", "Allen, Corey", "Birch,
 Paul", "Hudson, Rochelle", "Doran, Ann", "Hicks, Chuck", "Leigh, Nelson",
 "Williams, Robert", "Wessel, Dick", "Bryar, Paul", "Sessions, Almira", "McMahon,
 David", "Peters Jr., House"], "title": "Rebel Without a Cause"}
```

2. Führen Sie den folgenden Befehl im lokalen Verzeichnis aus, in dem die Datei gespeichert ist, um sie in die Domäne Film hochzuladen:

```
curl -XPOST -u 'master-user:master-user-password' 'domain-endpoint/movies/_bulk' --
data-binary @bulk_movies.json -H 'Content-Type: application/x-ndjson'
```

Weitere Informationen zum Massendateiformat finden Sie unter Indizierung von Daten.

Weiter:Suchen von Dokumenten

So suchen Sie Dokumente in Amazon OpenSearch Service

Verwenden Sie zur Suche nach Dokumenten in einer OpenSearch Amazon-Service-Domäne die OpenSearch Such-API. Alternativ können Sie OpenSearch Dashboards für die Suche nach Dokumenten in der Domäne verwenden.

So suchen Sie Dokumente über die Befehlszeile

Führen Sie den folgenden Befehl aus, um die Domäne movies (Filme) nach dem Wort mars zu durchsuchen:

```
curl -XGET -u 'master-user:master-user-password' 'domain-endpoint/movies/_search?
q=mars&pretty=true'
```

Wenn Sie die Massendaten auf der vorherigen Seite verwenden, suchen Sie stattdessen lieber nach rebel.

Es wird eine Antwort ähnlich der folgenden angezeigt:

```
{
  "took" : 5,
  "timed_out" : false,
  "_shards" : {
    "total" : 5,
    "successful" : 5,
    "skipped" : 0,
    "failed" : 0
  },
  "hits" : {
    "total" : {
      "value" : 1,
      "relation" : "eq"
    },
    "max_score" : 0.2876821,
    "hits" : [
      {
        "_index" : "movies",
        "_type" : "_doc",
        "_id" : "1",
        "_score" : 0.2876821,
        "_source" : {
          "director" : "Burton, Tim",
          "genre" : [
            "Comedy",
            "Sci-Fi"
          ],
          "year" : 1996,
          "actor" : [
            "Jack Nicholson",
            "Pierce Brosnan",
            "Sarah Jessica Parker"
          ],
          "title" : "Mars Attacks!"
        }
      }
    ]
  }
}
```

So suchen Sie Dokumente mit OpenSearch Dashboards

OpenSearch Dashboards ist ein beliebtes Open-Source-Visualisierungs-Tool, mit OpenSearch dem Sie arbeiten können. Es bietet eine hilfreiche Benutzeroberfläche für Sie, um Ihre Indizes zu suchen und zu überwachen.

So suchen Sie Dokumente aus einer OpenSearch Service-Domäne mithilfe von Dashboards

1. Navigieren Sie zur OpenSearch Dashboards-URL für Ihre Domäne. Sie finden die URL auf dem Dashboard der Domain in der OpenSearch Servicekonsole. Die URL weist das folgende Format auf:

   ```
   domain-endpoint/_dashboards/
   ```

2. Melden Sie sich mit Ihrem Hauptbenutzernamen und -passwort an.
3. Um Dashboards verwenden zu können, müssen Sie mindestens ein Indexmuster erstellen. Dashboards identifiziert anhand dieser Muster, welche Indizes Sie analysieren möchten. Öffnen Sie das linke Navigationspanel, wählen Sie Stack-Management, wählen Sie Indexmuster und dann Indexmuster erstellen. Geben Sie für dieses Tutorial Filme ein.
4. Wählen Sie Nächster Schritt aus und klicken Sie auf Indexmuster erstellen. Nachdem das Muster erstellt wurde, können Sie die verschiedenen Dokumentfelder anzeigen, z. B. `actor` und `director`.
5. Gehen Sie zurück zur Seite Indexmuster und stellen Sie sicher, dass `movies` als Standard eingestellt ist. Wenn dies nicht der Fall ist, wählen Sie das Muster aus und wählen Sie das Sternsymbol, um es zum Standardwert zu machen.
6. Um mit der Suche nach Ihren Daten zu beginnen, öffnen Sie erneut das linke Navigationsfeld und wählen Sie Entdecken.
7. Geben Sie in der Suchleiste mars ein, wenn Sie ein einzelnes Dokument hochgeladen haben, oder rebel, wenn Sie mehrere Dokumente hochgeladen haben, und drücken Sie dann die Eingabetaste. Sie können versuchen, andere Begriffe wie Schauspieler- oder Regisseurnamen zu durchsuchen.

Weiter:Domäne löschen

OpenSearch Amazon-Service-Domain löschen

Da die in diesem Tutorial erstellte Domäne Filme nur Testzwecken dient, sollten Sie sie löschen, wenn Sie mit dem Experimentieren fertig sind, um unnötige Gebühren zu vermeiden.

So löschen Sie eine OpenSearch Dienstdomäne aus der Konsole

1. Melden Sie sich bei der Amazon OpenSearch Service-Konsole an.
2. Wählen Sie unter Domänen die Filmdomäne aus.
3. Wählen Sie Löschen und bestätigen Sie das Löschen.

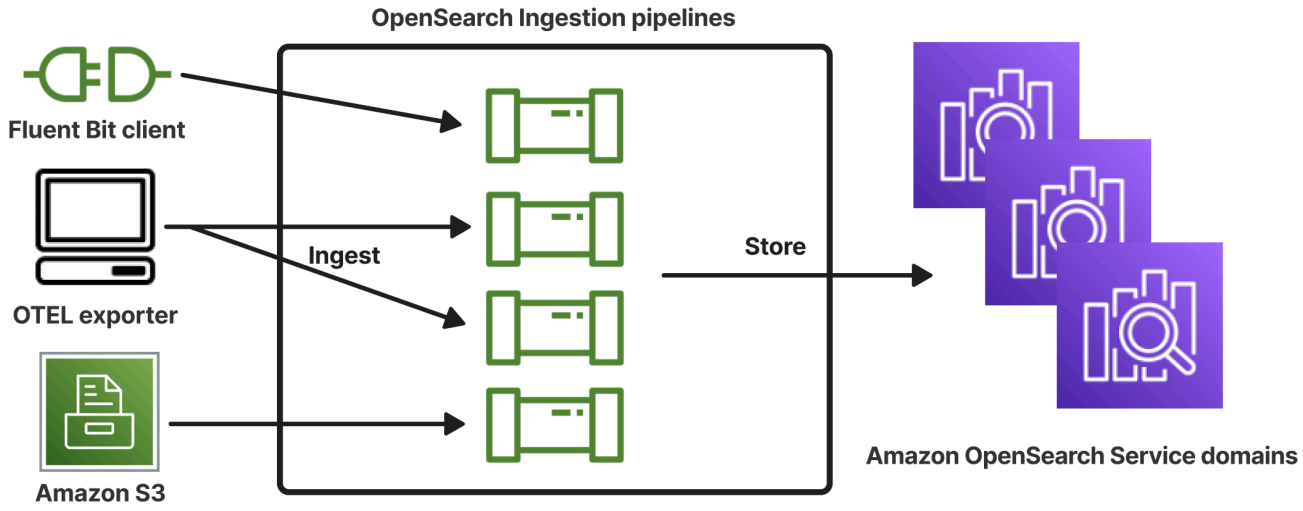
Überblick über Amazon OpenSearch Ingestion

Amazon OpenSearch Ingestion ist ein vollständig verwalteter, serverloser Datensammler, der Protokolle, Metriken und Trace-Daten in Echtzeit an Amazon OpenSearch Service-Domains und OpenSearch serverlose Sammlungen streamt.

Mit OpenSearch Ingestion benötigen Sie keine Tools von Drittanbietern wie Logstash oder Jaeger mehr, um Daten aufzunehmen. Sie konfigurieren Ihre Datenproduzenten so, dass sie Daten an OpenSearch Ingestion senden, und Ingestion sendet sie automatisch an Ihre angegebene Domain oder Sammlung. Sie können Daten auch vor der Auslieferung transformieren.

Da OpenSearch Ingestion serverlos ist, müssen Sie die Infrastruktur nicht manuell verwalten, Software patchen oder Cluster skalieren. Sie können Ingestion-Pipelines direkt in der bereitstellen AWS Management Console, und Ingestion kümmert sich um den Rest. OpenSearch

Als Bestandteil von Amazon OpenSearch Service wird OpenSearch Ingestion von Data Prepper unterstützt — einem Open-Source-Datensammler, der Daten für nachgelagerte Analysen und Visualisierungen filtert, anreichert, transformiert, normalisiert und aggregiert.



Die wichtigsten Konzepte von Amazon OpenSearch Ingestion

Bevor Sie mit der Verwendung von OpenSearch Ingestion beginnen, ist es hilfreich, diese Schlüsselkonzepte zu verstehen.

Pipeline

Aus Sicht der OpenSearch Datenerfassung bezieht sich eine Pipeline auf einen einzelnen bereitgestellten Datensammelpunkt, den Sie in Service erstellen. OpenSearch Sie können sich das als die gesamte YAML-Konfigurationsdatei vorstellen, die eine oder mehrere Unter-Pipelines enthält. Schritte zum Erstellen einer Ingestion-Pipeline finden Sie unter. the section called “Pipelines erstellen”

Unterpipeline

Sie definieren Sub-Pipelines in einer YAML-Konfigurationsdatei. Jede Subpipeline ist eine Kombination aus einer Quelle, einem Puffer, null oder mehr Prozessoren und einer oder mehreren Senken. Sie können mehrere Sub-Pipelines in einer einzigen YAML-Datei definieren, jede mit eigenen Quellen, Prozessoren und Senken. Um die Überwachung mit CloudWatch und anderen Diensten zu erleichtern, empfehlen wir Ihnen, einen Pipeline-Namen anzugeben, der sich von allen Unter-Pipelines unterscheidet.

Sie können mehrere Sub-Pipelines in einer einzigen YAML-Datei aneinanderreihen, sodass die Quelle für eine Sub-Pipeline eine andere Sub-Pipeline und deren Senke eine dritte Sub-Pipeline ist. Ein Beispiel finden Sie unter the section called “OpenTelemetry Kollektor”.

Quelle

Die Eingabekomponente einer Subpipeline. Sie definiert den Mechanismus, über den eine Pipeline Datensätze verarbeitet. Die Quelle kann Ereignisse verarbeiten, indem sie sie entweder über HTTPS empfängt oder sie von externen Endpunkten wie Amazon S3 liest. Es gibt zwei Arten von Quellen: Push-basierte und Pull-basierte. Push-basierte Quellen wie HTTP und OTel Logs streamen Datensätze an Aufnahmeendpunkte. Pull-basierte Quellen wie OTel Trace und S3 rufen Daten aus der Quelle ab.

Prozessoren

Zwischenverarbeitungseinheiten, die Datensätze filtern, transformieren und in ein gewünschtes Format anreichern können, bevor sie auf der Senke veröffentlicht werden. Der Prozessor ist eine optionale Komponente einer Pipeline. Wenn Sie keinen Prozessor definieren, werden Datensätze in dem Format veröffentlicht, das in der Quelle definiert ist. Sie können mehr als einen Prozessor haben. In einer Pipeline werden Prozessoren in der Reihenfolge ausgeführt, in der Sie sie definieren.

Sink

Die Ausgabekomponente einer Subpipeline. Sie definiert ein oder mehrere Ziele, an denen eine Unterpipeline Datensätze veröffentlicht. OpenSearch Ingestion unterstützt OpenSearch Dienstdomänen als Senken. Es unterstützt auch Sub-Pipelines als Senken. Das bedeutet, dass Sie mehrere Sub-Pipelines innerhalb einer einzigen OpenSearch Ingestion-Pipeline (YAML-Datei) aneinanderreihen können. Selbstverwaltete OpenSearch Cluster werden nicht als Senken unterstützt.

Buffer

Der Teil eines Prozessors, der als Schicht zwischen Quelle und Senke fungiert. Sie können einen Puffer in Ihrer Pipeline nicht manuell konfigurieren. OpenSearch Die Aufnahme verwendet eine Standard-Pufferkonfiguration.

Route

Der Teil eines Prozessors, der es Pipeline-Autoren ermöglicht, nur Ereignisse, die bestimmten Bedingungen entsprechen, an verschiedene Senken zu senden.

Eine gültige Sub-Pipeline-Definition muss eine Quelle und eine Senke enthalten. Weitere Informationen zu jedem dieser Pipeline-Elemente finden Sie in der Konfigurationsreferenz.

Vorteile von Amazon OpenSearch Ingestion

OpenSearch Die Einnahme hat die folgenden Hauptvorteile:

- Eliminiert die Notwendigkeit, eine selbst bereitgestellte Pipeline manuell zu verwalten.
- Skaliert Ihre Pipelines automatisch auf der Grundlage der von Ihnen definierten Kapazitätsgrenzen.
- Hält Ihre Pipeline mit Sicherheits- und Bug-Patches auf dem neuesten Stand.
- Bietet die Option, Pipelines mit Ihrer Virtual Private Cloud (VPC) zu verbinden, um eine zusätzliche Sicherheitsebene zu schaffen.
- Ermöglicht das Stoppen und Starten von Pipelines, um die Kosten zu kontrollieren.
- Bietet Pipeline-Konfigurations-Blueprints für beliebte Anwendungsfälle, damit Sie schneller loslegen können.
- Ermöglicht Ihnen die programmgesteuerte Interaktion mit Ihren Pipelines über die verschiedenen AWS SDKs und die Ingestion-API. OpenSearch

- Unterstützt die Leistungsüberwachung in Amazon CloudWatch und die Fehlerprotokollierung in CloudWatch Logs.

Einschränkungen von Amazon OpenSearch Ingestion

OpenSearch Bei Ingestion gelten die folgenden Einschränkungen:

- Sie können Daten nur in Domains aufnehmen, auf denen OpenSearch 1.0 oder höher oder Elasticsearch 6.8 oder höher ausgeführt wird. Wenn Sie die OTel Trace-Quelle verwenden, empfehlen wir die Verwendung von Elasticsearch 7.9 oder höher, damit Sie das Dashboards-Plugin verwenden können. OpenSearch
- Wenn eine Pipeline in eine OpenSearch Dienstdomäne schreibt, die sich innerhalb einer VPC befindet, muss die Pipeline in derselben Domäne AWS-Region wie die Domäne erstellt werden.
- Sie können nur eine einzelne Datenquelle innerhalb einer Pipeline-Definition konfigurieren.
- Sie können selbstverwaltete OpenSearch Cluster nicht als Senken angeben.
- Sie können keinen benutzerdefinierten Endpunkt als Senke angeben. Sie können immer noch in eine Domäne schreiben, für die benutzerdefinierte Endpunkte aktiviert sind, aber Sie müssen ihren Standardendpunkt angeben.
- Sie können Ressourcen innerhalb von Opt-in-Regionen nicht als Quellen oder Senken angeben.
- Es gibt einige Einschränkungen in Bezug auf die Parameter, die Sie in eine Pipeline-Konfiguration aufnehmen können. Weitere Informationen finden Sie unter the section called “Konfigurationsanforderungen und Einschränkungen”.

Unterstützte Data Prepper-Versionen

OpenSearch Ingestion unterstützt derzeit die folgenden Hauptversionen von Data Prepper:

- 2.x

Wenn Sie eine Pipeline mit dem Code-Editor erstellen, verwenden Sie die erforderliche `version` Option, um die zu verwendende Hauptversion von Data Prepper anzugeben. Zum Beispiel. `version: "2"` OpenSearch Ingestion ruft die neueste unterstützte Nebenversion dieser Hauptversion ab und stellt die Pipeline mit dieser Version bereit.

Wenn Sie den Code-Editor nicht zum Erstellen Ihrer Pipeline verwenden, stellt OpenSearch Ingestion Ihre Pipeline automatisch mit der neuesten unterstützten Version bereit.

Derzeit stellt OpenSearch Ingestion Pipelines mit Version 2.7 von Data Prepper bereit. Informationen finden Sie in den Versionshinweisen zu 2.7. Nicht jede Nebenversion einer bestimmten Hauptversion wird von OpenSearch Ingestion unterstützt.

Wenn Sie die Konfiguration einer Pipeline aktualisieren und eine neue Nebenversion von Data Prepper unterstützt wird, aktualisiert OpenSearch Ingestion die Pipeline automatisch auf die neueste unterstützte Nebenversion der Hauptversion, die in der Pipeline-Konfiguration angegeben ist. Möglicherweise haben Sie `version: "2"` in Ihrer Pipeline-Konfiguration und OpenSearch Ingestion die Pipeline zunächst mit Version 2.6.0 bereitgestellt. Wenn Unterstützung für Version 2.7.0 hinzugefügt wird und Sie eine Änderung an der Pipeline-Konfiguration vornehmen, aktualisiert OpenSearch Ingestion die Pipeline auf Version 2.7.0. Dieser Prozess hält Ihre Pipeline mit den neuesten Bugfixes und Leistungsverbesserungen auf dem neuesten Stand. OpenSearch Ingestion kann die Hauptversion Ihrer Pipeline nur aktualisieren, wenn Sie die `version` Option in der Pipeline-Konfiguration manuell ändern. Weitere Informationen finden Sie unter the section called “Pipelines aktualisieren”.

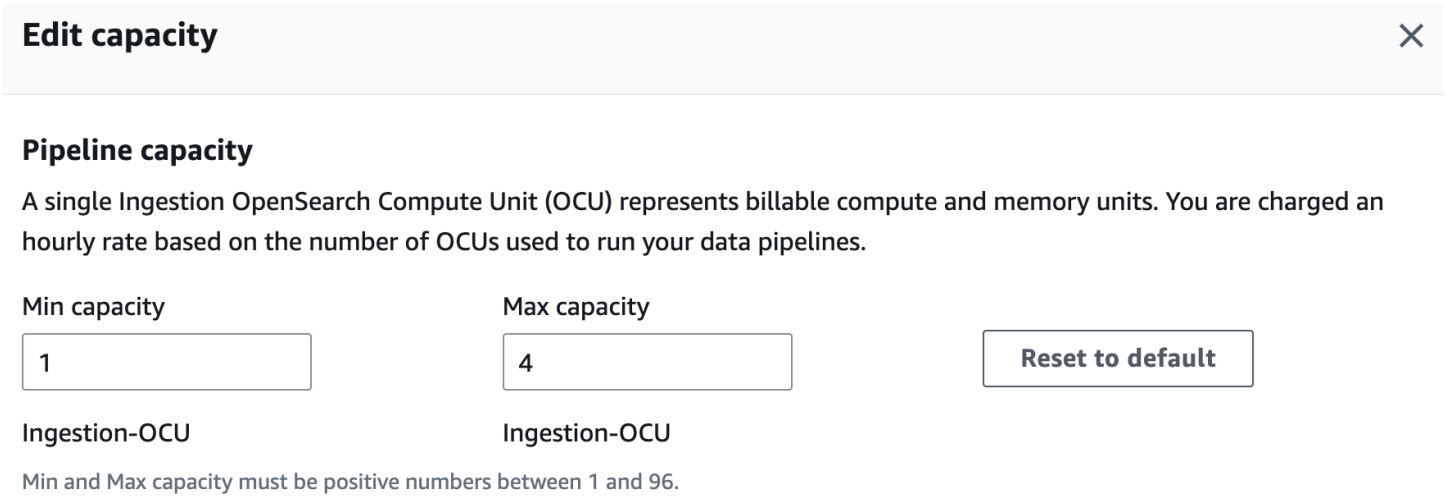
Skalierung von Pipelines in Amazon OpenSearch Ingestion

OpenSearch Ingestion skaliert die Pipeline-Kapazität automatisch auf der Grundlage Ihrer angegebenen minimalen und maximalen Ingestion-Recheneinheiten (OpenSearch Ingestion). OCUs Dadurch entfällt die Notwendigkeit einer manuellen Bereitstellung und Verwaltung.

Jede Ingestion-OCU ist eine Kombination aus etwa 15 GiB Arbeitsspeicher und 2 V. CPUs Sie können die minimalen und maximalen OCU-Werte für eine Pipeline angeben, und OpenSearch Ingestion skaliert Ihre Pipeline-Kapazität automatisch auf der Grundlage dieser Grenzwerte.

Sie geben die folgenden Werte an, wenn Sie eine Pipeline erstellen:

- Mindestkapazität — Die Pipeline kann die Kapazität bis auf diese Anzahl an Ingestions reduzieren. OCUs Die angegebene Mindestkapazität ist auch die Startkapazität für eine Pipeline.
- Maximale Kapazität — Die Pipeline kann die Kapazität bis zu dieser Anzahl an Aufnahmemengen erhöhen. OCUs



Stellen Sie sicher, dass die maximale Kapazität für eine Pipeline hoch genug ist, um Arbeitsspitzen zu bewältigen, und dass die Mindestkapazität niedrig genug ist, um die Kosten zu minimieren, wenn die Pipeline nicht ausgelastet ist. Basierend auf Ihren Einstellungen skaliert OpenSearch Ingestion automatisch die Anzahl der Ingestions OCUs für Ihre Pipeline, um die Ingestion-Arbeitslast zu verarbeiten. Zu einem bestimmten Zeitpunkt werden Ihnen nur die Ingestions in Rechnung gestellt, die von Ihrer Pipeline aktiv OCUs genutzt werden.

Die Ihrer OpenSearch Ingestion-Pipeline zugewiesene Kapazität wird je nach den Verarbeitungsanforderungen Ihrer Pipeline und der durch Ihre Client-Anwendung generierten Last nach oben oder unten skaliert. Wenn die Kapazität begrenzt ist, wird die OpenSearch Aufnahme skaliert, indem mehr Recheneinheiten (GiB Arbeitsspeicher) zugewiesen werden. Wenn Ihre Pipeline kleinere Workloads oder gar keine Daten verarbeitet, kann sie auf das konfigurierte Minimum herunterskaliert werden. OCUs

Sie können mindestens 1 Ingestion OCU, maximal 96 Ingestion für statusfreie Pipelines und maximal 48 Ingestion OCUs für statusbehaftete Pipelines angeben. OCUs Wir empfehlen mindestens 2 Ingestions für Push-basierte Quellen. OCUs Wenn die persistente Pufferung aktiviert ist, können Sie mindestens 2 und maximal 384 Ingestions angeben. OCUs

Bei einer Standard-Log-Pipeline mit einer einzigen Quelle, einem einfachen Grok-Muster und einer Senke kann jede Recheneinheit bis zu 2 MiB pro Sekunde unterstützen. Bei komplexeren Protokoll-Pipelines mit mehreren Prozessoren unterstützt jede Recheneinheit möglicherweise weniger Aufnahmelast. Basierend auf der Pipeline-Kapazität und der Ressourcennutzung setzt der Prozess der OpenSearch Ingestion-Skalierung ein.

Um eine hohe Verfügbarkeit zu gewährleisten, wird die Datenaufnahme auf mehrere Availability OCUs Zones () verteilt. AZs Die Anzahl von AZs hängt von der Mindestkapazität ab, die Sie angeben.

Wenn Sie beispielsweise mindestens 2 Recheneinheiten angeben, werden die Ingestion-Einheiten, OCUs die zu einem bestimmten Zeitpunkt verwendet werden, gleichmäßig auf 2 verteilt. AZs Wenn Sie mindestens 3 oder mehr Recheneinheiten angeben, OCUs werden die Ingestion gleichmäßig auf 3 verteilt. AZs Wir empfehlen, dass Sie mindestens zwei Ingestions bereitstellen, OCUs um eine Verfügbarkeit von 99,9% für Ihre Ingest-Pipelines sicherzustellen.

Wenn sich eine Pipeline in den Bundesstaaten,, und befindet, wird Ihnen keine OCUs Ingestion in Rechnung gestellt. `Create failed` `Creating` `Deleting` `Stopped`

Anweisungen zum Konfigurieren und Abrufen von Kapazitätseinstellungen für eine Pipeline finden Sie unter. the section called “Pipelines erstellen”

OpenSearch Preise für die Aufnahme

Zu einem bestimmten Zeitpunkt zahlen Sie nur für die Anzahl der Datenerfassungen, OCUs die einer Pipeline zugewiesen sind, unabhängig davon, ob Daten durch die Pipeline fließen. OpenSearch Ingestion passt sich Ihren Workloads sofort an, indem die Pipeline-Kapazität je nach Nutzung nach oben oder unten skaliert wird.

Vollständige Preisinformationen finden Sie unter Amazon OpenSearch Service-Preise.

Unterstützt AWS-Regionen

OpenSearch Die Aufnahme ist in einem Teil AWS-Regionen dieses OpenSearch Dienstes verfügbar. Eine Liste der unterstützten Regionen finden Sie unter Amazon OpenSearch Service-Endpunkte und Kontingente in der Allgemeine AWS-Referenz.

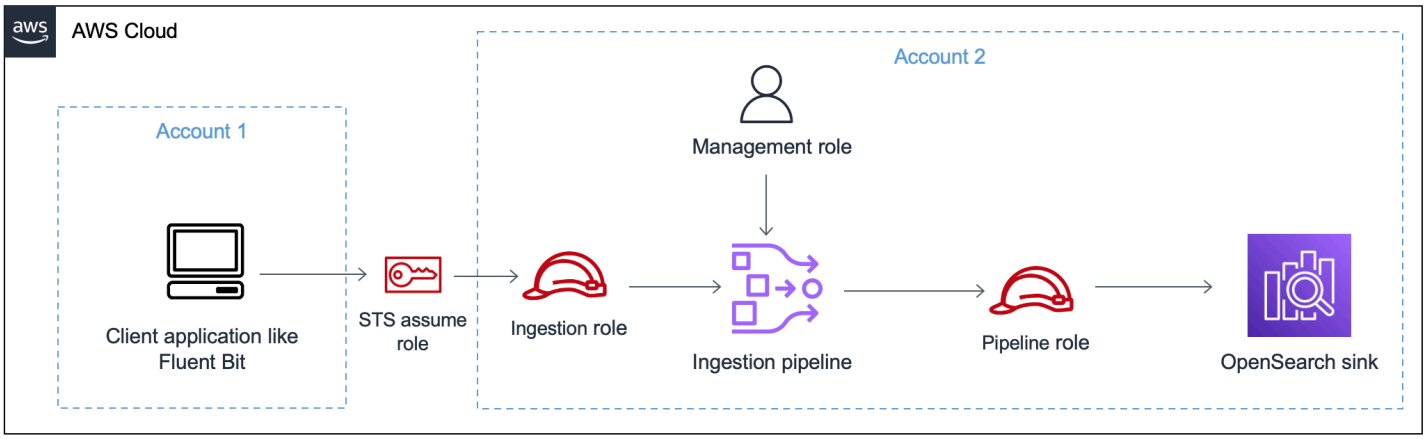
Rollen und Benutzer in Amazon OpenSearch Ingestion einrichten

Amazon OpenSearch Ingestion verwendet eine Vielzahl von Berechtigungsmodellen und IAM-Rollen, um Quellanwendungen das Schreiben in Pipelines und Pipelines das Schreiben in Senken zu ermöglichen. Bevor Sie mit der Datenaufnahme beginnen können, müssen Sie je nach Anwendungsfall eine oder mehrere IAM-Rollen mit spezifischen Berechtigungen erstellen.

Für die Einrichtung einer erfolgreichen Pipeline sind mindestens die folgenden Rollen erforderlich.

Name	Beschreibung
Rolle „Pipeline“	Die Pipeline-Rolle stellt die erforderlichen Berechtigungen für eine Pipeline bereit, um aus der Quelle zu lesen und in die Domäne oder Sammelsenke zu schreiben. Sie können die Pipeline-Rolle manuell erstellen, oder Sie können sie OpenSearch von Ingestion für Sie erstellen lassen.
Rolle „Ingestion“	Die Rolle „Ingestion“ enthält die `osis:Ingest` Berechtigung für die Pipeline-Ressource. Diese Berechtigung ermöglicht es Push-basierten Quellen, Daten in eine Pipeline aufzunehmen.

Die folgende Abbildung zeigt ein typisches Pipeline-Setup, bei dem eine Datenquelle wie Amazon S3 oder Fluent Bit in eine Pipeline in einem anderen Konto schreibt. In diesem Fall muss der Client die Rolle der Datenerfassung übernehmen, um auf die Pipeline zugreifen zu können. Weitere Informationen finden Sie unter the section called “Kontoübergreifende Aufnahme”.



Eine einfache Anleitung zur Einrichtung finden Sie unter. the section called “Tutorial: Daten in eine Domain aufnehmen”

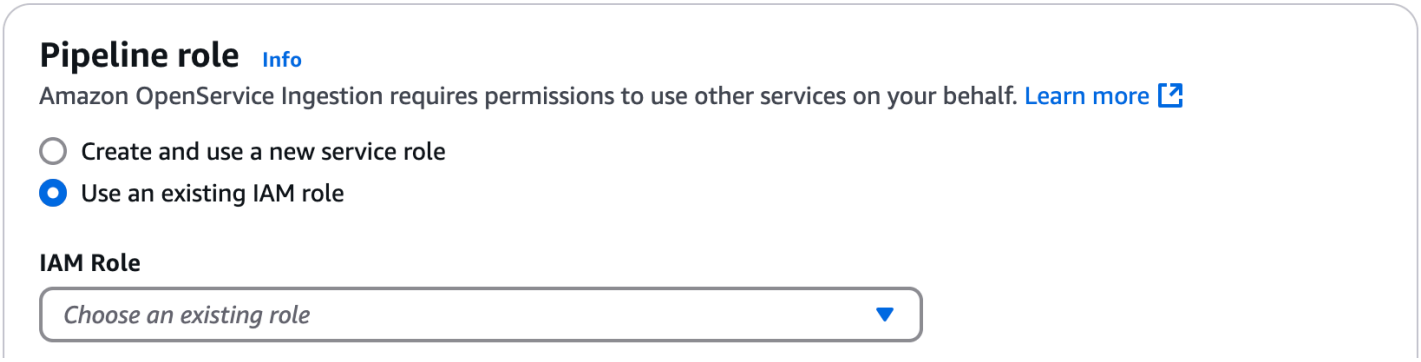
Topics

- the section called “Rolle „Pipeline““
- the section called “Rolle „Aufnahme““
- the section called “Kontoübergreifende Aufnahme”

Rolle „Pipeline“

Eine Pipeline benötigt bestimmte Berechtigungen, um aus ihrer Quelle lesen und in ihre Senke schreiben zu können. Diese Berechtigungen hängen von der Client-Anwendung oder der Client-Anwendung ab AWS-Service , die in die Pipeline schreibt, und davon, ob es sich bei der Senke um eine OpenSearch Service-Domain, eine OpenSearch serverlose Sammlung oder Amazon S3 handelt. Darüber hinaus benötigt eine Pipeline möglicherweise Berechtigungen zum physischen Abrufen von Daten aus der Quellanwendung (wenn es sich bei der Quelle um ein pullbasiertes Plug-In handelt) sowie Berechtigungen zum Schreiben in eine S3-Warteschlange mit unerlaubtem Schreiben, falls diese aktiviert sind.

Wenn Sie eine Pipeline erstellen, haben Sie die Möglichkeit, eine vorhandene IAM-Rolle anzugeben, die Sie manuell erstellt haben, oder OpenSearch Ingestion die Pipeline-Rolle automatisch auf der Grundlage der von Ihnen ausgewählten Quelle und Senke erstellen zu lassen. Die folgende Abbildung zeigt, wie Sie die Pipeline-Rolle in der angeben. AWS Management Console



Themen

- Automatisieren der Erstellung von Pipeline-Rollen
- Manuelles Erstellen der Pipeline-Rolle

Automatisieren der Erstellung von Pipeline-Rollen

Sie können festlegen, dass OpenSearch Ingestion die Pipeline-Rolle für Sie erstellt. Anhand der konfigurierten Quelle und Senken wird automatisch erkannt, welche Berechtigungen für die Rolle erforderlich sind. Es erstellt eine IAM-Rolle mit dem Präfix und dem Suffix`OpenSearchIngestion-`, das Sie eingeben. Wenn Sie beispielsweise das Suffix eingeben`PipelineRole`, erstellt OpenSearch Ingestion eine Rolle mit dem Namen. `OpenSearchIngestion-PipelineRole`

Die automatische Erstellung der Pipeline-Rolle vereinfacht den Einrichtungsprozess und verringert die Wahrscheinlichkeit von Konfigurationsfehlern. Durch die Automatisierung der Rollenerstellung können Sie die manuelle Zuweisung von Berechtigungen vermeiden und so sicherstellen, dass die richtigen Richtlinien angewendet werden, ohne Sicherheitsfehlkonfigurationen zu riskieren. Dies spart auch Zeit und verbessert die Einhaltung der Sicherheitsbestimmungen, indem bewährte Verfahren durchgesetzt und gleichzeitig die Konsistenz über mehrere Pipeline-Implementierungen hinweg gewährleistet wird.

Sie können nur festlegen, dass OpenSearch Ingestion automatisch die Pipeline-Rolle in der erstellt. AWS Management Console Wenn Sie die AWS CLI, die OpenSearch Ingestion-API oder eine der folgenden verwenden, müssen Sie eine manuell erstellte SDKs Pipeline-Rolle angeben.

Damit OpenSearch Ingestion die Rolle für Sie erstellt, wählen Sie Neue Servicerolle erstellen und verwenden aus.

> **Important**
>
> Sie müssen die Zugriffsrichtlinie für die Domäne oder Sammlung immer noch manuell ändern, um Zugriff auf die Pipeline-Rolle zu gewähren. Bei Domänen, die eine differenzierte Zugriffskontrolle verwenden, müssen Sie die Pipeline-Rolle auch einer Backend-Rolle zuordnen. Sie können diese Schritte vor oder nach dem Erstellen der Pipeline ausführen. Anweisungen finden Sie in den folgenden Themen:
>
> - Konfigurieren Sie den Datenzugriff für die Domain
> - Konfigurieren Sie den Daten- und Netzwerkzugriff für die Sammlung

Manuelles Erstellen der Pipeline-Rolle

Möglicherweise ziehen Sie es vor, die Pipeline-Rolle manuell zu erstellen, wenn Sie mehr Kontrolle über die Berechtigungen benötigen, um bestimmte Sicherheits- oder Compliance-Anforderungen zu erfüllen. Durch die manuelle Erstellung können Sie Rollen an bestehende Infrastruktur- oder Zugriffsverwaltungsstrategien anpassen. Sie können sich auch für die manuelle Einrichtung entscheiden, um die Rolle mit anderen zu integrieren AWS-Services oder sicherzustellen, dass sie Ihren individuellen betrieblichen Anforderungen entspricht.

Um eine manuell erstellte Pipeline-Rolle auszuwählen, wählen Sie Bestehende IAM-Rolle verwenden und wählen Sie eine vorhandene Rolle aus. Die Rolle muss über alle erforderlichen Berechtigungen

verfügen, um Daten von der ausgewählten Quelle zu empfangen und in die ausgewählte Senke zu schreiben. In den folgenden Abschnitten wird beschrieben, wie Sie eine Pipeline-Rolle manuell erstellen.

Themen

- Berechtigungen zum Lesen aus einer Quelle
- Berechtigungen zum Schreiben in eine Domain-Senke
- Berechtigungen zum Schreiben in eine Sammelsenke
- Berechtigungen zum Schreiben in Amazon S3 oder in eine Warteschlange mit unzustellbaren Briefen

Berechtigungen zum Lesen aus einer Quelle

Eine OpenSearch Ingestion-Pipeline benötigt die Berechtigung, Daten aus der angegebenen Quelle zu lesen und zu empfangen. Für eine Amazon DynamoDB DynamoDB-Quelle benötigt sie beispielsweise Berechtigungen wie `dynamodb:DescribeTable` und. `dynamodb:DescribeStream` Beispielrichtlinien für den Zugriff auf Pipeline-Rollen für gängige Quellen wie Amazon S3, Fluent Bit und OpenTelemetry Collector finden Sie unterthe section called “Integration von Pipelines”.

Berechtigungen zum Schreiben in eine Domain-Senke

Eine OpenSearch Ingestion-Pipeline benötigt die Berechtigung, in eine OpenSearch Dienstdomäne zu schreiben, die als Senke konfiguriert ist. Zu diesen Berechtigungen gehört die Fähigkeit, die Domain zu beschreiben und HTTP-Anfragen an sie zu senden. Diese Berechtigungen sind für öffentliche Domains und VPC-Domains identisch. Anweisungen zum Erstellen einer Pipeline-Rolle und deren Angabe in der Domänenzugriffsrichtlinie finden Sie unter Zulassen des Zugriffs von Pipelines auf Domänen.

Berechtigungen zum Schreiben in eine Sammelsenke

Eine OpenSearch Ingestion-Pipeline benötigt die Berechtigung, in eine OpenSearch serverlose Sammlung zu schreiben, die als Senke konfiguriert ist. Zu diesen Berechtigungen gehört die Fähigkeit, die Sammlung zu beschreiben und HTTP-Anfragen an sie zu senden.

Stellen Sie zunächst sicher, dass Ihre Pipeline-Rollenzugriffsrichtlinie die erforderlichen Berechtigungen gewährt. Nehmen Sie diese Rolle anschließend in eine Datenzugriffsrichtlinie auf und

gewähren Sie ihr Berechtigungen zum Erstellen von Indizes, Aktualisieren von Indizes, Beschreiben von Indizes und Schreiben von Dokumenten innerhalb der Sammlung. Anweisungen zum Ausführen der einzelnen Schritte finden Sie unter Zulassen des Zugriffs von Pipelines auf Sammlungen.

Berechtigungen zum Schreiben in Amazon S3 oder in eine Warteschlange mit unzustellbaren Briefen

Wenn Sie Amazon S3 als Sink-Ziel für Ihre Pipeline angeben oder wenn Sie eine Dead-Letter-Warteschlange (DLQ) aktivieren, muss die Pipeline-Rolle ihr den Zugriff auf den S3-Bucket ermöglichen, den Sie als Ziel angeben.

Fügen Sie der Pipeline-Rolle, die den DLQ-Zugriff gewährt, eine separate Berechtigungsrichtlinie hinzu. Der Rolle muss mindestens die `S3:PutObject` Aktion für die Bucket-Ressource gewährt werden:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "WriteToS3DLQ",
      "Effect": "Allow",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::my-dlq-bucket/*"
    }
  ]
}
```

Rolle „Aufnahme“

Die Aufnahmerolle ist eine IAM-Rolle, die es externen Diensten ermöglicht, sicher mit einer Ingestion-Pipeline zu interagieren und Daten an diese zu senden. OpenSearch Für Push-basierte Quellen wie Amazon Security Lake muss diese Rolle Berechtigungen zum Pushen von Daten in die Pipeline gewähren, einschließlich`osis:Ingest`. Bei pull-basierten Quellen wie Amazon S3 muss die Rolle es OpenSearch Ingestion ermöglichen, sie zu übernehmen und mit den erforderlichen Berechtigungen auf die Daten zuzugreifen.

Themen

- Rolle „Ingestion“ für Push-basierte Quellen

- Rolle „Ingestion“ für Pull-basierte Quellen
- Kontoübergreifende Aufnahme

Rolle „Ingestion“ für Push-basierte Quellen

Bei Push-basierten Quellen werden Daten von einem anderen Service, wie Amazon Security Lake oder Amazon DynamoDB, an die Aufnahme-Pipeline gesendet oder per Push übertragen. In diesem Szenario benötigt die Aufnahmerolle mindestens die Erlaubnis, mit der `osis:Ingest` Pipeline zu interagieren.

Die folgende IAM-Zugriffsrichtlinie zeigt, wie diese Berechtigung der Aufnahmerolle erteilt wird:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "osis:Ingest"
      ],
      "Resource": "arn:aws:osis:region:account-id:pipeline/pipeline-name/*"
    }
  ]
}
```

Rolle „Ingestion“ für Pull-basierte Quellen

Bei pull-basierten Quellen ruft die OpenSearch Ingestion-Pipeline aktiv Daten aus einer externen Quelle ab, z. B. Amazon S3. In diesem Fall muss die Pipeline eine IAM-Pipeline-Rolle übernehmen, die die erforderlichen Berechtigungen für den Zugriff auf die Datenquelle gewährt. In diesen Szenarien ist die Aufnahmerolle gleichbedeutend mit der Pipeline-Rolle.

Die Rolle muss eine Vertrauensstellung beinhalten, die es OpenSearch Ingestion ermöglicht, diese zu übernehmen, sowie spezifische Berechtigungen für die Datenquelle. Weitere Informationen finden Sie unter the section called “Berechtigungen zum Lesen aus einer Quelle”.

Kontoübergreifende Aufnahme

Möglicherweise müssen Sie Daten von einem anderen Konto, z. B. einem Anwendungskonto AWS-Konto, in eine Pipeline aufnehmen. Um die kontoübergreifende Erfassung zu konfigurieren, definieren Sie eine Aufnahmerolle innerhalb desselben Kontos wie die Pipeline und richten Sie eine Vertrauensbeziehung zwischen der Aufnahmerolle und dem Anwendungskonto ein:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
     "Effect": "Allow",
     "Principal": {
       "AWS": "arn:aws:iam::external-account-id:root"
      },
     "Action": "sts:AssumeRole"
  }]
}
```

Konfigurieren Sie dann Ihre Anwendung so, dass sie die Aufnahmerolle übernimmt. Das Anwendungskonto muss der Anwendungsrolle AssumeRoleBerechtigungen für die Aufnahmerolle im Pipeline-Konto gewähren.

Ausführliche Schritte und Beispiele für IAM-Richtlinien finden Sie unter. the section called “Bereitstellung von kontenübergreifendem Zugriff auf Datenerfassung”

Amazon OpenSearch Ingestion-Pipelines Zugriff auf Domains gewähren

Eine Amazon OpenSearch Ingestion-Pipeline benötigt die Berechtigung, in die OpenSearch Service-Domain zu schreiben, die als Senke konfiguriert ist. Um Zugriff zu gewähren, konfigurieren Sie eine AWS Identity and Access Management (IAM-) Rolle mit einer restriktiven Berechtigungsrichtlinie, die den Zugriff auf die Domain beschränkt, an die eine Pipeline Daten sendet. Beispielsweise möchten Sie eine Erfassungspipeline möglicherweise nur auf die Domäne und die Indizes beschränken, die zur Unterstützung ihres Anwendungsfalls erforderlich sind.

> **Important**
>
> Sie können wählen, ob Sie die Pipeline-Rolle manuell erstellen möchten, oder Sie können sie von OpenSearch Ingestion während der Pipelineerstellung für Sie erstellen lassen. Wenn Sie sich für die automatische Rollenerstellung entscheiden, fügt OpenSearch Ingestion der Pipeline-Rollenzugriffsrichtlinie alle erforderlichen Berechtigungen hinzu, basierend auf der von Ihnen ausgewählten Quelle und Senke. Es erstellt eine Pipeline-Rolle in IAM mit dem Präfix `OpenSearchIngestion-` und dem Suffix, die Sie eingeben. Weitere Informationen finden Sie unter the section called “Rolle „Pipeline“”.
> Wenn Sie OpenSearch Ingestion die Pipeline-Rolle für Sie erstellen lassen, müssen Sie die Rolle dennoch in die Domänenzugriffsrichtlinie aufnehmen und sie einer Backend-Rolle zuordnen (falls die Domäne eine differenzierte Zugriffskontrolle verwendet), entweder bevor oder nachdem Sie die Pipeline erstellt haben. Anweisungen finden Sie in Schritt 2.

Themen

- Schritt 1: Erstellen Sie die Pipeline-Rolle
- Schritt 2: Konfigurieren Sie den Datenzugriff für die Domain

Schritt 1: Erstellen Sie die Pipeline-Rolle

Der Pipeline-Rolle muss eine angehängte Berechtigungsrichtlinie zugeordnet sein, die es ihr ermöglicht, Daten an die Domänensenke zu senden. Außerdem muss sie über eine Vertrauensstellung verfügen, die es OpenSearch Ingestion ermöglicht, die Rolle zu übernehmen. Anweisungen zum Anhängen einer Richtlinie an eine Rolle finden Sie unter Hinzufügen von IAM-Identitätsberechtigungen im IAM-Benutzerhandbuch.

Die folgende Beispielrichtlinie zeigt die geringsten Rechte, die Sie einer Pipeline-Rolle gewähren können, damit sie in eine einzelne Domäne schreiben kann:

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
```

```
            "Action": "es:DescribeDomain",
            "Resource": "arn:aws:es:*:account-id:domain/*"
        },
        {
            "Effect": "Allow",
            "Action": "es:ESHttp*",
            "Resource": "arn:aws:es:*:account-id:domain/domain-name/*"
        }
    ]
}
```

Wenn Sie die Rolle wiederverwenden möchten, um in mehrere Domänen zu schreiben, können Sie die Richtlinie weiter fassen, indem Sie den Domänennamen durch ein Platzhalterzeichen (*) ersetzen.

Die Rolle muss über die folgende Vertrauensstellung verfügen, sodass OpenSearch Ingestion die Pipeline-Rolle übernehmen kann:

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"osis-pipelines.amazonaws.com"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

Schritt 2: Konfigurieren Sie den Datenzugriff für die Domain

Damit eine Pipeline Daten in eine Domäne schreiben kann, muss die Domäne über eine Zugriffsrichtlinie auf Domänenebene verfügen, die der Pipeline-Rolle den Zugriff darauf ermöglicht.

Die folgende Beispielrichtlinie für den Domänenzugriff ermöglicht es der genannten Pipeline-Rolle, Daten in die angegebene Domäne `pipeline-role` zu schreiben: `ingestion-domain`

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::account-id:role/pipeline-role"
      },
      "Action": ["es:DescribeDomain", "es:ESHttp*"],
      "Resource": "arn:aws:es:region:account-id:domain/domain-name/*"
    }
  ]
}
```

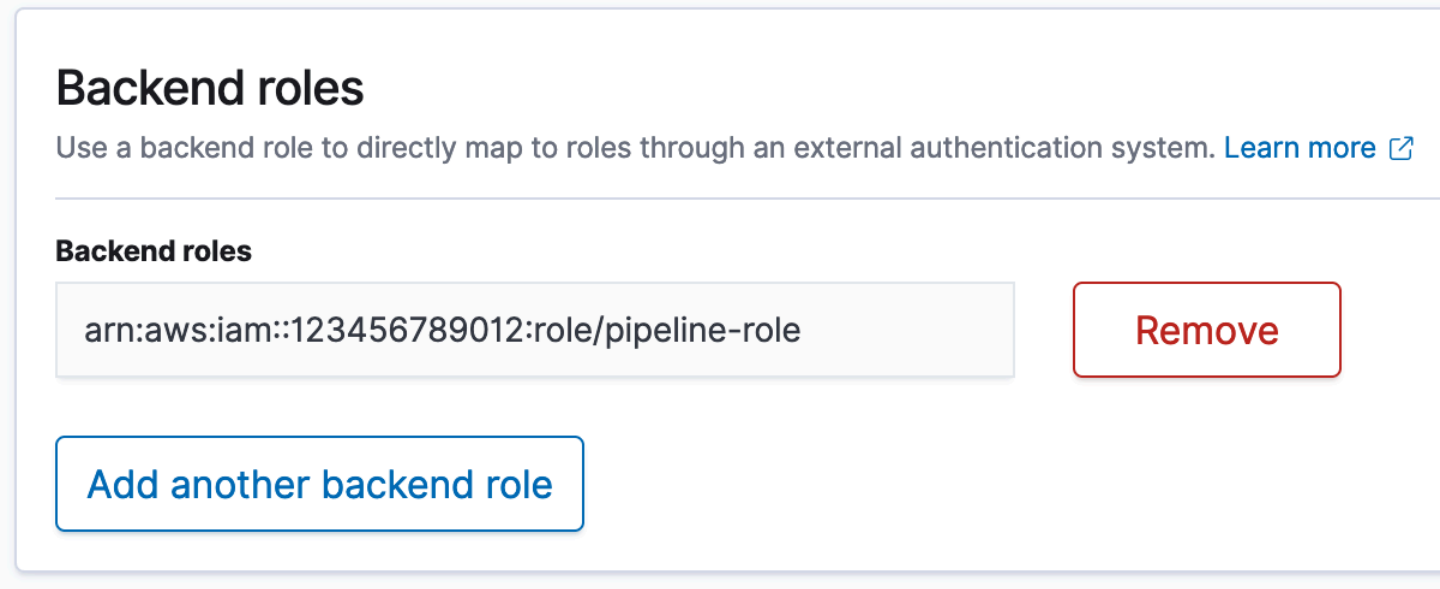
Ordnen Sie die Pipeline-Rolle zu (nur für Domänen, die eine differenzierte Zugriffskontrolle verwenden)

Wenn Ihre Domain eine differenzierte Zugriffskontrolle für die Authentifizierung verwendet, müssen Sie zusätzliche Schritte unternehmen, um Ihrer Pipeline Zugriff auf eine Domain zu gewähren. Die Schritte unterscheiden sich je nach Ihrer Domain-Konfiguration:

- Szenario 1: Verschiedene Master-Rolle und Pipeline-Rolle — Wenn Sie einen IAM-Amazon-Ressourcennamen (ARN) als Master-Benutzer verwenden und dieser sich von der Pipeline-Rolle unterscheidet, müssen Sie die Pipeline-Rolle der OpenSearch `all_access` Backend-Rolle zuordnen. Dadurch wird die Pipeline-Rolle als zusätzlicher Masterbenutzer hinzugefügt. Weitere Informationen finden Sie unter Zusätzliche Masterbenutzer.
- Szenario 2: Hauptbenutzer in der internen Benutzerdatenbank — Wenn Ihre Domain einen Masterbenutzer in der internen Benutzerdatenbank und die HTTP-Basisauthentifizierung für OpenSearch Dashboards verwendet, können Sie den Hauptbenutzernamen und das Kennwort nicht direkt an die Pipeline-Konfiguration übergeben. Ordnen Sie stattdessen die Pipeline-Rolle der OpenSearch `all_access` Backend-Rolle zu. Dadurch wird die Pipeline-Rolle als zusätzlicher Masterbenutzer hinzugefügt. Weitere Informationen finden Sie unter Zusätzliche Masterbenutzer.
- Szenario 3: Gleiche Master-Rolle und Pipeline-Rolle (ungewöhnlich) — Wenn Sie einen IAM-ARN als Master-Benutzer verwenden und es sich um denselben ARN handelt, den Sie als Pipeline-Rolle verwenden, müssen Sie keine weiteren Maßnahmen ergreifen. Die Pipeline verfügt über die erforderlichen Berechtigungen, um in die Domäne zu schreiben. Dieses Szenario ist ungewöhnlich,

da die meisten Umgebungen eine Administratorrolle oder eine andere Rolle als Masterrolle verwenden.

Die folgende Abbildung zeigt, wie die Pipeline-Rolle einer Backend-Rolle zugeordnet wird:



Amazon OpenSearch Ingestion-Pipelines Zugriff auf Sammlungen gewähren

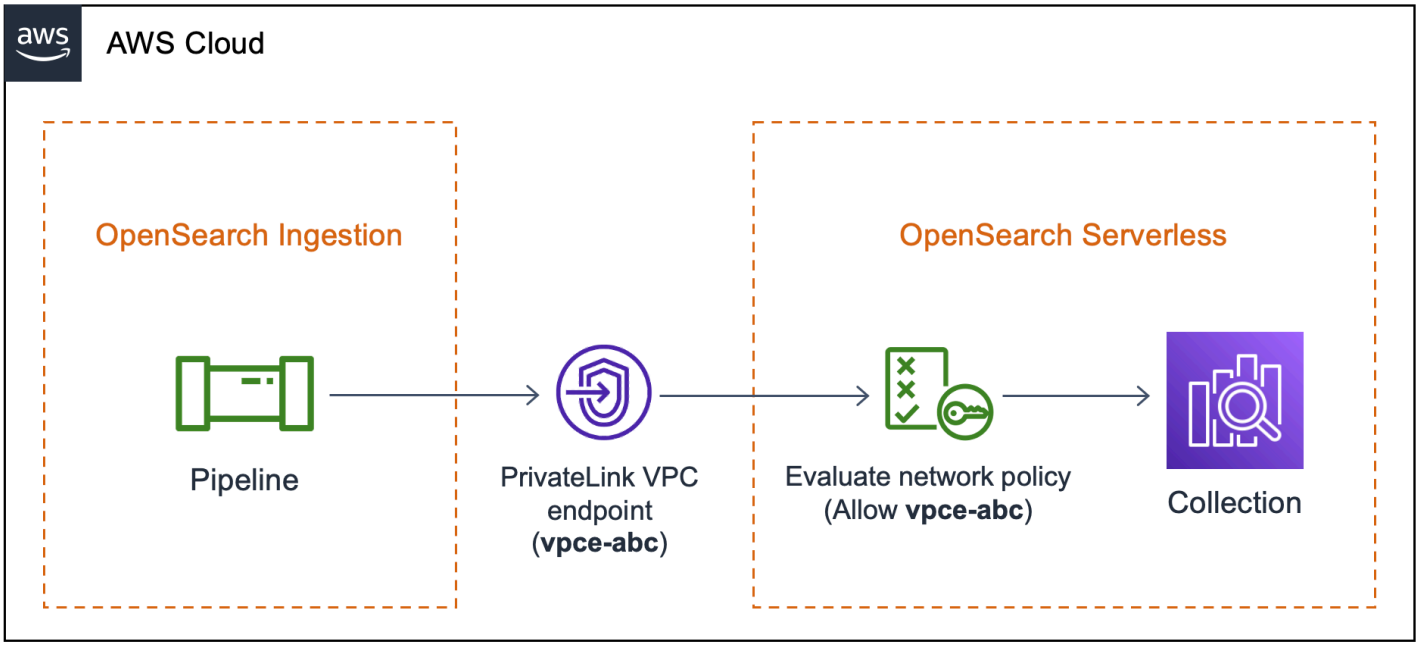
Eine Amazon OpenSearch Ingestion-Pipeline kann in eine OpenSearch serverlose öffentliche Sammlung oder VPC-Sammlung schreiben. Um Zugriff auf die Sammlung zu gewähren, konfigurieren Sie eine AWS Identity and Access Management (IAM-) Pipeline-Rolle mit einer Berechtigungsrichtlinie, die Zugriff auf die Sammlung gewährt. Die Pipeline übernimmt diese Rolle, um Anfragen an die OpenSearch serverlose Sammelsenke zu signieren.

Important

Sie können wählen, ob Sie die Pipeline-Rolle manuell erstellen möchten, oder Sie können sie von OpenSearch Ingestion während der Pipelineerstellung für Sie erstellen lassen. Wenn Sie sich für die automatische Rollenerstellung entscheiden, fügt OpenSearch Ingestion der Pipeline-Rollenzugriffsrichtlinie alle erforderlichen Berechtigungen hinzu, basierend auf der von Ihnen ausgewählten Quelle und Senke. Es erstellt eine Pipeline-Rolle in IAM mit dem Präfix `OpenSearchIngestion-` und dem Suffix, die Sie eingeben. Weitere Informationen finden Sie unter the section called “Rolle „Pipeline“”.

> Wenn Sie OpenSearch Ingestion die Pipeline-Rolle für Sie erstellen lassen, müssen Sie die Rolle dennoch in die Datenzugriffsrichtlinie der Sammlung aufnehmen, entweder vor oder nach dem Erstellen der Pipeline. Anweisungen finden Sie in Schritt 2.

Während der Pipelineerstellung stellt OpenSearch Ingestion eine AWS PrivateLink Verbindung zwischen der Pipeline und der OpenSearch Serverless-Sammlung her. Der gesamte Datenverkehr von der Pipeline durchläuft diesen VPC-Endpunkt und wird an die Sammlung weitergeleitet. Um die Sammlung zu erreichen, muss dem Endpunkt über eine Netzwerkzugriffsrichtlinie Zugriff auf die Sammlung gewährt werden.



Themen

- Schritt 1: Erstellen Sie die Pipeline-Rolle
- Schritt 2: Konfigurieren Sie den Daten- und Netzwerkzugriff für die Sammlung

Schritt 1: Erstellen Sie die Pipeline-Rolle

Der Pipeline-Rolle muss eine zugehörige Berechtigungsrichtlinie zugeordnet sein, die es ihr ermöglicht, Daten an die Sammelsenke zu senden. Außerdem muss sie über eine Vertrauensbeziehung verfügen, die es OpenSearch Ingestion ermöglicht, die Rolle zu übernehmen. Anweisungen zum Anhängen einer Richtlinie an eine Rolle finden Sie unter Hinzufügen von IAM-Identitätsberechtigungen im IAM-Benutzerhandbuch.

Die folgende Beispielrichtlinie zeigt die geringsten Rechte, die Sie in einer Pipeline-Rollenzugriffsrichtlinie für das Schreiben in Sammlungen gewähren können:

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Action": [
                "aoss:APIAccessAll",
                "aoss:BatchGetCollection",
                "aoss:CreateSecurityPolicy",
                "aoss:GetSecurityPolicy",
                "aoss:UpdateSecurityPolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

Die Rolle muss über die folgende Vertrauensstellung verfügen, damit OpenSearch Ingestion sie übernehmen kann:

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "osis-pipelines.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Schritt 2: Konfigurieren Sie den Daten- und Netzwerkzugriff für die Sammlung

Erstellen Sie eine OpenSearch serverlose Sammlung mit den folgenden Einstellungen. Anweisungen zum Erstellen einer Sammlung finden Sie unterthe section called “Erstellen von Sammlungen”.

Richtlinie für den Datenzugriff

Erstellen Sie eine Datenzugriffsrichtlinie für die Sammlung, die der Pipeline-Rolle die erforderlichen Berechtigungen gewährt. Zum Beispiel:

```
[
  {
    "Rules": [
      {
        "Resource": [
          "index/collection-name/*"
        ],
        "Permission": [
          "aoss:CreateIndex",
          "aoss:UpdateIndex",
          "aoss:DescribeIndex",
          "aoss:WriteDocument"
        ],
        "ResourceType": "index"
      }
    ],
    "Principal": [
      "arn:aws:iam::account-id:role/pipeline-role"
    ],
    "Description": "Pipeline role access"
  }
]
```

> **Note**
>
> Geben Sie im `Principal` Element den Amazon-Ressourcennamen (ARN) der Pipeline-Rolle an.

Richtlinie für den Netzwerkzugriff

Jeder Sammlung, die Sie in OpenSearch Serverless erstellen, ist mindestens eine Netzwerkzugriffsrichtlinie zugeordnet. Netzwerkzugriffsrichtlinien bestimmen, ob auf die Sammlung über das Internet von öffentlichen Netzwerken aus zugegriffen werden kann oder ob privat darauf zugegriffen werden muss. Weitere Informationen zu Netzwerkrichtlinien finden Sie unterthe section called “Netzwerkzugriff”.

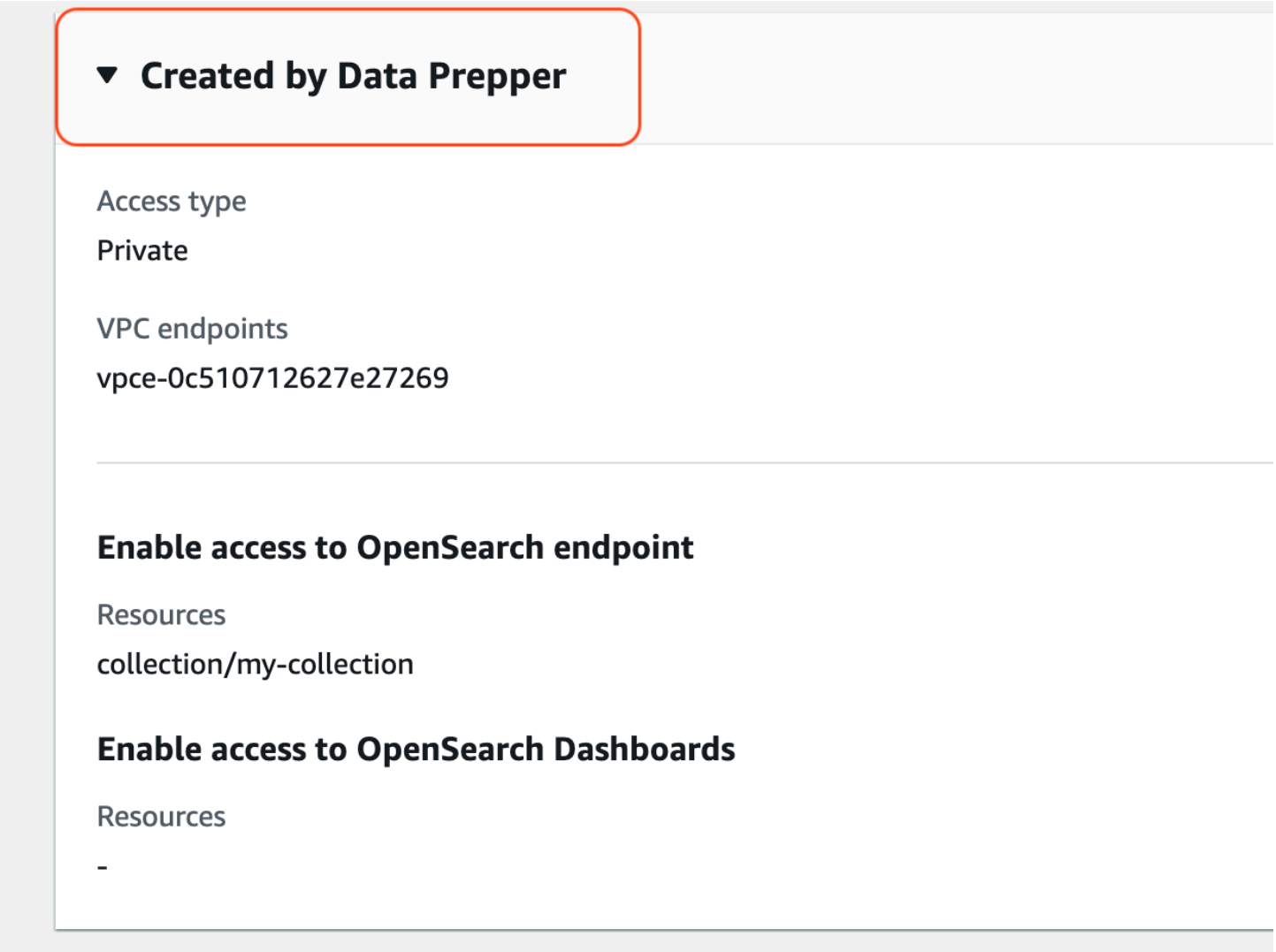
Innerhalb einer Netzwerkzugriffsrichtlinie können Sie nur OpenSearch serverlos verwaltete VPC-Endpunkte angeben. Weitere Informationen finden Sie unter the section called “VPC-Endpunkte”. Damit die Pipeline jedoch in die Sammlung schreiben kann, muss die Richtlinie auch Zugriff auf den VPC-Endpunkt gewähren, den OpenSearch Ingestion automatisch zwischen der Pipeline und der Sammlung erstellt. Wenn Sie also eine OpenSearch serverlose Sammlung als Zielsenke für eine Pipeline wählen, müssen Sie den Namen der zugehörigen Netzwerkrichtlinie in das Feld Netzwerkrichtlinienname eingeben.

Bei der Erstellung der Pipeline überprüft OpenSearch Ingestion, ob die angegebene Netzwerkrichtlinie existiert. Wenn sie nicht existiert, wird sie von OpenSearch Ingestion erstellt. Falls sie existiert, aktualisiert OpenSearch Ingestion sie, indem ihr eine neue Regel hinzugefügt wird. Die Regel gewährt Zugriff auf den VPC-Endpunkt, der die Pipeline und die Sammlung verbindet.

Zum Beispiel:

```
{
   "Rules":[
      {
         "Resource":[
            "collection/my-collection"
         ],
         "ResourceType":"collection"
      }
   ],
   "SourceVPCEs":[
      "vpce-0c510712627e27269" # The ID of the VPC endpoint that OpenSearch Ingestion
 creates between the pipeline and collection
   ],
   "Description":"Created by Data Prepper"
}
```

In der Konsole erhalten alle Regeln, die OpenSearch Ingestion Ihren Netzwerkrichtlinien hinzufügt, den Namen Created by Data Prepper:



> **Note**
>
> Im Allgemeinen hat eine Regel, die den öffentlichen Zugriff auf eine Sammlung festlegt, Vorrang vor einer Regel, die privaten Zugriff festlegt. Wenn für die Richtlinie bereits öffentlicher Zugriff konfiguriert war, ändert diese neue Regel, die OpenSearch Ingestion hinzufügt, das Verhalten der Richtlinie also nicht. Weitere Informationen finden Sie unter the section called “Vorrang der Richtlinie”.

Wenn Sie die Pipeline beenden oder löschen, löscht OpenSearch Ingestion den VPC-Endpunkt zwischen der Pipeline und der Sammlung. Es ändert auch die Netzwerkrichtlinie, um den VPC-Endpunkt aus der Liste der zulässigen Endpunkte zu entfernen. Wenn Sie die Pipeline neu starten, erstellt sie den VPC-Endpunkt neu und aktualisiert die Netzwerkrichtlinie erneut mit der Endpunkt-ID.

Erste Schritte mit Amazon OpenSearch Ingestion

Amazon OpenSearch Ingestion unterstützt die Aufnahme von Daten in verwaltete OpenSearch Service-Domains und OpenSearch serverlose Sammlungen. Die folgenden Tutorials führen Sie durch die grundlegenden Schritte, um eine Pipeline zum Laufen zu bringen.

Das erste Tutorial zeigt Ihnen, wie Sie Amazon OpenSearch Ingestion verwenden, um eine einfache Pipeline zu konfigurieren und Daten in eine Amazon OpenSearch Service-Domain aufzunehmen.

Das zweite Tutorial zeigt Ihnen, wie Sie Amazon OpenSearch Ingestion verwenden, um eine einfache Pipeline zu konfigurieren und Daten in eine Amazon OpenSearch Serverless-Sammlung aufzunehmen.

> **Note**
>
> Die Pipeline-Erstellung schlägt fehl, wenn Sie nicht die richtigen Berechtigungen einrichten. the section called “Rollen und Benutzer einrichten”Weitere Informationen zu den erforderlichen Rollen finden Sie unter, bevor Sie eine Pipeline erstellen.

Themen

- Tutorial: Daten mithilfe von Amazon OpenSearch Ingestion in eine Domain aufnehmen
- Tutorial: Daten mit Amazon OpenSearch Ingestion in eine Sammlung aufnehmen

Tutorial: Daten mithilfe von Amazon OpenSearch Ingestion in eine Domain aufnehmen

Dieses Tutorial zeigt Ihnen, wie Sie Amazon OpenSearch Ingestion verwenden, um eine einfache Pipeline zu konfigurieren und Daten in eine Amazon OpenSearch Service-Domain aufzunehmen. Eine Pipeline ist eine Ressource, die OpenSearch Ingestion bereitstellt und verwaltet. Sie können eine Pipeline verwenden, um Daten für nachgelagerte Analysen und Visualisierungen in OpenSearch Service zu filtern, anzureichern, zu transformieren, zu normalisieren und zu aggregieren.

Dieses Tutorial führt Sie durch die grundlegenden Schritte, um eine Pipeline schnell zum Laufen zu bringen. Umfassendere Anweisungen finden Sie unterthe section called “Pipelines erstellen”.

In diesem Tutorial führen Sie die folgenden Schritte durch:

1. Erstellen Sie eine Domain.
2. Erstellen Sie eine Pipeline.
3. Nehmen Sie einige Beispieldaten auf.

Im Rahmen des Tutorials erstellen Sie die folgenden Ressourcen:

- Eine Domäne mit dem Name`ingestion-domain`, in die die Pipeline schreibt
- Eine Pipeline mit dem Namen `ingestion-pipeline`

Erforderliche Berechtigungen

Um dieses Tutorial abschließen zu können, muss Ihrem Benutzer oder Ihrer Rolle eine identitätsbasierte Richtlinie mit den folgenden Mindestberechtigungen angehängt sein. Diese Berechtigungen ermöglichen es Ihnen, eine Pipeline-Rolle zu erstellen und eine Richtlinie anzuhängen (`iam:Create*`und`iam:Attach*`), eine Domäne (`es:*`) zu erstellen oder zu ändern und mit Pipelines zu arbeiten (). `osis:*`

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Resource":"*",
         "Action":[
            "osis:*",
            "iam:Create*",
            "iam:Attach*",
            "es:*"
         ]
      },
      {
         "Resource":[
            "arn:aws:iam::your-account-id:role/OpenSearchIngestion-PipelineRole"
         ],
         "Effect":"Allow",
         "Action":[
            "iam:CreateRole",
```

```
            "iam:AttachPolicy",
            "iam:PassRole"
        ]
      }
   ]
}
```

Schritt 1: Erstellen Sie die Pipeline-Rolle

Erstellen Sie zunächst eine Rolle, die die Pipeline für den Zugriff auf die OpenSearch Service-Domänensenke übernimmt. Sie werden diese Rolle später in diesem Tutorial in die Pipeline-Konfiguration aufnehmen.

Um die Pipeline-Rolle zu erstellen

1. Öffnen Sie die AWS Identity and Access Management Konsole unter https://console.aws.amazon.com/iamv2/.
2. Wählen Sie Richtlinien und dann Richtlinie erstellen aus.
3. In diesem Tutorial werden Sie Daten in eine Domain mit dem Namen aufnehmen`ingestion-domain`, die Sie im nächsten Schritt erstellen werden. Wählen Sie JSON aus und fügen Sie die folgende Richtlinie in den Editor ein. *`your-account-id`*Ersetzen Sie es durch Ihre Konto-ID und ändern Sie gegebenenfalls die Region.

   JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "es:DescribeDomain",
            "Resource": "arn:aws:es:us-east-1:your-account-id:domain/
ingestion-domain"
        },
        {
            "Effect": "Allow",
            "Action": "es:ESHttp*",
            "Resource": "arn:aws:es:us-east-1:your-account-id:domain/
ingestion-domain/*"
```

```
        }
    ]
}
```

Wenn Sie Daten in eine bestehende Domain schreiben möchten, `ingestion-domain` ersetzen Sie sie durch den Namen Ihrer Domain.

> **Note**
>
> Der Einfachheit halber verwenden wir in diesem Tutorial eine umfassende Zugriffsrichtlinie. In Produktionsumgebungen empfehlen wir jedoch, dass Sie eine restriktivere Zugriffsrichtlinie auf Ihre Pipeline-Rolle anwenden. Ein Beispiel für eine Richtlinie, die die erforderlichen Mindestberechtigungen bereitstellt, finden Sie unterthe section called “Pipelines Zugriff auf Domains gewähren”.

4. Wählen Sie Weiter, dann Weiter und geben Sie Ihrer Richtlinie einen Namen für Pipeline-Policy.
5. Wählen Sie Richtlinie erstellen aus.
6. Erstellen Sie als Nächstes eine Rolle und fügen Sie ihr die Richtlinie hinzu. Wählen Sie Roles (Rollen) und anschließend Create role (Rolle erstellen).
7. Wählen Sie Benutzerdefinierte Vertrauensrichtlinie und fügen Sie die folgende Richtlinie in den Editor ein:

   JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"osis-pipelines.amazonaws.com"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

8. Wählen Sie Weiter aus. Suchen Sie dann nach der Pipeline-Richtlinie (die Sie gerade erstellt haben) und wählen Sie sie aus.
9. Wählen Sie Weiter und geben Sie der Rolle einen Namen. PipelineRole
10. Wählen Sie Rolle erstellen aus.

Merken Sie sich den Amazon-Ressourcennamen (ARN) der Rolle (z. B.`arn:aws:iam::`*`your-account-id`*`:role/PipelineRole`). Sie benötigen ihn, wenn Sie Ihre Pipeline erstellen.

Schritt 2: Erstellen Sie eine Domain

Erstellen Sie zunächst eine Domain mit dem Name`ingestion-domain`, in die Daten aufgenommen werden sollen.

Navigieren Sie zu https://console.aws.amazon.com/aos/Hause zur Amazon OpenSearch Service-Konsole und erstellen Sie eine Domain, die die folgenden Anforderungen erfüllt:

- Läuft OpenSearch 1.0 oder höher oder Elasticsearch 7.4 oder höher
- Verwendet öffentlichen Zugriff
- Verwendet keine differenzierte Zugriffskontrolle

> **Note**
>
> Diese Anforderungen sollen die Einfachheit dieses Tutorials gewährleisten. In Produktionsumgebungen können Sie eine Domain mit VPC-Zugriff and/or mithilfe einer fein abgestuften Zugriffskontrolle konfigurieren. Informationen zur Verwendung einer detaillierten Zugriffskontrolle finden Sie unter Zuordnen der Pipeline-Rolle.

Die Domäne muss über eine Zugriffsrichtlinie verfügen, die Berechtigungen für die `OpenSearchIngestion-PipelineRole` IAM-Rolle gewährt. Diese wird vom OpenSearch Dienst im nächsten Schritt für Sie erstellt. Die Pipeline übernimmt diese Rolle, um Daten an die Domänensenke zu senden.

Stellen Sie sicher, dass die Domäne über die folgende Zugriffsrichtlinie auf Domänenebene verfügt, die der Pipeline-Rolle Zugriff auf die Domäne gewährt. Ersetzen Sie die Region und die Konto-ID durch Ihre eigene:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::your-account-id:role/OpenSearchIngestion-
PipelineRole"
      },
      "Action": "es:*",
      "Resource": "arn:aws:es:us-east-1:your-account-id:domain/ingestion-domain/
*"
    }
  ]
}
```

Weitere Informationen zum Erstellen von Zugriffsrichtlinien auf Domänenebene finden Sie unter. the section called “Ressourcenbasierte Richtlinien”

Wenn Sie bereits eine Domäne erstellt haben, ändern Sie deren bestehende Zugriffsrichtlinie, um die oben genannten Berechtigungen für bereitzustellen. `OpenSearchIngestion-PipelineRole`

Schritt 3: Erstellen Sie eine Pipeline

Jetzt, da Sie eine Domain haben, können Sie eine Pipeline erstellen.

So erstellen Sie eine Pipeline

1. Wählen Sie in der Amazon OpenSearch Service-Konsole im linken Navigationsbereich Pipelines aus.
2. Wählen Sie Create pipeline (Pipeline erstellen) aus.
3. Wählen Sie die Leere Pipeline und dann Blueprint auswählen aus.
4. In diesem Tutorial erstellen wir eine einfache Pipeline, die das HTTP-Quell-Plugin verwendet. Das Plugin akzeptiert Protokolldaten in einem JSON-Array-Format. Wir geben eine einzelne OpenSearch Service-Domain als Senke an und nehmen alle Daten in den `application_logs` Index auf.

Wählen Sie im Menü Quelle die Option HTTP aus. Geben Sie für den Pfad /logs ein.

5. Der Einfachheit halber konfigurieren wir in diesem Tutorial den öffentlichen Zugriff für die Pipeline. Wählen Sie für Quellnetzwerkoptionen die Option Öffentlicher Zugriff aus. Informationen zur Konfiguration des VPC-Zugriffs finden Sie unterthe section called “Konfigurieren des VPC-Zugriffs für Pipelines”.
6. Wählen Sie Weiter aus.
7. Geben Sie als Prozessor Datum ein und wählen Sie Hinzufügen aus.
8. Aktivieren Sie „Ab dem Zeitpunkt des Eingangs“. Behalten Sie für alle anderen Einstellungen die Standardwerte bei.
9. Wählen Sie Weiter aus.
10. Konfigurieren Sie die Senkendetails. Wählen Sie als OpenSearch Ressourcentyp Managed Cluster aus. Wählen Sie dann die OpenSearch Dienstdomäne aus, die Sie im vorherigen Abschnitt erstellt haben.

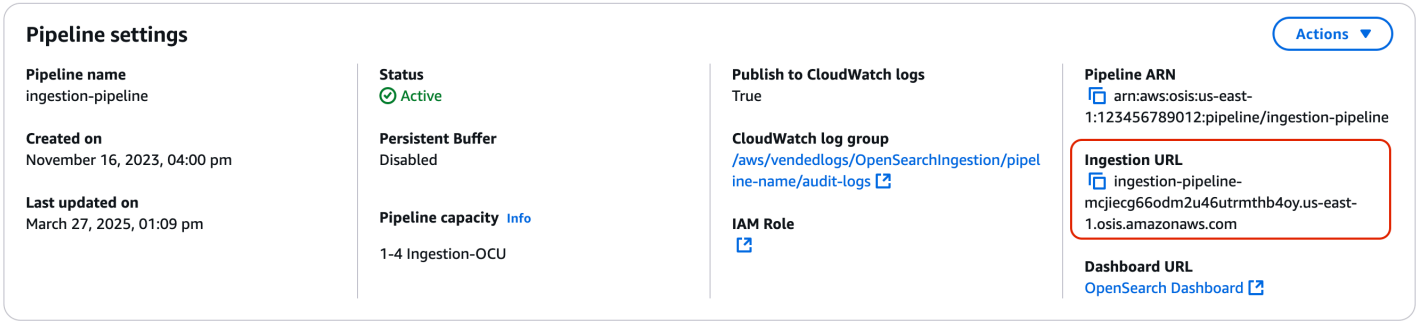
    Geben Sie als Indexname application_logs ein. OpenSearch Ingestion erstellt diesen Index automatisch in der Domain, falls er noch nicht existiert.
11. Wählen Sie Weiter aus.
12. Geben Sie der Pipeline den Namen Ingestion-Pipeline. Behalten Sie die Standardeinstellungen für die Kapazitätseinstellungen bei.
13. Wählen Sie für Pipeline-Rolle die Option Neue Servicerolle erstellen und verwenden aus. Die Pipeline-Rolle stellt die erforderlichen Berechtigungen für eine Pipeline bereit, um in die Domänensenke zu schreiben und aus Pull-basierten Quellen zu lesen. Wenn Sie diese Option auswählen, ermöglichen Sie OpenSearch Ingestion, die Rolle für Sie zu erstellen, anstatt sie manuell in IAM zu erstellen. Weitere Informationen finden Sie unter the section called “Rollen und Benutzer einrichten”.
14. Geben Sie als Suffix für den Namen der Servicerolle den Wert ein. PipelineRole In IAM wird die Rolle das Format haben. `arn:aws:iam::`*`your-account-id`*`:role/0penSearchIngestion-`**`PipelineRole`**
15. Wählen Sie Weiter aus. Überprüfen Sie Ihre Pipeline-Konfiguration und wählen Sie Pipeline erstellen aus. Es dauert 5—10 Minuten, bis die Pipeline aktiv wird.

Schritt 4: Nehmen Sie einige Beispieldaten auf

Wenn der Pipeline-Status lautet`Active`, können Sie damit beginnen, Daten in die Pipeline aufzunehmen. Sie müssen alle HTTP-Anfragen an die Pipeline mit Signature Version 4 signieren. Verwenden Sie ein HTTP-Tool wie Postman oder awscurl, um einige Daten an die Pipeline zu senden. Wie bei der direkten Indizierung von Daten in einer Domain erfordert die Aufnahme von Daten in eine Pipeline immer entweder eine IAM-Rolle oder einen IAM-Zugriffsschlüssel und einen geheimen Schlüssel.

> **Note**
>
> Der Principal, der die Anfrage signiert, muss über die IAM-Berechtigung verfügen. `osis:Ingest`

Rufen Sie zunächst die Aufnahme-URL von der Seite mit den Pipeline-Einstellungen ab:



Nehmen Sie dann einige Beispieldaten auf. Die folgende Anfrage verwendet awscurl, um eine einzelne Protokolldatei an die Pipeline zu senden:

```
awscurl --service osis --region us-east-1 \
    -X POST \
    -H "Content-Type: application/json" \
    -d
 '[{"time":"2014-08-11T11:40:13+00:00","remote_addr":"122.226.223.69","status":"404","request":
 http://www.k2proxy.com//hello.html HTTP/1.1","http_user_agent":"Mozilla/4.0
 (compatible; WOW64; SLCC2;)"}]' \
    https://pipeline-endpoint.us-east-1.osis.amazonaws.com/logs
```

Sie sollten eine `200 OK` Antwort sehen. Wenn Sie einen Authentifizierungsfehler erhalten, liegt das möglicherweise daran, dass Sie Daten von einem anderen Konto als dem der Pipeline aufnehmen. Siehe the section called “Behebung von Problemen mit Berechtigungen”.

Fragen Sie nun den `application_logs` Index ab, um sicherzustellen, dass Ihr Protokolleintrag erfolgreich aufgenommen wurde:

```
awscurl --service es --region us-east-1 \
     -X GET \
     https://search-ingestion-domain.us-east-1.es.amazonaws.com/application_logs/
_search | json_pp
```

Beispielantwort:

```
{
   "took":984,
   "timed_out":false,
   "_shards":{
      "total":1,
      "successful":5,
      "skipped":0,
      "failed":0
   },
   "hits":{
      "total":{
         "value":1,
         "relation":"eq"
      },
      "max_score":1.0,
      "hits":[
         {
            "_index":"application_logs",
            "_type":"_doc",
            "_id":"z6VY_IMBRpceX-DU6V4O",
            "_score":1.0,
            "_source":{
               "time":"2014-08-11T11:40:13+00:00",
               "remote_addr":"122.226.223.69",
               "status":"404",
               "request":"GET http://www.k2proxy.com//hello.html HTTP/1.1",
               "http_user_agent":"Mozilla/4.0 (compatible; WOW64; SLCC2;)",
               "@timestamp":"2022-10-21T21:00:25.502Z"
            }
```

```
            }
        ]
    }
}
```

Behebung von Problemen mit Berechtigungen

Wenn Sie die Schritte im Tutorial befolgt haben und immer noch Authentifizierungsfehler auftreten, wenn Sie versuchen, Daten aufzunehmen, liegt das möglicherweise daran, dass sich die Rolle, die in eine Pipeline schreibt, in einer anderen Rolle befindet AWS-Konto als die Pipeline selbst. In diesem Fall müssen Sie eine Rolle erstellen und übernehmen, die Ihnen speziell das Ingestieren von Daten ermöglicht. Detaillierte Anweisungen finden Sie unter the section called “Bereitstellung von kontenübergreifendem Zugriff auf Datenerfassung”.

Zugehörige Ressourcen

In diesem Tutorial wurde ein einfacher Anwendungsfall für die Aufnahme eines einzelnen Dokuments über HTTP vorgestellt. In Produktionsszenarien konfigurieren Sie Ihre Client-Anwendungen (wie Fluent Bit, Kubernetes oder OpenTelemetry Collector) so, dass Daten an eine oder mehrere Pipelines gesendet werden. Ihre Pipelines werden wahrscheinlich komplexer sein als das einfache Beispiel in diesem Tutorial.

Informationen zu den ersten Schritten zur Konfiguration Ihrer Clients und zur Datenaufnahme finden Sie in den folgenden Ressourcen:

- Pipelines erstellen und verwalten
- Konfiguration Ihrer Clients für das Senden von Daten an Ingestion OpenSearch
- Data Prepper-Dokumentation

Tutorial: Daten mit Amazon OpenSearch Ingestion in eine Sammlung aufnehmen

Dieses Tutorial zeigt Ihnen, wie Sie Amazon OpenSearch Ingestion verwenden, um eine einfache Pipeline zu konfigurieren und Daten in eine Amazon OpenSearch Serverless-Sammlung aufzunehmen. Eine Pipeline ist eine Ressource, die OpenSearch Ingestion bereitstellt und verwaltet. Sie können eine Pipeline verwenden, um Daten für nachgelagerte Analysen und Visualisierungen in OpenSearch Service zu filtern, anzureichern, zu transformieren, zu normalisieren und zu aggregieren.

Ein Tutorial, das zeigt, wie Daten in eine bereitgestellte OpenSearch Dienstdomäne aufgenommen werden, finden Sie unter. the section called “Tutorial: Daten in eine Domain aufnehmen”

In diesem Tutorial werden Sie die folgenden Schritte ausführen:.

1. Erstellen Sie eine Sammlung.
2. Erstellen Sie eine Pipeline.
3. Nehmen Sie einige Beispieldaten auf.

Im Rahmen des Tutorials erstellen Sie die folgenden Ressourcen:

- Eine Sammlung mit dem Name`ingestion-collection`, in die die Pipeline schreiben wird
- Eine Pipeline mit dem Namen `ingestion-pipeline-serverless`

Erforderliche Berechtigungen

Um dieses Tutorial abschließen zu können, muss Ihrem Benutzer oder Ihrer Rolle eine identitätsbasierte Richtlinie mit den folgenden Mindestberechtigungen angehängt sein.
Mit diesen Berechtigungen können Sie eine Pipeline-Rolle erstellen und eine Richtlinie (`iam:Create*`und`iam:Attach*`) anhängen, eine Sammlung erstellen oder ändern (`aoss:*`) und mit Pipelines arbeiten (). `osis:*`

Darüber hinaus sind mehrere IAM-Berechtigungen erforderlich, um die Pipeline-Rolle automatisch zu erstellen und an OpenSearch Ingestion zu übergeben, damit sie Daten in die Sammlung schreiben kann.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Resource":"*",
         "Action":[
            "osis:*",
            "iam:Create*",
            "iam:Attach*",
```

```
            "aoss:*"
         ]
      },
      {
         "Resource":[
            "arn:aws:iam::your-account-id:role/OpenSearchIngestion-PipelineRole"
         ],
         "Effect":"Allow",
         "Action":[
            "iam:CreateRole",
            "iam:AttachPolicy",
            "iam:PassRole"
         ]
      }
   ]
}
```

Schritt 1: Erstellen Sie eine Sammlung

Erstellen Sie zunächst eine Sammlung, in die Daten aufgenommen werden sollen. Wir geben der Sammlung `ingestion-collection` einen Namen.

1. Navigieren Sie zu https://console.aws.amazon.com/aos/Hause zur Amazon OpenSearch Service-Konsole.
2. Wählen Sie in der linken Navigationsleiste Sammlungen und dann Sammlung erstellen aus.
3. Nennen Sie die Sammlung ingestion-collection.
4. Wählen Sie unter Sicherheit die Option Standard create aus.
5. Ändern Sie unter Netzwerkzugriffseinstellungen den Zugriffstyp auf Öffentlich.
6. Behalten Sie alle anderen Einstellungen als Standardwerte bei und wählen Sie Next (Weiter) aus.
7. Konfigurieren Sie jetzt eine Datenzugriffsrichtlinie für die Sammlung. Deaktivieren Sie die Option Zugriffsrichtlinien-Einstellungen automatisch anpassen.
8. Wählen Sie unter Definitionsmethode die Option JSON aus und fügen Sie die folgende Richtlinie in den Editor ein. Diese Richtlinie bewirkt zwei Dinge:

   - Ermöglicht der Pipeline-Rolle, in die Sammlung zu schreiben.

- Ermöglicht es Ihnen, aus der Sammlung zu lesen. Später, nachdem Sie einige Beispieldaten in die Pipeline aufgenommen haben, fragen Sie die Sammlung ab, um sicherzustellen, dass die Daten erfolgreich aufgenommen und in den Index geschrieben wurden.

```
[
  {
    "Rules": [
      {
        "Resource": [
          "index/ingestion-collection/*"
        ],
        "Permission": [
          "aoss:CreateIndex",
          "aoss:UpdateIndex",
          "aoss:DescribeIndex",
          "aoss:ReadDocument",
          "aoss:WriteDocument"
        ],
        "ResourceType": "index"
      }
    ],
    "Principal": [
      "arn:aws:iam::your-account-id:role/OpenSearchIngestion-PipelineRole",
      "arn:aws:iam::your-account-id:role/Admin"
    ],
    "Description": "Rule 1"
  }
]
```

9. Ändern Sie die `Principal` Elemente so, dass sie Ihre AWS-Konto ID enthalten. Geben Sie für den zweiten Prinzipal einen Benutzer oder eine Rolle an, mit der Sie die Sammlung später abfragen können.
10. Wählen Sie Weiter aus. Geben Sie der Zugriffsrichtlinie einen Namen pipeline-collection-accessund klicken Sie erneut auf Weiter.
11. Überprüfen Sie Ihre Sammlungskonfiguration und wählen Sie Submit (Senden) aus.

Schritt 2: Erstellen Sie eine Pipeline

Jetzt, wo Sie eine Sammlung haben, können Sie eine Pipeline erstellen.

So erstellen Sie eine Pipeline

1. Wählen Sie in der Amazon OpenSearch Service-Konsole im linken Navigationsbereich Pipelines aus.
2. Wählen Sie Create pipeline (Pipeline erstellen) aus.
3. Wählen Sie die Leere Pipeline und dann Blueprint auswählen aus.
4. In diesem Tutorial erstellen wir eine einfache Pipeline, die das HTTP-Quell-Plugin verwendet. Das Plugin akzeptiert Protokolldaten in einem JSON-Array-Format. Wir geben eine einzelne OpenSearch serverlose Sammlung als Datenspeicher an und nehmen alle Daten in den `my_logs` Index auf.

   Wählen Sie im Menü Quelle die Option HTTP. Geben Sie für den Pfad /logs ein.
5. Der Einfachheit halber konfigurieren wir in diesem Tutorial den öffentlichen Zugriff für die Pipeline. Wählen Sie für Quellnetzwerkoptionen die Option Öffentlicher Zugriff aus. Informationen zur Konfiguration des VPC-Zugriffs finden Sie unterthe section called “Konfigurieren des VPC-Zugriffs für Pipelines”.
6. Wählen Sie Weiter aus.
7. Geben Sie als Prozessor Datum ein und wählen Sie Hinzufügen aus.
8. Aktivieren Sie „Ab dem Zeitpunkt des Eingangs“. Behalten Sie für alle anderen Einstellungen die Standardwerte bei.
9. Wählen Sie Weiter aus.
10. Konfigurieren Sie die Senkendetails. Wählen Sie als OpenSearch Ressourcentyp Collection (Serverless) aus. Wählen Sie dann die OpenSearch Servicesammlung aus, die Sie im vorherigen Abschnitt erstellt haben.

    Behalten Sie den Namen der Netzwerkrichtlinie als Standard bei. Geben Sie als Indexname my_logs ein. OpenSearch Ingestion erstellt diesen Index automatisch in der Sammlung, falls er noch nicht vorhanden ist.
11. Wählen Sie Weiter aus.
12. Benennen Sie die Pipeline. ingestion-pipeline-serverless Behalten Sie die Standardeinstellungen für die Kapazitätseinstellungen bei.
13. Wählen Sie für Pipeline-Rolle die Option Neue Servicerolle erstellen und verwenden aus. Die Pipeline-Rolle stellt die erforderlichen Berechtigungen für eine Pipeline bereit, um in die Sammelsenke zu schreiben und aus Pull-basierten Quellen zu lesen. Wenn Sie diese Option auswählen, ermöglichen Sie OpenSearch Ingestion, die Rolle für Sie zu erstellen, anstatt sie

manuell in IAM zu erstellen. Weitere Informationen finden Sie unter the section called “Rollen und Benutzer einrichten”.

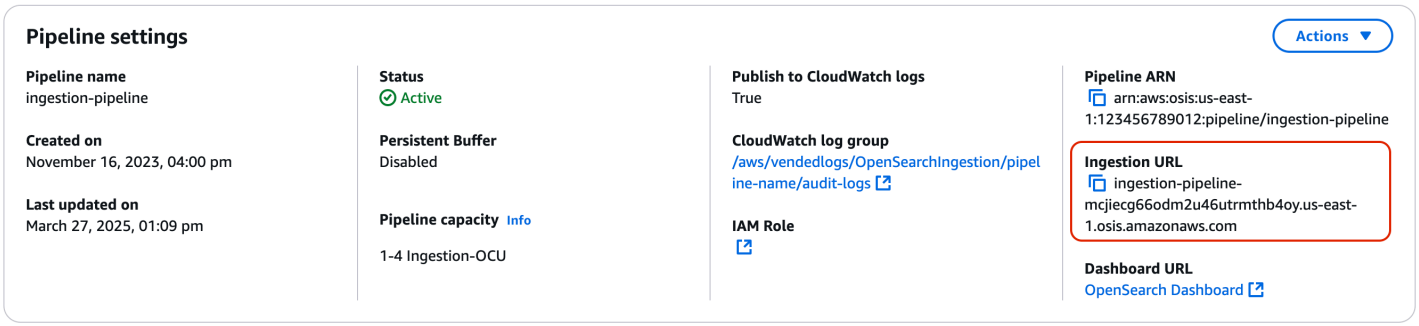
14. Geben Sie als Suffix für den Namen der Servicerolle den Wert ein. PipelineRole In IAM wird die Rolle das Format haben. `arn:aws:iam::your-account-id:role/OpenSearchIngestion-PipelineRole`
15. Wählen Sie Weiter aus. Überprüfen Sie Ihre Pipeline-Konfiguration und wählen Sie Pipeline erstellen aus. Es dauert 5—10 Minuten, bis die Pipeline aktiv wird.

Schritt 3: Nehmen Sie einige Beispieldaten auf

Wenn der Pipeline-Status lautet`Active`, können Sie damit beginnen, Daten in die Pipeline aufzunehmen. Sie müssen alle HTTP-Anfragen an die Pipeline mit Signature Version 4 signieren. Verwenden Sie ein HTTP-Tool wie Postman oder awscurl, um einige Daten an die Pipeline zu senden. Wie bei der direkten Indizierung von Daten für eine Sammlung ist auch für die Aufnahme von Daten in eine Pipeline immer entweder eine IAM-Rolle oder ein IAM-Zugriffsschlüssel und ein geheimer Schlüssel erforderlich.

> **Note**
>
> Der Principal, der die Anfrage signiert, muss über die IAM-Berechtigung verfügen. `osis:Ingest`

Rufen Sie zunächst die Aufnahme-URL von der Seite mit den Pipeline-Einstellungen ab:



Senden Sie dann einige Beispieldaten an den Aufnahmepfad. Die folgende Beispielanforderung verwendet awscurl, um eine einzelne Protokolldatei an die Pipeline zu senden:

```
awscurl --service osis --region us-east-1 \
    -X POST \
```

```
    -H "Content-Type: application/json" \
    -d
'[{"time":"2014-08-11T11:40:13+00:00","remote_addr":"122.226.223.69","status":"404","request":
http://www.k2proxy.com//hello.html HTTP/1.1","http_user_agent":"Mozilla/4.0
(compatible; WOW64; SLCC2;)"}]' \
   https://pipeline-endpoint.us-east-1.osis.amazonaws.com/logs
```

Sie sollten eine `200 OK` Antwort sehen.

Fragen Sie nun den `my_logs` Index ab, um sicherzustellen, dass der Protokolleintrag erfolgreich aufgenommen wurde:

```
awscurl --service aoss --region us-east-1 \
     -X GET \
     https://collection-id.us-east-1.aoss.amazonaws.com/my_logs/_search | json_pp
```

Beispielantwort:

```
{
   "took":348,
   "timed_out":false,
   "_shards":{
      "total":0,
      "successful":0,
      "skipped":0,
      "failed":0
   },
   "hits":{
      "total":{
         "value":1,
         "relation":"eq"
      },
      "max_score":1.0,
      "hits":[
         {
            "_index":"my_logs",
            "_id":"1%3A0%3ARJgDvIcBTy5m12xrKE-y",
            "_score":1.0,
            "_source":{
               "time":"2014-08-11T11:40:13+00:00",
               "remote_addr":"122.226.223.69",
               "status":"404",
               "request":"GET http://www.k2proxy.com//hello.html HTTP/1.1",
```

```
                "http_user_agent":"Mozilla/4.0 (compatible; WOW64; SLCC2;)",
                "@timestamp":"2023-04-26T05:22:16.204Z"
            }
        }
    ]
  }
}
```

Zugehörige Ressourcen

In diesem Tutorial wurde ein einfacher Anwendungsfall für die Aufnahme eines einzelnen Dokuments über HTTP vorgestellt. In Produktionsszenarien konfigurieren Sie Ihre Client-Anwendungen (wie Fluent Bit, Kubernetes oder OpenTelemetry Collector) so, dass Daten an eine oder mehrere Pipelines gesendet werden. Ihre Pipelines werden wahrscheinlich komplexer sein als das einfache Beispiel in diesem Tutorial.

Informationen zu den ersten Schritten zur Konfiguration Ihrer Clients und zur Datenaufnahme finden Sie in den folgenden Ressourcen:

- Pipelines erstellen und verwalten
- Konfiguration Ihrer Clients für das Senden von Daten an Ingestion OpenSearch
- Data Prepper-Dokumentation

Überblick über die Pipeline-Funktionen in Amazon OpenSearch Ingestion

Amazon OpenSearch Ingestion stellt Pipelines bereit, die aus einer Quelle, einem Puffer, null oder mehr Prozessoren und einer oder mehreren Senken bestehen. Ingestion-Pipelines werden von Data Prepper als Daten-Engine unterstützt. Einen Überblick über die verschiedenen Komponenten einer Pipeline finden Sie unter. the section called “Die wichtigsten Konzepte”

Die folgenden Abschnitte bieten einen Überblick über einige der am häufigsten verwendeten Funktionen in Amazon OpenSearch Ingestion.

> **Note**
>
> Dies ist keine vollständige Liste der Funktionen, die für Pipelines verfügbar sind. Eine umfassende Dokumentation aller verfügbaren Pipeline-Funktionen finden Sie in der Data

Prepper-Dokumentation. Beachten Sie, dass OpenSearch Ingestion einige Einschränkungen hinsichtlich der Plugins und Optionen auferlegt, die Sie verwenden können. Weitere Informationen finden Sie unter the section called “Unterstützte Plugins und Optionen”.

Themen

- Dauerhafte Pufferung
- Aufteilen
- Verkettung
- Warteschlangen für unzustellbare Nachrichten
- Indexverwaltung
- End-to-end Bestätigung
- Gegendruck an der Quelle

Dauerhafte Pufferung

Ein persistenter Puffer speichert Ihre Daten in einem festplattenbasierten Puffer in mehreren Availability Zones, um die Datenbeständigkeit zu erhöhen. Mithilfe der persistenten Pufferung können Sie Daten aus allen unterstützten Push-basierten Quellen aufnehmen, ohne einen eigenständigen Puffer einrichten zu müssen. Zu diesen Quellen gehören HTTP sowie Logs, Traces und OpenTelemetry Metriken. Um die persistente Pufferung zu aktivieren, wählen Sie Persistenten Puffer aktivieren, wenn Sie eine Pipeline erstellen oder aktualisieren. Weitere Informationen finden Sie unter the section called “Pipelines erstellen”.

OpenSearch Die Aufnahme bestimmt dynamisch die Anzahl der für die persistente Pufferung OCUs zu verwendenden Daten, wobei die Datenquelle, die Streaming-Transformationen und das Senkenziel berücksichtigt werden. Da ein Teil der Pufferung zugewiesen wird, müssen Sie möglicherweise OCUs die Mindest- und Höchstwerte erhöhen, um den gleichen Aufnahmedurchsatz aufrechtzuerhalten. OCUs Pipelines speichern Daten bis zu 72 Stunden im Puffer.

Wenn Sie die persistente Pufferung für eine Pipeline aktivieren, lauten die standardmäßigen maximalen Anforderungs-Payloadgrößen wie folgt:

- HTTP-Quellen — 10 MB
- OpenTelemetry Quellen — 4 MB

Für HTTP-Quellen können Sie die maximale Payload-Größe auf 20 MB erhöhen. Die Größe der Anforderungsnutzlast umfasst die gesamte HTTP-Anfrage, die in der Regel mehrere Ereignisse enthält. Jedes Ereignis darf 3,5 MB nicht überschreiten.

Pipelines mit persistenter Pufferung teilen die konfigurierten Pipelineeinheiten zwischen Rechen- und Puffereinheiten auf. Wenn eine Pipeline einen CPU-intensiven Prozessor wie Grok, Key-Value oder Split String verwendet, ordnet sie die Einheiten im Verhältnis 1:1 zu. buffer-to-compute Andernfalls werden sie im Verhältnis 3:1 zugewiesen, wobei Recheneinheiten immer bevorzugt werden.

Zum Beispiel:

- Pipeline mit Grok und 2 Max-Einheiten — 1 Recheneinheit und 1 Puffereinheit
- Pipeline mit Grok und 5 Max-Einheiten — 3 Recheneinheiten und 2 Puffereinheiten
- Pipeline ohne Prozessoren und maximal 2 Einheiten — 1 Recheneinheit und 1 Puffereinheit
- Pipeline ohne Prozessoren und maximal 4 Einheiten — 1 Recheneinheit und 3 Puffereinheiten
- Pipeline mit Grok- und 5 Max-Einheiten — 2 Recheneinheiten und 3 Puffereinheiten

Standardmäßig verwenden Pipelines an, um Pufferdaten AWS-eigener Schlüssel zu verschlüsseln. Diese Pipelines benötigen keine zusätzlichen Berechtigungen für die Pipeline-Rolle.

Alternativ können Sie einen vom Kunden verwalteten Schlüssel angeben und der Pipeline-Rolle die folgenden IAM-Berechtigungen hinzufügen:

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "KeyAccess",
            "Effect": "Allow",
            "Action": [
              "kms:Decrypt",
              "kms:GenerateDataKeyWithoutPlaintext"
            ],
            "Resource": "arn:aws:kms:{region}:{aws-account-
id}:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
```

```
    ]
}
```

Weitere Informationen finden Sie unter Kundenverwaltete Schlüssel im AWS Key Management Service Entwicklerhandbuch.

> **Note**
>
> Wenn Sie die persistente Pufferung deaktivieren, wird Ihre Pipeline vollständig mit speicherinterner Pufferung ausgeführt.

Aufteilen

Sie können eine OpenSearch Ingestion-Pipeline so konfigurieren, dass eingehende Ereignisse in eine Unterpipeline aufgeteilt werden, sodass Sie verschiedene Arten der Verarbeitung desselben eingehenden Ereignisses durchführen können.

Die folgende Beispielpipeline teilt eingehende Ereignisse in zwei Unter-Pipelines auf. Jede Unterpipeline verwendet ihren eigenen Prozessor, um die Daten anzureichern und zu bearbeiten, und sendet die Daten dann an verschiedene Indizes. OpenSearch

```
version: "2"
log-pipeline:
  source:
    http:
    ...
  sink:
    - pipeline:
        name: "logs_enriched_one_pipeline"
    - pipeline:
        name: "logs_enriched_two_pipeline"

logs_enriched_one_pipeline:
  source:
    log-pipeline
  processor:
   ...
  sink:
    - opensearch:
```

```
        # Provide a domain or collection endpoint
        # Enable the 'serverless' flag if the sink is an OpenSearch Serverless
 collection
        aws:
          ...
        index: "enriched_one_logs"

logs_enriched_two_pipeline:
  source:
    log-pipeline
  processor:
   ...
  sink:
    - opensearch:
        # Provide a domain or collection endpoint
        # Enable the 'serverless' flag if the sink is an OpenSearch Serverless
 collection
        aws:
          ...
          index: "enriched_two_logs"
```

Verkettung

Sie können mehrere Sub-Pipelines miteinander verketten, um die Datenverarbeitung und -anreicherung in Abschnitten durchzuführen. Mit anderen Worten, Sie können ein eingehendes Ereignis mit bestimmten Verarbeitungsfunktionen in einer Subpipeline anreichern, es dann zur weiteren Anreicherung mit einem anderen Prozessor an eine andere Subpipeline senden und es schließlich an dessen Senke senden. OpenSearch

Im folgenden Beispiel reichert die `log_pipeline` Subpipeline ein eingehendes Protokollereignis mit einer Reihe von Prozessoren an und sendet das Ereignis dann an einen Index mit dem Namen. OpenSearch `enriched_logs` Die Pipeline sendet dasselbe Ereignis an die `log_advanced_pipeline` Subpipeline, die es verarbeitet und an einen anderen OpenSearch Index mit dem Namen sendet. `enriched_advanced_logs`

```
version: "2"
log-pipeline:
  source:
    http:
    ...
  processor:
```

```
    ...
  sink:
    - opensearch:
        # Provide a domain or collection endpoint
        # Enable the 'serverless' flag if the sink is an OpenSearch Serverless
 collection
        aws:
          ...
          index: "enriched_logs"
    - pipeline:
        name: "log_advanced_pipeline"

log_advanced_pipeline:
  source:
    log-pipeline
  processor:
   ...
  sink:
    - opensearch:
        # Provide a domain or collection endpoint
        # Enable the 'serverless' flag if the sink is an OpenSearch Serverless
 collection
        aws:
          ...
          index: "enriched_advanced_logs"
```

Warteschlangen für unzustellbare Nachrichten

Warteschlangen mit unerlaubten Buchstaben (DLQs) sind Ziele für Ereignisse, bei denen eine Pipeline nicht in eine Senke schreiben kann. In OpenSearch Ingestion müssen Sie einen Amazon S3 S3-Bucket mit entsprechenden Schreibberechtigungen angeben, der als DLQ verwendet werden soll. Sie können jeder Senke innerhalb einer Pipeline eine DLQ-Konfiguration hinzufügen. Wenn eine Pipeline auf Schreibfehler stößt, erstellt sie DLQ-Objekte im konfigurierten S3-Bucket. DLQ-Objekte existieren in einer JSON-Datei als Array von fehlgeschlagenen Ereignissen.

Eine Pipeline schreibt Ereignisse in den DLQ, wenn eine der folgenden Bedingungen erfüllt ist:

- Die maximale Anzahl von Wiederholungsversuchen für die OpenSearch Senke ist erschöpft. OpenSearch Für diese Einstellung sind mindestens 16 für die Aufnahme erforderlich.
- Die Senke lehnt Ereignisse aufgrund eines Fehlers ab.

Konfiguration

Um eine Warteschlange mit unerlaubten Briefen für eine Subpipeline zu konfigurieren, wählen Sie bei der Konfiguration Ihres Senkenziels die Option S3-DLQ aktivieren aus. Geben Sie dann die erforderlichen Einstellungen für die Warteschlange an. Weitere Informationen finden Sie unter Konfiguration in der Data Prepper DLQ-Dokumentation.

Dateien, die in diesen S3-DLQ geschrieben wurden, haben das folgende Benennungsmuster:

```
dlq-v${version}-${pipelineName}-${pluginId}-${timestampIso8601}-${uniqueId}
```

Anweisungen zur manuellen Konfiguration der Pipeline-Rolle, um den Zugriff auf den S3-Bucket zu ermöglichen, in den der DLQ schreibt, finden Sie unter. the section called “Berechtigungen zum Schreiben in Amazon S3 oder in eine Warteschlange mit unzustellbaren Briefen”

Beispiel

Betrachten Sie die folgende Beispiel-DLQ-Datei:

```
dlq-v2-apache-log-pipeline-opensearch-2023-04-05T15:26:19.152938Z-e7eb675a-
f558-4048-8566-dac15a4f8343
```

Hier ist ein Beispiel für Daten, die nicht in die Senke geschrieben werden konnten und die zur weiteren Analyse an den DLQ S3-Bucket gesendet werden:

```
Record_0
pluginId            "opensearch"
pluginName          "opensearch"
pipelineName        "apache-log-pipeline"
failedData
index    "logs"
indexId   null
status    0
message  "Number of retries reached the limit of max retries (configured value 15)"
document
log      "sample log"
timestamp     "2023-04-14T10:36:01.070Z"

Record_1
pluginId            "opensearch"
```

```
pluginName          "opensearch"
pipelineName        "apache-log-pipeline"
failedData
index               "logs"
indexId   null
status    0
message  "Number of retries reached the limit of max retries (configured value 15)"
document
log                 "another sample log"
timestamp           "2023-04-14T10:36:01.071Z"
```

Indexverwaltung

Amazon OpenSearch Ingestion bietet viele Funktionen zur Indexverwaltung, darunter die folgenden.

Erstellen von Indizes

Sie können einen Indexnamen in einer Pipeline-Senke angeben, und OpenSearch Ingestion erstellt den Index, wenn die Pipeline bereitgestellt wird. Wenn bereits ein Index vorhanden ist, verwendet die Pipeline ihn, um eingehende Ereignisse zu indizieren. Wenn Sie eine Pipeline beenden und neu starten oder wenn Sie ihre YAML-Konfiguration aktualisieren, versucht die Pipeline, neue Indizes zu erstellen, sofern diese noch nicht vorhanden sind. Eine Pipeline kann niemals einen Index löschen.

Die folgenden Beispielsenken erstellen zwei Indizes, wenn die Pipeline bereitgestellt wird:

```
sink:
  - opensearch:
      index: apache_logs
  - opensearch:
      index: nginx_logs
```

Generieren von Indexnamen und -mustern

Sie können dynamische Indexnamen generieren, indem Sie Variablen aus den Feldern eingehender Ereignisse verwenden. Verwenden Sie in der Senkenkonfiguration das Format, `string${}` um die Interpolation von Zeichenketten zu signalisieren, und verwenden Sie einen JSON-Zeiger, um Felder aus Ereignissen zu extrahieren. Die Optionen für `index_type` sind `custom` oder. `management_disabled` Da die `index_type` Standardeinstellung `custom` für OpenSearch Domänen und `management_disabled` für OpenSearch serverlose Sammlungen ist, kann sie nicht konfiguriert werden.

Die folgende Pipeline wählt beispielsweise das `metadataType` Feld aus eingehenden Ereignissen aus, um Indexnamen zu generieren.

```
pipeline:
  ...
  sink:
    opensearch:
      index: "metadata-${metadataType}"
```

Die folgende Konfiguration generiert weiterhin jeden Tag oder jede Stunde einen neuen Index.

```
pipeline:
  ...
  sink:
    opensearch:
      index: "metadata-${metadataType}-%{yyyy.MM.dd}"

pipeline:
  ...
  sink:
    opensearch:
      index: "metadata-${metadataType}-%{yyyy.MM.dd.HH}"
```

Der Indexname kann auch eine einfache Zeichenfolge mit einem Datums-/Uhrzeitmuster als Suffix sein, z. B. `my-index-%{yyyy.MM.dd}` Wenn die Senke Daten an sendet OpenSearch, ersetzt sie das Datums-/Uhrzeitmuster durch die UTC-Zeit und erstellt für jeden Tag einen neuen Index, z. B. `my-index-2022.01.25` Weitere Informationen finden Sie in der DateTimeFormatterKlasse.

Dieser Indexname kann auch eine formatierte Zeichenfolge sein (mit oder ohne ein Datums-/Uhrzeit-Mustersuffix), z. B. `my-${index}-name` Wenn die Senke Daten an sendet OpenSearch, ersetzt sie den `"${index}"` Teil durch den Wert in dem Ereignis, das gerade verarbeitet wird. Wenn das Format `"${index1/index2/index3}"` zutrifft, ersetzt es das Feld `index1/index2/index3` durch seinen Wert im Ereignis.

Dokument wird generiert IDs

Eine Pipeline kann beim Indizieren von Dokumenten eine Dokument-ID generieren. OpenSearch Sie kann diese Dokumente IDs aus den Feldern in eingehenden Ereignissen ableiten.

In diesem Beispiel wird das `uuid` Feld aus einem eingehenden Ereignis verwendet, um eine Dokument-ID zu generieren.

```
pipeline:
  ...
  sink:
    opensearch:
      index_type: custom
      index: "metadata-${metadataType}-%{yyyy.MM.dd}"
      "document_id": "uuid"
```

Im folgenden Beispiel führt der Prozessor „Einträge hinzufügen“ die Felder `uuid` `other_field` aus dem eingehenden Ereignis zusammen, um eine Dokument-ID zu generieren.

Die `create` Aktion stellt sicher, dass Dokumente mit identischem Wert IDs nicht überschrieben werden. Die Pipeline löscht doppelte Dokumente ohne erneuten Versuch oder DLQ-Ereignis. Dies ist für Pipeline-Autoren, die diese Aktion verwenden, durchaus zu erwarten, da das Ziel darin besteht, die Aktualisierung vorhandener Dokumente zu vermeiden.

```
pipeline:
  ...
  processor:
   - add_entries:
      entries:
        - key: "my_doc_id_field"
          format: "${uuid}-${other_field}"
  sink:
    - opensearch:
       ...
       action: "create"
       document_id: "my_doc_id"
```

Möglicherweise möchten Sie die Dokument-ID eines Ereignisses auf ein Feld aus einem Unterobjekt festlegen. Im folgenden Beispiel verwendet das OpenSearch Sink-Plug-In das Unterobjekt, um eine Dokument-ID `info/id` zu generieren.

```
sink:
  - opensearch:
       ...
       document_id: info/id
```

Bei dem folgenden Ereignis generiert die Pipeline ein Dokument, bei dem das `_id` Feld wie folgt gesetzt `json001` ist:

```
{
   "fieldA":"arbitrary value",
   "info":{
      "id":"json001",
      "fieldA":"xyz",
      "fieldB":"def"
   }
}
```

Routing wird generiert IDs

Sie können die `routing_field` Option innerhalb des OpenSearch Sink-Plug-ins verwenden, um den Wert einer Dokumentweiterleitungseigenschaft (`_routing`) auf einen Wert aus einem eingehenden Ereignis festzulegen.

Routing unterstützt die JSON-Zeigersyntax, sodass auch verschachtelte Felder verfügbar sind, nicht nur Felder der obersten Ebene.

```
sink:
  - opensearch:
       ...
       routing_field: metadata/id
       document_id: id
```

Bei dem folgenden Ereignis generiert das Plugin ein Dokument, bei dem das `_routing` Feld auf gesetzt ist: `abcd`

```
{
   "id":"123",
   "metadata":{
      "id":"abcd",
      "fieldA":"valueA"
   },
   "fieldB":"valueB"
}
```

Anweisungen zum Erstellen von Indexvorlagen, die Pipelines bei der Indexerstellung verwenden können, finden Sie unter Indexvorlagen.

End-to-end Bestätigung

OpenSearch Die Datenaufnahme gewährleistet die Haltbarkeit und Zuverlässigkeit von Daten, indem deren Übertragung von der Quelle bis zu den Senken in zustandslosen Pipelines mithilfe von Quittierung nachverfolgt wird. end-to-end

> **Note**
>
> Derzeit unterstützt nur das S3-Quell-Plugin die Bestätigung. end-to-end

Bei der end-to-end Bestätigung erstellt das Pipeline-Quell-Plugin einen Bestätigungssatz zur Überwachung einer Reihe von Ereignissen. Es erhält eine positive Bestätigung, wenn diese Ereignisse erfolgreich an ihre Senken gesendet wurden, oder eine negative Bestätigung, wenn eines der Ereignisse nicht an ihre Senken gesendet werden konnte.

Im Falle eines Fehlers oder Absturzes einer Pipeline-Komponente oder wenn eine Quelle keine Bestätigung erhält, läuft die Quelle ab und ergreift die erforderlichen Maßnahmen, wie z. B. einen erneuten Versuch oder die Protokollierung des Fehlers. Wenn für die Pipeline mehrere Senken oder mehrere Sub-Pipelines konfiguriert sind, werden Bestätigungen auf Ereignisebene erst gesendet, nachdem das Ereignis an alle Senken in allen Unter-Pipelines gesendet wurde. Wenn für eine Senke ein DLQ konfiguriert ist, verfolgt die Bestätigungsfunktion auch Ereignisse, die in den DLQ geschrieben wurden. end-to-end

Um die end-to-end Bestätigung zu aktivieren, erweitern Sie Zusätzliche Optionen in der Amazon S3 S3-Quellkonfiguration und wählen Sie end-to-endNachrichtenbestätigung aktivieren aus.

Gegendruck an der Quelle

In einer Pipeline kann es zu Gegendruck kommen, wenn sie mit der Verarbeitung von Daten beschäftigt ist oder wenn ihre Senken vorübergehend ausgefallen sind oder nur langsam Daten aufnehmen. OpenSearch Je nachdem, welches Quell-Plugin eine Pipeline verwendet, gibt es bei der Datenaufnahme unterschiedliche Methoden, mit Gegendruck umzugehen.

HTTP-Quelle

Pipelines, die das HTTP-Quell-Plugin verwenden, behandeln Gegendruck unterschiedlich, je nachdem, welche Pipeline-Komponente überlastet ist:

- Puffer — Wenn die Puffer voll sind, gibt die Pipeline den HTTP-Status `REQUEST_TIMEOUT` mit dem Fehlercode 408 zurück zum Quellendpunkt. Sobald Puffer freigegeben werden, beginnt die Pipeline erneut mit der Verarbeitung von HTTP-Ereignissen.
- Quell-Threads — Wenn alle HTTP-Quell-Threads mit der Ausführung von Anfragen beschäftigt sind und die Größe der Warteschlange für unbearbeitete Anfragen die maximal zulässige Anzahl von Anfragen überschritten hat, gibt die Pipeline den HTTP-Status `TOO_MANY_REQUESTS` mit dem Fehlercode 429 zurück an den Quellendpunkt. Wenn die Anforderungswarteschlange die maximal zulässige Warteschlangengröße unterschreitet, beginnt die Pipeline erneut mit der Verarbeitung der Anfragen.

OTel Quelle

Wenn die Puffer für Pipelines, die OpenTelemetry Quellen (OTel Logs, OTel Metriken und OTel Trace) verwenden, voll sind, beginnt die Pipeline, den HTTP-Status `REQUEST_TIMEOUT` mit dem Fehlercode 408 an den Quellendpunkt zurückzugeben. Sobald Puffer freigegeben werden, beginnt die Pipeline erneut mit der Verarbeitung von Ereignissen.

S3-Quelle

Wenn die Puffer für Pipelines mit einer S3-Quelle voll sind, beenden die Pipelines die Verarbeitung von SQS-Benachrichtigungen. Sobald die Puffer freigegeben sind, beginnen die Pipelines wieder mit der Verarbeitung von Benachrichtigungen.

Wenn eine Senke ausgefallen ist oder keine Daten aufnehmen kann und die end-to-end Bestätigung für die Quelle aktiviert ist, stoppt die Pipeline die Verarbeitung von SQS-Benachrichtigungen, bis sie eine erfolgreiche Bestätigung von allen Senken erhält.

Amazon OpenSearch Ingestion-Pipelines erstellen

Eine Pipeline ist der Mechanismus, den Amazon OpenSearch Ingestion verwendet, um Daten von ihrer Quelle (wo die Daten herkommen) zu ihrer Senke (wo die Daten hingehen) zu verschieben. Bei OpenSearch Ingestion wird die Senke immer eine einzelne Amazon OpenSearch Service-Domain sein, während die Quelle Ihrer Daten Clients wie Amazon S3, Fluent Bit oder Collector sein kann. OpenTelemetry

Weitere Informationen finden Sie in der Dokumentation unter Pipelines. OpenSearch

Themen

- Voraussetzungen und erforderliche IAM-Rolle
- Erforderliche IAM-Berechtigungen
- Angabe der Pipeline-Version
- Angeben des Aufnahmepfads
- Pipelines erstellen
- Den Status der Pipeline-Erstellung verfolgen
- Mit Blueprints arbeiten

Voraussetzungen und erforderliche IAM-Rolle

Um eine OpenSearch Ingestion-Pipeline zu erstellen, benötigen Sie die folgenden Ressourcen:

- Eine IAM-Rolle, die so genannte Pipeline-Rolle, die OpenSearch Ingestion übernimmt, um in die Senke zu schreiben. Sie können diese Rolle im Voraus erstellen, oder Sie können festlegen, dass OpenSearch Ingestion sie automatisch erstellt, während Sie die Pipeline erstellen.
- Eine OpenSearch Service-Domain oder eine OpenSearch Serverless-Sammlung, die als Senke fungiert. Wenn Sie in eine Domain schreiben, muss sie OpenSearch 1.0 oder höher oder Elasticsearch 7.4 oder höher ausführen. Die Senke muss über eine Zugriffsrichtlinie verfügen, die Ihrer IAM-Pipeline-Rolle die entsprechenden Berechtigungen gewährt.

Anweisungen zum Erstellen dieser Ressourcen finden Sie in den folgenden Themen:

- the section called “Pipelines Zugriff auf Domains gewähren”
- the section called “Pipelines Zugriff auf Sammlungen gewähren”

> **Note**
>
> Wenn Sie in eine Domäne schreiben, die eine differenzierte Zugriffskontrolle verwendet, müssen Sie zusätzliche Schritte ausführen. Siehe the section called “Ordnen Sie die Pipeline-Rolle zu (nur für Domänen, die eine differenzierte Zugriffskontrolle verwenden)”.

Erforderliche IAM-Berechtigungen

OpenSearch Ingestion verwendet die folgenden IAM-Berechtigungen für die Erstellung von Pipelines:

- `osis:CreatePipeline`— Erstellen Sie eine Pipeline.
- `osis:ValidatePipeline`— Prüft, ob eine Pipeline-Konfiguration gültig ist.
- `iam:CreateRole`und `iam:AttachPolicy` — Lassen Sie OpenSearch Ingestion die Pipeline-Rolle automatisch für Sie erstellen.
- `iam:PassRole`— Übergeben Sie die Pipeline-Rolle an OpenSearch Ingestion, damit Ingestion Daten in die Domain schreiben kann. Diese Berechtigung muss für die Pipeline-Rollenressource gelten, oder einfach, `*` wenn Sie beabsichtigen, in jeder Pipeline unterschiedliche Rollen zu verwenden.

Mit der folgenden Richtlinie wird beispielsweise die Berechtigung zum Erstellen einer Pipeline erteilt:

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Resource":"*",
         "Action":[
            "osis:CreatePipeline",
            "osis:ListPipelineBlueprints",
            "osis:ValidatePipeline"
         ]
      },
      {
         "Resource":[
            "arn:aws:iam::your-account-id:role/pipeline-role"
         ],
         "Effect":"Allow",
         "Action":[
            "iam:CreateRole",
            "iam:AttachPolicy",
            "iam:PassRole"
         ]
      }
   ]
}
```

OpenSearch Die Erfassung umfasst auch eine sogenannte Berechtigung, die erforderlich istosis:Ingest, um signierte Anfragen mithilfe von Signature Version 4 an die Pipeline zu senden. Weitere Informationen finden Sie unter the section called “Eine Aufnahmerolle erstellen”.

> **Note**
>
> Darüber hinaus muss der erste Benutzer, der eine Pipeline in einem Konto erstellt, über Berechtigungen für die iam:CreateServiceLinkedRole Aktion verfügen. Weitere Informationen finden Sie unter Pipeline-Rollenressource.

Weitere Informationen zu den einzelnen Berechtigungen finden Sie in der Serviceautorisierungsreferenz unter Aktionen, Ressourcen und OpenSearch Bedingungsschlüssel für die Datenerfassung.

Angabe der Pipeline-Version

Wenn Sie eine Pipeline mit dem Konfigurationseditor erstellen, müssen Sie die Hauptversion von Data Prepper angeben, die die Pipeline ausführen soll. Um die Version anzugeben, nehmen Sie die version Option in Ihre Pipeline-Konfiguration auf:

```
version: "2"
log-pipeline:
  source:
    ...
```

Wenn Sie Create wählen, ermittelt OpenSearch Ingestion die neueste verfügbare Nebenversion der von Ihnen angegebenen Hauptversion und stellt die Pipeline mit dieser Version bereit. Wenn Sie beispielsweise angeben version: "2" und die neueste unterstützte Version von Data Prepper 2.1.1 ist, stellt OpenSearch Ingestion Ihrer Pipeline Version 2.1.1 zur Verfügung. Wir zeigen die Nebenversion, die in Ihrer Pipeline läuft, nicht öffentlich an.

Um Ihre Pipeline zu aktualisieren, wenn eine neue Hauptversion von Data Prepper verfügbar ist, bearbeiten Sie die Pipeline-Konfiguration und geben Sie die neue Version an. Sie können eine Pipeline nicht auf eine frühere Version herunterstufen.

> **Note**
>
> OpenSearch Ingestion unterstützt neue Versionen von Data Prepper nicht sofort, sobald sie veröffentlicht werden. Es wird eine gewisse Verzögerung zwischen der Veröffentlichung einer neuen Version und der Unterstützung in Ingestion geben. OpenSearch Darüber hinaus unterstützt OpenSearch Ingestion möglicherweise bestimmte Haupt- oder Nebenversionen ausdrücklich nicht. Eine umfangreiche Liste finden Sie unter the section called “Unterstützte Data Prepper-Versionen”.

Jedes Mal, wenn Sie eine Änderung an Ihrer Pipeline vornehmen, die eine blue/green Bereitstellung initiiert, kann OpenSearch Ingestion sie auf die neueste Nebenversion der Hauptversion aktualisieren, die derzeit für die Pipeline konfiguriert ist. Weitere Informationen finden Sie unter. the section called “Blaue/grüne Bereitstellungen für Pipeline-Updates” OpenSearch Durch die Aufnahme kann die Hauptversion Ihrer Pipeline nur geändert werden, wenn Sie die `version` Option in der Pipeline-Konfiguration explizit aktualisieren.

Angeben des Aufnahmepfads

Für Pull-basierte Quellen wie OTel Trace und OTel Metriken erfordert OpenSearch Ingestion die zusätzliche `path` Option in Ihrer Quellkonfiguration. Der Pfad ist eine Zeichenfolge wie`/log/ingest`, die den URI-Pfad für die Aufnahme darstellt. Dieser Pfad definiert den URI, den Sie verwenden, um Daten an die Pipeline zu senden.

Angenommen, Sie geben den folgenden Pfad für eine Pipeline mit einer HTTP-Quelle an:



Wenn Sie Daten in die Pipeline aufnehmen, müssen Sie den folgenden Endpunkt in Ihrer Client-Konfiguration angeben:`https://pipeline-name-abc123.us-west-2.osis.amazonaws.com/my/test_path`.

Der Pfad muss mit einem Schrägstrich (/) beginnen und kann die Sonderzeichen '-', '_', 'enthalten . 'und'/'sowie der `${pipelineName}` Platzhalter. Wenn Sie `${pipelineName}` (z. B./

`${pipelineName}/test_path`) verwenden, ersetzt OpenSearch Ingestion die Variable durch den Namen der zugehörigen Subpipeline.

Pipelines erstellen

In diesem Abschnitt wird beschrieben, wie Sie OpenSearch Ingestion-Pipelines mithilfe der OpenSearch Servicekonsole und der erstellen. AWS CLI

Konsole

Um eine Pipeline zu erstellen, melden Sie sich zu https://console.aws.amazon.com/aos/Hause bei der Amazon OpenSearch Service-Konsole an und wählen Sie Pipeline erstellen.

Wählen Sie entweder eine leere Pipeline oder einen Konfigurations-Blueprint aus. Blueprints enthalten eine vorkonfigurierte Pipeline für eine Vielzahl gängiger Anwendungsfälle. Weitere Informationen finden Sie unter the section called “Mit Blueprints arbeiten”.

Wählen Sie Blueprint auswählen.

Quelle konfigurieren

1. Wenn Sie mit einer leeren Pipeline beginnen, wählen Sie eine Quelle aus dem Drop-down-Menü aus. Zu den verfügbaren Quellen können andere AWS-Services OpenTelemetry, oder HTTP gehören. Weitere Informationen finden Sie unter the section called “Integration von Pipelines”.
2. Je nachdem, welche Quelle Sie wählen, konfigurieren Sie zusätzliche Einstellungen für die Quelle. Um beispielsweise Amazon S3 als Quelle zu verwenden, müssen Sie die URL der Amazon SQS SQS-Warteschlange aus der Pipeline angeben, die Nachrichten empfängt. Eine Liste der unterstützten Quell-Plugins und Links zu deren Dokumentation finden Sie unter. the section called “Unterstützte Plugins und Optionen”
3. Für einige Quellen müssen Sie die Quellnetzwerkoptionen angeben. Wählen Sie entweder VPC-Zugriff oder Öffentlicher Zugriff. Fahren Sie bei Wahl von Public access (Öffentlicher Zugriff) mit dem nächsten Schritt fort. Wenn Sie VPC-Zugriff wählen, konfigurieren Sie die folgenden Einstellungen:

Einstellung	Beschreibung
Endpunktv erwaltung	Wählen Sie, ob Sie Ihre Virtual Private Cloud (VPC) -Endpoints selbst erstellen möchten oder ob Sie sie von OpenSearch Ingestion für Sie

Einstellung	Beschreibung
	erstellen lassen möchten. Endpoint Management verwendet standardm äßig Endpoints, die von Ingestion verwaltet werden. OpenSearch
VPC	Wählen Sie die ID der VPC aus, die Sie verwenden möchten. Die VPC und die Pipeline müssen identisch AWS-Region sein.
Subnets	Wählen Sie ein oder mehrere Subnetze aus. OpenSearch Der Service platziert einen VPC-Endpunkt und elastische Netzwerkschnittstellen in den Subnetzen.
Sicherhei tsgruppen	Wählen Sie eine oder mehrere VPC-Sicherheitsgruppen aus, die es Ihrer gewünschten Anwendung ermöglichen, die OpenSearch Ingestion-Pipeline auf den von der Pipeline bereitgestellten Ports (80 oder 443) und Protokollen (HTTP oder HTTPs) zu erreichen.
VPC-Anhan gsoptionen	Wenn Ihre Quelle ein selbstverwalteter Endpunkt ist, fügen Sie Ihre Pipeline einer VPC hinzu. Wählen Sie eine der bereitgestellten Standard-CIDR-Optionen oder verwenden Sie ein benutzerdefiniertes CIDR.

Weitere Informationen finden Sie unter the section called “Konfigurieren des VPC-Zugriffs für Pipelines”.

4. Wählen Sie Weiter aus.

Prozessor konfigurieren

Fügen Sie Ihrer Pipeline einen oder mehrere Prozessoren hinzu. Prozessoren sind Komponenten innerhalb einer Subpipeline, mit denen Sie Ereignisse filtern, transformieren und anreichern können, bevor Sie Datensätze in der Domain oder Sammelsenke veröffentlichen. Eine Liste der unterstützten Prozessoren und Links zu deren Dokumentation finden Sie unterthe section called “Unterstützte Plugins und Optionen”.

Sie können Aktionen auswählen und Folgendes hinzufügen:

- Bedingtes Routing — Leitet Ereignisse auf der Grundlage bestimmter Bedingungen an verschiedene Senken weiter. Weitere Informationen finden Sie unter Bedingtes Routing.

- Subpipeline — Jede Subpipeline ist eine Kombination aus einer einzelnen Quelle, null oder mehr Prozessoren und einer einzelnen Senke. Nur eine Subpipeline kann eine externe Quelle haben. Alle anderen müssen über Quellen verfügen, bei denen es sich um andere Unter-Pipelines innerhalb der gesamten Pipeline-Konfiguration handelt. Eine einzelne Pipeline-Konfiguration kann 1—10 Unter-Pipelines enthalten.

Wählen Sie Weiter aus.

Senke konfigurieren

Wählen Sie das Ziel aus, an dem die Pipeline Datensätze veröffentlicht. Jede Unterpipeline muss mindestens eine Senke enthalten. Sie können einer Pipeline maximal 10 Senken hinzufügen.

Konfigurieren Sie für OpenSearch Senken die folgenden Felder:

Einstellung	Beschreibung
Name der Netzwerkrichtlinie (Nur serverlose Senken)	Wenn Sie eine OpenSearch serverlose Sammlung ausgewählt haben, geben Sie einen Namen für die Netzwerkrichtlinie ein. OpenSearch Die Aufnahme erstellt entweder die Richtlinie, falls sie nicht existiert, oder aktualisiert sie mit einer Regel, die Zugriff auf den VPC-Endpunkt gewährt, der die Pipeline und die Sammlung verbindet. Weitere Informationen finden Sie unter the section called “Pipelines Zugriff auf Sammlungen gewähren”.
Name des Indexes	Der Name des Indexes, an den die Pipeline Daten sendet. OpenSearch Ingestion erstellt diesen Index, falls er noch nicht vorhanden ist.
Optionen für die Indexzuweisung	Wählen Sie aus, wie die Pipeline Dokumente und ihre Felder in der OpenSearch Senke speichert und indexiert. Wenn Sie Dynamisches Mapping auswählen, werden Felder automatisch OpenSearch hinzugefü gt, wenn Sie ein Dokument indizieren. Wenn Sie Zuordnung anpassen auswählen, geben Sie eine Indexzuordnungsvorlage ein. Weitere Informati onen finden Sie unter Indexvorlagen.
Aktivieren Sie DLQ	Konfigurieren Sie eine Amazon S3 S3-Warteschlange (DLQ) für die Pipeline. Weitere Informationen finden Sie unter the section called “Warteschlangen für unzustellbare Nachrichten”.

Einstellung	Beschreibung
Zusätzliche Einstellungen	Konfigurieren Sie erweiterte Optionen für die OpenSearch Spüle. Weitere Informationen finden Sie unter Konfigurationsoptionen in der Data Prepper-Dokumentation.

Um eine Amazon S3-Senke hinzuzufügen, wählen Sie Add sink und Amazon S3. Weitere Informationen finden Sie unter the section called “Amazon S3 als Ziel”.

Wählen Sie Weiter aus.

Pipeline konfigurieren

Konfigurieren Sie die folgenden zusätzlichen Pipeline-Einstellungen:

Einstellung	Beschreibung
Name der Pipeline	Ein eindeutiger Name für die Pipeline.
Persistenter Puffer	Ein persistenter Puffer speichert Ihre Daten in einem festplattenbasierten Puffer in mehreren Availability Zones. Weitere Informationen finden Sie unter the section called “Dauerhafte Pufferung”. Wenn Sie die persistente Pufferung aktivieren, wählen Sie den AWS Key Management Service Schlüssel zum Verschlüsseln der Pufferdaten aus.
Kapazität der Pipeline	Die minimale und maximale Pipeline-Kapazität in OpenSearch Ingestion-Recheneinheiten ()OCUs. Weitere Informationen finden Sie unter the section called “Skalierung von Pipelines”.
Rolle „Pipeline“	Die IAM-Rolle, die die erforderlichen Berechtigungen für die Pipeline bereitstellt, um in die Senke zu schreiben und aus Pull-basierten Quellen zu lesen. Sie können die Rolle selbst erstellen oder sie anhand des ausgewählten Anwendungsfalls von OpenSearch Ingestion für Sie erstellen lassen. Weitere Informationen finden Sie unter the section called “Rollen und Benutzer einrichten”.

Einstellung	Beschreibung
Tags	Fügen Sie Ihrer Pipeline ein oder mehrere Tags hinzu. Weitere Informationen finden Sie unter the section called “Markieren von Pipelines”.
Optionen für die Veröffentlichung von Protokollen	Aktivieren Sie die Veröffentlichung von Pipeline-Protokollen in Amazon CloudWatch Logs. Wir empfehlen, die Protokollveröffentlichung zu aktiviere n, damit Sie Pipeline-Probleme einfacher beheben können. Weitere Informati onen finden Sie unter the section called “Überwachen der Pipeline-Protokoll e”.

Wählen Sie Weiter., überprüfen Sie dann Ihre Pipeline-Konfiguration und wählen Sie Pipeline erstellen aus.

OpenSearch Bei der Aufnahme wird ein asynchroner Prozess ausgeführt, um die Pipeline zu erstellen. Sobald der Pipeline-Status lautet`Active`, können Sie mit der Datenaufnahme beginnen.

AWS CLI

Der Befehl create-pipeline akzeptiert die Pipeline-Konfiguration als Zeichenfolge oder in einer .yaml- oder .json-Datei. Wenn Sie die Konfiguration als Zeichenfolge angeben, muss jede neue Zeile mit einem Escapezeichen versehen werden. `\n` Beispiel: `"log-pipeline:\n source:\n http:\n processor:\n - grok:\n ..."`

Der folgende Beispielbefehl erstellt eine Pipeline mit der folgenden Konfiguration:

- Mindestens 4 Ingestions OCUs, maximal 10 Ingestions OCUs
- Bereitgestellt in einer Virtual Private Cloud (VPC)
- Veröffentlichung von Protokollen aktiviert

```
aws osis create-pipeline \
  --pipeline-name my-pipeline \
  --min-units 4 \
  --max-units 10 \
  --log-publishing-options
 IsLoggingEnabled=true,CloudWatchLogDestination={LogGroup="MyLogGroup"} \
  --vpc-options
 SecurityGroupIds={sg-12345678,sg-9012345},SubnetIds=subnet-1212234567834asdf \
```

```
  --pipeline-configuration-body "file://pipeline-config.yaml" \
  --pipeline-role-arn  arn:aws:iam::1234456789012:role/pipeline-role
```

OpenSearch Bei der Aufnahme wird ein asynchroner Prozess zum Erstellen der Pipeline ausgeführt. Sobald der Pipeline-Status lautet`Active`, können Sie mit der Datenaufnahme beginnen. Verwenden Sie den GetPipelineBefehl, um den Status der Pipeline zu überprüfen.

OpenSearch Aufnahme-API

Rufen Sie den Vorgang auf, um eine OpenSearch Ingestion-Pipeline mithilfe der OpenSearch Ingestion-API zu erstellen. CreatePipeline

Nachdem Ihre Pipeline erfolgreich erstellt wurde, können Sie Ihren Client konfigurieren und mit der Aufnahme von Daten in Ihre Service-Domain beginnen. OpenSearch Weitere Informationen finden Sie unter the section called “Integration von Pipelines”.

Den Status der Pipeline-Erstellung verfolgen

Sie können den Status einer Pipeline verfolgen, während sie von OpenSearch Ingestion bereitgestellt und für die Datenaufnahme vorbereitet wird.

Konsole

Nachdem Sie eine Pipeline zum ersten Mal erstellt haben, durchläuft sie mehrere Phasen, während OpenSearch Ingestion sie für die Datenaufnahme vorbereitet. Um die verschiedenen Phasen der Pipeline-Erstellung zu sehen, wählen Sie den Namen der Pipeline aus, um die Seite mit den Pipeline-Einstellungen aufzurufen. Wählen Sie unter Status die Option Details anzeigen aus.

Eine Pipeline durchläuft die folgenden Phasen, bevor sie für die Datenaufnahme verfügbar ist:

- Validierung — Überprüfung der Pipeline-Konfiguration. Wenn diese Phase abgeschlossen ist, waren alle Validierungen erfolgreich.
- Umgebung erstellen — Ressourcen vorbereiten und bereitstellen. Wenn diese Phase abgeschlossen ist, wurde die neue Pipeline-Umgebung erstellt.
- Pipeline bereitstellen — Bereitstellung der Pipeline. Wenn diese Phase abgeschlossen ist, wurde die Pipeline erfolgreich bereitgestellt.
- Zustand der Pipeline überprüfen — Überprüfung des Zustands der Pipeline. Wenn diese Phase abgeschlossen ist, wurden alle Integritätsprüfungen bestanden.

- Datenverkehr aktivieren — Ermöglicht der Pipeline, Daten aufzunehmen. Wenn diese Phase abgeschlossen ist, können Sie mit der Aufnahme von Daten in die Pipeline beginnen.

CLI

Verwenden Sie den get-pipeline-change-progressBefehl, um den Status einer Pipeline zu überprüfen. Die folgende AWS CLI Anfrage überprüft den Status einer Pipeline mit dem Namen`my-pipeline`:

```
aws osis get-pipeline-change-progress \
    --pipeline-name my-pipeline
```

Antwort:

```
{
   "ChangeProgressStatuses": {
      "ChangeProgressStages": [
         {
            "Description": "Validating pipeline configuration",
            "LastUpdated": 1.671055851E9,
            "Name": "VALIDATION",
            "Status": "PENDING"
         }
      ],
      "StartTime": 1.671055851E9,
      "Status": "PROCESSING",
      "TotalNumberOfStages": 5
   }
}
```

OpenSearch Aufnahme-API

Rufen Sie den Vorgang auf, um den Status der Pipeline-Erstellung mithilfe der OpenSearch Ingestion-API zu verfolgen. GetPipelineChangeProgress

Mit Blueprints arbeiten

Anstatt eine Pipeline-Definition von Grund auf neu zu erstellen, können Sie Konfigurations-Blueprints verwenden. Dabei handelt es sich um vorkonfigurierte Vorlagen für gängige Aufnahmeszenarien wie Trace Analytics oder Apache-Protokolle. Mithilfe von Konfigurations-Blueprints können Sie Pipelines einfach bereitstellen, ohne eine Konfiguration von Grund auf neu erstellen zu müssen.

Konsole

Um einen Pipeline-Blueprint zu verwenden

1. Melden Sie sich zu https://console.aws.amazon.com/aos/Hause bei der Amazon OpenSearch Service-Konsole an.
2. Wählen Sie im linken Navigationsbereich Pipelines und dann Pipeline erstellen aus.
3. Wählen Sie einen Blueprint aus der Liste der Anwendungsfälle aus und wählen Sie dann Blueprint auswählen aus. Die Pipeline-Konfiguration wird mit einer Sub-Pipeline für den von Ihnen ausgewählten Anwendungsfall aufgefüllt.

   Der Pipeline-Blueprint ist in seiner jetzigen Form nicht gültig. Abhängig von der ausgewählten Quelle müssen Sie zusätzliche Einstellungen angeben.

CLI

Um mit dem eine Liste aller verfügbaren Blueprints zu erhalten AWS CLI, senden Sie eine list-pipeline-blueprintsAnfrage.

```
aws osis list-pipeline-blueprints
```

Die Anfrage gibt eine Liste aller verfügbaren Blueprints zurück.

Verwenden Sie den folgenden Befehl, um detailliertere Informationen zu einem bestimmten Blueprint zu erhalten: get-pipeline-blueprint

```
aws osis get-pipeline-blueprint --blueprint-name AWS-ApacheLogPipeline
```

Diese Anfrage gibt den Inhalt des Apache-Protokoll-Pipeline-Blueprints zurück:

```
{
   "Blueprint":{
      "PipelineConfigurationBody":"###\n  # Limitations: https://docs.aws.amazon.com/
opensearch-service/latest/ingestion/ingestion.html#ingestion-limitations\n###\n###\n
 # apache-log-pipeline:\n    # This pipeline receives logs via http (e.g. FluentBit),
 extracts important values from the logs by matching\n    # the value in the 'log' key
 against the grok common Apache log pattern. The grokked logs are then sent\n    # to
 OpenSearch to an index named 'logs'\n###\n\nversion: \"2\"\napache-log-pipeline:\n
 source:\n    http:\n      # Provide the path for ingestion. ${pipelineName} will be
```

```
 replaced with pipeline name configured for this pipeline.\n      # In this case it
 would be \"/apache-log-pipeline/logs\". This will be the FluentBit output URI value.
\n      path: \"/${pipelineName}/logs\"\n  processor:\n    - grok:\n        match:\n
         log: [ \"%{COMMONAPACHELOG_DATATYPED}\" ]\n  sink:\n    - opensearch:\n
   # Provide an AWS OpenSearch Service domain endpoint\n        # hosts: [ \"https://
search-mydomain-1a2a3a4a5a6a7a8a9a0a9a8a7a.us-east-1.es.amazonaws.com\" ]\n        aws:
\n          # Provide the region of the domain.\n          # region: \"us-east-1\"\n
        # Enable the 'serverless' flag if the sink is an Amazon OpenSearch Serverless
 collection\n          # serverless: true\n        index: \"logs\"\n        # Enable
 the S3 DLQ to capture any failed requests in an S3 bucket\n        # dlq:\n
  # s3:\n            # Provide an S3 bucket\n            # bucket: \"your-dlq-bucket-
name\"\n            # Provide a key path prefix for the failed requests\n
  # key_path_prefix: \"${pipelineName}/logs/dlq\"\n            # Provide the region
 of the bucket.\n            # region: \"us-east-1\"\n            # Provide a Role
 ARN with access to the bucket. This role should have a trust relationship with osis-
pipelines.amazonaws.com\n"
      "BlueprintName":"AWS-ApacheLogPipeline"
   }
}
```

OpenSearch Aufnahme-API

Um Informationen zu Pipeline-Blueprints mithilfe der OpenSearch Ingestion-API zu erhalten, verwenden Sie die Operationen und. ListPipelineBlueprintsGetPipelineBlueprint

Amazon OpenSearch Ingestion-Pipelines anzeigen

Sie können die Details zu einer Amazon OpenSearch Ingestion-Pipeline mithilfe der AWS Management Console, der oder der AWS CLI OpenSearch Ingestion-API anzeigen.

Konsole

So zeigen Sie eine Pipeline an

1. Melden Sie sich zu https://console.aws.amazon.com/aos/Hause bei der Amazon OpenSearch Service-Konsole an.
2. Wählen Sie im linken Navigationsbereich Pipelines.
3. (Optional) Um Pipelines mit einem bestimmten Status anzuzeigen, wählen Sie Beliebiger Status und dann einen Status aus, nach dem gefiltert werden soll.

   Eine Pipelines kann folgende Status aufweisen:

- `Active`— Die Pipeline ist aktiv und bereit, Daten aufzunehmen.
- `Creating`— Die Pipeline wird gerade erstellt.
- `Updating`— Die Pipelines werden aktualisiert.
- `Deleting`— Die Pipelines werden gelöscht.
- `Create failed`— Die Pipeline konnte nicht erstellt werden.
- `Update failed`— Die Pipeline konnte nicht aktualisiert werden.
- `Stop failed`— Die Pipeline konnte nicht gestoppt werden.
- `Start failed`— Die Pipeline konnte nicht gestartet werden.
- `Stopping`— Die Pipelines werden gestoppt.
- `Stopped`— Die Pipeline ist gestoppt und kann jederzeit neu gestartet werden.
- `Starting`— Die Pipeline wird gestartet.

Ihnen wird die Datenaufnahme nicht in Rechnung gestellt, OCUs wenn sich eine Pipeline in den BundesstaatenCreate failed, CreatingDeleting, und befindet. Stopped

CLI

Um Pipelines mithilfe von anzuzeigen AWS CLI, senden Sie eine List-Pipeline-Anfrage:

```
aws osis list-pipelines
```

Die Anfrage gibt eine Liste aller vorhandenen Pipelines zurück:

```
{
    "NextToken": null,
    "Pipelines": [
        {
            "CreatedAt": 1.671055851E9,
            "LastUpdatedAt": 1.671055851E9,
            "MaxUnits": 4,
            "MinUnits": 2,
            "PipelineArn": "arn:aws:osis:us-west-2:123456789012:pipeline/log-pipeline",
            "PipelineName": "log-pipeline",
            "Status": "ACTIVE",
            "StatusReason": {
                "Description": "The pipeline is ready to ingest data."
            }
```

```
        },
            "CreatedAt": 1.671055851E9,
            "LastUpdatedAt": 1.671055851E9,
            "MaxUnits": 2,
            "MinUnits": 8,
            "PipelineArn": "arn:aws:osis:us-west-2:123456789012:pipeline/another-
pipeline",
            "PipelineName": "another-pipeline",
            "Status": "CREATING",
            "StatusReason": {
                "Description": "The pipeline is being created. It is not able to ingest
 data."
            }
        }
    ]
}
```

Verwenden Sie den Befehl get-pipeline, um Informationen zu einer einzelnen Pipeline abzurufen:

```
aws osis get-pipeline --pipeline-name "my-pipeline"
```

Die Anforderung gibt Konfigurationsinformationen für die angegebene Pipeline zurück:

```
{
    "Pipeline": {
        "PipelineName": "my-pipeline",
        "PipelineArn": "arn:aws:osis:us-east-1:123456789012:pipeline/my-pipeline",
        "MinUnits": 9,
        "MaxUnits": 10,
        "Status": "ACTIVE",
        "StatusReason": {
            "Description": "The pipeline is ready to ingest data."
        },
        "PipelineConfigurationBody": "log-pipeline:\n source:\n http:\n processor:\n
 - grok:\n match:\nlog: [ '%{COMMONAPACHELOG}' ]\n - date:\n from_time_received: true
\n destination: \"@timestamp\"\n  sink:\n - opensearch:\n hosts: [ \"https://search-
mdp-performance-test-duxkb4qnycd63rpy6svmvyvfpi.us-east-1.es.amazonaws.com\" ]\n index:
 \"apache_logs\"\n aws_sts_role_arn: \"arn:aws:iam::123456789012:role/my-domain-role
\"\n  aws_region: \"us-east-1\"\n  aws_sigv4: true",,
        "CreatedAt": "2022-10-01T15:28:05+00:00",
        "LastUpdatedAt": "2022-10-21T21:41:08+00:00",
        "IngestEndpointUrls": [
            "my-pipeline-123456789012.us-east-1.osis.amazonaws.com"
```

```
        ]
    }
}
```

OpenSearch Aufnahme-API

Rufen Sie die Operationen and auf, OpenSearch um Ingestion-Pipelines mithilfe der OpenSearch Ingestion-API anzuzeigen. ListPipelinesGetPipeline

Aktualisierung der Amazon OpenSearch Ingestion-Pipelines

Sie können Amazon OpenSearch Ingestion-Pipelines mithilfe der AWS Management Console, der oder der AWS CLI OpenSearch Ingestion-API aktualisieren. OpenSearch Ingestion initiiert eine Bereitstellung, wenn Sie eine blue/green Pipeline-Konfiguration aktualisieren. Weitere Informationen finden Sie unter the section called “Blaue/grüne Bereitstellungen für Pipeline-Updates”.

Themen

- Überlegungen
- Erforderliche Berechtigungen
- Pipelines werden aktualisiert
- Blaue/grüne Bereitstellungen für Pipeline-Updates

Überlegungen

Beachten Sie beim Aktualisieren einer Pipeline Folgendes:

- Sie können den Namen oder die Netzwerkeinstellungen einer Pipeline nicht aktualisieren.
- Wenn Ihre Pipeline in eine VPC-Domänensenke schreibt, können Sie nicht zurückgehen und die Senke in eine andere VPC-Domäne ändern, nachdem die Pipeline erstellt wurde. Sie müssen die Pipeline löschen und mit der neuen Senke neu erstellen. Sie können die Senke immer noch von einer VPC-Domain zu einer Public Domain, von einer Public Domain zu einer VPC-Domain oder von einer Public Domain zu einer anderen Public Domain wechseln.
- Sie können die Pipeline-Senke jederzeit zwischen einer öffentlichen OpenSearch Dienstdomäne und einer OpenSearch serverlosen Sammlung wechseln.
- Wenn Sie die Quell-, Prozessor- oder Senkenkonfiguration für eine Pipeline aktualisieren, initiiert OpenSearch Ingestion eine Bereitstellung. blue/green Weitere Informationen finden Sie unter the section called “Blaue/grüne Bereitstellungen für Pipeline-Updates”.

- Wenn Sie die Quell-, Prozessor- oder Senkenkonfiguration für eine Pipeline aktualisieren, aktualisiert OpenSearch Ingestion Ihre Pipeline automatisch auf die neueste unterstützte Nebenversion der Hauptversion von Data Prepper, die in der Pipeline ausgeführt wird. Dieser Prozess hält Ihre Pipeline mit den neuesten Bugfixes und Leistungsverbesserungen auf dem neuesten Stand.
- Sie können Ihre Pipeline immer noch aktualisieren, wenn sie gestoppt ist.

Erforderliche Berechtigungen

OpenSearch Ingestion verwendet die folgenden IAM-Berechtigungen für die Aktualisierung von Pipelines:

- `osis:UpdatePipeline`— Aktualisieren Sie eine Pipeline.
- `osis:ValidatePipeline`— Prüfen Sie, ob eine Pipeline-Konfiguration gültig ist.
- `iam:PassRole`— Übergeben Sie die Pipeline-Rolle an OpenSearch Ingestion, damit diese Daten in die Domain schreiben kann. Diese Berechtigung ist nur erforderlich, wenn Sie die Pipeline-Konfiguration aktualisieren, nicht, wenn Sie andere Einstellungen wie die Veröffentlichung von Protokollen oder Kapazitätsgrenzen ändern.

Die folgende Richtlinie gewährt beispielsweise die Erlaubnis, eine Pipeline zu aktualisieren:

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Resource":"*",
         "Action":[
            "osis:UpdatePipeline",
            "osis:ValidatePipeline"
         ]
      },
      {
         "Resource":[
            "arn:aws:iam::your-account-id:role/pipeline-role"
         ],
```

```
            "Effect":"Allow",
            "Action":[
               "iam:PassRole"
            ]
         }
      ]
}
```

Pipelines werden aktualisiert

Sie können Amazon OpenSearch Ingestion-Pipelines mithilfe der AWS Management Console, der oder der AWS CLI OpenSearch Ingestion-API aktualisieren.

Konsole

Um eine Pipeline zu aktualisieren

1. Melden Sie sich zu https://console.aws.amazon.com/aos/Hause bei der Amazon OpenSearch Service-Konsole an.
2. Wählen Sie im linken Navigationsbereich Pipelines aus.
3. Wählen Sie eine Pipeline aus, um ihre Einstellungen zu öffnen. Wählen Sie dann eine der Bearbeitungsoptionen.
4. Wenn Sie die gewünschten Änderungen vorgenommen haben, wählen Sie Save (Speichern) aus.

CLI

Um eine Pipeline mit dem zu aktualisieren AWS CLI, senden Sie eine Update-Pipeline-Anfrage. Die folgende Beispielanforderung lädt eine neue Konfigurationsdatei hoch und aktualisiert die Mindest- und Höchstkapazitätswerte:

```
aws osis update-pipeline \
  --pipeline-name "my-pipeline" \
  --pipline-configuration-body "file://new-pipeline-config.yaml" \
  --min-units 11 \
  --max-units 18
```

OpenSearch Aufnahme-API

Rufen Sie den Vorgang auf, um eine OpenSearch Ingestion-Pipeline mithilfe der OpenSearch Ingestion-API zu aktualisieren. UpdatePipeline

Blaue/grüne Bereitstellungen für Pipeline-Updates

OpenSearch Die Aufnahme leitet einen blauen/grünen Bereitstellungsprozess ein, wenn Sie eine Pipeline-Konfiguration aktualisieren.

Blue/green refers to the practice of creating a new environment for pipeline updates and routing traffic to the new environment after those updates are complete. The practice minimizes downtime and maintains the original environment in the event that deployment to the new environment is unsuccessful. Blue/greenBereitstellungen selbst haben keine Auswirkungen auf die Leistung, aber die Leistung kann sich ändern, wenn sich Ihre Pipeline-Konfiguration so ändert, dass die Leistung beeinträchtigt wird.

OpenSearch Die Aufnahme blockiert die auto-scaling bei Bereitstellungen. blue/green Ihnen wird weiterhin nur der Datenverkehr zur alten Pipeline in Rechnung gestellt, bis dieser zur neuen Pipeline umgeleitet wird. Sobald der Verkehr umgeleitet wurde, wird Ihnen nur die neue Pipeline in Rechnung gestellt. Ihnen werden niemals zwei Pipelines gleichzeitig in Rechnung gestellt.

Wenn Sie die Quell-, Prozessor- oder Senkenkonfiguration einer Pipeline aktualisieren, kann OpenSearch Ingestion Ihre Pipeline automatisch auf die neueste unterstützte Nebenversion der Hauptversion aktualisieren, auf der die Pipeline ausgeführt wird. Möglicherweise haben Sie `version: "2"` in Ihrer Pipeline-Konfiguration und OpenSearch Ingestion die Pipeline ursprünglich mit Version 2.1.0 bereitgestellt. Wenn Unterstützung für Version 2.1.1 hinzugefügt wird und Sie eine Änderung an Ihrer Pipeline-Konfiguration vornehmen, aktualisiert OpenSearch Ingestion Ihre Pipeline auf Version 2.1.1.

Dieser Prozess hält Ihre Pipeline mit den neuesten Bugfixes und Leistungsverbesserungen auf dem neuesten Stand. OpenSearch Ingestion kann die Hauptversion Ihrer Pipeline nur aktualisieren, wenn Sie die `version` Option in der Pipeline-Konfiguration manuell ändern.

Verwaltung der Kosten für die Amazon OpenSearch Ingestion-Pipeline

Sie können Erfassungspipelines in Amazon OpenSearch Ingestion starten und beenden, um den Datenfluss Ihren Bedürfnissen entsprechend zu steuern. Durch das Stoppen einer Pipeline wird die

Datenverarbeitung angehalten, wobei die Konfigurationen beibehalten werden, sodass Sie sie neu starten können, ohne sie neu zu konfigurieren. Dies kann dazu beitragen, Kosten zu optimieren, die Ressourcennutzung zu verwalten oder Probleme zu beheben. Wenn Sie eine Pipeline beenden, verarbeitet OpenSearch Ingestion keine eingehenden Daten, aber zuvor aufgenommene Daten bleiben in verfügbar. OpenSearch

Durch das Starten und Stoppen werden die Einrichtungs- und Deinstallvorgänge für Pipelines erleichtert, die Sie für die Entwicklung, für Tests oder ähnliche Aktivitäten verwenden, die keine kontinuierliche Verfügbarkeit erfordern. Solange Ihre Pipeline gestoppt ist, werden Ihnen keine Ingestion-OCU-Stunden in Rechnung gestellt. Sie können gestoppte Pipelines weiterhin aktualisieren, und sie erhalten automatische Updates für kleinere Versionen und Sicherheitspatches. Beim Neustart einer Pipeline wird die Verarbeitung neuer eingehender Daten fortgesetzt.

> **Note**
>
> Wenn Ihre Pipeline über Überkapazität verfügt, sie aber weiterhin betriebsbereit sein muss, sollten Sie in Erwägung ziehen, ihre maximalen Kapazitätsgrenzen anzupassen, anstatt sie zu stoppen und neu zu starten. Dies kann zur Kostenkontrolle beitragen und gleichzeitig sicherstellen, dass die Pipeline weiterhin Daten effizient verarbeitet. Weitere Details finden Sie unter the section called “Skalierung von Pipelines”.

In den folgenden Themen wird erklärt, wie Pipelines mithilfe der AWS Management Console AWS CLI, und OpenSearch Ingestion-API gestartet und gestoppt werden.

Themen

- Eine Amazon OpenSearch Ingestion-Pipeline stoppen
- Starten einer Amazon OpenSearch Ingestion-Pipeline

Eine Amazon OpenSearch Ingestion-Pipeline stoppen

Um eine OpenSearch Ingestion-Pipeline zu verwenden oder die Verwaltung durchzuführen, beginnen Sie immer mit einer aktiven Pipeline, beenden dann die Pipeline und starten sie dann erneut. Solange Ihre Pipeline gestoppt ist, werden Ihnen keine Ingestion-OCU-Stunden in Rechnung gestellt.

Konsole

Zum Stoppen einer Pipeline

1. Melden Sie sich zu https://console.aws.amazon.com/aos/Hause bei der Amazon OpenSearch Service-Konsole an.
2. Wählen Sie im Navigationsbereich Pipeline und anschließend eine Pipeline aus. Sie können den Stoppvorgang von dieser Seite ausführen oder zur Detailseite für die Pipeline navigieren, die Sie stoppen möchten.
3. Wählen Sie unter Aktionen die Option Pipeline beenden aus.

   Wenn eine Pipeline nicht gestoppt und gestartet werden kann, ist die Aktion Pipeline stoppen nicht verfügbar.

AWS CLI

Zum Stoppen einer Pipeline über die AWS CLI rufen Sie den Befehl stop-Pipeline mit den folgenden Parametern auf:

- `--pipeline-name`— der Name der Pipeline.

Example

```
aws osis stop-pipeline --pipeline-name my-pipeline
```

OpenSearch Aufnahme-API

Zum Stoppen einer Pipeline über die OpenSearch Ingestion-API rufen Sie den StopPipelineVorgang mit dem folgenden Parameter auf:

- `PipelineName`— der Name der Pipeline.

Starten einer Amazon OpenSearch Ingestion-Pipeline

Ausgangspunkt für den Start einer OpenSearch Ingestion-Pipeline ist immer eine Pipeline, die sich bereits im gestoppten Zustand befindet. Die Pipeline behält ihre Konfigurationseinstellungen, wie z. B. Kapazitätsgrenzen, Netzwerkeinstellungen und Optionen zur Protokollveröffentlichung, bei.

Der Neustart einer Pipeline dauert in der Regel mehrere Minuten.

Konsole

Um eine Pipeline zu starten

1. Melden Sie sich zu https://console.aws.amazon.com/aos/Hause bei der Amazon OpenSearch Service-Konsole an.
2. Wählen Sie im Navigationsbereich Pipeline und anschließend eine Pipeline aus. Sie können den Startvorgang von dieser Seite ausführen oder zur Detailseite für die Pipeline navigieren, die Sie starten möchten.
3. Wählen Sie für Aktionen die Option Pipeline starten aus.

AWS CLI

Zum Starten einer Pipeline über die rufen Sie den AWS CLI Befehl start--Pipeline mit den folgenden Parametern auf:

- `--pipeline-name`— der Name der Pipeline.

Example

```
aws osis start-pipeline --pipeline-name my-pipeline
```

OpenSearch Aufnahme-API

Um eine OpenSearch Ingestion-Pipeline mithilfe der OpenSearch Ingestion-API zu starten, rufen Sie den Vorgang mit dem StartPipelinefolgenden Parameter auf:

- `PipelineName`— der Name der Pipeline.

Löschen von Amazon OpenSearch Ingestion-Pipelines

Sie können eine Amazon OpenSearch Ingestion-Pipeline mithilfe der AWS Management Console, der oder der AWS CLI OpenSearch Ingestion-API löschen. Sie können eine Pipeline nicht löschen, wenn sie den Status oder hat. `Creating` `Updating`

Konsole

So löschen Sie eine Pipeline

1. Melden Sie sich zu https://console.aws.amazon.com/aos/Hause bei der Amazon OpenSearch Service-Konsole an.
2. Wählen Sie im linken Navigationsbereich Pipelines.
3. Wählen Sie die Pipeline aus, die Sie löschen möchten, und wählen Sie Aktionen, Löschen aus.
4. Bestätigen Sie den Löschvorgang und wählen Sie Delete (Löschen) aus.

CLI

Um eine Pipeline mit dem zu löschen AWS CLI, senden Sie eine Delete-Pipeline-Anfrage:

```
aws osis delete-pipeline --pipeline-name "my-pipeline"
```

OpenSearch Aufnahme-API

Um eine OpenSearch Ingestion-Pipeline mithilfe der OpenSearch Ingestion-API zu löschen, rufen Sie den Vorgang mit dem DeletePipelinefolgenden Parameter auf:

- `PipelineName`— der Name der Pipeline.

Unterstützte Plugins und Optionen für Amazon OpenSearch Ingestion-Pipelines

Amazon OpenSearch Ingestion unterstützt eine Teilmenge von Quellen, Prozessoren und Senken innerhalb von Open Source Data Prepper. OpenSearch Darüber hinaus gibt es einige Einschränkungen, die OpenSearch Ingestion den verfügbaren Optionen für jedes unterstützte Plugin auferlegt. In den folgenden Abschnitten werden die Plugins und die zugehörigen Optionen beschrieben, die OpenSearch Ingestion unterstützt.

> **Note**
>
> OpenSearch Ingestion unterstützt keine Puffer-Plugins, da es automatisch einen Standardpuffer konfiguriert. Sie erhalten einen Validierungsfehler, wenn Sie einen Puffer in Ihre Pipeline-Konfiguration aufnehmen.

Themen

- Unterstützte Plugins
- Stateless versus statusbehaftete Prozessoren
- Konfigurationsanforderungen und Einschränkungen

Unterstützte Plugins

OpenSearch Ingestion unterstützt die folgenden Data Prepper-Plugins:

Quellen:

- DocumentDB
- DynamoDB

- HTTP
- Kafka
- Kinesis
- OpenSearch
- OTel logs
- OTel Metriken
- OTel verfolgen
- S3

Prozessoren:

- Einträge hinzufügen
- Aggregate

- Anomaliedetektor
- AWS Lambda
- Eintragstyp konvertieren
- Werte kopieren
- CSV
- Date (Datum)
- Verzögerung
- Dekomprimieren
- Einträge löschen
- Sezieren
- Ereignisse löschen
- Verflachen
- Geo-IP
- Grok
- Schlüsselwert
- Liste zur Zuordnung
- Zeichenfolge in Kleinbuchstaben
- Karte zur Liste
- Ereignis mutieren (Reihe von Prozessoren)
- Zeichenfolge mutieren (Reihe von Prozessoren)
- Verschleiern
- OTel Metriken
- OTel Gruppe verfolgen
- OTel verfolgen
- Analysieren Sie Ion
- Analysieren Sie JSON
- Analysieren Sie XML
- Schlüssel umbenennen
- Routen

- Wählen Sie Einträge aus
- Service-Übersicht
- Veranstaltung aufteilen
- Zeichenfolge teilen
- Zeichenkettenkonverter
- Ersetzen Sie die Zeichenfolge
- Peer-Forwarder verfolgen
- Translate (Übersetzen)
- Zeichenfolge kürzen
- Kürzen
- Zeichenfolge in Großbuchstaben
- Benutzeragent
- Schreiben Sie JSON

Senkt:

- OpenSearch(unterstützt OpenSearch Service, OpenSearch Serverless und Elasticsearch 6.8 oder höher)
- S3

Sink-Codecs:

- Avro
- NDJSON
- JSON
- Parkett

Stateless versus statusbehaftete Prozessoren

Zustandslose Prozessoren führen Operationen wie Transformationen und Filterung durch, während statusbehaftete Prozessoren Operationen wie Aggregationen ausführen, die sich an das Ergebnis der vorherigen Ausführung erinnern. OpenSearch Ingestion unterstützt die Stateful-Prozessoren Aggregate und Service-MAP. Alle anderen unterstützten Prozessoren sind statuslos.

Für Pipelines, die nur statuslose Prozessoren enthalten, liegt die maximale Kapazitätsgrenze bei 96 Ingestion. OCUs Wenn eine Pipeline statusbehaftete Prozessoren enthält, beträgt die maximale Kapazitätsgrenze 48 Ingestion. OCUs Wenn für eine Pipeline jedoch die persistente Pufferung aktiviert ist, kann sie maximal 384 Ingestion haben, wenn sie nur statusfreie Prozessoren enthält, oder 192 OCUs Ingestion OCUs , wenn sie Stateful-Prozessoren enthält. Weitere Informationen finden Sie unter the section called “Skalierung von Pipelines”.

End-to-end Die Bestätigung wird nur für statuslose Prozessoren unterstützt. Weitere Informationen finden Sie unter the section called “End-to-end Bestätigung”.

Konfigurationsanforderungen und Einschränkungen

Sofern unten nicht anders angegeben, sind alle in der Data Prepper-Konfigurationsreferenz für die oben aufgeführten unterstützten Plugins beschriebenen Optionen in OpenSearch Ingestion-Pipelines zulässig. In den folgenden Abschnitten werden die Einschränkungen erläutert, die OpenSearch Ingestion bestimmten Plugin-Optionen auferlegt.

> **Note**
>
> OpenSearch Ingestion unterstützt keine Puffer-Plugins, da es automatisch einen Standardpuffer konfiguriert. Sie erhalten einen Validierungsfehler, wenn Sie einen Puffer in Ihre Pipeline-Konfiguration aufnehmen.

Viele Optionen werden intern von OpenSearch Ingestion konfiguriert und verwaltet, z. B. `authentication` und. `acm_certificate_arn` Andere Optionen, wie z. B. `thread_count` und, haben Auswirkungen auf die Leistung`request_timeout`, wenn sie manuell geändert werden. Daher werden diese Werte intern festgelegt, um eine optimale Leistung Ihrer Pipelines sicherzustellen.

Schließlich können einige Optionen nicht an OpenSearch Ingestion übergeben werden, z. B. `ism_policy_file` und`sink_template`, da es sich bei der Ausführung im Open-Source-Data Prepper um lokale Dateien handelt. Diese Werte werden nicht unterstützt.

Themen

- Allgemeine Pipeline-Optionen
- Grok-Prozessor
- HTTP-Quelle

- OpenSearch Sink
- OTel Metrik-Quelle, OTel Trace-Quelle und OTel Log-Quelle
- OTel Prozessor für Trace-Gruppen
- OTel Prozessor verfolgen
- Service-Map-Prozessor
- S3-Quelle

Allgemeine Pipeline-Optionen

Die folgenden allgemeinen Pipeline-Optionen werden von OpenSearch Ingestion festgelegt und in Pipeline-Konfigurationen nicht unterstützt:

- `workers`
- `delay`

Grok-Prozessor

Die folgenden Grok-Prozessoroptionen werden nicht unterstützt:

- `patterns_directories`
- `patterns_files_glob`

HTTP-Quelle

Für das HTTP-Quell-Plugin gelten die folgenden Anforderungen und Einschränkungen:

- Die `path` Option ist erforderlich. Der Pfad ist eine Zeichenfolge wie`/log/ingest`, die den URI-Pfad für die Protokollaufnahme darstellt. Dieser Pfad definiert den URI, den Sie verwenden, um Daten an die Pipeline zu senden. Beispiel, `https://log-pipeline.us-west-2.osis.amazonaws.com`*`/log/ingest`*. Der Pfad muss mit einem Schrägstrich (/) beginnen und kann die Sonderzeichen '-', '_', 'enthalten . 'und'/'sowie der `${pipelineName}` Platzhalter.
- Die folgenden HTTP-Quelloptionen werden von OpenSearch Ingestion festgelegt und in Pipeline-Konfigurationen nicht unterstützt:
  - `port`

- `ssl`
- `ssl_key_file`
- `ssl_certificate_file`
- `aws_region`
- `authentication`
- `unauthenticated_health_check`
- `use_acm_certificate_for_ssl`
- `thread_count`
- `request_timeout`
- `max_connection_count`
- `max_pending_requests`
- `health_check_service`
- `acm_private_key_password`
- `acm_certificate_timeout_millis`
- `acm_certificate_arn`

OpenSearch Sink

Das OpenSearchSink-Plugin hat die folgenden Anforderungen und Einschränkungen.

- Die `aws` Option ist erforderlich und muss die folgenden Optionen enthalten:
  - `sts_role_arn`
  - `region`
  - `hosts`
  - `serverless`(wenn es sich bei der Senke um eine OpenSearch serverlose Sammlung handelt)
- Die `sts_role_arn` Option muss für jede Senke innerhalb einer YAML-Definitionsdatei auf dieselbe Rolle verweisen.
- Die `hosts` Option muss einen OpenSearch Dienstdomänenendpunkt oder einen OpenSearch serverlosen Sammlungsendpunkt angeben. Sie können keinen benutzerdefinierten Endpunkt für eine Domäne angeben. Es muss sich um den Standardendpunkt handeln.
- Wenn es sich bei der `hosts` Option um einen serverlosen Erfassungsendpunkt handelt, müssen Sie die `serverless` Option auf `true` setzen. Wenn Ihre YAML-Definitionsdatei die `index_type`

Option enthält, muss sie außerdem auf gesetzt sein`management_disabled`, andernfalls schlägt die Validierung fehl.

- Die folgenden Optionen werden nicht unterstützt:
  - `username`
  - `password`
  - `cert`
  - `proxy`
  - `dlq_file`— Wenn Sie fehlgeschlagene Ereignisse in eine Warteschlange (Dead Letter Queue, DLQ) auslagern möchten, müssen Sie die `dlq` Option verwenden und einen S3-Bucket angeben.
  - `ism_policy_file`
  - `socket_timeout`
  - `template_file`
  - `insecure`

OTel Metrik-Quelle, OTel Trace-Quelle und OTel Log-Quelle

Für die Plug-ins „OTel Metrikquelle“, „OTel Trace-Quelle“ und „OTel Logquelle“ gelten die folgenden Anforderungen und Einschränkungen:

- Die `path` Option ist erforderlich. Der Pfad ist eine Zeichenfolge wie`/log/ingest`, die den URI-Pfad für die Protokollaufnahme darstellt. Dieser Pfad definiert den URI, den Sie verwenden, um Daten an die Pipeline zu senden. Beispiel, `https://log-pipeline.us-west-2.osis.amazonaws.com`*`/log/ingest`*. Der Pfad muss mit einem Schrägstrich (/) beginnen und kann die Sonderzeichen '-', '_', 'enthalten . 'und'/'sowie der `${pipelineName}` Platzhalter.
- Die folgenden Optionen werden von OpenSearch Ingestion festgelegt und in Pipeline-Konfigurationen nicht unterstützt:
  - `port`
  - `ssl`
  - `sslKeyFile`
  - `sslKeyCertChainFile`
  - `authentication`

- `unauthenticated_health_check`
- `useAcmCertForSSL`
- `unframed_requests`
- `proto_reflection_service`
- `thread_count`
- `request_timeout`
- `max_connection_count`
- `acmPrivateKeyPassword`
- `acmCertIssueTimeOutMillis`
- `health_check_service`
- `acmCertificateArn`
- `awsRegion`

OTel Prozessor für Trace-Gruppen

Für den OTel Trace-Gruppenprozessor gelten die folgenden Anforderungen und Einschränkungen:

- Die `aws` Option ist erforderlich und muss die folgenden Optionen enthalten:
  - `sts_role_arn`
  - `region`
  - `hosts`
- Die `sts_role_arn` Option gibt dieselbe Rolle an wie die Pipeline-Rolle, die Sie in der OpenSearch Senkenkonfiguration angeben.
- Die `insecure` Optionen `username`,`password`,`cert`, und werden nicht unterstützt.
- Die `aws_sigv4` Option ist erforderlich und muss auf „true“ festgelegt werden.
- Die `serverless` Option im OpenSearch Sink Plugin wird nicht unterstützt. Der Otel Trace Group Processor funktioniert derzeit nicht mit OpenSearch serverlosen Sammlungen.
- Die Anzahl der `otel_trace_group` Prozessoren im Pipeline-Konfigurationstext darf 8 nicht überschreiten.

OTel Prozessor verfolgen

Für den OTel Trace-Prozessor gelten die folgenden Anforderungen und Einschränkungen:

- Der Wert der `trace_flush_interval` Option darf 300 Sekunden nicht überschreiten.

Service-Map-Prozessor

Für den Service-MAP-Prozessor gelten die folgenden Anforderungen und Einschränkungen:

- Der Wert der `window_duration` Option darf 300 Sekunden nicht überschreiten.

S3-Quelle

Für das Quell-Plugin für S3 gelten die folgenden Anforderungen und Einschränkungen:

- Die `aws` Option ist erforderlich und muss `sts_role_arn` Optionen enthaltenregion.
- Der Wert der `records_to_accumulate` Option darf 200 nicht überschreiten.
- Der Wert der `maximum_messages` Option darf 10 nicht überschreiten.
- Wenn angegeben ist, muss die `disable_bucket_ownership_validation` Option auf „false“ festgelegt werden.
- Falls angegeben, muss die `input_serialization` Option auf gesetzt werdenparquet.

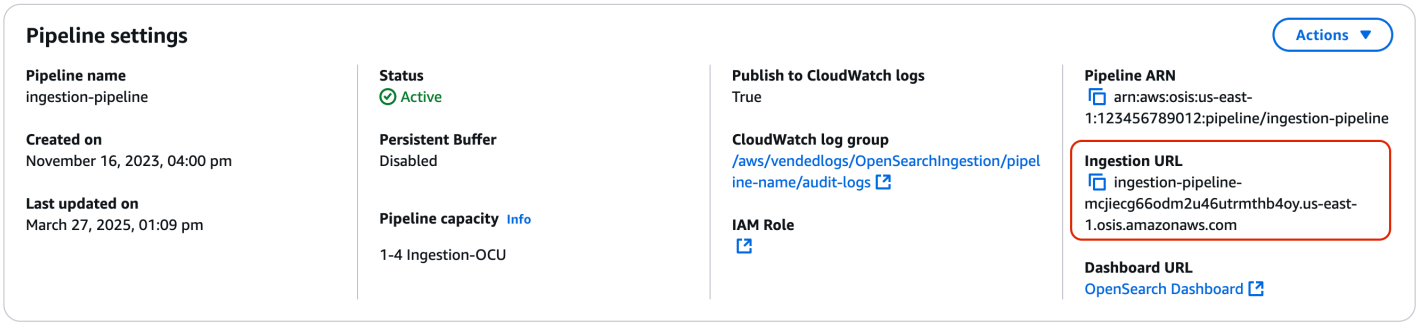
Integration von Amazon OpenSearch Ingestion-Pipelines mit anderen Services und Anwendungen

Um Daten erfolgreich in eine Amazon OpenSearch Ingestion-Pipeline aufzunehmen, müssen Sie Ihre Client-Anwendung (die Quelle) so konfigurieren, dass sie Daten an den Pipeline-Endpunkt sendet. Ihre Quelle könnten Clients wie Fluent Bit Logs, der OpenTelemetry Collector oder ein einfacher S3-Bucket sein. Die genaue Konfiguration ist für jeden Client unterschiedlich.

Die wichtigsten Unterschiede bei der Quellkonfiguration (im Vergleich zum direkten Senden von Daten an eine OpenSearch Dienstdomäne oder eine OpenSearch serverlose Sammlung) sind der AWS Dienstname (`osis`) und der Host-Endpunkt, der der Pipeline-Endpunkt sein muss.

Aufbau des Aufnahmeendpunkts

Um Daten in eine Pipeline aufzunehmen, senden Sie sie an den Aufnahmeendpunkt. Um die Aufnahme-URL zu finden, navigieren Sie zur Seite mit den Pipeline-Einstellungen und kopieren Sie die Aufnahme-URL.



Um den vollständigen Aufnahmeendpunkt für pullbasierte Quellen wie OTel Trace und OTel Metriken zu erstellen, fügen Sie der Aufnahme-URL den Aufnahmepfad aus Ihrer Pipeline-Konfiguration hinzu.

Nehmen wir zum Beispiel an, dass Ihre Pipeline-Konfiguration den folgenden Aufnahmepfad hat:



Der vollständige Aufnahmeendpunkt, den Sie in Ihrer Client-Konfiguration angeben, hat das folgende Format:. `https://ingestion-pipeline-abcdefg.us-east-1.osis.amazonaws.com/my/test_path`

Eine Aufnahmerolle erstellen

Alle Anfragen zur OpenSearch Datenerfassung müssen mit Signature Version 4 signiert sein. Der Rolle, die die Anfrage signiert, muss mindestens die Berechtigung für die `osis:Ingest` Aktion erteilt werden, sodass sie Daten an eine OpenSearch Ingestion-Pipeline senden kann.

Die folgende AWS Identity and Access Management (IAM-) Richtlinie ermöglicht es der entsprechenden Rolle beispielsweise, Daten an eine einzelne Pipeline zu senden:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
      "Effect": "Allow",
      "Action": "osis:Ingest",
      "Resource": "arn:aws:osis:region:account-id:pipeline/pipeline-name"
    }
  ]
}
```

> **Note**
>
> Um die Rolle für alle Pipelines zu verwenden, ersetzen Sie den ARN im `Resource` Element durch einen Platzhalter (*).

Bereitstellung von kontenübergreifendem Zugriff auf Datenerfassung

> **Note**
>
> Sie können kontenübergreifenden Zugriff auf die Erfassung nur für öffentliche Pipelines bereitstellen, nicht für VPC-Pipelines.

Möglicherweise müssen Sie Daten von einem anderen Konto in eine Pipeline aufnehmen AWS-Konto, z. B. von einem Konto, in dem Ihre Quellanwendung gespeichert ist. Wenn sich der Principal, der in eine Pipeline schreibt, in einem anderen Konto befindet als die Pipeline selbst, müssen Sie den Principal so konfigurieren, dass er einer anderen IAM-Rolle vertraut, um Daten in die Pipeline aufzunehmen.

Um kontoübergreifende Aufnahmeberechtigungen zu konfigurieren

1. Erstellen Sie die Aufnahmerolle mit der entsprechenden `osis:Ingest` Berechtigung (im vorherigen Abschnitt beschrieben) innerhalb derselben Pipeline. AWS-Konto Anweisungen finden Sie unter IAM-Rollen erstellen.
2. Fügen Sie der Aufnahmerolle eine Vertrauensrichtlinie hinzu, die es einem Principal in einem anderen Konto ermöglicht, sie zu übernehmen:

   JSON

   ```
   {
   ```

```
  "Version": "2012-10-17",
  "Statement": [{
     "Effect": "Allow",
     "Principal": {
       "AWS": "arn:aws:iam::external-account-id:root"
      },
     "Action": "sts:AssumeRole"
  }]
}
```

3. Konfigurieren Sie in dem anderen Konto Ihre Client-Anwendung (z. B. Fluent Bit) so, dass sie die Aufnahmerolle übernimmt. Damit dies funktioniert, muss das Anwendungskonto dem Anwendungsbenutzer oder der Rolle der Anwendung die Berechtigungen zur Übernahme der Aufnahmerolle gewähren.

   Das folgende Beispiel für eine identitätsbasierte Richtlinie ermöglicht es dem angehängten Prinzipal, `ingestion-role` vom Pipeline-Konto auszugehen:

   JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::account-id:role/ingestion-role"
    }
  ]
}
```

Die Client-Anwendung kann dann den AssumeRoleVorgang verwenden, um Daten anzunehmen `ingestion-role` und in die zugehörige Pipeline aufzunehmen.

Verwenden einer OpenSearch Ingestion-Pipeline mit Atlassian Services

Du kannst die Quell-Plugins von Atlassian Jira und Confluence verwenden, um Daten aus Atlassian-Services in deine Ingestion-Pipeline aufzunehmen. OpenSearch Diese Integrationen ermöglichen es dir, eine einheitliche, durchsuchbare Wissensdatenbank zu erstellen, indem du komplette Jira-

Projekte und Confluence-Bereiche synchronisierst und gleichzeitig die Relevanz in Echtzeit durch kontinuierliche Überwachung und automatische Synchronisation von Updates aufrechterhältst.

Integrating with Jira

Transformieren Sie Ihr Jira-Erlebnis mit leistungsstarken Funktionen für die kontextbezogene Suche, indem Sie Ihre Jira-Inhalte in integrieren. OpenSearch Mit dem Data Prepper Atlassian Jira Source Plugin kannst du eine einheitliche, durchsuchbare Wissensdatenbank erstellen, indem du komplette Jira-Projekte synchronisierst und gleichzeitig die Relevanz in Echtzeit durch kontinuierliche Überwachung und automatische Synchronisation von Updates sicherstellst. Diese Integration ermöglicht die Datensynchronisierung mit flexiblen Filteroptionen für bestimmte Projekte, Problemtypen und Status, sodass sichergestellt wird, dass nur die Informationen importiert werden, die du benötigst.

Um eine sichere und zuverlässige Konnektivität zu gewährleisten, unterstützt das Plugin mehrere Authentifizierungsmethoden, darunter die grundlegende API-Schlüsselauthentifizierung und OAuth2 -authentifizierung, mit der zusätzlichen Sicherheit, Anmeldeinformationen mithilfe eines in gespeicherten Geheimcodes zu verwalten AWS Secrets Manager. Es bietet auch eine automatische Token-Erneuerung für einen unterbrechungsfreien Zugriff und gewährleistet so einen kontinuierlichen Betrieb. Diese Integration basiert auf der API-Version 2 von Atlassian und ermöglicht es Teams, mithilfe OpenSearch der erweiterten Suchfunktionen wertvolle Erkenntnisse aus ihren Jira-Daten zu gewinnen.

Integrating with Confluence

Verbessern Sie das Wissensmanagement und die Möglichkeiten zur Zusammenarbeit in Ihrem Team, indem Sie Inhalte von Atlassian Confluence in OpenSearch das Confluence-Quell-Plugin von Data Prepper integrieren. Diese Integration ermöglicht es dir, ein zentrales, durchsuchbares Repository für kollektives Wissen zu erstellen und so die Informationssuche und die Teamproduktivität zu verbessern. Durch die Synchronisation von Confluence-Inhalten und die kontinuierliche Überwachung auf Updates stellt das Plugin sicher, dass Ihr OpenSearch Index erhalten bleibt und umfassend ist. up-to-date

Die Integration bietet flexible Filteroptionen, mit denen Sie Inhalte aus bestimmten Bereichen oder Seitentypen selektiv importieren und die synchronisierten Inhalte so an die Bedürfnisse Ihres Unternehmens anpassen können. Das Plugin unterstützt sowohl grundlegende API-Schlüssel- als auch OAuth2 Authentifizierungsmethoden mit der Option, Anmeldeinformationen sicher zu verwalten. AWS Secrets Manager Die automatische Token-Erneuerungsfunktion des Plugins gewährleistet einen unterbrechungsfreien Zugriff und einen reibungslosen Betrieb.

Diese Integration basiert auf der Confluence-API von Atlassian und ermöglicht es Teams, die erweiterten Suchfunktionen für ihre gesamten Confluence-Inhalte zu nutzen und OpenSearch so die Zugänglichkeit und Nutzung von Informationen innerhalb des Unternehmens zu verbessern.

Themen

- Voraussetzungen
- Konfigurieren Sie eine Pipeline-Rolle
- Konfiguration der Jira-Connector-Pipeline
- Konfiguration der Confluence-Connector-Pipeline
- Datenkonsistenz
- Einschränkungen
- Metriken CloudWatch für Atlassian-Konnektoren
- Eine Amazon OpenSearch Ingestion-Pipeline mithilfe von 2.0 mit Atlassian Jira oder Confluence verbinden OAuth

Voraussetzungen

Bevor du deine OpenSearch Ingestion-Pipeline erstellst, führe die folgenden Schritte durch:

1. Bereiten Sie die Anmeldeinformationen für Ihre Jira-Site vor, indem Sie eine der folgenden Optionen wählen. OpenSearch Für die Aufnahme ist nur die `ReadOnly` Autorisierung des Inhalts erforderlich.
   a. Option 1: API-Schlüssel — Melde dich bei deinem Atlassian-Konto an und verwende die Informationen im folgenden Thema, um deinen API-Schlüssel zu generieren:
      - Verwalte API-Token für dein Atlassian-Konto
   b. Option 2: OAuth2 — Melde dich bei deinem Atlassian-Konto an und verwende die Informationen in. the section called “Eine Amazon OpenSearch Ingestion-Pipeline mithilfe von 2.0 mit Atlassian Jira oder Confluence verbinden OAuth ”
2. Erstelle einen geheimen Schlüssel AWS Secrets Manager, um die im vorherigen Schritt erstellten Anmeldeinformationen zu speichern. Treffen Sie bei der Ausführung des Verfahrens die folgenden Optionen:
   - Als Secret-Typ wählen Sie Anderer Secret-Typ aus.
   - Erstellen Sie für Schlüssel/Wert-Paare je nach ausgewähltem Autorisierungstyp die folgenden Paare:

API key

```
{
   "username": user-name-usualy-email-id,
   "password": api-key
}
```

OAuth 2.0

```
{
   "clientId": client-id
   "clientSecret": client-secret
   "accessKey": access-key
   "refreshKey": refresh-key
}
```

Nachdem Sie das Secret erstellt haben, kopieren Sie den Amazon-Ressourcennamen (ARN) des Secrets. Sie werden ihn in die Richtlinie für Berechtigungen für Pipeline-Rollen aufnehmen.

Konfigurieren Sie eine Pipeline-Rolle

Der Rolle, die in der Pipeline übergeben wurde, muss die folgende Richtlinie zum Lesen und Schreiben an den im Abschnitt Voraussetzungen erstellten geheimen Schlüssel angehängt sein.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SecretReadWrite",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetResourcePolicy",
                "secretsmanager:GetSecretValue",
                "secretsmanager:DescribeSecret",
                "secretsmanager:PutSecretValue",
                "secretsmanager:ListSecretVersionIds"
            ],
            "Resource": "secret-arn-created-in-step-2"
```

```
        }
    ]
}
```

Der Rolle sollte außerdem eine Richtlinie für den Zugriff und das Schreiben auf die von Ihnen gewählte Senke zugewiesen sein. Wenn Sie beispielsweise OpenSearch als Datenspeicher wählen, sieht die Richtlinie etwa wie folgt aus:

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "OpenSearchWritePolicy",
            "Effect": "Allow",
            "Action": "aoss:*",
            "Resource": "aoss-collection-arn"
        }
    ]
}
```

Konfiguration der Jira-Connector-Pipeline

Du kannst einen vorkonfigurierten Atlassian Jira-Blueprint verwenden, um diese Pipeline zu erstellen. Weitere Informationen finden Sie unter the section called “Mit Blueprints arbeiten”.

Ersetzen Sie *placeholder values* durch Ihre Informationen.

```
version: "2"
extension:
  aws:
    secrets:
      jira-account-credentials:
        secret_id: "secret-arn"
        region: "secret-region"
        sts_role_arn: "arn:aws:iam::123456789012:role/Example-Role"
atlassian-jira-pipeline:
  source:
    jira:
```

```
      # We only support one host url for now
      hosts: ["jira-host-url"]
      acknowledgments: true
      authentication:
        # Provide one of the authentication method to use. Supported methods are
'basic' and 'oauth2'.
        # For basic authentication, password is the API key that you generate using
your jira account
        basic:
          username: ${{aws_secrets:jira-account-credentials:username}}
          password: ${{aws_secrets:jira-account-credentials:password}}
        # For OAuth2 based authentication, we require the following 4 key values stored
in the secret
        # Follow atlassian instructions at the below link to generate these keys.
        # https://developer.atlassian.com/cloud/confluence/oauth-2-3lo-apps/
        # If you are using OAuth2 authentication, we also require, write permission to
your AWS secret to
        # be able to write the renewed tokens back into the secret.
        # oauth2:
          # client_id: ${{aws_secrets:jira-account-credentials:clientId}}
          # client_secret: ${{aws_secrets:jira-account-credentials:clientSecret}}
          # access_token: ${{aws_secrets:jira-account-credentials:accessToken}}
          # refresh_token: ${{aws_secrets:jira-account-credentials:refreshToken}}
      filter:
        project:
          key:
            include:
              # This is not project name.
              # It is an alphanumeric project key that you can find under project
details in Jira.
              - "project-key"
              - "project-key"
            # exclude:
              # - "project-key"
              # - "project-key"
        issue_type:
          include:
            - "issue-type"
            # - "Story"
            # - "Bug"
            # - "Task"
          # exclude:
              # - "Epic"
        status:
```

```
          include:
            - "ticket-status"
            # - "To Do"
            # - "In Progress"
            # - "Done"
          # exclude:
            # - "Backlog"

  sink:
    - opensearch:
        # Provide an Amazon OpenSearch Service domain endpoint
        hosts: [ "https://search-mydomain-1a2a3a4a5a6a7a8a9a0a9a8a7a.us-
east-1.es.amazonaws.com" ]
        index: "index_${getMetadata(\"project\")}"
        # Ensure adding unique document id which is the unique ticket id in this case
        document_id: '${/id}'
        aws:
          # Provide a Role ARN with access to the domain. This role should have a trust
 relationship with osis-pipelines.amazonaws.com
          sts_role_arn: "arn:aws:iam::123456789012:role/Example-Role"
          # Provide the region of the domain.
          region: "us-east-1"
          # Enable the 'serverless' flag if the sink is an Amazon OpenSearch Serverless
 collection
          serverless: false
          # serverless_options:
            # Specify a name here to create or update network policy for the serverless
 collection
            # network_policy_name: "network-policy-name"
        # Enable the 'distribution_version' setting if the Amazon OpenSearch Service
 domain is of version Elasticsearch 6.x
        # distribution_version: "es6"
        # Enable and switch the 'enable_request_compression' flag if the default
 compression setting is changed in the domain.
        # See the section called “Komprimieren von HTTP-Anforderungen”
        # enable_request_compression: true/false
        # Optional: Enable the S3 DLQ to capture any failed requests in an S3 bucket.
 Delete this entire block if you don't want a DLQ.
        dlq:
          s3:
            # Provide an S3 bucket
            bucket: "your-dlq-bucket-name"
            # Provide a key path prefix for the failed requests
            # key_path_prefix: "kinesis-pipeline/logs/dlq"
```

```
            # Provide the region of the bucket.
            region: "us-east-1"
            # Provide a Role ARN with access to the bucket. This role should have a
 trust relationship with osis-pipelines.amazonaws.com
            sts_role_arn: "arn:aws:iam::123456789012:role/Example-Role"
```

Schlüssel zu den Attributen in der Jira-Quelle:

1. hosts: Ihre Jira-Cloud- oder On-Premises-URL. Im Allgemeinen sieht es so aus. `https://your-domain-name.atlassian.net/`
2. Bestätigungen: Um die Lieferung von Daten bis zur Senke zu garantieren.
3. Authentifizierung: Beschreibt, wie die Pipeline auf Ihre Jira-Instanz zugreifen soll. Wählen Sie `Basic` oder `0Auth2` und geben Sie die entsprechenden Schlüsselattribute an, die auf die Schlüssel in Ihrem AWS Geheimnis verweisen.
4. Filter: In diesem Abschnitt können Sie auswählen, welcher Teil Ihrer Jira-Daten extrahiert und synchronisiert werden soll.
   a. Projekt: Listet im `include` Abschnitt die Projektschlüssel auf, die Sie synchronisieren möchten. Andernfalls listen Sie die Projekte, die Sie ausschließen möchten, in dem `exclude` Abschnitt auf. Geben Sie jeweils nur eine der Optionen zum Einschließen oder Ausschließen an.
   b. issue_type: Bestimmte Problemtypen, die Sie synchronisieren möchten. Folgen Sie einem ähnlichen `exclude` Muster `include` oder einem Muster, das Ihren Bedürfnissen entspricht. Beachten Sie, dass Anlagen als Ankerlinks zum ursprünglichen Anhang angezeigt werden, der Inhalt des Anhangs jedoch nicht extrahiert wird.
   c. Status: Spezifischer Statusfilter, den Sie für die Datenextraktionsabfrage anwenden möchten. Wenn Sie angeben`include`, werden nur Tickets mit diesem Status synchronisiert. Wenn Sie dies angeben`exclude`, werden alle Tickets mit Ausnahme der Tickets mit dem angegebenen Status „Ausgeschlossen“ synchronisiert.

Konfiguration der Confluence-Connector-Pipeline

Du kannst einen vorkonfigurierten Atlassian Confluence-Blueprint verwenden, um diese Pipeline zu erstellen. Weitere Informationen finden Sie unter the section called “Mit Blueprints arbeiten”.

```
version: "2"
extension:
  aws:
    secrets:
```

```
      confluence-account-credentials:
        secret_id: "secret-arn"
        region: "secret-region"
        sts_role_arn: "arn:aws:iam::123456789012:role/Example-Role"
atlassian-confluence-pipeline:
  source:
    confluence:
      # We currently support only one host URL.
      hosts: ["confluence-host-url"]
      acknowledgments: true
      authentication:
        # Provide one of the authentication method to use. Supported methods are
 'basic' and 'oauth2'.
        # For basic authentication, password is the API key that you generate using
 your Confluence account
        basic:
          username: ${{aws_secrets:confluence-account-credentials:confluenceId}}
          password: ${{aws_secrets:confluence-account-
credentials:confluenceCredential}}
        # For OAuth2 based authentication, we require the following 4 key values stored
 in the secret
        # Follow atlassian instructions at the following link to generate these keys:
        # https://developer.atlassian.com/cloud/confluence/oauth-2-3lo-apps/
        # If you are using OAuth2 authentication, we also require write permission to
 your AWS secret to
        # be able to write the renewed tokens back into the secret.
        # oauth2:
          # client_id: ${{aws_secrets:confluence-account-credentials:clientId}}
          # client_secret: ${{aws_secrets:confluence-account-credentials:clientSecret}}
          # access_token: ${{aws_secrets:confluence-account-credentials:accessToken}}
          # refresh_token: ${{aws_secrets:confluence-account-credentials:refreshToken}}
      filter:
        space:
          key:
            include:
              # This is not space name.
              # It is a space key that you can find under space details in Confluence.
              - "space key"
              - "space key"
           # exclude:
             #  - "space key"
             #  - "space key"
        page_type:
          include:
```

```
            - "content type"
            # - "page"
            # - "blogpost"
            # - "comment"
         # exclude:
            # - "attachment"

  sink:
    - opensearch:
        # Provide an Amazon OpenSearch Service domain endpoint
        hosts: [ "https://search-mydomain-1a2a3a4a5a6a7a8a9a0a9a8a7a.us-
east-1.es.amazonaws.com" ]
         index: "index_${getMetadata(\"space\")}"
        # Ensure adding unique document id which is the unique ticket ID in this case.
        document_id: '${/id}'
        aws:
          # Provide the Amazon Resource Name (ARN) for a role with access to the
 domain. This role should have a trust relationship with osis-pipelines.amazonaws.com.
          sts_role_arn: "arn:aws:iam::123456789012:role/Example-Role"
          # Provide the Region of the domain.
          region: "us-east-1"
          # Enable the 'serverless' flag if the sink is an Amazon OpenSearch Serverless
 collection
          serverless: false
          # serverless_options:
            # Specify a name here to create or update network policy for the serverless
 collection.
            # network_policy_name: "network-policy-name"
        # Enable the 'distribution_version' setting if the Amazon OpenSearch Service
 domain is of version Elasticsearch 6.x
        # distribution_version: "es6"
        # Enable and switch the 'enable_request_compression' flag if the default
 compression setting is changed in the domain.
        # For more information, see the section called “Komprimieren von HTTP-
Anforderungen”.
        # enable_request_compression: true/false
        # Optional: Enable the S3 DLQ to capture any failed requests in an S3 bucket.
 Delete this entire block if you don't want a DLQ.
        dlq:
          s3:
            # Provide an S3 bucket
            bucket: "your-dlq-bucket-name"
            # Provide a key path prefix for the failed requests
            # key_path_prefix: "kinesis-pipeline/logs/dlq"
```

```
            # Provide the Rregion of the bucket.
            region: "us-east-1"
            # Provide the Amazon Resource Name (ARN) for a role with access to the
 bucket. This role should have a trust relationship with osis-pipelines.amazonaws.com
            sts_role_arn: "arn:aws:iam::123456789012:role/Example-Role"
```

Die wichtigsten Attribute in der Confluence-Quelle:

1. hosts: Ihre Confluence-Cloud- oder On-Premises-URL. Im Allgemeinen sieht es so aus `https://your-domain-name.atlassian.net/`
2. Bestätigungen: Um die Lieferung von Daten bis zur Senke zu garantieren.
3. Authentifizierung: Beschreibt, wie die Pipeline auf Ihre Confluence-Instanz zugreifen soll. Wählen Sie `Basic` oder `0Auth2` und geben Sie die entsprechenden Schlüsselattribute an, die auf die Schlüssel in Ihrem Secret verweisen. AWS
4. Filter: In diesem Abschnitt können Sie auswählen, welcher Teil Ihrer Confluence-Daten extrahiert und synchronisiert werden soll.
   a. Leertaste: Listet in dem Abschnitt die Leertaste auf, die `include` Sie synchronisieren möchten. Andernfalls listen Sie die Leerzeichen, die Sie ausschließen möchten, unter dem `exclude` Abschnitt auf. Geben Sie jeweils nur eine der Optionen zum Einschließen oder Ausschließen an.
   b. page_type: Bestimmte Seitentypen (wie Seite, Blogpost oder Anlagen), die du synchronisieren möchtest. Folgen Sie dem ähnlichen `exclude` Muster `include` oder dem Muster, das Ihren Bedürfnissen entspricht. Beachten Sie, dass Anlagen als Ankerlinks zum ursprünglichen Anhang angezeigt werden, der Inhalt des Anhangs jedoch nicht extrahiert wird.

Datenkonsistenz

Basierend auf den in der Pipeline-YAML-Pipeline angegebenen Filtern werden ausgewählte Projekte (oder Bereiche) einmal extrahiert und vollständig mit der Zielsenke synchronisiert. Anschließend erfasst die kontinuierliche Änderungsüberwachung die Änderungen, sobald sie auftreten, und aktualisiert die Daten in der Senke. Eine Ausnahme besteht darin, dass bei der Änderungsüberwachung nur `update` Aktionen `create` und keine `delete` Aktionen synchronisiert werden.

Einschränkungen

- Aktionen zum Löschen von Benutzern werden nicht synchronisiert. Daten, die einmal in der Senke aufgezeichnet wurden, verbleiben in der Senke. Aktualisierungen überschreiben den vorhandenen Inhalt mit neuen Änderungen, wenn die ID-Zuordnung in den Senkeneinstellungen angegeben ist.
- Lokale Instanzen, die ältere Versionen der Atlassian-Software verwenden und Folgendes nicht unterstützen, APIs sind mit dieser Quelle nicht kompatibel:
  - Jira Search API, Version 3
    - `rest/api/3/search`
    - `rest/api/3/issue`
  - Confluence
    - `wiki/rest/api/content/search`
    - `wiki/rest/api/content`
    - `wiki/rest/api/settings/systemInfo`

Metriken CloudWatch für Atlassian-Konnektoren

Typ: Metriken für den Jira-Konnektor

Quelle	Metrik	Metrik: Typ
acknowledgementSetSuccesses.count	Zähler	Wenn Bestätigungen aktiviert sind, gibt diese Metrik die Anzahl der erfolgreich synchronisierten Tickets an.
acknowledgementSetFailures.count	Zähler	Wenn Bestätigungen aktiviert sind, gibt diese Metrik die Anzahl der Tickets an, die nicht synchronisiert werden konnten.
CrawlingTime.avg	Timer	Die Zeit, die benötigt wurde, um alle neuen Änderungen zu durchforsten.

Quelle	Metrik	Metrik: Typ
ticketFetchLatency.avg	Timer	Die durchschnittliche Latenz der API zum Abrufen von Tickets.
ticketFetchLatency.max	Timer	Die maximale Latenz der API zum Abrufen von Tickets.
Anzahl der angeforderten Tickets	Zähler	Anzahl der gestellten Anfragen zum Abrufen von Tickets.
ticketRequestedFailed. Anzahl	Zähler	Anzahl der Anfragen zum Abrufen von Tickets ist fehlgeschlagen.
ticketRequestedSuccess.count	Zähler	Anzahl der erfolgreichen Anfragen zum Abrufen von Tickets.
searchCallLatency. avg	Timer	Durchschnittliche Latenz bei Aufrufen der Such-API.
searchCallLatency. max	Timer	Maximale Latenz bei Aufrufen der Such-API.
searchResultsFound. Anzahl	Zähler	Anzahl der bei einem bestimmten Suchaufruf gefundenen Artikel.

Quelle	Metrik	Metrik: Typ
searchRequestFailed. Anzahl	Zähler	Anzahl fehlgeschlagener Such-API-Aufrufe.
authFailures.Count	Zähler	Anzahl der Authentifizierungsfehler.

Typ: Metriken für den Confluence-Konnektor

Quelle	Metrik	Metrik: Typ
acknowledgementSetSuccesses.count	Zähler	Wenn Bestätigungen aktiviert sind, gibt diese Metrik die Anzahl der erfolgreich synchronisierten Seiten an.
acknowledgementSetFailures.count	Zähler	Wenn Bestätigungen aktiviert sind, gibt diese Metrik die Anzahl der Seiten an, die nicht synchronisiert werden konnten.
CrawlingTime.avg	Timer	Die Zeit, die benötigt wurde, um alle neuen Änderungen zu durchforsten.
pageFetchLatency.avg	Timer	API-Latenz beim Abrufen von Inhalten (durchschnittlich).
pageFetchLatency.max	Timer	API-Latenz beim Abrufen von Inhalten (maximal).
Anzahl der angeforde	Zähler	Anzahl der Aufrufe der API zum Abrufen von Inhalten.

Quelle	Metrik	Metrik: Typ
rten Seiten		
pageRequestFailed. Anzahl	Zähler	Anzahl der fehlgeschlagenen Anfragen der API zum Abrufen von Inhalten.
pageRequestedSuccess.count	Zähler	Anzahl erfolgreicher Anfragen der API zum Abrufen von Inhalten.
searchCallLatency. avg	Timer	Durchschnittliche Latenz bei Aufrufen der Such-API.
searchCallLatency. max	Timer	Max. Latenz bei Aufrufen der Such-API
searchResultsFound . Anzahl	Zähler	Anzahl der bei einem bestimmten Suchaufruf gefundenen Artikel.
searchRequestsFailed. Anzahl	Zähler	Anzahl fehlgeschlagener Such-API-Aufrufe.
authFailures.Count	Zähler	Anzahl der Authentifizierungsfehler.

Eine Amazon OpenSearch Ingestion-Pipeline mithilfe von 2.0 mit Atlassian Jira oder Confluence verbinden OAuth

Mithilfe der Informationen in diesem Thema können Sie mithilfe der 2.0-Authentifizierung eine Amazon OpenSearch Ingestion-Pipeline konfigurieren und mit einem Jira- oder Confluence-Konto

verbinden. OAuth Führe diese Aufgabe aus, wenn du die the section called “Voraussetzungen” für die Nutzung einer OpenSearch Ingestion-Pipeline mit Atlassian Services erstellst, dich aber dafür entscheidest, keine API-Schlüsselanmeldedaten zu verwenden.

Themen

- Erstelle eine 2.0-Integrations-App OAuth
- Ein Atlassian Developer-Zugriffstoken generieren und aktualisieren

Erstelle eine 2.0-Integrations-App OAuth

Verwende das folgende Verfahren, um dir bei der Erstellung einer OAuth 2.0-Integrations-App auf der Atlassian Developer-Website zu helfen.

So erstellst du eine OAuth 2.0-Integrations-App

1. Melde dich bei deinem Atlassian Developer-Konto unter myapps/ an https://developer.atlassian.com/console/.
2. Wähle Create, 2.0-Integration. OAuth
3. Geben Sie unter Name einen Namen ein, um den Zweck der App zu identifizieren.
4. Aktiviere das Kontrollkästchen Ich stimme zu, an die Nutzungsbedingungen von Atlassian für Entwickler gebunden zu sein, und wähle dann Erstellen aus.
5. Wähle in der linken Navigationsleiste Autorisierung und dann Hinzufügen aus.
6. Geben Sie für Callback-URL eine beliebige URL ein, z. B. **`https://www.amazon.com`** oder**`https://www.example.com`**, und wählen Sie dann Änderungen speichern aus.
7. Wählen Sie in der linken Navigationsleiste die Seite „Berechtigungen“ und dann in der Zeile für Jira API die Option Hinzufügen und dann „Konfigurieren“ aus. Wählen Sie alle Leseberechtigungen für Classic Scopes aus (Liste unten) und wählen Sie dann Speichern
8. Wählen Sie die Registerkarte Granular Scopes und dann Edit Scopes aus, um das Dialogfeld „Jira-API bearbeiten“ zu öffnen.
9. Wählen Sie die Berechtigungen für das Quell-Plugin aus, das Sie verwenden:

   Jira

```
read:audit-log:jira
read:issue:jira
read:issue-meta:jira
read:attachment:jira
```

```
read:comment:jira
read:comment.property:jira
read:field:jira
read:field.default-value:jira
read:field.option:jira
read:field-configuration-scheme:jira
read:field-configuration:jira
read:issue-link:jira
read:issue-link-type:jira
read:issue-link-type:jira
read:issue.remote-link:jira
read:issue.property:jira
read:resolution:jira
read:issue-details:jira
read:issue-type:jira
read:issue-worklog:jira
read:issue-field-values:jira
read:issue.changelog:jira
read:issue.transition:jira
read:issue.vote:jira
read:jira-expressions:jira
```

Confluence

```
read:content:confluence
read:content-details:confluence
read:space-details:confluence
read:audit-log:confluence
read:page:confluence
read:blogpost:confluence
read:custom-content:confluence
read:comment:confluence
read:space:confluence
read:space.property:confluence
read:space.setting:confluence
read:content.property:confluence
read:content.metadata:confluence
read:task:confluence
read:whiteboard:confluence
read:app-data:confluence
manage:confluence-configuration
```

10. Wählen Sie Speichern.

Weitere Informationen findest du auf der Atlassian Developer-Website unter Implementierung von OAuth 2.0 (3LO) und Bestimmung der für einen Vorgang erforderlichen Bereiche.

Ein Atlassian Developer-Zugriffstoken generieren und aktualisieren

Verwende das folgende Verfahren, um dir bei der Generierung und Aktualisierung eines Atlassian Developer-Zugriffstoken auf der Atlassian Developer-Website zu helfen.

So generierst und aktualisierst du ein Jira-Zugriffstoken

1. Melde dich bei deinem Atlassian Developer-Konto unter myapps/ an. https://developer.atlassian.com/console/
2. Wähle die App aus, in der du sie erstellt hast. the section called “Erstelle eine 2.0-Integrations-App OAuth ”
3. Wählen Sie in der linken Navigationsleiste Autorisierung aus.
4. Kopiere den detaillierten URL-Wert für die Atlassian-API-Autorisierung unten auf der Seite und füge ihn in den Texteditor deiner Wahl ein.

   Das Format der URL lautet wie folgt:

   ```
   https://auth.atlassian.com/authorize?
   audience=api.atlassian.com
   &client_id=YOUR_CLIENT_ID
   &scope=REQUESTED_SCOPE%20REQUESTED_SCOPE_TWO
   &redirect_uri=https://YOUR_APP_CALLBACK_URL
   &state=YOUR_USER_BOUND_VALUE
   &response_type=code
   &prompt=consent
   ```

5. Ändern Sie für `state=YOUR_USER_BOUND_VALUE` den Parameterwert einen beliebigen Wert, z. B. state=“**`sample_text`**“.

   Weitere Informationen finden Sie unter Wofür wird der State-Parameter verwendet? auf der Atlassian Developer-Website.

6. Beachte, dass in `scope` diesem Abschnitt die detaillierten Bereiche aufgeführt sind, die du in einer früheren Aufgabe ausgewählt hast. Beispiel: `scope=read%3Ajira-work%20read%3Ajira-user%20offline_access`

   `offline_access`gibt an, dass Sie eine generieren möchten. `refresh_token`

7. Öffnen Sie ein Webbrowser-Fenster und geben Sie die Autorisierungs-URL, die Sie kopiert haben, in die Adressleiste des Browserfensters ein.
8. Wenn die Zielseite geöffnet wird, überprüfen Sie, ob die Informationen korrekt sind, und wählen Sie dann Akzeptieren, um auf Ihre Jira- oder Confluence-Homepage weitergeleitet zu werden.
9. Nachdem die Homepage geladen wurde, kopieren Sie die URL dieser Seite. Sie enthält den Autorisierungscode für Ihre Anwendung. Sie verwenden diesen Code, um Ihr Zugriffstoken zu generieren. Der gesamte Abschnitt danach `code=` ist der Autorisierungscode.
10. Verwenden Sie den folgenden cURL-Befehl, um das Zugriffstoken zu generieren. Ersetzen Sie *`placeholder values`* durch Ihre Informationen.

> **Tip**
>
> Sie können auch einen Drittanbieterdienst wie Postman verwenden.

```
curl --request POST --url 'https://auth.atlassian.com/oauth/token' \
--header 'Content-Type: application/json' \
--data '{"grant_type": "authorization_code",
"client_id": "YOUR_CLIENT_ID",
"client_secret": "YOUR_CLIENT_SECRET",
"code": "AUTHORIZATION_CODE",
"redirect_uri": "YOUR_CALLBACK_URL"}'
```

Die Antwort auf diesen Befehl enthält die Werte für `access_code` und`refresh_token`.

Verwenden einer OpenSearch Ingestion-Pipeline mit Amazon DynamoDB

Sie können das DynamoDB-Plug-In verwenden, um Tabellenereignisse wie Erstellungen, Aktualisierungen und Löschungen an Amazon OpenSearch Service-Domains und Amazon OpenSearch Serverless-Sammlungen zu streamen. Die Pipeline verwendet Change Data Capture (CDC) für hochskaliertes Streaming mit niedriger Latenz.

Sie können DynamoDB-Daten mit oder ohne vollständigen Anfangssnapshot verarbeiten.

- Mit einem vollständigen Snapshot — DynamoDB verwendet point-in-time Recovery (PITR), um ein Backup zu erstellen und es auf Amazon S3 hochzuladen. OpenSearch Ingestion indexiert den Snapshot dann in einem oder mehreren Indizes. OpenSearch Um die Konsistenz

aufrechtzuerhalten, synchronisiert die Pipeline alle DynamoDB-Änderungen mit. OpenSearch Für diese Option müssen Sie sowohl PITR- als auch DynamoDB Streams aktivieren.

- Ohne Snapshot — OpenSearch Ingestion streamt nur neue DynamoDB-Ereignisse. Wählen Sie diese Option, wenn Sie bereits über einen Snapshot verfügen oder Echtzeit-Streaming ohne historische Daten benötigen. Für diese Option müssen Sie nur DynamoDB Streams aktivieren.

Weitere Informationen finden Sie unter DynamoDB Zero-ETL-Integration mit Amazon OpenSearch Service im Entwicklerhandbuch.Amazon DynamoDB

Themen

- Voraussetzungen
- Schritt 1: Konfigurieren Sie die Pipeline-Rolle
- Schritt 2: Erstellen Sie die Pipeline
- Datenkonsistenz
- Datentypen zuordnen
- Einschränkungen
- Empfohlene CloudWatch Alarme für DynamoDB

Voraussetzungen

Um Ihre Pipeline einzurichten, benötigen Sie eine DynamoDB-Tabelle mit aktivierten DynamoDB Streams. Ihr Stream sollte den Stream-View-Typ verwenden. `NEW_IMAGE` OpenSearch Ingestion-Pipelines können jedoch auch Ereignisse streamen, `NEW_AND_OLD_IMAGES` sofern dieser Stream-View-Typ zu Ihrem Anwendungsfall passt.

Wenn Sie Snapshots verwenden, müssen Sie auch die point-in-time Wiederherstellung für Ihre Tabelle aktivieren. Weitere Informationen finden Sie unter Erstellen einer Tabelle, Aktivieren der point-in-time Wiederherstellung und Aktivieren eines Streams im Amazon DynamoDB DynamoDB-Entwicklerhandbuch.

Schritt 1: Konfigurieren Sie die Pipeline-Rolle

Nachdem Sie Ihre DynamoDB-Tabelle eingerichtet haben, richten Sie die Pipeline-Rolle ein, die Sie in Ihrer Pipeline-Konfiguration verwenden möchten, und fügen Sie der Rolle die folgenden DynamoDB-Berechtigungen hinzu:

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "allowRunExportJob",
            "Effect": "Allow",
            "Action": [
                "dynamodb:DescribeTable",
                "dynamodb:DescribeContinuousBackups",
                "dynamodb:ExportTableToPointInTime"
            ],
            "Resource": [
                "arn:aws:dynamodb:region:account-id:table/my-table"
            ]
        },
        {
            "Sid": "allowCheckExportjob",
            "Effect": "Allow",
            "Action": [
                "dynamodb:DescribeExport"
            ],
            "Resource": [
                "arn:aws:dynamodb:region:account-id:table/my-table/export/*"
            ]
        },
        {
            "Sid": "allowReadFromStream",
            "Effect": "Allow",
            "Action": [
                "dynamodb:DescribeStream",
                "dynamodb:GetRecords",
                "dynamodb:GetShardIterator"
            ],
            "Resource": [
                "arn:aws:dynamodb:region:account-id:table/my-table/stream/*"
            ]
        },
        {
            "Sid": "allowReadAndWriteToS3ForExport",
            "Effect": "Allow",
            "Action": [
```

```
                "s3:GetObject",
                "s3:AbortMultipartUpload",
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Resource": [
                "arn:aws:s3:::my-bucket/export-folder/*"
            ]
        }
    ]
}
```

Sie können auch einen vom AWS KMS Kunden verwalteten Schlüssel verwenden, um die Exportdatendateien zu verschlüsseln. Um die exportierten Objekte zu entschlüsseln, geben Sie `s3_sse_kms_key_id` für die Schlüssel-ID in der Exportkonfiguration der Pipeline das folgende Format an:. `arn:aws:kms:region:account-id:key/my-key-id` Die folgende Richtlinie umfasst die erforderlichen Berechtigungen für die Verwendung eines vom Kunden verwalteten Schlüssels:

```
{
    "Sid": "allowUseOfCustomManagedKey",
    "Effect": "Allow",
    "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt"
    ],
    "Resource": arn:aws:kms:region:account-id:key/my-key-id
}
```

Schritt 2: Erstellen Sie die Pipeline

Anschließend können Sie eine OpenSearch Ingestion-Pipeline wie die folgende konfigurieren, die DynamoDB als Quelle angibt. Diese Beispielpipeline nimmt Daten aus `table-a` dem PITR-Snapshot auf, gefolgt von Ereignissen aus DynamoDB Streams. Die Startposition von `LATEST` gibt an, dass die Pipeline die neuesten Daten aus DynamoDB Streams lesen soll.

```
version: "2"
cdc-pipeline:
  source:
    dynamodb:
```

```
    tables:
    - table_arn: "arn:aws:dynamodb:region:account-id:table/table-a"
      export:
        s3_bucket: "my-bucket"
        s3_prefix: "export/"
      stream:
        start_position: "LATEST"
    aws:
      region: "us-east-1"
sink:
- opensearch:
    hosts: ["https://search-mydomain.region.es.amazonaws.com"]
    index: "${getMetadata(\"table-name\")}"
    index_type: custom
    normalize_index: true
    document_id: "${getMetadata(\"primary_key\")}"
    action: "${getMetadata(\"opensearch_action\")}"
    document_version: "${getMetadata(\"document_version\")}"
    document_version_type: "external"
```

Sie können einen vorkonfigurierten DynamoDB-Blueprint verwenden, um diese Pipeline zu erstellen. Weitere Informationen finden Sie unter the section called “Mit Blueprints arbeiten”.

Datenkonsistenz

OpenSearch Die Datenaufnahme unterstützt end-to-end die Bestätigung, um die Datenbeständigkeit sicherzustellen. Wenn eine Pipeline Snapshots oder Streams liest, erstellt sie dynamisch Partitionen für die Parallelverarbeitung. Die Pipeline markiert eine Partition als abgeschlossen, wenn sie nach der Aufnahme aller Datensätze in der OpenSearch Domäne oder Sammlung eine Bestätigung erhält.

Wenn Sie Daten in eine OpenSearch serverlose Suchsammlung aufnehmen möchten, können Sie in der Pipeline eine Dokument-ID generieren. Wenn Sie Daten in eine OpenSearch serverlose Zeitreihensammlung aufnehmen möchten, beachten Sie, dass die Pipeline keine Dokument-ID generiert.

Eine OpenSearch Ingestion-Pipeline ordnet außerdem eingehende Ereignisaktionen den entsprechenden Massenindizierungsaktionen zu, um das Ingestieren von Dokumenten zu erleichtern. Dadurch bleiben die Daten konsistent, sodass jede Datenänderung in DynamoDB mit den entsprechenden Dokumentänderungen in abgeglichen wird. OpenSearch

Datentypen zuordnen

OpenSearch Service ordnet Datentypen in jedem eingehenden Dokument dynamisch dem entsprechenden Datentyp in DynamoDB zu. Die folgende Tabelle zeigt, wie OpenSearch Service verschiedene Datentypen automatisch zuordnet.

Datentyp	OpenSearch	DynamoDB
Anzahl	OpenSearch ordnet numerische Daten automatisch zu. Wenn es sich bei der Zahl um eine ganze Zahl OpenSearch handelt, wird sie einem langen Wert zugeordnet. Wenn es sich bei der Zahl um eine Bruchzahl handelt, wird OpenSearch sie einem Gleitkommawert zugeordnet. OpenSearch ordnet verschiedene Attribute dynamisch auf der Grundlage des ersten gesendeten Dokuments zu. Wenn Sie in DynamoDB eine Mischung aus Datentypen für dasselbe Attribut haben, z. B. sowohl eine ganze Zahl als auch eine Bruchzahl, schlägt die Zuordnung möglicherweise fehl. Wenn Ihr erstes Dokument beispielsweise ein Attribut hat, das eine ganze Zahl ist, und ein späteres Dokument dasselbe Attribut wie eine Bruchzahl hat, OpenSearch kann das zweite Dokument nicht aufgenommen werden. In diesen Fällen sollten Sie eine explizite Zuordnungsvorlage bereitstellen, z. B. die folgende: `{ "template": {`	DynamoDB unterstützt Zahlen.

Datentyp	OpenSearch	DynamoDB

	<pre>"mappings": {
	"properties": {
	"MixedNumberAttribute": {
	"type": "float"
	}
	}
	}
	}
	}</pre>
	Wenn Sie doppelte Genauigke it benötigen, verwenden Sie eine Feldzuordnung vom Typ Zeichenfo lge. Es gibt keinen entsprechenden numerischen Typ, der eine Genauigkeit von 38 Ziffern unterstützt. OpenSearch	

Zahlensat z	OpenSearch ordnet einen Zahlensatz automatisch einem Array von Langwerte n oder Gleitkommawerten zu. Wie bei den Skalarzahlen hängt dies davon ab, ob es sich bei der ersten aufgenomm enen Zahl um eine ganze Zahl oder um eine Bruchzahl handelt. Sie können Zuordnungen für Zahlensätze auf die gleiche Weise bereitstellen, wie Sie skalare Zeichenketten zuordnen.	DynamoDB unterstützt Typen, die Gruppen von Zahlen darstellen.

Datentyp	OpenSearch	DynamoDB
String	OpenSearch ordnet Zeichenkettenwerte automatisch als Text zu. In einigen Situationen, z. B. bei Aufzählungswerten, können Sie sie dem Schlüsselworttyp zuordnen. Das folgende Beispiel zeigt, wie ein benanntes DynamoDB-Attribut einem Schlüsselwort `PartType` zugeordnet wird OpenSearch . `{ "template": { "mappings": { "properties": { "PartType": { "type": "keyword" } } } } }`	DynamoDB unterstützt Zeichenketten.
Zeichenkettensatz	OpenSearch ordnet einen Zeichenkettensatz automatisch einem Zeichenketten-Array zu. Sie können Zuordnungen für Zeichenkettensätze auf die gleiche Weise bereitstellen, wie Sie skalare Zeichenketten zuordnen.	DynamoDB unterstützt Typen, die Sätze von Zeichenketten darstellen.

Datentyp	OpenSearch	DynamoDB
Binär	OpenSearch ordnet Binärdaten automatisch als Text zu. Sie können ein Mapping bereitstellen, in das Sie diese als Binärfelder schreiben können OpenSearch. Das folgende Beispiel zeigt, wie ein benanntes DynamoDB-Attribut einem `ImageData` OpenSearch Binärfeld zugeordnet wird. `{ "template": { "mappings": { "properties": { "ImageData": { "type": "binary" } } } } }`	DynamoDB unterstützt binäre Typattribute.
Binärer Satz	OpenSearch ordnet eine Binärmenge automatisch einem Array von Binärdaten als Text zu. Sie können Zuordnungen für Zahlensätze auf die gleiche Weise bereitstellen, wie Sie skalare Binärwerte zuordnen.	DynamoDB unterstützt Typen, die Sätze von Binärwerten darstellen.
Boolesch	OpenSearch ordnet einen booleschen DynamoDB-Typ einem booleschen Typ zu. OpenSearch	DynamoDB unterstützt Attribute vom Typ Boolean.

Datentyp	OpenSearch	DynamoDB
Null	OpenSearch kann Dokumente mit dem DynamoDB-Nulltyp aufnehmen. Es speichert den Wert als Nullwert im Dokument. Für diesen Typ gibt es keine Zuordnung, und dieses Feld ist weder indexiert noch durchsuchbar. Wenn derselbe Attributname für einen Null-Typ verwendet wird und später zu einem anderen Typ, wie z. B. einer Zeichenfolge, geändert OpenSearch wird, wird eine dynamische Zuordnung für den ersten Wert, der nicht Null ist, erstellt. Nachfolgende Werte können immer noch DynamoDB-Nullwerte sein.	DynamoDB unterstützt Attribute vom Typ Null.

Datentyp	OpenSearch	DynamoDB
Zuordnung	OpenSearch ordnet DynamoDB-Zuordnungsattribute verschachtelten Feldern zu. Dieselben Zuordnungen gelten für ein verschachteltes Feld. Das folgende Beispiel ordnet eine Zeichenfolge in einem verschachtelten Feld einem Schlüsselworttyp in zu: OpenSearch `{ "template": { "mappings": { "properties": { "AdditionalDescriptions": { "properties": { "PartType": { "type": "keyword" } } } } } } }`	DynamoDB unterstützt Map-Typ-Attribute.

Datentyp	OpenSearch	DynamoDB
Auflisten	OpenSearch liefert unterschiedliche Ergebnisse für DynamoDB-Listen, je nachdem, was in der Liste steht. Wenn eine Liste alle Skalartypen desselben Typs enthält (z. B. eine Liste aller Zeichenketten), wird die Liste als Array dieses Typs OpenSearch aufgenommen. Dies funktioniert für die Typen Zeichenfolge, Zahl, Boolean und Null. Die Einschränkungen für jeden dieser Typen sind dieselben wie die Einschränkungen für einen Skalar dieses Typs. Sie können auch Zuordnungen für Kartenlisten bereitstellen, indem Sie dieselbe Zuordnung verwenden, die Sie für eine Karte verwenden würden. Sie können keine Liste mit gemischten Typen bereitstellen.	DynamoDB unterstützt Listentypattribute.

Datentyp	OpenSearch	DynamoDB
Einstellen	OpenSearch liefert unterschiedliche Ergebnisse für DynamoDB-Sets, je nachdem, was in der Gruppe enthalten ist. Wenn ein Satz alle Skalartypen desselben Typs enthält (z. B. eine Menge aller Zeichenketten), wird die Menge als Array dieses Typs OpenSearch aufgenommen. Dies funktioniert für die Typen Zeichenfolge, Zahl, Boolean und Null. Die Einschränkungen für jeden dieser Typen sind dieselben wie die Einschränkungen für einen Skalar dieses Typs. Sie können auch Zuordnungen für Kartengruppen bereitstellen, indem Sie dieselbe Zuordnung verwenden, die Sie für eine Karte verwenden würden. Sie können keinen Satz gemischter Typen bereitstellen.	DynamoDB unterstützt Typen, die Mengen darstellen.

Wir empfehlen, dass Sie die Dead-Letter-Warteschlange (DLQ) in Ihrer Ingestion-Pipeline konfigurieren. OpenSearch Wenn Sie die Warteschlange konfiguriert haben, sendet OpenSearch Service alle fehlgeschlagenen Dokumente, die aufgrund von Fehlern bei der dynamischen Zuordnung nicht aufgenommen werden konnten, an die Warteschlange.

Falls automatische Zuordnungen fehlschlagen, können Sie `template_type` und `template_content` in Ihrer Pipeline-Konfiguration verwenden, um explizite Zuordnungsregeln zu definieren. Alternativ können Sie Zuordnungsvorlagen direkt in Ihrer Suchdomain oder Sammlung erstellen, bevor Sie die Pipeline starten.

Einschränkungen

Beachten Sie die folgenden Einschränkungen, wenn Sie eine OpenSearch Ingestion-Pipeline für DynamoDB einrichten:

- Die OpenSearch Ingestion-Integration mit DynamoDB unterstützt derzeit keine regionsübergreifende Aufnahme. Ihre DynamoDB-Tabelle und die OpenSearch Ingestion-Pipeline müssen identisch sein. AWS-Region
- Ihre DynamoDB-Tabelle und die OpenSearch Ingestion-Pipeline müssen identisch sein. AWS-Konto
- Eine OpenSearch Ingestion-Pipeline unterstützt nur eine DynamoDB-Tabelle als Quelle.
- DynamoDB Streams speichert Daten nur bis zu 24 Stunden in einem Protokoll. Wenn die Aufnahme von einem ersten Snapshot einer großen Tabelle 24 Stunden oder länger dauert, kommt es zu einem anfänglichen Datenverlust. Um diesen Datenverlust zu minimieren, schätzen Sie die Größe der Tabelle und konfigurieren Sie die entsprechenden Recheneinheiten der OpenSearch Datenerfassungspipelines.

Empfohlene CloudWatch Alarme für DynamoDB

Die folgenden CloudWatch Metriken werden für die Überwachung der Leistung Ihrer Datenerfassungspipeline empfohlen. Mithilfe dieser Metriken können Sie die Menge der im Rahmen von Exporten verarbeiteten Daten, die Anzahl der aus Streams verarbeiteten Ereignisse, die Fehler bei der Verarbeitung von Exporten und Stream-Ereignissen sowie die Anzahl der Dokumente, die an das Ziel geschrieben wurden, ermitteln. Sie können CloudWatch Alarme einrichten, um eine Aktion auszuführen, wenn eine dieser Metriken für einen bestimmten Zeitraum einen bestimmten Wert überschreitet.

Metrik	Beschreibung
`dynamodb-pipeline.BlockingBuffer.bufferUsage.value`	Gibt an, wie viel Puffer genutzt wird.
`dynamodb-pipeline.dynamodb.activeExportS3ObjectConsumers.value`	Zeigt die Gesamtzahl derjenigen an OCUs , die aktiv Amazon S3 S3-Objekte für den Export verarbeiten.

Metrik	Beschreibung
dynamodb-pipeline.dynamodb.bytesProcessed.count	Anzahl der aus der DynamoDB-Quelle verarbeiteten Byte.
dynamodb-pipeline.dynamodb.changeEventsProcessed.count	Anzahl der aus dem DynamoDB-Stream verarbeiteten Änderungsereignisse.
dynamodb-pipeline.dynamodb.changeEventsProcessingErrors.count	Anzahl der Fehler aufgrund von Änderungsereignissen, die von DynamoDB verarbeitet wurden.
dynamodb-pipeline.dynamodb.exportJobFailure.count	Anzahl der fehlgeschlagenen Übermittlungsversuche für Exportaufträge.
dynamodb-pipeline.dynamodb.exportJobSuccess.count	Anzahl der erfolgreich eingereichten Exportaufträge.
dynamodb-pipeline.dynamodb.exportRecordsProcessed.count	Gesamtzahl der beim Export verarbeiteten Datensätze.
dynamodb-pipeline.dynamodb.exportRecordsTotal.count	Gesamtzahl der aus DynamoDB exportierten Datensätze, unverzichtbar für die Verfolgung von Datenexportvolumen.
dynamodb-pipeline.dynamodb.exportS3ObjectsProcessed.count	Gesamtzahl der Exportdatendateien, die erfolgreich von Amazon S3 verarbeitet wurden.
dynamodb-pipeline.opensearch.bulkBadRequestErrors.count	Anzahl der Fehler bei Massenanfragen aufgrund einer falsch formatierten Anfrage.
dynamodb-pipeline.opensearch.bulkRequestLatency.avg	Durchschnittliche Latenz bei Massen-Schreibanfragen an OpenSearch.
dynamodb-pipeline.opensearch.bulkRequestNotFoundErrors.count	Anzahl der Massenanfragen, die fehlgeschlagen sind, weil die Zieldaten nicht gefunden werden konnten.

Metrik	Beschreibung
dynamodb-pipeline.opensearch.bulkRequestNumberOfRetries.count	Anzahl der Wiederholungen von OpenSearch Ingestion-Pipelines, den Cluster zu schreiben. OpenSearch
dynamodb-pipeline.opensearch.bulkRequestSizeBytes.sum	Gesamtgröße aller Massenanfragen in Byte, an. OpenSearch
dynamodb-pipeline.opensearch.documentErrors.count	Anzahl der Fehler beim Senden von Dokumenten an OpenSearch. Die Dokumente , die die Fehler verursacht haben, werden an DLQ gesendet.
dynamodb-pipeline.opensearch.documentsSuccess.count	Anzahl der Dokumente, die erfolgreich in einen OpenSearch Cluster oder eine Sammlung geschrieben wurden.
dynamodb-pipeline.opensearch.documentsSuccessFirstAttempt.count	Anzahl der Dokumente, die beim ersten Versuch erfolgreich indexiert wurden. OpenSearch
dynamodb-pipeline.opensearch.documentsVersionConflictErrors.count	Anzahl der Fehler aufgrund von Versionsk onflikten in Dokumenten während der Verarbeit ung.
dynamodb-pipeline.opensearch.PipelineLatency.avg	Durchschnittliche Latenz der OpenSearch Ingestion-Pipeline bei der Verarbeitung der Daten durch Lesen von der Quelle bis hin zum Schreiben an das Ziel.
dynamodb-pipeline.opensearch.PipelineLatency.max	Maximale Latenz der OpenSearch Ingestion -Pipeline zur Verarbeitung der Daten durch Lesen von der Quelle bis hin zum Schreiben des Ziels.

Metrik	Beschreibung
`dynamodb-pipeline.opensearch.recordsIn.count`	Anzahl der Datensätze, in die erfolgreich aufgenommen wurden. OpenSearch Diese Metrik ist wichtig, um die Menge der verarbeiteten und gespeicherten Daten zu verfolgen.
`dynamodb-pipeline.opensearch.s3.dlqS3RecordsFailed.count`	Anzahl der Datensätze, die nicht in DLQ geschrieben werden konnten.
`dynamodb-pipeline.opensearch.s3.dlqS3RecordsSuccess.count`	Anzahl der Datensätze, die in DLQ geschrieben wurden.
`dynamodb-pipeline.opensearch.s3.dlqS3RequestLatency.count`	Anzahl der Latenzmessungen für Anfragen an die Amazon S3 S3-Warteschlange für unzustellbare Briefe.
`dynamodb-pipeline.opensearch.s3.dlqS3RequestLatency.sum`	Gesamtlatenz für alle Anfragen an die Amazon S3 S3-Warteschlange für unzustellbare Briefe
`dynamodb-pipeline.opensearch.s3.dlqS3RequestSizeBytes.sum`	Gesamtgröße aller Anfragen in Byte, die an die Amazon S3-Warteschlange für unzustellbare Briefe gestellt wurden.
`dynamodb-pipeline.recordsProcessed.count`	Gesamtzahl der in der Pipeline verarbeiteten Datensätze, eine wichtige Kennzahl für den Gesamtdurchsatz.
`dynamodb.changeEventsProcessed.count`	Es werden keine Datensätze aus DynamoDB-Streams gesammelt. Dies könnte daran liegen, dass in der Tabelle keine Aktivität vorhanden ist, dass gerade ein Export ausgeführt wird oder dass ein Problem beim Zugriff auf die DynamoDB-Streams aufgetreten ist.
`dynamodb.exportJobFailure.count`	Der Versuch, einen Export nach S3 auszulösen, ist fehlgeschlagen.

Metrik	Beschreibung
`dynamodb-pipeline.opensearch.bulkRequestInvalidInputErrors.count`	Anzahl der Fehler bei Massenanfragen OpenSearch aufgrund ungültiger Eingaben, was für die Überwachung der Datenqualität und für Betriebsprobleme von entscheidender Bedeutung ist.
`opensearch.EndToEndLatency.avg`	Die End-to-End-Latenz ist beim Lesen aus DynamoDB-Streams höher als gewünscht. Dies könnte auf einen unterskalierten OpenSearch Cluster oder eine maximale Pipeline-OCU-Kapazität zurückzuführen sein, die für den WCU-Durchsatz in der DynamoDB-Tabelle zu niedrig ist. Diese durchgehende Latenz wird nach einem Export hoch sein und sollte mit der Zeit abnehmen, wenn sie sich an die neuesten DynamoDB-Streams anpasst.

Verwenden einer OpenSearch Ingestion-Pipeline mit Amazon DocumentDB

Sie können das DocumentDB-Plugin verwenden, um Dokumentänderungen wie Erstellungen, Aktualisierungen und Löschungen an Amazon OpenSearch Service zu streamen. Die Pipeline unterstützt Change Data Capture (CDC), falls verfügbar, oder API-Polling für hochskaliertes Streaming mit niedriger Latenz.

Sie können Daten mit oder ohne einen vollständigen ersten Snapshot verarbeiten. Ein vollständiger Snapshot erfasst eine gesamte Amazon DocumentDB-Sammlung und lädt sie auf Amazon S3 hoch. Die Pipeline sendet die Daten dann an einen oder mehrere OpenSearch Indizes. Nachdem sie den Snapshot aufgenommen hat, synchronisiert die Pipeline laufende Änderungen, um die Konsistenz zu wahren, und holt schließlich Aktualisierungen fast in Echtzeit auf.

Wenn Sie bereits über einen vollständigen Snapshot aus einer anderen Quelle verfügen oder nur neue Ereignisse verarbeiten müssen, können Sie auch ohne Snapshot streamen. In diesem Fall liest die Pipeline direkt aus Amazon DocumentDB DocumentDB-Change-Streams, ohne dass ein anfängliches Massenladen erforderlich ist.

Wenn Sie Streaming aktivieren, müssen Sie einen Change-Stream in Ihrer Amazon DocumentDB-Sammlung aktivieren. Wenn Sie jedoch nur einen vollständigen Ladevorgang oder Export durchführen, benötigen Sie keinen Change-Stream.

Voraussetzungen

Bevor Sie Ihre OpenSearch Ingestion-Pipeline erstellen, führen Sie die folgenden Schritte aus:

1. Erstellen Sie einen Amazon DocumentDB-Cluster mit der Berechtigung zum Lesen von Daten, indem Sie die Schritte unter Erstellen eines Amazon DocumentDB-Clusters im Amazon DocumentDB DocumentDB-Entwicklerhandbuch befolgen. Wenn Sie die CDC-Infrastruktur verwenden, konfigurieren Sie Ihren Amazon DocumentDB-Cluster für die Veröffentlichung von Change-Streams.
2. Aktivieren Sie TLS in Ihrem Amazon-DocumentDB-Cluster.
3. Richten Sie eine VPC-CIDR eines privaten Adressraums zur Verwendung mit OpenSearch Ingestion ein.
4. Richten Sie die Authentifizierung in Ihrem Amazon DocumentDB-Cluster mit AWS Secrets Manager ein. Aktivieren Sie die Rotation von Geheimnissen, indem Sie die Schritte unter Automatisches Rotieren von Passwörtern für Amazon DocumentDB befolgen. Weitere Informationen finden Sie unter Datenbankzugriff mit rollenbasierter Zugriffskontrolle und Sicherheit in Amazon DocumentDB.
5. Wenn Sie einen Change-Stream verwenden, um Datenänderungen in Ihrer Amazon DocumentDB-Sammlung zu abonnieren, vermeiden Sie Datenverlust, indem Sie den Aufbewahrungszeitraum mithilfe des `change_stream_log_retention_duration` Parameters auf bis zu 7 Tage verlängern. Change-Streams-Ereignisse werden standardmäßig für 3 Stunden gespeichert, nachdem das Ereignis aufgezeichnet wurde, was für große Sammlungen nicht ausreichend ist. Informationen zum Ändern der Aufbewahrungsdauer für Change-Stream-Protokolle finden Sie unter Ändern der Aufbewahrungsdauer für das Change-Stream-Protokoll.
6. Erstellen Sie eine OpenSearch Dienstdomäne oder eine OpenSearch serverlose Sammlung. Weitere Informationen erhalten Sie unter the section called “ OpenSearch Dienstdomänen erstellen” und the section called “Erstellen von Sammlungen”.
7. Fügen Sie Ihrer Domain eine ressourcenbasierte Richtlinie oder Ihrer Sammlung eine Datenzugriffsrichtlinie hinzu. Diese Zugriffsrichtlinien ermöglichen es OpenSearch Ingestion, Daten aus Ihrem Amazon DocumentDB-Cluster in Ihre Domain oder Sammlung zu schreiben.

Die folgende Beispielrichtlinie für den Domänenzugriff ermöglicht es der Pipeline-Rolle, die Sie im nächsten Schritt erstellen, Daten in eine Domain zu schreiben. Stellen Sie sicher, dass Sie das `resource` mit Ihrem eigenen ARN aktualisieren.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::pipeline-account-id:role/pipeline-role"
      },
      "Action": [
        "es:DescribeDomain",
        "es:ESHttp*"
      ],
      "Resource": [
        "arn:aws:es:region:account-id:domain/domain-name"
      ]
    }
  ]
}
```

Informationen zum Erstellen einer IAM-Rolle mit den richtigen Berechtigungen für den Zugriff auf Schreibdaten für die Sammlung oder Domäne finden Sie unterthe section called “Rollen und Benutzer einrichten”.

Schritt 1: Konfigurieren Sie die Pipeline-Rolle

Nachdem Sie die Voraussetzungen für Ihre Amazon DocumentDB-Pipeline eingerichtet haben, konfigurieren Sie die Pipeline-Rolle, die Sie in Ihrer Pipeline-Konfiguration verwenden möchten, und fügen Sie der Rolle die folgenden Amazon DocumentDB DocumentDB-Berechtigungen hinzu:

JSON

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Sid": "allowS3ListObjectAccess",
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::s3-bucket"
            ],
            "Condition": {
                "StringLike": {
                    "s3:prefix": "s3-prefix/*"
                }
            }
        },
        {
            "Sid": "allowReadAndWriteToS3ForExportStream",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject"
            ],
            "Resource": [
                "arn:aws:s3:::s3-bucket/s3-prefix/*"
            ]
        },
        {
            "Sid": "SecretsManagerReadAccess",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": ["arn:aws:secretsmanager:region:account-id:secret:secret-
name"]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachNetworkInterface",
                "ec2:CreateNetworkInterface",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DeleteNetworkInterface",
```

```
                "ec2:DeleteNetworkInterfacePermission",
                "ec2:DetachNetworkInterface",
                "ec2:DescribeNetworkInterfaces"
            ],
            "Resource": [
                "arn:aws:ec2:*:account-id:network-interface/*",
                "arn:aws:ec2:*:account-id:subnet/*",
                "arn:aws:ec2:*:account-id:security-group/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:Describe*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:*:*:network-interface/*",
            "Condition": {
               "StringEquals":
                    {
                        "aws:RequestTag/OSISManaged": "true"
                    }
            }
        }
    ]
}
```

Sie müssen die oben genannten EC2 Amazon-Berechtigungen für die IAM-Rolle bereitstellen, mit der Sie die OpenSearch Ingestion-Pipeline erstellen, da die Pipeline diese Berechtigungen verwendet, um eine Netzwerkschnittstelle in Ihrer VPC zu erstellen und zu löschen. Die Pipeline kann nur über diese Netzwerkschnittstelle auf den Amazon DocumentDB-Cluster zugreifen.

Schritt 2: Erstellen Sie die Pipeline

Anschließend können Sie eine OpenSearch Ingestion-Pipeline wie die folgende konfigurieren, die Amazon DocumentDB als Quelle angibt. Beachten Sie, dass die `getMetadata` Funktion zum Auffüllen des Indexnamens einen Metadatenschlüssel verwendet*`documentdb_collection`*. Wenn Sie einen anderen Indexnamen ohne die `getMetadata` Methode verwenden möchten, können Sie die Konfiguration `index: "`*`my_index_name`*`"` verwenden.

```
version: "2"
documentdb-pipeline:
  source:
    documentdb:
      acknowledgments: true
      host: "https://docdb-cluster-id.us-east-1.docdb.amazonaws.com"
      port: 27017
      authentication:
        username: ${aws_secrets:secret:username}
        password: ${aws_secrets:secret:password}
      aws:
      s3_bucket: "bucket-name"
      s3_region: "bucket-region"
      s3_prefix: "path" #optional path for storing the temporary data
      collections:
        - collection: "dbname.collection"
          export: true
          stream: true
  sink:
  - opensearch:
      hosts: ["https://search-mydomain.us-east-1.es.amazonaws.com"]
      index: "${getMetadata(\"documentdb_collection\")}"
      index_type: custom
      document_id: "${getMetadata(\"primary_key\")}"
      action: "${getMetadata(\"opensearch_action\")}"
      document_version: "${getMetadata(\"document_version\")}"
      document_version_type: "external"
extension:
  aws:
    secrets:
      secret:
        secret_id: "my-docdb-secret"
        region: "us-east-1"
        refresh_interval: PT1H
```

Sie können einen vorkonfigurierten Amazon DocumentDB-Blueprint verwenden, um diese Pipeline zu erstellen. Weitere Informationen finden Sie unter the section called “Mit Blueprints arbeiten”.

Wenn Sie die verwenden, AWS Management Console um Ihre Pipeline zu erstellen, müssen Sie Ihre Pipeline auch an Ihre VPC anhängen, um Amazon DocumentDB als Quelle verwenden zu können. Suchen Sie dazu den Abschnitt Quellnetzwerkoptionen, aktivieren Sie das Kontrollkästchen An VPC anhängen und wählen Sie Ihr CIDR aus einer der bereitgestellten Standardoptionen aus. Sie können jedes CIDR aus einem privaten Adressraum verwenden, wie in RFC 1918 Best Current Practice definiert.

Um ein benutzerdefiniertes CIDR bereitzustellen, wählen Sie im Dropdownmenü die Option Andere aus. Um eine Kollision der IP-Adressen zwischen OpenSearch Ingestion und Amazon DocumentDB zu vermeiden, stellen Sie sicher, dass sich die Amazon DocumentDB VPC CIDR von der CIDR für Ingestion unterscheidet. OpenSearch

Weitere Informationen finden Sie unter VPC-Zugriff für eine Pipeline konfigurieren.

Datenkonsistenz

Die Pipeline gewährleistet die Datenkonsistenz, indem sie kontinuierlich Änderungen vom Amazon DocumentDB-Cluster abfragt oder empfängt und die entsprechenden Dokumente im OpenSearch Index aktualisiert.

OpenSearch Die Datenaufnahme unterstützt die end-to-end Bestätigung, um die Beständigkeit der Daten sicherzustellen. Wenn eine Pipeline Snapshots oder Streams liest, erstellt sie dynamisch Partitionen für die Parallelverarbeitung. Die Pipeline markiert eine Partition als abgeschlossen, wenn sie nach der Aufnahme aller Datensätze in der OpenSearch Domäne oder Sammlung eine Bestätigung erhält.

Wenn Sie Daten in eine OpenSearch serverlose Suchsammlung aufnehmen möchten, können Sie in der Pipeline eine Dokument-ID generieren. Wenn Sie Daten in eine OpenSearch serverlose Zeitreihensammlung aufnehmen möchten, beachten Sie, dass die Pipeline keine Dokument-ID generiert. Daher müssen Sie diese `document_id: "${getMetadata(\"primary_key\")}"` in Ihrer Pipeline-Senkenkonfiguration weglassen.

Eine OpenSearch Ingestion-Pipeline ordnet auch eingehende Ereignisaktionen entsprechenden Massenindizierungsaktionen zu, um das Ingestieren von Dokumenten zu erleichtern. Dadurch bleiben die Daten konsistent, sodass jede Datenänderung in Amazon DocumentDB mit den entsprechenden Dokumentänderungen in abgeglichen wird. OpenSearch

Datentypen zuordnen

OpenSearch Der Service ordnet Datentypen in jedem eingehenden Dokument dynamisch dem entsprechenden Datentyp in Amazon DocumentDB zu. Die folgende Tabelle zeigt, wie OpenSearch Service verschiedene Datentypen automatisch zuordnet.

Datentyp	OpenSearch	Amazon DocumentDB
Ganzzahl	OpenSearch ordnet Amazon DocumentDB DocumentDB-Integer-Werte automatisch OpenSearch Ganzzahlen zu. OpenSearch ordnet das Feld dynamisch auf der Grundlage des ersten gesendeten Dokuments zu. Wenn Sie eine Mischung von Datentypen für dasselbe Attribut in Amazon DocumentDB haben, schlägt die automatische Zuordnung möglicherweise fehl. Wenn Ihr erstes Dokument beispielsweise ein Long-Attribut hat und ein späteres Dokument dasselbe Attribut als Ganzzahl hat, OpenSearch kann das zweite Dokument nicht aufgenommen werden. In diesen Fällen sollten Sie eine explizite Zuordnungsvorlage bereitstellen, die den flexibelsten Zahlentyp auswählt, z. B. den folgenden: `{ "template": { "mappings": { "properties": { "MixedNumberField": { "type": "float" } } } }`	Amazon DocumentDB unterstützt Ganzzahlen.

Datentyp	OpenSearch	Amazon DocumentDB
	<pre> } }</pre>	

Long	OpenSearch ordnet Amazon DocumentDB DocumentDB-Long-Werte automatisch OpenSearch Long-Werten zu.
	
	OpenSearch ordnet das Feld dynamisch auf der Grundlage des ersten gesendeten Dokuments zu. Wenn Sie eine Mischung von Datentypen für dasselbe Attribut in Amazon DocumentDB haben, schlägt die automatische Zuordnung möglicherweise fehl.
	
	Wenn Ihr erstes Dokument beispielsweise ein Long-Attribut hat und ein späteres Dokument dasselbe Attribut als Ganzzahl hat, OpenSearch kann das zweite Dokument nicht aufgenommen werden. In diesen Fällen sollten Sie eine explizite Zuordnungsvorlage bereitstellen, die den flexibelsten Zahlentyp auswählt, z. B. den folgenden:
	
	<pre>{
	 "template": {
	  "mappings": {
	   "properties": {
	    "MixedNumberField": {
	     "type": "float"
	    }
	   }
	  }
	 }
	}</pre>
		Amazon DocumentDB unterstützt Longs.

Datentyp	OpenSearch	Amazon DocumentDB
String	OpenSearch ordnet Zeichenkettenwerte automatisch als Text zu. In einigen Situationen, z. B. bei Aufzählungswerten, können Sie sie dem Schlüsselworttyp zuordnen. Das folgende Beispiel zeigt, wie ein Amazon DocumentDB-Attribut mit dem Namen einem OpenSearch Schlüssel wort `PartType` zugeordnet wird. `{ "template": { "mappings": { "properties": { "PartType": { "type": "keyword" } } } } }`	Amazon DocumentDB unterstützt Zeichenketten.

Datentyp	OpenSearch	Amazon DocumentDB
Double	OpenSearch ordnet Amazon DocumentDB DocumentDB-Doppelwerte automatisch OpenSearch Doubles zu. OpenSearch ordnet das Feld dynamisch auf der Grundlage des ersten gesendeten Dokuments zu. Wenn Sie eine Mischung von Datentypen für dasselbe Attribut in Amazon DocumentDB haben, schlägt die automatische Zuordnung möglicherweise fehl. Wenn Ihr erstes Dokument beispielsweise ein Long-Attribut hat und ein späteres Dokument dasselbe Attribut als Ganzzahl hat, OpenSearch kann das zweite Dokument nicht aufgenommen werden. In diesen Fällen sollten Sie eine explizite Zuordnungsvorlage bereitstellen, die den flexibelsten Zahlentyp auswählt, z. B. den folgenden: `{ "template": { "mappings": { "properties": { "MixedNumberField": { "type": "float" } } } } }`	Amazon DocumentDB unterstützt Doubles.

Datentyp	OpenSearch	Amazon DocumentDB
Datum	Standardmäßig wird das Datum einer Ganzzahl in zugeordnet. OpenSearch Sie können eine benutzerdefinierte Zuordnungsvorlage definieren, um ein Datum einem OpenSearch Datum zuzuordnen. `{ "template": { "mappings": { "properties": { "myDateField": { "type": "date", "format": "epoch_second" } } } } }`	Amazon DocumentDB unterstützt Datumsangaben.

Datentyp	OpenSearch	Amazon DocumentDB
Zeitstempel	Standardmäßig wird der Zeitstempel einer Ganzzahl in zugeordnet. OpenSearch Sie können eine benutzerdefinierte Zuordnungsvorlage definieren, um ein Datum einem Datum zuzuordnen. OpenSearch `{ "template": { "mappings": { "properties": { "myTimestampField": { "type": "date", "format": "epoch_second" } } } } }`	Amazon DocumentDB unterstützt Zeitstempel.
Boolesch	OpenSearch ordnet einen booleschen Amazon DocumentDB-Typ einem OpenSearch booleschen Typ zu.	Amazon DocumentDB unterstützt Attribute vom Typ Boolean.

Datentyp	OpenSearch	Amazon DocumentDB
Dezimal	OpenSearch ordnet Amazon DocumentDB DocumentDB-Zuordnungsattribute verschachtelten Feldern zu. Dieselben Zuordnungen gelten für ein verschachteltes Feld. Das folgende Beispiel ordnet eine Zeichenfolge in einem verschachtelten Feld einem Schlüsselworttyp in zu: OpenSearch `{ "template": { "mappings": { "properties": { "myDecimalField": { "type": "double" } } } } }` Mit dieser benutzerdefinierten Zuordnung können Sie das Feld mit doppelter Genauigkeit abfragen und aggregieren. Der ursprüngliche Wert behält die volle Genauigkeit in der `_source` Eigenschaft des OpenSearch Dokuments bei. Ohne diese Zuordnung wird standardmäßig Text OpenSearch verwendet.	Amazon DocumentDB unterstützt Dezimalzahlen.

Datentyp	OpenSearch	Amazon DocumentDB
Regulärer Ausdruck	Der Regex-Typ erstellt verschachtelte Felder. Dazu gehören und. *<myFieldName>* `.pattern` *<myFieldName>* `.options`	Amazon DocumentDB unterstützt reguläre Ausdrücke.
Binäre Daten	OpenSearch ordnet Amazon DocumentDB-Binärdaten automatisch OpenSearch Text zu. Sie können eine Zuordnung angeben, in OpenSearch die Sie diese als Binärfelder schreiben können. Das folgende Beispiel zeigt, wie ein `imageData` benanntes Amazon DocumentDB-Feld einem OpenSearch Binärfeld zugeordnet wird. `{ "template": { "mappings": { "properties": { "imageData": { "type": "binary" } } } } }`	Amazon DocumentDB unterstützt binäre Datenfelder.
ObjectId	Felder mit einem ObjectID-Typ werden OpenSearch Textfeldern zugeordnet. Der Wert entspricht der Zeichenkettendarstellung der ObjectID.	Amazon DocumentDB unterstützt ObjectIDs.

Datentyp	OpenSearch	Amazon DocumentDB
Null	OpenSearch kann Dokumente mit dem Nulltyp Amazon DocumentDB aufnehmen. Es speichert den Wert als Nullwert im Dokument. Für diesen Typ gibt es keine Zuordnung, und dieses Feld ist weder indexiert noch durchsuch bar. Wenn derselbe Attributname für einen Null-Typ verwendet wird und später zu einem anderen Typ, wie z. B. einer Zeichenfolge, geändert OpenSearch wird, wird eine dynamische Zuordnung für den ersten Wert, der nicht Null ist, erstellt. Nachfolgende Werte können immer noch Nullwerte von Amazon DocumentDB sein.	Amazon DocumentDB unterstützt Felder vom Typ Null.
Undefined	OpenSearch kann Dokumente mit dem undefinierten Typ Amazon DocumentD B aufnehmen. Es speichert den Wert als Nullwert im Dokument. Für diesen Typ gibt es keine Zuordnung, und dieses Feld ist weder indexiert noch durchsuch bar. Wenn derselbe Feldname für einen undefinierten Typ verwendet wird und später zu einem anderen Typ, z. B. einer Zeichenfolge, geändert OpenSearch wird, wird eine dynamische Zuordnung für den ersten nicht definierten Wert erstellt. Nachfolgende Werte können immer noch undefinierte Amazon DocumentDB DocumentDB-Werte sein.	Amazon DocumentDB unterstützt undefinierte Typfelder.

Datentyp	OpenSearch	Amazon DocumentDB
MinKey	OpenSearch kann Dokumente mit dem MinKey-Typ Amazon DocumentDB aufnehmen. Es speichert den Wert als Nullwert im Dokument. Für diesen Typ gibt es keine Zuordnung, und dieses Feld ist weder indexiert noch durchsuch bar. Wenn derselbe Feldname für einen MinKey-Typ verwendet wird und später zu einem anderen Typ, z. B. einer Zeichenfolge, geändert OpenSearch wird, wird eine dynamische Zuordnung für den ersten Nicht-Minkey-Wert erstellt. Nachfolgende Werte können weiterhin Amazon DocumentDB MinKey-Werte sein.	Amazon DocumentDB unterstützt Felder vom Typ MinKey.
MaxKey	OpenSearch kann Dokumente mit dem Typ Amazon DocumentDB MaxKey aufnehmen. Es speichert den Wert als Nullwert im Dokument. Für diesen Typ gibt es keine Zuordnung, und dieses Feld ist weder indexiert noch durchsuch bar. Wenn derselbe Feldname für einen MaxKey-Typ verwendet wird und später zu einem anderen Typ, z. B. einer Zeichenfolge, geändert OpenSearch wird, wird eine dynamische Zuordnung für den ersten Nicht-MaxKey-Wert erstellt. Nachfolgende Werte können weiterhin Amazon DocumentDB MaxKey-Werte sein.	Amazon DocumentDB unterstützt Felder vom Typ MaxKey.

Wir empfehlen Ihnen, die Dead-Letter-Warteschlange (DLQ) in Ihrer Ingestion-Pipeline zu konfigurieren. OpenSearch Wenn Sie die Warteschlange konfiguriert haben, sendet OpenSearch Service alle fehlgeschlagenen Dokumente, die aufgrund von Fehlern bei der dynamischen Zuordnung nicht aufgenommen werden konnten, an die Warteschlange.

Falls automatische Zuordnungen fehlschlagen, können Sie `template_type` und `template_content` in Ihrer Pipeline-Konfiguration verwenden, um explizite Zuordnungsregeln zu definieren. Alternativ können Sie Zuordnungsvorlagen direkt in Ihrer Suchdomain oder Sammlung erstellen, bevor Sie die Pipeline starten.

Einschränkungen

Beachten Sie die folgenden Einschränkungen, wenn Sie eine OpenSearch Ingestion-Pipeline für Amazon DocumentDB einrichten:

- Die OpenSearch Ingestion-Integration mit Amazon DocumentDB unterstützt derzeit keine regionsübergreifende Aufnahme. Ihr Amazon DocumentDB-Cluster und Ihre OpenSearch Ingestion-Pipeline müssen identisch sein. AWS-Region
- Die OpenSearch Ingestion-Integration mit Amazon DocumentDB unterstützt derzeit keine kontoübergreifende Erfassung. Ihr Amazon DocumentDB-Cluster und Ihre OpenSearch Ingestion-Pipeline müssen identisch sein. AWS-Konto
- Eine OpenSearch Ingestion-Pipeline unterstützt nur einen Amazon DocumentDB-Cluster als Quelle.
- Die OpenSearch Ingestion-Integration mit Amazon DocumentDB unterstützt speziell instanzbasierte Amazon DocumentDB-Cluster. Elastische Amazon DocumentDB-Cluster werden nicht unterstützt.
- Die OpenSearch Ingestion-Integration wird nur AWS Secrets Manager als Authentifizierungsmechanismus für Ihren Amazon DocumentDB-Cluster unterstützt.
- Sie können die bestehende Pipeline-Konfiguration nicht aktualisieren, um Daten aus einer anderen Datenbank oder Sammlung aufzunehmen. Stattdessen müssen Sie eine neue Pipeline erstellen.

Empfohlene CloudWatch Alarme

Für eine optimale Leistung empfehlen wir, die folgenden CloudWatch Alarme zu verwenden, wenn Sie eine OpenSearch Ingestion-Pipeline für den Zugriff auf einen Amazon DocumentDB-Cluster als Quelle erstellen.

CloudWatch Alarm	Beschreibung
<pipeline-name> .documentDB.Credentials geändert	Diese Metrik gibt an, wie oft Geheimnisse ausgetauscht werden. AWS
<pipeline-name> .documentdb. executorR efreshErrors	Diese Metrik weist auf Fehler beim Aktualisi eren von AWS Geheimnissen hin.
<pipeline-name> .documentdb. exportRec ordsTotal	Diese Metrik gibt die Anzahl der aus Amazon DocumentDB exportierten Datensätze an.
<pipeline-name> .documentdb. exportRec ordsProcessed	Diese Metrik gibt die Anzahl der Datensätze an, die von der OpenSearch Ingestion-Pipeline verarbeitet wurden.
<pipeline-name> .documentdb. exportRec ordProcessingFehler	Diese Metrik gibt die Anzahl der Verarbeit ungsfehler in einer OpenSearch Ingestion-Pipeline beim Lesen der Daten aus einem Amazon DocumentDB-Cluster an.
<pipeline-name> .documentdb. exportRec ordsSuccessInsgesamt	Diese Metrik gibt die Gesamtzahl der erfolgrei ch verarbeiteten Exportdatensätze an.
<pipeline-name> .documentdb. exportRec ordsFailedInsgesamt	Diese Metrik gibt die Gesamtzahl der Exportdat ensätze an, die nicht verarbeitet werden konnten.
<pipeline-name> .documentDB.BytesR eceived	Diese Metrik gibt die Gesamtzahl der Byte an, die von einer Ingestion-Pipeline empfangen wurden. OpenSearch
<pipeline-name> .documentDB.BytesP rocessed	Diese Metrik gibt die Gesamtzahl der Byte an, die von einer Ingestion-Pipeline verarbeitet wurden. OpenSearch
<pipeline-name> .documentdb. exportPar titionQueryInsgesamt	Diese Metrik gibt die Gesamtsumme der Exportpartition an.

CloudWatch Alarm	Beschreibung
<pipeline-name> .documentdb. streamRecordsSuccessInsgesamt	Diese Metrik gibt die Anzahl der erfolgreich verarbeiteten Datensätze aus dem Stream an.
<pipeline-name> .documentdb. streamRecordsFailedInsgesamt	Diese Metrik gibt die Gesamtzahl der Datensätze aus dem Stream an, die nicht verarbeitet werden konnten.

Verwenden einer OpenSearch Ingestion-Pipeline mit Confluent Cloud Kafka

Sie können eine OpenSearch Ingestion-Pipeline verwenden, um Daten von Confluent Cloud Kafka-Clustern zu Amazon OpenSearch Service-Domains und serverlosen Sammlungen zu streamen. OpenSearch OpenSearch Ingestion unterstützt sowohl öffentliche als auch private Netzwerkkonfigurationen für das Streaming von Daten aus Confluent Cloud Kafka-Clustern zu Domains oder Sammlungen, die von Service oder Serverless verwaltet werden. OpenSearch OpenSearch

Konnektivität zu öffentlichen Kafka-Clustern von Confluent Cloud

Sie können OpenSearch Ingestion-Pipelines verwenden, um Daten aus einem Confluent Cloud Kafka-Cluster mit einer öffentlichen Konfiguration zu migrieren, was bedeutet, dass der Domain-DNS-Name öffentlich aufgelöst werden kann. Richten Sie dazu eine OpenSearch Ingestion-Pipeline mit dem öffentlichen Kafka-Cluster von Confluent Cloud als Quelle und Service oder Serverless als Ziel ein. OpenSearch OpenSearch Dadurch werden Ihre Streaming-Daten von einem selbstverwalteten Quellcluster zu einer verwalteten Zieldomäne oder -sammlung verarbeitet. AWS

Voraussetzungen

Bevor Sie Ihre OpenSearch Ingestion-Pipeline erstellen, führen Sie die folgenden Schritte aus:

1. Erstellen Sie einen Confluent Cloud Kafka-Cluster-Cluster, der als Quelle fungiert. Der Cluster sollte die Daten enthalten, die Sie in den Service aufnehmen möchten. OpenSearch
2. Erstellen Sie eine OpenSearch Dienstdomäne oder eine OpenSearch serverlose Sammlung, in die Sie Daten migrieren möchten. Weitere Informationen erhalten Sie unter the section called “ OpenSearch Dienstdomänen erstellen” und the section called “Erstellen von Sammlungen”.

3. Richten Sie die Authentifizierung auf Ihrem Confluent Cloud Kafka-Cluster mit ein. AWS Secrets ManagerAktivieren Sie die Rotation von Geheimnissen, indem Sie die Schritte unter Geheimnisse rotieren befolgen. AWS Secrets Manager
4. Fügen Sie Ihrer Domain eine ressourcenbasierte Richtlinie oder Ihrer Sammlung eine Datenzugriffsrichtlinie hinzu. Diese Zugriffsrichtlinien ermöglichen es OpenSearch Ingestion, Daten aus Ihrem selbstverwalteten Cluster in Ihre Domain oder Sammlung zu schreiben.

   Die folgende Beispielrichtlinie für den Domänenzugriff ermöglicht es der Pipeline-Rolle, die Sie im nächsten Schritt erstellen, Daten in eine Domäne zu schreiben. Stellen Sie sicher, dass Sie das `resource` mit Ihrem eigenen ARN aktualisieren.

   JSON

   ```
   {
     "Version": "2012-10-17",
     "Statement": [
       {
         "Effect": "Allow",
         "Principal": {
           "AWS": "arn:aws:iam::pipeline-account-id:role/pipeline-role"
         },
         "Action": [
           "es:DescribeDomain",
           "es:ESHttp*"
         ],
         "Resource": [
           "arn:aws:es:region:account-id:domain/domain-name"
         ]
       }
     ]
   }
   ```

   Informationen zum Erstellen einer IAM-Rolle mit den richtigen Berechtigungen für den Zugriff auf Schreibdaten für die Sammlung oder Domäne finden Sie unterthe section called “Rollen und Benutzer einrichten”.

Schritt 1: Konfigurieren Sie die Pipeline-Rolle

Nachdem Sie die Voraussetzungen für Ihre Confluent Cloud Kafka-Cluster-Pipeline eingerichtet haben, konfigurieren Sie die Pipeline-Rolle, die Sie in Ihrer Pipeline-Konfiguration verwenden

möchten, und fügen Sie die Berechtigung hinzu, in eine OpenSearch Service-Domain oder eine OpenSearch Serverless-Sammlung zu schreiben, sowie die Erlaubnis, Geheimnisse aus Secrets Manager zu lesen.

Für die Verwaltung der Netzwerkschnittstelle ist die folgende Berechtigung erforderlich:

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachNetworkInterface",
                "ec2:CreateNetworkInterface",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteNetworkInterfacePermission",
                "ec2:DetachNetworkInterface",
                "ec2:DescribeNetworkInterfaces"
            ],
            "Resource": [
                "arn:aws:ec2:*:account-id:network-interface/*",
                "arn:aws:ec2:*:account-id:subnet/*",
                "arn:aws:ec2:*:account-id:security-group/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:Describe*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [ "ec2:CreateTags" ],
```

```
            "Resource": "arn:aws:ec2:*:*:network-interface/*",
            "Condition": {
               "StringEquals": { "aws:RequestTag/OSISManaged": "true" }
            }
        }
    ]
}
```

Die folgende Berechtigung ist erforderlich, um Geheimnisse aus dem AWS Secrets Manager Dienst zu lesen:

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SecretsManagerReadAccess",
            "Effect": "Allow",
            "Action": ["secretsmanager:GetSecretValue"],
            "Resource": ["arn:aws:secretsmanager:region:account-
id:secret:,secret-name"]
        }
    ]
}
```

Die folgenden Berechtigungen sind erforderlich, um in eine Amazon OpenSearch Service-Domain zu schreiben:

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::account-id:role/pipeline-role"
      },
      "Action": ["es:DescribeDomain", "es:ESHttp*"],
      "Resource": "arn:aws:es:region:account-id:domain/domain-name/*"
    }
  ]
```

```
}
```

Schritt 2: Erstellen Sie die Pipeline

Anschließend können Sie eine OpenSearch Ingestion-Pipeline wie die folgende konfigurieren, die Ihr Confluent Cloud Kafka als Quelle angibt.

Sie können mehrere OpenSearch Service-Domains als Ziele für Ihre Daten angeben. Diese Funktion ermöglicht das bedingte Routing oder die Replikation eingehender Daten in mehrere OpenSearch Dienstdomänen.

Sie können auch Daten von einem Confluent Kafka-Quellcluster zu einer OpenSearch serverlosen VPC-Sammlung migrieren. Stellen Sie sicher, dass Sie in der Pipeline-Konfiguration eine Netzwerkzugriffsrichtlinie angeben. Sie können eine Confluent-Schemaregistrierung verwenden, um ein Confluent-Schema zu definieren.

```
version: "2"
kafka-pipeline:
  source:
    kafka:
      encryption:
        type: "ssl"
      topics:
        - name: "topic-name"
          group_id: "group-id"
      bootstrap_servers:
        - "bootstrap-server.us-east-1.aws.private.confluent.cloud:9092"
      authentication:
        sasl:
          plain:
            username: ${aws_secrets:confluent-kafka-secret:username}
            password: ${aws_secrets:confluent-kafka-secret:password}
      schema:
        type: confluent
        registry_url: https://my-registry.us-east-1.aws.confluent.cloud
        api_key: "${{aws_secrets:schema-secret:schema_registry_api_key}}"
        api_secret: "${{aws_secrets:schema-secret:schema_registry_api_secret}}"
        basic_auth_credentials_source: "USER_INFO"
  sink:
  - opensearch:
      hosts: ["https://search-mydomain.us-east-1.es.amazonaws.com"]
      aws:
          region: "us-east-1"
```

```
  aws:
    secrets:
      confluent-kafka-secret:
        secret_id: "my-kafka-secret"
        region: "us-east-1"
      schema-secret:
        secret_id: "my-self-managed-kafka-schema"
        region: "us-east-1"
```

Sie können einen vorkonfigurierten Blueprint verwenden, um diese Pipeline zu erstellen. Weitere Informationen finden Sie unter the section called “Mit Blueprints arbeiten”.

Konnektivität zu Confluent Cloud Kafka-Clustern in einer VPC

Sie können OpenSearch Ingestion-Pipelines auch verwenden, um Daten aus einem Confluent Cloud Kafka-Cluster zu migrieren, der in einer VPC ausgeführt wird. Richten Sie dazu eine OpenSearch Ingestion-Pipeline mit einem Confluent Cloud Kafka-Cluster als Quelle und Service oder Serverless als Ziel ein. OpenSearch OpenSearch Dadurch werden Ihre Streaming-Daten von einem Confluent Cloud Kafka-Quellcluster zu einer verwalteten Zieldomain oder -sammlung verarbeitet. AWS

OpenSearch Ingestion unterstützt Confluent Cloud Kafka-Cluster, die in allen unterstützten Netzwerkmodi in Confluent konfiguriert sind. Die folgenden Modi der Netzwerkkonfiguration werden als Quelle in Ingestion unterstützt: OpenSearch

- AWS VPC-Peering
- AWS PrivateLink für dedizierte Cluster
- AWS PrivateLink für Unternehmenscluster
- AWS Transit Gateway

Voraussetzungen

Bevor Sie Ihre OpenSearch Ingestion-Pipeline erstellen, führen Sie die folgenden Schritte aus:

1. Erstellen Sie einen Confluent Cloud Kafka-Cluster mit einer VPC-Netzwerkkonfiguration, die die Daten enthält, die Sie in Service aufnehmen möchten. OpenSearch
2. Erstellen Sie eine OpenSearch Service-Domain oder eine OpenSearch serverlose Sammlung, in die Sie Daten migrieren möchten. Weitere Informationen finden Sie unter Weitere Informationen finden Sie unter the section called “ OpenSearch Dienstdomänen erstellen” undthe section called “Erstellen von Sammlungen”.

3. Richten Sie die Authentifizierung auf Ihrem Confluent Cloud Kafka-Cluster mit ein. AWS Secrets ManagerAktivieren Sie die Rotation von Geheimnissen, indem Sie die Schritte unter Geheimnisse rotieren befolgen. AWS Secrets Manager
4. Rufen Sie die ID der VPC ab, die Zugriff auf den Confluent Cloud Kafka-Cluster hat. Wählen Sie die VPC CIDR aus, die von OpenSearch Ingestion verwendet werden soll.

> **Note**
>
> Wenn Sie die verwenden, um Ihre Pipeline AWS Management Console zu erstellen, müssen Sie auch Ihre OpenSearch Ingestion-Pipeline an Ihre VPC anhängen, um den Confluent Cloud Kafka-Cluster verwenden zu können. Suchen Sie dazu den Abschnitt Netzwerkkonfiguration, aktivieren Sie das Kontrollkästchen An VPC anhängen und wählen Sie Ihr CIDR aus einer der bereitgestellten Standardoptionen oder wählen Sie Ihre eigene aus. Sie können jedes CIDR aus einem privaten Adressraum verwenden, wie in der RFC 1918 Best Current Practice definiert.
> Um ein benutzerdefiniertes CIDR bereitzustellen, wählen Sie im Dropdownmenü die Option Andere aus. Um eine Kollision der IP-Adressen zwischen OpenSearch Ingestion und Self-managed zu vermeiden, stellen Sie sicher OpenSearch, dass sich das selbstverwaltete OpenSearch VPC-CIDR vom CIDR für Ingestion unterscheidet. OpenSearch

5. Fügen Sie Ihrer Domain eine ressourcenbasierte Richtlinie oder Ihrer Sammlung eine Datenzugriffsrichtlinie hinzu. Diese Zugriffsrichtlinien ermöglichen es OpenSearch Ingestion, Daten aus Ihrem selbstverwalteten Cluster in Ihre Domain oder Sammlung zu schreiben.

> **Note**
>
> Wenn Sie Ihre Confluent Cloud Kafka für die Verbindung verwenden AWS PrivateLink , müssen Sie die VPC-DHCP-Optionen konfigurieren. DNS-Hostnamen und DNS-Auflösung sollten aktiviert sein.
> Verwenden Sie insbesondere die folgenden Optionssatzwerte:
>
> ```
> domain-name: aws.private.confluent.cloud
> domain-name-servers: AmazonProvidedDNS
> ```
>
> Diese Änderung stellt sicher, dass die DNS-Auflösung für den PrivateLink Confluent-Endpunkt innerhalb der VPC korrekt funktioniert.

Die folgende Beispielrichtlinie für den Domänenzugriff ermöglicht es der Pipeline-Rolle, die Sie im nächsten Schritt erstellen, Daten in eine Domain zu schreiben. Stellen Sie sicher, dass Sie das `resource` mit Ihrem eigenen ARN aktualisieren.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::pipeline-account-id:role/pipeline-role"
      },
      "Action": [
        "es:DescribeDomain",
        "es:ESHttp*"
      ],
      "Resource": [
        "arn:aws:es:region:account-id:domain/domain-name"
      ]
    }
  ]
}
```

Informationen zum Erstellen einer IAM-Rolle mit den richtigen Berechtigungen für den Zugriff auf Schreibdaten für die Sammlung oder Domäne finden Sie unterthe section called “Rollen und Benutzer einrichten”.

Schritt 1: Konfigurieren Sie die Pipeline-Rolle

Nachdem Sie Ihre Pipeline-Voraussetzungen eingerichtet haben, konfigurieren Sie die Pipeline-Rolle, die Sie in Ihrer Pipeline-Konfiguration verwenden möchten, und fügen Sie der Rolle die folgenden Berechtigungen hinzu:

JSON

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Sid": "SecretsManagerReadAccess",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": ["arn:aws:secretsmanager:region:account-id:secret:secret-
name"]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachNetworkInterface",
                "ec2:CreateNetworkInterface",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteNetworkInterfacePermission",
                "ec2:DetachNetworkInterface",
                "ec2:DescribeNetworkInterfaces"
            ],
            "Resource": [
                "arn:aws:ec2:*:account-id:network-interface/*",
                "arn:aws:ec2:*:account-id:subnet/*",
                "arn:aws:ec2:*:account-id:security-group/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:Describe*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
```

```
            "Resource": "arn:aws:ec2:*:*:network-interface/*",
            "Condition": {
               "StringEquals":
                    {
                        "aws:RequestTag/OSISManaged": "true"
                    }
            }
        }
    ]
}
```

Sie müssen die oben genannten EC2 Amazon-Berechtigungen für die IAM-Rolle bereitstellen, mit der Sie die OpenSearch Ingestion-Pipeline erstellen, da die Pipeline diese Berechtigungen verwendet, um eine Netzwerkschnittstelle in Ihrer VPC zu erstellen und zu löschen. Die Pipeline kann nur über diese Netzwerkschnittstelle auf den Kafka-Cluster zugreifen.

Schritt 2: Erstellen Sie die Pipeline

Anschließend können Sie eine OpenSearch Ingestion-Pipeline wie die folgende konfigurieren, die Kafka als Quelle angibt.

Sie können mehrere OpenSearch Dienstdomänen als Ziele für Ihre Daten angeben. Diese Funktion ermöglicht das bedingte Routing oder die Replikation eingehender Daten in mehrere OpenSearch Dienstdomänen.

Sie können auch Daten von einem Confluent Kafka-Quellcluster zu einer OpenSearch serverlosen VPC-Sammlung migrieren. Stellen Sie sicher, dass Sie in der Pipeline-Konfiguration eine Netzwerkzugriffsrichtlinie angeben. Sie können eine Confluent-Schemaregistrierung verwenden, um ein Confluent-Schema zu definieren.

```
 version: "2"
kafka-pipeline:
  source:
    kafka:
      encryption:
        type: "ssl"
      topics:
        - name: "topic-name"
          group_id: "group-id"
      bootstrap_servers:
        - "bootstrap-server.us-east-1.aws.private.confluent.cloud:9092"
```

```
      authentication:
        sasl:
          plain:
            username: ${aws_secrets:confluent-kafka-secret:username}
            password: ${aws_secrets:confluent-kafka-secret:password}
      schema:
        type: confluent
        registry_url: https://my-registry.us-east-1.aws.confluent.cloud
        api_key: "${{aws_secrets:schema-secret:schema_registry_api_key}}"
        api_secret: "${{aws_secrets:schema-secret:schema_registry_api_secret}}"
        basic_auth_credentials_source: "USER_INFO"
  sink:
  - opensearch:
      hosts: ["https://search-mydomain.us-east-1.es.amazonaws.com"]
      aws:
          region: "us-east-1"
      index: "confluent-index"
extension:
  aws:
    secrets:
      confluent-kafka-secret:
        secret_id: "my-kafka-secret"
        region: "us-east-1"
      schema-secret:
        secret_id: "my-self-managed-kafka-schema"
        region: "us-east-2"
```

Verwenden Sie eine Ingestion-Pipeline mit OpenSearch Amazon Managed Streaming for Apache Kafka

Sie können das Kafka-Plugin verwenden, um Daten aus Amazon Managed Streaming for Apache Kafka (Amazon MSK) in Ihre Ingestion-Pipeline aufzunehmen. OpenSearch Mit Amazon MSK können Sie Anwendungen erstellen und ausführen, die Apache Kafka zur Verarbeitung von Streaming-Daten verwenden. OpenSearch Ingestion verwendet, um eine Verbindung AWS PrivateLink zu Amazon MSK herzustellen. Sie können Daten sowohl aus Amazon MSK- als auch aus Amazon MSK Serverless-Clustern aufnehmen. Der einzige Unterschied zwischen den beiden Prozessen besteht in den erforderlichen Schritten, die Sie ergreifen müssen, bevor Sie Ihre Pipeline einrichten.

Themen

- Bereitgestellte Amazon MSK-Voraussetzungen
- Voraussetzungen für Amazon MSK Serverless

- Schritt 1: Konfigurieren Sie eine Pipeline-Rolle
- Schritt 2: Erstellen Sie die Pipeline
- Schritt 3: (Optional) Verwenden Sie die Schemaregistrierung AWS Glue
- Schritt 4: (Optional) Empfohlene Recheneinheiten (OCUs) für die Amazon MSK-Pipeline konfigurieren

Bereitgestellte Amazon MSK-Voraussetzungen

Bevor Sie Ihre OpenSearch Ingestion-Pipeline erstellen, führen Sie die folgenden Schritte aus:

1. Erstellen Sie einen von Amazon MSK bereitgestellten Cluster, indem Sie die Schritte unter Erstellen eines Clusters im Amazon Managed Streaming for Apache Kafka Developer Guide befolgen. Wählen Sie als Broker-Typ eine beliebige Option außer `t3` Typen aus, da diese von Ingestion nicht unterstützt werden. OpenSearch
2. Wenn der Cluster den Status Aktiv hat, folgen Sie den Schritten unter Multi-VPC-Konnektivität aktivieren.
3. Folgen Sie den Schritten unter Anhängen einer Clusterrichtlinie an den MSK-Cluster, um eine der folgenden Richtlinien anzuhängen, je nachdem, ob Ihr Cluster und Ihre Pipeline identisch sind. AWS-Konto Diese Richtlinie ermöglicht es OpenSearch Ingestion, eine AWS PrivateLink Verbindung zu Ihrem Amazon MSK-Cluster herzustellen und Daten aus Kafka-Themen zu lesen. Stellen Sie sicher, dass Sie das `resource` mit Ihrem eigenen ARN aktualisieren.

   Die folgenden Richtlinien gelten, wenn sich Ihr Cluster und Ihre Pipeline in derselben Einheit befinden AWS-Konto:

   JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "osis.amazonaws.com"
      },
      "Action": [
        "kafka:CreateVpcConnection",
        "kafka:DescribeClusterV2"
      ],
```

```
      "Resource": "arn:aws:kafka:region:account-id:cluster/cluster-
name/cluster-id"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "osis-pipelines.amazonaws.com"
      },
      "Action": [
        "kafka:CreateVpcConnection",
        "kafka:GetBootstrapBrokers",
        "kafka:DescribeClusterV2"
      ],
      "Resource": "arn:aws:kafka:region:account-id:cluster/cluster-
name/cluster-id"
    }
  ]
}
```

Wenn sich Ihr Amazon MSK-Cluster in einer anderen Pipeline AWS-Konto als Ihrer Pipeline befindet, fügen Sie stattdessen die folgende Richtlinie bei. Beachten Sie, dass kontenübergreifender Zugriff nur mit bereitgestellten Amazon MSK-Clustern und nicht mit Amazon MSK Serverless-Clustern möglich ist. Der ARN für AWS `principal` sollte der ARN für dieselbe Pipeline-Rolle sein, die Sie für Ihre Pipeline-Konfiguration angeben:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "osis.amazonaws.com"
      },
      "Action": [
        "kafka:CreateVpcConnection",
        "kafka:DescribeClusterV2"
      ],
      "Resource": "arn:aws:kafka:region:msk-account-id:cluster/cluster-
name/cluster-id"
    },
    {
```

```
      "Effect": "Allow",
      "Principal": {
        "Service": "osis-pipelines.amazonaws.com"
      },
      "Action": [
        "kafka:CreateVpcConnection",
        "kafka:GetBootstrapBrokers",
        "kafka:DescribeClusterV2"
      ],
      "Resource": "arn:aws:kafka:region:msk-account-id:cluster/cluster-
name/cluster-id"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::pipeline-account-id:role/pipeline-role"
      },
      "Action": [
        "kafka-cluster:*",
        "kafka:*"
      ],
      "Resource": [
        "arn:aws:kafka:us-east-1:msk-account-id:cluster/cluster-name/cluster-
id",
        "arn:aws:kafka:us-east-1:msk-account-id:topic/cluster-name/cluster-id/
*",
        "arn:aws:kafka:us-east-1:msk-account-id:group/cluster-name/*"
      ]
    }
  ]
}
```

4. Erstellen Sie ein Kafka-Thema, indem Sie den Schritten unter Thema erstellen folgen. Stellen Sie sicher, dass *BootstrapServerString* es sich um einen Bootstrap für private Endgeräte (Single-VPC) handelt. URLs Der Wert für `--replication-factor` sollte 2 oder sein3, basierend auf der Anzahl der Zonen, die Ihr Amazon MSK-Cluster hat. Der Wert für `--partitions` sollte mindestens `1` sein.
5. Erzeugen und konsumieren Sie Daten, indem Sie die Schritte unter Daten produzieren und konsumieren befolgen. Stellen Sie auch hier sicher, dass *BootstrapServerString* es sich um einen Ihrer privaten Endgeräte (Single-VPC) -Bootstrap handelt. URLs

Voraussetzungen für Amazon MSK Serverless

Bevor Sie Ihre OpenSearch Ingestion-Pipeline erstellen, führen Sie die folgenden Schritte aus:

1. Erstellen Sie einen serverlosen Amazon MSK-Cluster, indem Sie den Schritten unter Create an MSK Serverless Cluster im Amazon Managed Streaming for Apache Kafka Developer Guide folgen.
2. Wenn der Cluster den Status Aktiv hat, folgen Sie den Schritten unter Eine Cluster-Richtlinie an den MSK-Cluster anhängen, um die folgende Richtlinie anzuhängen. Stellen Sie sicher, dass Sie das `resource` mit Ihrem eigenen ARN aktualisieren.

   JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "osis.amazonaws.com"
      },
      "Action": [
        "kafka:CreateVpcConnection",
        "kafka:DescribeClusterV2"
      ],
      "Resource": "arn:aws:kafka:region:account-id:cluster/cluster-
name/cluster-id"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "osis-pipelines.amazonaws.com"
      },
      "Action": [
        "kafka:CreateVpcConnection",
        "kafka:GetBootstrapBrokers",
        "kafka:DescribeClusterV2"
      ],
      "Resource": "arn:aws:kafka:region:account-id:cluster/cluster-
name/cluster-id"
    }
  ]
```

```
}
```

Diese Richtlinie ermöglicht es OpenSearch Ingestion, eine AWS PrivateLink Verbindung zu Ihrem Amazon MSK Serverless-Cluster herzustellen und Daten aus Kafka-Themen zu lesen. Diese Richtlinie gilt, wenn sich Ihr Cluster und Ihre Pipeline im selben System befinden. Dies muss zutreffen AWS-Konto, da Amazon MSK Serverless keinen kontoübergreifenden Zugriff unterstützt.

3. Erstellen Sie ein Kafka-Thema, indem Sie den Schritten unter Thema erstellen folgen. Stellen Sie sicher, dass *BootstrapServerString* es sich dabei um einen Ihrer SASL-IAM-Bootstraps (Simple Authentication and Security Layer) handelt. URLs Der Wert für `--replication-factor` sollte 2 oder sein3, basierend auf der Anzahl der Zonen, über die Ihr Amazon MSK Serverless-Cluster verfügt. Der Wert für `--partitions` sollte mindestens sein. `10`
4. Erzeugen und konsumieren Sie Daten, indem Sie die Schritte unter Daten produzieren und konsumieren befolgen. Stellen Sie auch hier sicher, dass *BootstrapServerString* es sich um einen Ihrer SASL-IAM-Bootstraps (Simple Authentication and Security Layer) handelt. URLs

Schritt 1: Konfigurieren Sie eine Pipeline-Rolle

Nachdem Sie Ihren von Amazon MSK bereitgestellten oder serverlosen Cluster eingerichtet haben, fügen Sie der Pipeline-Rolle, die Sie in Ihrer Pipeline-Konfiguration verwenden möchten, die folgenden Kafka-Berechtigungen hinzu:

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kafka-cluster:Connect",
                "kafka-cluster:AlterCluster",
                "kafka-cluster:DescribeCluster",
                "kafka:DescribeClusterV2",
                "kafka:GetBootstrapBrokers"
            ],
            "Resource": [
                "arn:aws:kafka:region:account-id:cluster/cluster-name/cluster-id"
            ]
```

```
        },
        {
            "Effect": "Allow",
            "Action": [
                "kafka-cluster:*Topic*",
                "kafka-cluster:ReadData"
            ],
            "Resource": [
                "arn:aws:kafka:region:account-id:topic/cluster-name/cluster-
id/topic-name"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "kafka-cluster:AlterGroup",
                "kafka-cluster:DescribeGroup"
            ],
            "Resource": [
                "arn:aws:kafka:region:account-id:group/cluster-name/*"
            ]
        }
    ]
}
```

Schritt 2: Erstellen Sie die Pipeline

Anschließend können Sie eine OpenSearch Ingestion-Pipeline wie die folgende konfigurieren, die Kafka als Quelle angibt:

```
version: "2"
log-pipeline:
  source:
    kafka:
      acknowledgements: true
      topics:
      - name: "topic-name"
        group_id: "grouplambd-id"
      aws:
        msk:
          arn: "arn:aws:kafka:region:account-id:cluster/cluster-name/cluster-id"
        region: "us-west-2"
```

```
  processor:
  - grok:
      match:
        message:
        - "%{COMMONAPACHELOG}"
  - date:
      destination: "@timestamp"
      from_time_received: true
  sink:
  - opensearch:
      hosts: ["https://search-domain-endpoint.us-east-1es.amazonaws.com"]
      index: "index_name"
      aws_region: "region"
      aws_sigv4: true
```

Sie können einen vorkonfigurierten Amazon MSK-Blueprint verwenden, um diese Pipeline zu erstellen. Weitere Informationen finden Sie unter the section called “Mit Blueprints arbeiten”.

Schritt 3: (Optional) Verwenden Sie die Schemaregistrierung AWS Glue

Wenn Sie OpenSearch Ingestion mit Amazon MSK verwenden, können Sie das AVRO-Datenformat für Schemas verwenden, die in der Schema Registry gehostet werden. AWS Glue Mit der AWS Glue Schema Registry können Sie Datenstromschemas zentral erkennen, steuern und weiterentwickeln.

Um diese Option zu verwenden, aktivieren Sie das Schema `type` in Ihrer Pipeline-Konfiguration:

```
schema:
  type: "aws_glue"
```

Sie müssen in Ihrer Pipeline-Rolle auch Lesezugriffsberechtigungen bereitstellen AWS Glue . Sie können die AWS verwaltete Richtlinie namens verwenden AWSGlueSchemaRegistryReadonlyAccess. Darüber hinaus muss sich Ihre Registrierung in derselben AWS-Konto Region wie Ihre OpenSearch Ingestion-Pipeline befinden.

Schritt 4: (Optional) Empfohlene Recheneinheiten (OCUs) für die Amazon MSK-Pipeline konfigurieren

Jede Recheneinheit hat einen Nutzer pro Thema. Makler gleichen die Partitionen zwischen diesen Verbrauchern für ein bestimmtes Thema aus. Wenn jedoch die Anzahl der Partitionen die Anzahl der Verbraucher übersteigt, hostet Amazon MSK mehrere Partitionen auf jedem Verbraucher.

OpenSearch Ingestion verfügt über eine integrierte auto Skalierung, mit der je nach CPU-Auslastung oder Anzahl ausstehender Datensätze in der Pipeline nach oben oder unten skaliert werden kann.

Um eine optimale Leistung zu erzielen, verteilen Sie Ihre Partitionen zur Parallelverarbeitung auf viele Recheneinheiten. Wenn Themen eine große Anzahl von Partitionen haben (z. B. mehr als 96, was das Maximum OCUs pro Pipeline ist), empfehlen wir, eine Pipeline mit 1—96 OCUs zu konfigurieren. Das liegt daran, dass sie bei Bedarf automatisch skaliert wird. Wenn ein Thema eine geringe Anzahl von Partitionen hat (z. B. weniger als 96), sollten Sie die maximale Recheneinheit der Anzahl der Partitionen anpassen.

Wenn eine Pipeline mehr als ein Thema enthält, wählen Sie das Thema mit der höchsten Anzahl von Partitionen als Referenz für die Konfiguration der maximalen Recheneinheiten aus. Indem Sie eine weitere Pipeline mit einem neuen Satz von OCUs zu demselben Thema und derselben Benutzergruppe hinzufügen, können Sie den Durchsatz nahezu linear skalieren.

Verwenden einer OpenSearch Ingestion-Pipeline mit Amazon S3

Mit OpenSearch Ingestion können Sie Amazon S3 als Quelle oder als Ziel verwenden. Wenn Sie Amazon S3 als Quelle verwenden, senden Sie Daten an eine OpenSearch Ingestion-Pipeline. Wenn Sie Amazon S3 als Ziel verwenden, schreiben Sie Daten aus einer OpenSearch Ingestion-Pipeline in einen oder mehrere S3-Buckets.

Themen

- Amazon S3 als Quelle
- Amazon S3 als Ziel
- Amazon S3 Cross-Konto als Quelle

Amazon S3 als Quelle

Es gibt zwei Möglichkeiten, Amazon S3 als Quelle für die Datenverarbeitung zu verwenden — mit der S3-SQS-Verarbeitung und mit geplanten Scans.

Verwenden Sie die S3-SQS-Verarbeitung, wenn Sie Dateien fast in Echtzeit scannen möchten, nachdem sie in S3 geschrieben wurden. Sie können Amazon S3 S3-Buckets so konfigurieren, dass sie jedes Mal ein Ereignis auslösen, wenn ein Objekt im Bucket gespeichert oder geändert wird. Verwenden Sie einen einmaligen oder wiederkehrenden geplanten Scan, um Daten in einem S3-Bucket stapelweise zu verarbeiten.

Themen

- Voraussetzungen
- Schritt 1: Konfigurieren Sie die Pipeline-Rolle
- Schritt 2: Erstellen Sie die Pipeline

Voraussetzungen

Um Amazon S3 als Quelle für eine OpenSearch Ingestion-Pipeline sowohl für einen geplanten Scan als auch für eine S3-SQS-Verarbeitung zu verwenden, erstellen Sie zunächst einen S3-Bucket.

> **Note**
>
> Wenn sich der S3-Bucket, der als Quelle in der OpenSearch Ingestion-Pipeline verwendet wird, in einem anderen befindet AWS-Konto, müssen Sie auch kontoübergreifende Leseberechtigungen für den Bucket aktivieren. Dadurch kann die Pipeline die Daten lesen und verarbeiten. Informationen zum Aktivieren kontoübergreifender Berechtigungen finden Sie unter Bucket-Besitzer, der kontoübergreifende Bucket-Berechtigungen erteilt im Amazon S3 S3-Benutzerhandbuch.
> Wenn sich Ihre S3-Buckets in mehreren Konten befinden, verwenden Sie eine Map. `bucket_owners` Ein Beispiel finden Sie in der Dokumentation unter Kontoübergreifender S3-Zugriff. OpenSearch

Um die S3-SQS-Verarbeitung einzurichten, müssen Sie außerdem die folgenden Schritte ausführen:

1. Erstellen Sie eine Amazon SQS SQS-Warteschlange.
2. Aktivieren Sie Ereignisbenachrichtigungen im S3-Bucket mit der SQS-Warteschlange als Ziel.

Schritt 1: Konfigurieren Sie die Pipeline-Rolle

Im Gegensatz zu anderen Quell-Plugins, die Daten in eine Pipeline übertragen, verfügt das S3-Quell-Plug-In über eine lesebasierte Architektur, bei der die Pipeline Daten aus der Quelle bezieht.

Damit eine Pipeline aus S3 lesen kann, müssen Sie daher eine Rolle in der S3-Quellkonfiguration der Pipeline angeben, die Zugriff sowohl auf den S3-Bucket als auch auf die Amazon SQS SQS-Warteschlange hat. Die Pipeline übernimmt diese Rolle, um Daten aus der Warteschlange zu lesen.

> **Note**
>
> Die Rolle, die Sie in der S3-Quellkonfiguration angeben, muss die Pipeline-Rolle sein. Daher muss Ihre Pipeline-Rolle zwei separate Berechtigungsrichtlinien enthalten — eine zum Schreiben in eine Senke und eine zum Abrufen aus der S3-Quelle. Sie müssen dasselbe `sts_role_arn` in allen Pipeline-Komponenten verwenden.

Die folgende Beispielrichtlinie zeigt die erforderlichen Berechtigungen für die Verwendung von S3 als Quelle:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action":[
          "s3:ListBucket",
          "s3:GetBucketLocation",
          "s3:GetObject"
       ],
      "Resource": "arn:aws:s3:::bucket-name/*"
    },
    {
       "Effect":"Allow",
       "Action":"s3:ListAllMyBuckets",
       "Resource":"arn:aws:s3:::*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "sqs:DeleteMessage",
        "sqs:ReceiveMessage",
        "sqs:ChangeMessageVisibility"
      ],
      "Resource": "arn:aws:sqs:us-west-2:account-id:MyS3EventSqsQueue"
    }
  ]
}
```

Sie müssen diese Berechtigungen an die IAM-Rolle anhängen, die Sie in der `sts_role_arn` Option in der Konfiguration des S3-Quell-Plug-ins angeben:

```
version: "2"
source:
  s3:
    ...
    aws:
      ...
processor:
  ...
sink:
  - opensearch:
      ...
```

Schritt 2: Erstellen Sie die Pipeline

Nachdem Sie Ihre Berechtigungen eingerichtet haben, können Sie je nach Ihrem Amazon OpenSearch S3-Anwendungsfall eine Ingestion-Pipeline konfigurieren.

S3-SQS-Verarbeitung

Um die S3-SQS-Verarbeitung einzurichten, konfigurieren Sie Ihre Pipeline so, dass sie S3 als Quelle angibt, und richten Sie Amazon SQS-Benachrichtigungen ein:

```
version: "2"
s3-pipeline:
  source:
    s3:
      notification_type: "sqs"
      codec:
        newline: null
      sqs:
        queue_url: "https://sqs.us-east-1amazonaws.com/account-id/ingestion-queue"
      compression: "none"
      aws:
        region: "region"
  processor:
  - grok:
      match:
        message:
        - "%{COMMONAPACHELOG}"
```

```
  - date:
      destination: "@timestamp"
      from_time_received: true
  sink:
  - opensearch:
      hosts: ["https://search-domain-endpoint.us-east-1es.amazonaws.com"]
      index: "index-name"
      aws:
        region: "region"
```

Wenn Sie bei der Verarbeitung kleiner Dateien auf Amazon S3 eine geringe CPU-Auslastung feststellen, sollten Sie erwägen, den Durchsatz zu erhöhen, indem Sie den Wert der `workers` Option ändern. Weitere Informationen finden Sie in den Konfigurationsoptionen des S3-Plug-ins.

Geplanter Scan

Um einen geplanten Scan einzurichten, konfigurieren Sie Ihre Pipeline mit einem Zeitplan auf Scanebene, der für alle Ihre S3-Buckets gilt, oder auf Bucket-Ebene. Ein Zeitplan auf Bucket-Ebene oder eine Konfiguration mit Scan-Intervallen überschreibt immer eine Konfiguration auf Scan-Ebene.

Sie können geplante Scans entweder mit einem einmaligen Scan konfigurieren, der sich ideal für die Datenmigration eignet, oder mit einem wiederkehrenden Scan, der sich ideal für die Stapelverarbeitung eignet.

Verwenden Sie die vorkonfigurierten Amazon S3-Blueprints, um Ihre Pipeline für das Lesen aus Amazon S3 zu konfigurieren. Sie können den `scan` Teil Ihrer Pipeline-Konfiguration bearbeiten, um Ihre Planungsanforderungen zu erfüllen. Weitere Informationen finden Sie unter the section called “Mit Blueprints arbeiten”.

Einmaliger Scan

Ein einmaliger geplanter Scan wird einmal ausgeführt. In Ihrer Pipeline-Konfiguration können Sie mit einem `start_time` und angebenend_time, wann die Objekte im Bucket gescannt werden sollen. Alternativ können `range` Sie das Zeitintervall im Verhältnis zur aktuellen Uhrzeit angeben, in dem die Objekte im Bucket gescannt werden sollen.

Zum Beispiel ein Bereich, der so eingestellt ist, dass alle Dateien PT4H gescannt werden, die in den letzten vier Stunden erstellt wurden. Um einen einmaligen Scan so zu konfigurieren, dass er ein zweites Mal ausgeführt wird, müssen Sie die Pipeline beenden und neu starten. Wenn Sie keinen Bereich konfiguriert haben, müssen Sie auch die Start- und Endzeiten aktualisieren.

Die folgende Konfiguration richtet einen einmaligen Scan für alle Buckets und alle Objekte in diesen Buckets ein:

```
version: "2"
log-pipeline:
  source:
    s3:
      codec:
        csv:
      compression: "none"
      aws:
        region: "region"
      acknowledgments: true
      scan:
        buckets:
          - bucket:
              name: my-bucket
              filter:
                include_prefix:
                  - Objects1/
                exclude_suffix:
                  - .jpeg
                  - .png
          - bucket:
              name: my-bucket-2
              key_prefix:
                include:
                  - Objects2/
                exclude_suffix:
                  - .jpeg
                  - .png
      delete_s3_objects_on_read: false
  processor:
    - date:
        destination: "@timestamp"
        from_time_received: true
  sink:
    - opensearch:
        hosts: ["https://search-domain-endpoint.us-east-1es.amazonaws.com"]
        index: "index-name"
        aws:
          region: "region"
        dlq:
```

```
          s3:
            bucket: "dlq-bucket"
            region: "us-east-1"
```

Die folgende Konfiguration richtet einen einmaligen Scan für alle Buckets während eines bestimmten Zeitfensters ein. Das bedeutet, dass S3 nur die Objekte verarbeitet, deren Erstellungszeiten in dieses Fenster fallen.

```
scan:
  start_time: 2023-01-21T18:00:00.000Z
  end_time: 2023-04-21T18:00:00.000Z
  buckets:
    - bucket:
        name: my-bucket-1
        filter:
          include:
            - Objects1/
          exclude_suffix:
            - .jpeg
            - .png
    - bucket:
        name: my-bucket-2
        filter:
          include:
            - Objects2/
          exclude_suffix:
            - .jpeg
            - .png
```

Die folgende Konfiguration richtet einen einmaligen Scan sowohl auf Scan- als auch auf Bucket-Ebene ein. Start- und Endzeiten auf Bucket-Ebene haben Vorrang vor Start- und Endzeiten auf Scan-Ebene.

```
scan:
  start_time: 2023-01-21T18:00:00.000Z
  end_time: 2023-04-21T18:00:00.000Z
  buckets:
    - bucket:
        start_time: 2023-01-21T18:00:00.000Z
        end_time: 2023-04-21T18:00:00.000Z
        name: my-bucket-1
        filter:
```

```
        include:
          - Objects1/
        exclude_suffix:
          - .jpeg
          - .png
    - bucket:
        start_time: 2023-01-21T18:00:00.000Z
        end_time: 2023-04-21T18:00:00.000Z
        name: my-bucket-2
        filter:
          include:
            - Objects2/
          exclude_suffix:
            - .jpeg
            - .png
```

Beim Stoppen einer Pipeline werden alle bereits vorhandenen Verweise darauf entfernt, welche Objekte vor dem Stopp von der Pipeline gescannt wurden. Wenn eine einzelne Scan-Pipeline gestoppt wird, werden alle Objekte nach dem Start erneut gescannt, auch wenn sie bereits gescannt wurden. Wenn Sie eine einzelne Scan-Pipeline beenden müssen, empfiehlt es sich, Ihr Zeitfenster zu ändern, bevor Sie die Pipeline erneut starten.

Wenn Sie Objekte nach Start- und Endzeit filtern müssen, ist das Stoppen und Starten der Pipeline die einzige Option. Wenn Sie nicht nach Start- und Endzeit filtern müssen, können Sie Objekte nach Namen filtern. Um nach Namen zu filtern, müssen Sie Ihre Pipeline nicht beenden und starten. Verwenden `include_prefix` Sie dazu und. `exclude_suffix`

Wiederkehrender Scan

Bei einem wiederkehrenden geplanten Scan werden Ihre angegebenen S3-Buckets in regelmäßigen, geplanten Intervallen gescannt. Sie können diese Intervalle nur auf Scanebene konfigurieren, da einzelne Konfigurationen auf Bucket-Ebene nicht unterstützt werden.

In Ihrer Pipeline-Konfiguration `interval` gibt der die Häufigkeit des wiederkehrenden Scans an und kann zwischen 30 Sekunden und 365 Tagen liegen. Der erste dieser Scans erfolgt immer, wenn Sie die Pipeline erstellen. Das `count` definiert die Gesamtzahl der Scan-Instanzen.

Die folgende Konfiguration richtet einen wiederkehrenden Scan mit einer Verzögerung von 12 Stunden zwischen den Scans ein:

```
scan:
```

```
  scheduling:
    interval: PT12H
    count: 4
  buckets:
    - bucket:
        name: my-bucket-1
        filter:
          include:
            - Objects1/
          exclude_suffix:
            - .jpeg
            - .png
    - bucket:
        name: my-bucket-2
        filter:
          include:
            - Objects2/
          exclude_suffix:
            - .jpeg
            - .png
```

Amazon S3 als Ziel

Um Daten aus einer OpenSearch Ingestion-Pipeline in einen S3-Bucket zu schreiben, verwenden Sie den vorkonfigurierten S3-Blueprint, um eine Pipeline mit einer S3-Senke zu erstellen. Diese Pipeline leitet selektive Daten an eine OpenSearch Senke weiter und sendet gleichzeitig alle Daten zur Archivierung in S3. Weitere Informationen finden Sie unter the section called “Mit Blueprints arbeiten”.

Wenn Sie Ihre S3-Senke erstellen, können Sie Ihre bevorzugte Formatierung anhand einer Vielzahl von Senken-Codecs angeben. Wenn Sie beispielsweise Daten im Spaltenformat schreiben möchten, wählen Sie den Parquet- oder Avro-Codec. Wenn Sie ein zeilenbasiertes Format bevorzugen, wählen Sie JSON oder NDJSON. Um Daten in einem bestimmten Schema nach S3 zu schreiben, können Sie mithilfe des Avro-Formats auch ein Inline-Schema innerhalb von Sink-Codecs definieren.

Das folgende Beispiel definiert ein Inline-Schema in einer S3-Senke:

```
- s3:
  codec:
    parquet:
      schema: >
        {
```

```
          "type" : "record",
          "namespace" : "org.vpcFlowLog.examples",
          "name" : "VpcFlowLog",
          "fields" : [
            { "name" : "version", "type" : "string"},
            { "name" : "srcport", "type": "int"},
            { "name" : "dstport", "type": "int"},
            { "name" : "start", "type": "int"},
            { "name" : "end", "type": "int"},
            { "name" : "protocol", "type": "int"},
            { "name" : "packets", "type": "int"},
            { "name" : "bytes", "type": "int"},
            { "name" : "action", "type": "string"},
            { "name" : "logStatus", "type" : "string"}
          ]
        }
```

Wenn Sie dieses Schema definieren, geben Sie eine Obermenge aller Schlüssel an, die in den verschiedenen Ereignistypen vorhanden sein könnten, die Ihre Pipeline an eine Senke übermittelt.

Wenn bei einem Ereignis beispielsweise die Möglichkeit besteht, dass ein Schlüssel fehlt, fügen Sie diesen Schlüssel mit einem `null` Wert in Ihr Schema ein. Nullwertdeklarationen ermöglichen es dem Schema, ungleichmäßige Daten zu verarbeiten (wobei einige Ereignisse diese Schlüssel haben und andere nicht). Wenn bei eingehenden Ereignissen diese Schlüssel vorhanden sind, werden ihre Werte in Senken geschrieben.

Diese Schemadefinition fungiert als Filter, der nur das Senden definierter Schlüssel an Senken ermöglicht und undefinierte Schlüssel aus eingehenden Ereignissen löscht.

Sie können auch `include_keys` und `exclude_keys` in Ihrer Senke verwenden, um Daten zu filtern, die an andere Senken weitergeleitet werden. Diese beiden Filter schließen sich gegenseitig aus, sodass Sie in Ihrem Schema jeweils nur einen Filter verwenden können. Darüber hinaus können Sie sie nicht in benutzerdefinierten Schemas verwenden.

Verwenden Sie den vorkonfigurierten Senkenfilter-Blueprint, um Pipelines mit solchen Filtern zu erstellen. Weitere Informationen finden Sie unter the section called “Mit Blueprints arbeiten”.

Amazon S3 Cross-Konto als Quelle

Sie können bei Amazon S3 kontenübergreifenden Zugriff gewähren, sodass OpenSearch Ingestion-Pipelines auf S3-Buckets in einem anderen Konto als Quelle zugreifen können. Informationen zum

Aktivieren des kontoübergreifenden Zugriffs finden Sie unter Bucket-Besitzer, der kontoübergreifende Bucket-Berechtigungen erteilt im Amazon S3 S3-Benutzerhandbuch. Nachdem Sie den Zugriff gewährt haben, stellen Sie sicher, dass Ihre Pipeline-Rolle über die erforderlichen Berechtigungen verfügt.

Anschließend können Sie eine Pipeline erstellen, die `bucket_owners` den kontoübergreifenden Zugriff auf einen Amazon S3 S3-Bucket als Quelle ermöglicht:

```
s3-pipeline:
 source:
  s3:
   notification_type: "sqs"
   codec:
    csv:
     delimiter: ","
     quote_character: "\""
     detect_header: True
   sqs:
    queue_url: "https://sqs.ap-northeast-1.amazonaws.com/401447383613/test-s3-queue"
   bucket_owners:
    my-bucket-01: 123456789012
    my-bucket-02: 999999999999
   compression: "gzip"
```

Verwenden einer OpenSearch Ingestion-Pipeline mit Amazon Security Lake

Sie können das S3-Quell-Plugin verwenden, um Daten von Amazon Security Lake in Ihre OpenSearch Ingestion-Pipeline aufzunehmen. Security Lake zentralisiert automatisch Sicherheitsdaten aus AWS Umgebungen, lokalen Umgebungen und SaaS-Anbietern in einem speziell dafür entwickelten Data Lake. Sie können ein Abonnement erstellen, das Daten aus Security Lake in Ihre OpenSearch Ingestion-Pipeline repliziert, die sie dann in Ihre Service-Domain oder Serverless-Sammlung schreibt. OpenSearch OpenSearch

Verwenden Sie den vorkonfigurierten Security Lake-Blueprint, um Ihre Pipeline so zu konfigurieren, dass sie aus Security Lake liest. Der Blueprint enthält eine Standardkonfiguration für die Aufnahme von Open Cybersecurity Schema Framework (OCSF) -Parkettdateien aus Security Lake. Weitere Informationen finden Sie unter the section called “Mit Blueprints arbeiten”.

Themen

- Verwenden einer OpenSearch Ingestion-Pipeline mit Amazon Security Lake als Quelle

- Verwendung einer OpenSearch Ingestion-Pipeline mit Amazon Security Lake als Senke

Verwenden einer OpenSearch Ingestion-Pipeline mit Amazon Security Lake als Quelle

Sie können das Amazon S3 S3-Quell-Plug-In in Ihrer OpenSearch Ingestion-Pipeline verwenden, um Daten aus Amazon Security Lake aufzunehmen. Security Lake zentralisiert automatisch Sicherheitsdaten aus AWS Umgebungen, lokalen Systemen und SaaS-Anbietern in einem speziell dafür entwickelten Data Lake.

Amazon Security Lake hat die folgenden Metadatenattribute innerhalb einer Pipeline:

- `bucket_name`: Der Name des Amazon S3 S3-Buckets, der von Security Lake zum Speichern von Sicherheitsdaten erstellt wurde.
- `path_prefix`: Der benutzerdefinierte Quellname, der in der Security Lake IAM-Rollenrichtlinie definiert ist.
- `region`: Der AWS-Region Ort, an dem sich der Security Lake S3-Bucket befindet.
- `accountID`: Die AWS-Konto ID, in der Security Lake aktiviert ist.
- `sts_role_arn`: Der ARN der IAM-Rolle, der für die Verwendung mit Security Lake vorgesehen ist.

Voraussetzungen

Bevor Sie Ihre OpenSearch Ingestion-Pipeline erstellen, führen Sie die folgenden Schritte aus:

- Aktivieren Sie Security Lake.
- Erstellen Sie einen Abonnenten in Security Lake.
  - Wählen Sie die Quellen aus, die Sie in Ihre Pipeline aufnehmen möchten.
  - Fügen Sie für Abonnentenanmeldedaten die ID des Ortes hinzu AWS-Konto , in dem Sie die Pipeline erstellen möchten. Geben Sie für die externe ID an`OpenSearchIngestion-{accountid}`.
  - Wählen Sie als Datenzugriffsmethode S3 aus.
  - Wählen Sie für Benachrichtigungsdetails die Option SQS-Warteschlange aus.

Wenn Sie einen Abonnenten erstellen, erstellt Security Lake automatisch zwei Inline-Berechtigungsrichtlinien — eine für S3 und eine für SQS. Die Richtlinien haben das folgende Format: und. `AmazonSecurityLake-{12345}-S3` `AmazonSecurityLake-{12345}-SQS`

Damit Ihre Pipeline auf die Abonnentenquellen zugreifen kann, müssen Sie Ihrer Pipeline-Rolle die erforderlichen Berechtigungen zuordnen.

Konfigurieren Sie die Pipeline-Rolle

Erstellen Sie eine neue Berechtigungsrichtlinie in IAM, die nur die erforderlichen Berechtigungen aus den beiden Richtlinien kombiniert, die Security Lake automatisch erstellt hat. Die folgende Beispielrichtlinie zeigt die geringste Berechtigung, die für eine OpenSearch Ingestion-Pipeline zum Lesen von Daten aus mehreren Security Lake-Quellen erforderlich ist:

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetObject"
         ],
         "Resource":[
            "arn:aws:s3:::aws-security-data-lake-region-abcde/aws/
LAMBDA_EXECUTION/1.0/*",
            "arn:aws:s3:::aws-security-data-lake-region-abcde/aws/S3_DATA/1.0/*",
            "arn:aws:s3:::aws-security-data-lake-region-abcde/aws/VPC_FLOW/1.0/
*",
            "arn:aws:s3:::aws-security-data-lake-region-abcde/aws/ROUTE53/1.0/*",
            "arn:aws:s3:::aws-security-data-lake-region-abcde/aws/
SH_FINDINGS/1.0/*"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "sqs:ReceiveMessage",
            "sqs:DeleteMessage"
         ],
         "Resource":[
            "arn:aws:sqs:region:account-id:AmazonSecurityLake-abcde-Main-Queue"
         ]
      }
   ]
```

```
}
```

> **Important**
>
> Security Lake verwaltet die Pipeline-Rollenrichtlinie nicht für Sie. Wenn Sie Quellen zu Ihrem Security Lake-Abonnement hinzufügen oder daraus entfernen, müssen Sie die Richtlinie manuell aktualisieren. Security Lake erstellt Partitionen für jede Protokollquelle, sodass Sie der Pipeline-Rolle manuell Berechtigungen hinzufügen oder entfernen müssen.

Sie müssen diese Berechtigungen der IAM-Rolle zuordnen, die Sie in der `sts_role_arn` Option in der Konfiguration des S3-Quell-Plug-ins unter `sqs` angeben.

```
version: "2"
source:
  s3:
    ...
    sqs:
      queue_url: "https://sqs.us-east-1amazonaws.com/account-id/
AmazonSecurityLake-abcde-Main-Queue"
    aws:
      ...
processor:
  ...
sink:
  - opensearch:
      ...
```

Erstellen Sie die Pipeline

Nachdem Sie der Pipeline-Rolle die Berechtigungen hinzugefügt haben, verwenden Sie den vorkonfigurierten Security Lake-Blueprint, um die Pipeline zu erstellen. Weitere Informationen finden Sie unter the section called “Mit Blueprints arbeiten”.

Sie müssen die `queue_url` Option in der `s3` Quellkonfiguration angeben. Dabei handelt es sich um die Amazon SQS SQS-Warteschlangen-URL, aus der gelesen werden soll. Um die URL zu formatieren, suchen Sie den Abonnement-Endpunkt in der Abonnentenkonfiguration und wechseln Sie `arn:aws:` zu`https://`. Beispiel, `https://sqs.us-east-1amazonaws.com/account-id/AmazonSecurityLake-abdcef-Main-Queue`.

`sts_role_arn`Das, was Sie in der S3-Quellkonfiguration angeben, muss der ARN der Pipeline-Rolle sein.

Verwendung einer OpenSearch Ingestion-Pipeline mit Amazon Security Lake als Senke

Verwenden Sie das Amazon S3 S3-Sink-Plugin in OpenSearch Ingestion, um Daten von jeder unterstützten Quelle an Amazon Security Lake zu senden. Security Lake sammelt und speichert Sicherheitsdaten von AWS lokalen Umgebungen und SaaS-Anbietern in einem speziellen Data Lake.

Um Ihre Pipeline so zu konfigurieren, dass Protokolldaten in Security Lake geschrieben werden, verwenden Sie den vorkonfigurierten Firewall-Datenverkehrsprotokoll-Blueprint. Der Blueprint beinhaltet eine Standardkonfiguration für das Abrufen von unformatierten Sicherheitsprotokollen oder anderen in einem Amazon S3 S3-Bucket gespeicherten Daten, für die Verarbeitung der Datensätze und deren Normalisierung. Anschließend ordnet er die Daten dem Open Cybersecurity Schema Framework (OCSF) zu und sendet die transformierten OCSF-konformen Daten an Security Lake.

Die Pipeline hat die folgenden Metadatenattribute:

- `bucket_name`: Der Name des Amazon S3 S3-Buckets, der von Security Lake zum Speichern von Sicherheitsdaten erstellt wurde.
- `path_prefix`: Der benutzerdefinierte Quellname, der in der Security Lake IAM-Rollenrichtlinie definiert ist.
- `region`: Der AWS-Region Ort, an dem sich der Security Lake S3-Bucket befindet.
- `accountID`: Die AWS-Konto ID, in der Security Lake aktiviert ist.
- `sts_role_arn`: Der ARN der IAM-Rolle, der für die Verwendung mit Security Lake vorgesehen ist.

Voraussetzungen

Bevor Sie eine Pipeline zum Senden von Daten an Security Lake erstellen, führen Sie die folgenden Schritte aus:

- Amazon Security Lake aktivieren und konfigurieren: Richten Sie Amazon Security Lake ein, um Sicherheitsdaten aus verschiedenen Quellen zu zentralisieren. Anweisungen finden Sie unter Security Lake über die Konsole aktivieren.

Wenn Sie eine Quelle auswählen, wählen Sie Bestimmte AWS Quellen aufnehmen und wählen Sie eine oder mehrere Protokoll- und Ereignisquellen aus, die Sie aufnehmen möchten.

- Berechtigungen einrichten: Konfigurieren Sie die Pipeline-Rolle mit den erforderlichen Berechtigungen, um Daten in Security Lake zu schreiben. Weitere Informationen finden Sie unter Pipeline-Rolle.

Erstellen Sie die Pipeline

Verwenden Sie den vorkonfigurierten Security Lake-Blueprint, um die Pipeline zu erstellen. Weitere Informationen finden Sie unter Verwenden von Blueprints zum Erstellen einer Pipeline.

Verwenden einer OpenSearch Ingestion-Pipeline mit Fluent Bit

Diese Fluent Bit-Beispielkonfigurationsdatei sendet Protokolldaten von Fluent Bit an eine Ingestion-Pipeline. OpenSearch Weitere Informationen zur Erfassung von Protokolldaten finden Sie unter Log Analytics in der Data Prepper-Dokumentation.

Beachten Sie Folgendes:

- Der `host` Wert muss Ihr Pipeline-Endpunkt sein. Beispiel, *`pipeline-endpoint`*`.`*`us-east-1`*`osis.amazonaws.com`.
- Der `aws_service`-Wert muss `osis` lauten.
- Der `aws_role_arn` Wert ist der ARN der AWS IAM-Rolle, den der Client annehmen und für die Signature Version 4-Authentifizierung verwenden soll.

```
[INPUT]
  name                  tail
  refresh_interval      5
  path                  /var/log/test.log
  read_from_head        true

[OUTPUT]
  Name http
  Match *
  Host pipeline-endpoint.us-east-1osis.amazonaws.com
  Port 443
  URI /log/ingest
  Format json
```

```
  aws_auth true
  aws_region region
  aws_service osis
  aws_role_arn arn:aws:iam::account-id:role/ingestion-role
  Log_Level trace
  tls On
```

Anschließend können Sie eine OpenSearch Ingestion-Pipeline wie die folgende konfigurieren, deren Quelle HTTP ist:

```
version: "2"
unaggregated-log-pipeline:
  source:
    http:
      path: "/log/ingest"
  processor:
    - grok:
        match:
          log:
            - "%{TIMESTAMP_ISO8601:timestamp} %{NOTSPACE:network_node}
 %{NOTSPACE:network_host} %{IPORHOST:source_ip}:%{NUMBER:source_port:int} ->
 %{IPORHOST:destination_ip}:%{NUMBER:destination_port:int} %{GREEDYDATA:details}"
    - grok:
        match:
          details:
            - "'%{NOTSPACE:http_method} %{NOTSPACE:http_uri}' %{NOTSPACE:protocol}"
            - "TLS%{NOTSPACE:tls_version} %{GREEDYDATA:encryption}"
            - "%{NUMBER:status_code:int} %{NUMBER:response_size:int}"
    - delete_entries:
        with_keys: ["details", "log"]

  sink:
    - opensearch:
        hosts: ["https://search-domain-endpoint.us-east-1es.amazonaws.com"]
        index: "index_name"
        index_type: custom
        bulk_size: 20
        aws:
          region: "region"
```

Verwenden einer OpenSearch Ingestion-Pipeline mit Fluentd

Fluentd ist ein Open-Source-Ökosystem zur Datenerfassung, das verschiedene Sprachen und Unterprojekte wie Fluent SDKs Bit bietet. Diese Fluentd-Beispielkonfigurationsdatei sendet Protokolldaten von Fluentd an eine Ingestion-Pipeline. OpenSearch Weitere Informationen zur Erfassung von Protokolldaten finden Sie unter Log Analytics in der Data Prepper-Dokumentation.

Beachten Sie Folgendes:

- Der `endpoint` Wert muss Ihr Pipeline-Endpunkt sein. Beispiel, *`pipeline-endpoint`*`.`*`us-east-1`*`osis.amazonaws.com/apache-log-pipeline/logs`.
- Der `aws_service`-Wert muss `osis` lauten.
- Der `aws_role_arn` Wert ist der ARN der AWS IAM-Rolle, den der Client annehmen und für die Signature Version 4-Authentifizierung verwenden soll.

```
<source>
  @type tail
  path logs/sample.log
  path_key log
  tag apache
  <parse>
    @type none
  </parse>
</source>

<filter apache>
  @type record_transformer
  <record>
    log ${record["message"]}
  </record>
</filter>

<filter apache>
  @type record_transformer
  remove_keys message
</filter>

<match apache>
  @type http
  endpoint pipeline-endpoint.us-east-1osis.amazonaws.com/apache-log-pipeline/logs
  json_array true
```

```
  <auth>
    method aws_sigv4
    aws_service osis
    aws_region region
    aws_role_arn arn:aws:iam::account-id:role/ingestion-role
  </auth>

  <format>
    @type json
  </format>

  <buffer>
    flush_interval 1s
  </buffer>
</match>
```

Anschließend können Sie eine OpenSearch Ingestion-Pipeline wie die folgende konfigurieren, deren Quelle HTTP ist:

```
version: "2"
apache-log-pipeline:
  source:
    http:
      path: "/${pipelineName}/logs"
  processor:
    - grok:
        match:
          log:
            - "%{TIMESTAMP_ISO8601:timestamp} %{NOTSPACE:network_node}
 %{NOTSPACE:network_host} %{IPORHOST:source_ip}:%{NUMBER:source_port:int} ->
 %{IPORHOST:destination_ip}:%{NUMBER:destination_port:int} %{GREEDYDATA:details}"
  sink:
    - opensearch:
        hosts: ["https://search-domain-endpoint.us-east-1es.amazonaws.com"]
        index: "index_name"
        aws_region: "region"
        aws_sigv4: true
```

Verwenden einer OpenSearch Ingestion-Pipeline mit Collector OpenTelemetry

Diese OpenTelemetry Beispielkonfigurationsdatei exportiert Trace-Daten aus dem OpenTelemetry Collector und sendet sie an eine OpenSearch Ingestion-Pipeline. Weitere Informationen zur Erfassung von Trace-Daten finden Sie unter Trace Analytics in der Data Prepper-Dokumentation.

Beachten Sie Folgendes:

- Der `endpoint` Wert muss Ihren Pipeline-Endpunkt enthalten. Beispiel, `https://pipeline-endpoint.us-east-1osis.amazonaws.com`.
- Der `service`-Wert muss `osis` lauten.
- Die `compression` Option für den OTLP/HTTP Exporter muss mit der `compression` Option für die OpenTelemetry Quelle der Pipeline übereinstimmen.

```
extensions:
  sigv4auth:
    region: "region"
    service: "osis"

receivers:
  jaeger:
    protocols:
      grpc:

exporters:
  otlphttp:
    traces_endpoint: "https://pipeline-endpoint.us-east-1.osis.amazonaws.com/v1/traces"
    auth:
      authenticator: sigv4auth
    compression: none

service:
  extensions: [sigv4auth]
  pipelines:
    traces:
      receivers: [jaeger]
      exporters: [otlphttp]
```

Sie können dann eine OpenSearch Ingestion-Pipeline wie die folgende konfigurieren, die das OTel Trace-Plugin als Quelle angibt:

```
version: "2"
otel-trace-pipeline:
  source:
    otel_trace_source:
      path: "/v1/traces"
  processor:
    - trace_peer_forwarder:
  sink:
    - pipeline:
        name: "trace-pipeline"
    - pipeline:
        name: "service-map-pipeline"
trace-pipeline:
  source:
    pipeline:
      name: "otel-trace-pipeline"
  processor:
    - otel_traces:
  sink:
    - opensearch:
        hosts: ["https://search-domain-endpoint.us-east-1.es.amazonaws.com"]
        index_type: trace-analytics-raw
        aws:
          region: "region"
service-map-pipeline:
  source:
    pipeline:
      name: "otel-trace-pipeline"
  processor:
    - service_map:
  sink:
    - opensearch:
        hosts: ["https://search-domain-endpoint.us-east-1.es.amazonaws.com"]
        index_type: trace-analytics-service-map
        aws:
          region: "region"
```

Ein weiteres Beispiel für eine Pipeline finden Sie im vorkonfigurierten Trace Analytics-Blueprint. Weitere Informationen finden Sie unter the section called “Mit Blueprints arbeiten”.

Verwenden einer OpenSearch Ingestion-Pipeline mit Kafka

Sie können das Kafka-Plugin verwenden, um Daten aus selbstverwalteten Kafka-Clustern zu Amazon OpenSearch Service-Domains und OpenSearch serverlosen Sammlungen zu streamen. OpenSearch Ingestion unterstützt Verbindungen von Kafka-Clustern, die entweder mit öffentlichen oder privaten Netzwerken (VPC) konfiguriert sind. In diesem Thema werden die Voraussetzungen und Schritte für die Einrichtung einer Ingestion-Pipeline beschrieben, einschließlich der Konfiguration von Netzwerkeinstellungen und Authentifizierungsmethoden wie Mutual TLS (mTLS), SASL/SCRAM oder IAM.

Migrieren von Daten aus öffentlichen Kafka-Clustern

Sie können OpenSearch Ingestion-Pipelines verwenden, um Daten aus einem öffentlichen, selbstverwalteten Kafka-Cluster zu migrieren, was bedeutet, dass der Domain-DNS-Name öffentlich aufgelöst werden kann. Richten Sie dazu eine OpenSearch Ingestion-Pipeline mit selbstverwaltetem Kafka als Quelle und Service oder Serverless als Ziel ein. OpenSearch OpenSearch Dadurch werden Ihre Streaming-Daten von einem selbstverwalteten Quellcluster zu einer AWS verwalteten Zieldomäne oder -sammlung verarbeitet.

Voraussetzungen

Bevor Sie Ihre OpenSearch Ingestion-Pipeline erstellen, führen Sie die folgenden Schritte aus:

1. Erstellen Sie einen selbstverwalteten Kafka-Cluster mit einer öffentlichen Netzwerkkonfiguration. Der Cluster sollte die Daten enthalten, die Sie in den Service aufnehmen möchten. OpenSearch
2. Erstellen Sie eine OpenSearch Dienstdomäne oder eine OpenSearch serverlose Sammlung, in die Sie Daten migrieren möchten. Weitere Informationen erhalten Sie unter the section called “ OpenSearch Dienstdomänen erstellen” und the section called “Erstellen von Sammlungen”.
3. Richten Sie die Authentifizierung auf Ihrem selbstverwalteten Cluster mit ein. AWS Secrets Manager Aktivieren Sie die Rotation von Geheimnissen, indem Sie die Schritte unter AWS Secrets Manager Geheimnisse rotieren befolgen.
4. Fügen Sie Ihrer Domain eine ressourcenbasierte Richtlinie oder Ihrer Sammlung eine Datenzugriffsrichtlinie hinzu. Diese Zugriffsrichtlinien ermöglichen es OpenSearch Ingestion, Daten aus Ihrem selbstverwalteten Cluster in Ihre Domain oder Sammlung zu schreiben.

   Die folgende Beispielrichtlinie für den Domänenzugriff ermöglicht es der Pipeline-Rolle, die Sie im nächsten Schritt erstellen, Daten in eine Domäne zu schreiben. Stellen Sie sicher, dass Sie das `resource` mit Ihrem eigenen ARN aktualisieren.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::pipeline-account-id:role/pipeline-role"
      },
      "Action": [
        "es:DescribeDomain",
        "es:ESHttp*"
      ],
      "Resource": [
        "arn:aws:es:region:account-id:domain/domain-name"
      ]
    }
  ]
}
```

Informationen zum Erstellen einer IAM-Rolle mit den richtigen Berechtigungen für den Zugriff auf Schreibdaten für die Sammlung oder Domäne finden Sie unterthe section called “Rollen und Benutzer einrichten”.

Schritt 1: Konfigurieren Sie die Pipeline-Rolle

Nachdem Sie Ihre Voraussetzungen für die Kafka-Pipeline eingerichtet haben, konfigurieren Sie die Pipeline-Rolle, die Sie in Ihrer Pipeline-Konfiguration verwenden möchten, und fügen Sie die Berechtigung zum Schreiben in eine OpenSearch Service-Domain oder eine OpenSearch Serverless-Sammlung sowie die Berechtigung zum Lesen von Geheimnissen aus Secrets Manager hinzu.

Schritt 2: Erstellen Sie die Pipeline

Anschließend können Sie eine OpenSearch Ingestion-Pipeline wie die folgende konfigurieren, die Kafka als Quelle angibt.

Sie können mehrere OpenSearch Dienstdomänen als Ziele für Ihre Daten angeben. Diese Funktion ermöglicht das bedingte Routing oder die Replikation eingehender Daten in mehrere OpenSearch Dienstdomänen.

Sie können auch Daten von einem Confluent Kafka-Quellcluster zu einer OpenSearch serverlosen VPC-Sammlung migrieren. Stellen Sie sicher, dass Sie in der Pipeline-Konfiguration eine Netzwerkzugriffsrichtlinie angeben. Sie können eine Confluent-Schemaregistrierung verwenden, um ein Confluent-Schema zu definieren.

```
version: "2"
kafka-pipeline:
  source:
    kafka:
      encryption:
        type: "ssl"
      topics:
        - name: "topic-name"
          group_id: "group-id"
      bootstrap_servers:
        - "bootstrap-server.us-east-1.aws.private.confluent.cloud:9092"
      authentication:
        sasl:
          plain:
            username: ${aws_secrets:confluent-kafka-secret:username}
            password: ${aws_secrets:confluent-kafka-secret:password}
      schema:
        type: confluent
        registry_url: https://my-registry.us-east-1.aws.confluent.cloud
        api_key: "${{aws_secrets:schema-secret:schema_registry_api_key}}"
        api_secret: "${{aws_secrets:schema-secret:schema_registry_api_secret}}"
        basic_auth_credentials_source: "USER_INFO"
  sink:
  - opensearch:
      hosts: ["https://search-mydomain.us-east-1.es.amazonaws.com"]
      aws:
          region: "us-east-1"
      index: "confluent-index"
extension:
  aws:
    secrets:
      confluent-kafka-secret:
        secret_id: "my-kafka-secret"
        region: "us-east-1"
      schema-secret:
        secret_id: "my-self-managed-kafka-schema"
        region: "us-east-1"
```

Sie können einen vorkonfigurierten Blueprint verwenden, um diese Pipeline zu erstellen. Weitere Informationen finden Sie unter the section called “Mit Blueprints arbeiten”.

Migrieren von Daten aus Kafka-Clustern in einer VPC

Sie können OpenSearch Ingestion-Pipelines auch verwenden, um Daten aus einem selbstverwalteten Kafka-Cluster zu migrieren, der in einer VPC ausgeführt wird. Richten Sie dazu eine OpenSearch Ingestion-Pipeline mit selbstverwaltetem Kafka als Quelle und Service oder Serverless als Ziel ein. OpenSearch OpenSearch Dadurch werden Ihre Streaming-Daten von einem selbstverwalteten Quellcluster zu einer AWS verwalteten Zieldomäne oder -sammlung verarbeitet.

Voraussetzungen

Bevor Sie Ihre OpenSearch Ingestion-Pipeline erstellen, führen Sie die folgenden Schritte aus:

1. Erstellen Sie einen selbstverwalteten Kafka-Cluster mit einer VPC-Netzwerkkonfiguration, die die Daten enthält, die Sie in Service aufnehmen möchten. OpenSearch
2. Erstellen Sie eine OpenSearch Dienstdomäne oder eine OpenSearch serverlose Sammlung, in die Sie Daten migrieren möchten. Weitere Informationen finden Sie unter OpenSearch Dienstdomänen erstellen und Sammlungen erstellen.
3. Richten Sie die Authentifizierung auf Ihrem selbstverwalteten Cluster mit AWS Secrets Manager ein. Aktivieren Sie die Rotation von Geheimnissen, indem Sie die Schritte unter AWS Secrets Manager Geheimnisse rotieren befolgen.
4. Rufen Sie die ID der VPC ab, die Zugriff auf selbstverwaltetes Kafka hat. Wählen Sie die VPC CIDR aus, die von OpenSearch Ingestion verwendet werden soll.

> **Note**
>
> Wenn Sie die AWS Management Console zum Erstellen Ihrer Pipeline verwenden, müssen Sie auch Ihre OpenSearch Ingestion-Pipeline an Ihre VPC anhängen, um selbstverwaltetes Kafka verwenden zu können. Suchen Sie dazu den Abschnitt Netzwerkkonfiguration, aktivieren Sie das Kontrollkästchen An VPC anhängen und wählen Sie Ihr CIDR aus einer der bereitgestellten Standardoptionen oder wählen Sie Ihre eigene aus. Sie können jedes CIDR aus einem privaten Adressraum verwenden, wie in der RFC 1918 Best Current Practice definiert.
> Um ein benutzerdefiniertes CIDR bereitzustellen, wählen Sie im Dropdownmenü die Option Andere aus. Um eine Kollision der IP-Adressen zwischen OpenSearch

Ingestion und Self-managed zu vermeiden, stellen Sie sicher OpenSearch, dass sich das selbstverwaltete OpenSearch VPC-CIDR vom CIDR für Ingestion unterscheidet. OpenSearch

5. Fügen Sie Ihrer Domain eine ressourcenbasierte Richtlinie oder Ihrer Sammlung eine Datenzugriffsrichtlinie hinzu. Diese Zugriffsrichtlinien ermöglichen es OpenSearch Ingestion, Daten aus Ihrem selbstverwalteten Cluster in Ihre Domain oder Sammlung zu schreiben.

   Die folgende Beispielrichtlinie für den Domänenzugriff ermöglicht es der Pipeline-Rolle, die Sie im nächsten Schritt erstellen, Daten in eine Domäne zu schreiben. Stellen Sie sicher, dass Sie das `resource` mit Ihrem eigenen ARN aktualisieren.

   JSON

   ```
   {
     "Version": "2012-10-17",
     "Statement": [
       {
         "Effect": "Allow",
         "Principal": {
           "AWS": "arn:aws:iam::pipeline-account-id:role/pipeline-role"
         },
         "Action": [
           "es:DescribeDomain",
           "es:ESHttp*"
         ],
         "Resource": [
           "arn:aws:es:region:account-id:domain/domain-name"
         ]
       }
     ]
   }
   ```

   Informationen zum Erstellen einer IAM-Rolle mit den richtigen Berechtigungen für den Zugriff auf Schreibdaten für die Sammlung oder Domäne finden Sie unterthe section called “Rollen und Benutzer einrichten”.

Schritt 1: Konfigurieren Sie die Pipeline-Rolle

Nachdem Sie Ihre Pipeline-Voraussetzungen eingerichtet haben, konfigurieren Sie die Pipeline-Rolle, die Sie in Ihrer Pipeline-Konfiguration verwenden möchten, und fügen Sie der Rolle die folgenden Berechtigungen hinzu:

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SecretsManagerReadAccess",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": ["arn:aws:secretsmanager:region:account-id:secret:secret-
name"]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachNetworkInterface",
                "ec2:CreateNetworkInterface",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteNetworkInterfacePermission",
                "ec2:DetachNetworkInterface",
                "ec2:DescribeNetworkInterfaces"
            ],
            "Resource": [
                "arn:aws:ec2:*:account-id:network-interface/*",
                "arn:aws:ec2:*:account-id:subnet/*",
                "arn:aws:ec2:*:account-id:security-group/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
```

```
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:Describe*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:*:*:network-interface/*",
            "Condition": {
               "StringEquals":
                    {
                        "aws:RequestTag/OSISManaged": "true"
                    }
            }
        }
    ]
}
```

Sie müssen die oben genannten EC2 Amazon-Berechtigungen für die IAM-Rolle bereitstellen, mit der Sie die OpenSearch Ingestion-Pipeline erstellen, da die Pipeline diese Berechtigungen verwendet, um eine Netzwerkschnittstelle in Ihrer VPC zu erstellen und zu löschen. Die Pipeline kann nur über diese Netzwerkschnittstelle auf den Kafka-Cluster zugreifen.

Schritt 2: Erstellen Sie die Pipeline

Anschließend können Sie eine OpenSearch Ingestion-Pipeline wie die folgende konfigurieren, die Kafka als Quelle angibt.

Sie können mehrere OpenSearch Dienstdomänen als Ziele für Ihre Daten angeben. Diese Funktion ermöglicht das bedingte Routing oder die Replikation eingehender Daten in mehrere OpenSearch Dienstdomänen.

Sie können auch Daten von einem Confluent Kafka-Quellcluster zu einer OpenSearch serverlosen VPC-Sammlung migrieren. Stellen Sie sicher, dass Sie in der Pipeline-Konfiguration eine Netzwerkzugriffsrichtlinie angeben. Sie können eine Confluent-Schemaregistrierung verwenden, um ein Confluent-Schema zu definieren.

```
 version: "2"
kafka-pipeline:
  source:
    kafka:
      encryption:
        type: "ssl"
      topics:
        - name: "topic-name"
          group_id: "group-id"
      bootstrap_servers:
        - "bootstrap-server.us-east-1.aws.private.confluent.cloud:9092"
      authentication:
        sasl:
          plain:
            username: ${aws_secrets:confluent-kafka-secret:username}
            password: ${aws_secrets:confluent-kafka-secret:password}
      schema:
        type: confluent
        registry_url: https://my-registry.us-east-1.aws.confluent.cloud
        api_key: "${{aws_secrets:schema-secret:schema_registry_api_key}}"
        api_secret: "${{aws_secrets:schema-secret:schema_registry_api_secret}}"
        basic_auth_credentials_source: "USER_INFO"
  sink:
  - opensearch:
      hosts: ["https://search-mydomain.us-east-1.es.amazonaws.com"]
      aws:
          region: "us-east-1"
      index: "confluent-index"
extension:
  aws:
    secrets:
      confluent-kafka-secret:
        secret_id: "my-kafka-secret"
        region: "us-east-1"
      schema-secret:
        secret_id: "my-self-managed-kafka-schema"
        region: "us-east-1"
```

Sie können einen vorkonfigurierten Blueprint verwenden, um diese Pipeline zu erstellen. Weitere Informationen finden Sie unter the section called “Mit Blueprints arbeiten”.

Migrieren von Daten aus selbstverwalteten OpenSearch Clustern mit Amazon Ingestion OpenSearch

Sie können eine Amazon OpenSearch Ingestion-Pipeline mit Selbstverwaltung OpenSearch oder Elasticsearch verwenden, um Daten zu Amazon OpenSearch Service-Domains und serverlosen Sammlungen zu migrieren. OpenSearch OpenSearch Ingestion unterstützt sowohl öffentliche als auch private Netzwerkkonfigurationen für die Migration von Daten aus Self-Managed und Elasticsearch. OpenSearch

Migration aus öffentlichen Clustern OpenSearch

Sie können OpenSearch Ingestion-Pipelines verwenden, um Daten aus einem selbstverwalteten Cluster OpenSearch oder einem Elasticsearch-Cluster mit einer öffentlichen Konfiguration zu migrieren, was bedeutet, dass der Domain-DNS-Name öffentlich aufgelöst werden kann. Richten Sie dazu eine OpenSearch Ingestion-Pipeline mit Self-managed OpenSearch oder Elasticsearch als Quelle und Service oder Serverless als Ziel ein. OpenSearch OpenSearch Dadurch werden Ihre Daten effektiv von einem selbstverwalteten Quell-Cluster zu einer -verwalteten Zieldomain oder -sammlung migriert. AWS

Voraussetzungen

Bevor Sie Ihre OpenSearch Ingestion-Pipeline erstellen, führen Sie die folgenden Schritte aus:

1. Erstellen Sie einen selbstverwalteten Cluster OpenSearch oder Elastisearch-Cluster, der die Daten enthält, die Sie migrieren möchten, und konfigurieren Sie einen öffentlichen DNS-Namen. Anweisungen finden Sie in der Dokumentation unter Einen Cluster erstellen. OpenSearch
2. Erstellen Sie eine OpenSearch Dienstdomäne oder eine OpenSearch serverlose Sammlung, in die Sie Daten migrieren möchten. Weitere Informationen erhalten Sie unter the section called “ OpenSearch Dienstdomänen erstellen” und the section called “Erstellen von Sammlungen”.
3. Richten Sie die Authentifizierung auf Ihrem selbstverwalteten Cluster mit ein. AWS Secrets Manager Aktivieren Sie die Rotation von Geheimnissen, indem Sie die Schritte unter AWS Secrets Manager Geheimnisse rotieren befolgen.
4. Fügen Sie Ihrer Domain eine ressourcenbasierte Richtlinie oder Ihrer Sammlung eine Datenzugriffsrichtlinie hinzu. Diese Zugriffsrichtlinien ermöglichen es OpenSearch Ingestion, Daten aus Ihrem selbstverwalteten Cluster in Ihre Domain oder Sammlung zu schreiben.

Die folgende Beispielrichtlinie für den Domänenzugriff ermöglicht es der Pipeline-Rolle, die Sie im nächsten Schritt erstellen, Daten in eine Domäne zu schreiben. Stellen Sie sicher, dass Sie das `resource` mit Ihrem eigenen ARN aktualisieren.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::pipeline-account-id:role/pipeline-role"
      },
      "Action": [
        "es:DescribeDomain",
        "es:ESHttp*"
      ],
      "Resource": [
        "arn:aws:es:region:account-id:domain/domain-name"
      ]
    }
  ]
}
```

Informationen zum Erstellen einer IAM-Rolle mit den richtigen Berechtigungen für den Zugriff auf Schreibdaten für die Sammlung oder Domäne finden Sie unterthe section called “Rollen und Benutzer einrichten”.

Schritt 1: Konfigurieren Sie die Pipeline-Rolle

Nachdem Sie Ihre OpenSearch Pipeline-Voraussetzungen eingerichtet haben, konfigurieren Sie die Pipeline-Rolle, die Sie in Ihrer Pipeline-Konfiguration verwenden möchten, und fügen Sie die Berechtigung zum Schreiben in eine OpenSearch Service-Domain oder OpenSearch Serverless-Sammlung sowie die Berechtigung zum Lesen von Geheimnissen aus Secrets Manager hinzu.

Schritt 2: Erstellen Sie die Pipeline

Anschließend können Sie eine OpenSearch Ingestion-Pipeline wie die folgende konfigurieren, die OpenSearch als Quelle angegeben wird.

Sie können mehrere OpenSearch Dienstdomänen als Ziele für Ihre Daten angeben. Diese Funktion ermöglicht das bedingte Routing oder die Replikation eingehender Daten in mehrere OpenSearch Dienstdomänen.

Sie können auch Daten von einem Quell OpenSearch - oder Elasticsearch-Cluster zu einer OpenSearch serverlosen VPC-Sammlung migrieren. Stellen Sie sicher, dass Sie in der Pipeline-Konfiguration eine Netzwerkzugriffsrichtlinie angeben.

```
version: "2"
opensearch-migration-pipeline:
  source:
    opensearch:
      acknowledgments: true
      host: [ "https://my-self-managed-cluster-name:9200" ]
      indices:
        include:
          - index_name_regex: "include-.*"
        exclude:
          - index_name_regex: '\..*'
      authentication:
        username: ${aws_secrets:secret:username}
        password: ${aws_secrets:secret:password}
        scheduling:
           interval: "PT2H"
           index_read_count: 3
           start_time: "2023-06-02T22:01:30.00Z"
  sink:
  - opensearch:
      hosts: ["https://search-mydomain.us-east-1.es.amazonaws.com"]
      aws:
          region: "us-east-1"
          #Uncomment the following lines if your destination is an OpenSearch
 Serverless collection
          #serverless: true
          # serverless_options:
          #     network_policy_name: "network-policy-name"
      index: "${getMetadata(\"opensearch-index\")}"
      document_id: "${getMetadata(\"opensearch-document_id\")}"
      enable_request_compression: true
      dlq:
        s3:
          bucket: "bucket-name"
          key_path_prefix: "apache-log-pipeline/logs/dlq"
```

```
          region: "us-east-1"
extension:
  aws:
    secrets:
      secret:
        secret_id: "my-opensearch-secret"
        region: "us-east-1"
        refresh_interval: PT1H
```

Sie können einen vorkonfigurierten Blueprint verwenden, um diese Pipeline zu erstellen. Weitere Informationen finden Sie unter the section called “Mit Blueprints arbeiten”.

Daten aus OpenSearch Clustern in einer VPC migrieren

Sie können OpenSearch Ingestion-Pipelines auch verwenden, um Daten aus einem selbstverwalteten OpenSearch oder Elasticsearch-Cluster zu migrieren, der in einer VPC ausgeführt wird. Richten Sie dazu eine OpenSearch Ingestion-Pipeline mit Self-managed OpenSearch oder Elasticsearch als Quelle und Service oder Serverless als Ziel ein. OpenSearch OpenSearch Dadurch werden Ihre Daten effektiv von einem selbstverwalteten Quell-Cluster zu einer -verwalteten Zieldomain oder -sammlung migriert. AWS

Voraussetzungen

Bevor Sie Ihre OpenSearch Ingestion-Pipeline erstellen, führen Sie die folgenden Schritte aus:

1. Erstellen Sie einen selbstverwalteten Cluster OpenSearch oder Elastisearch-Cluster mit einer VPC-Netzwerkkonfiguration, die die Daten enthält, die Sie migrieren möchten.
2. Erstellen Sie eine OpenSearch Service-Domain oder eine OpenSearch serverlose Sammlung, in die Sie Daten migrieren möchten. Weitere Informationen finden Sie unter OpenSearch Dienstdomänen erstellen und Sammlungen erstellen.
3. Richten Sie die Authentifizierung auf Ihrem selbstverwalteten Cluster mit AWS Secrets Manager ein. Aktivieren Sie die Rotation von Geheimnissen, indem Sie die Schritte unter AWS Secrets Manager Geheimnisse rotieren befolgen.
4. Rufen Sie die ID der VPC ab, die Zugriff auf Self-Managed OpenSearch oder Elasticsearch hat. Wählen Sie die VPC CIDR aus, die von OpenSearch Ingestion verwendet werden soll.

> **Note**
>
> Wenn Sie die verwenden, um Ihre Pipeline AWS Management Console zu erstellen, müssen Sie auch Ihre OpenSearch Ingestion-Pipeline an Ihre VPC anhängen, um

OpenSearch Self-Managed oder Elasticsearch verwenden zu können. Suchen Sie dazu den Abschnitt Quellnetzwerkoptionen, aktivieren Sie das Kontrollkästchen An VPC anhängen und wählen Sie Ihr CIDR aus einer der bereitgestellten Standardoptionen aus. Sie können jedes CIDR aus einem privaten Adressraum verwenden, wie in RFC 1918 Best Current Practice definiert.
Um ein benutzerdefiniertes CIDR bereitzustellen, wählen Sie im Dropdownmenü die Option Andere aus. Um eine Kollision der IP-Adressen zwischen OpenSearch Ingestion und Self-managed zu vermeiden, stellen Sie sicher OpenSearch, dass sich das selbstverwaltete OpenSearch VPC-CIDR vom CIDR für Ingestion unterscheidet. OpenSearch

5. Fügen Sie Ihrer Domain eine ressourcenbasierte Richtlinie oder Ihrer Sammlung eine Datenzugriffsrichtlinie hinzu. Diese Zugriffsrichtlinien ermöglichen es OpenSearch Ingestion, Daten aus Ihrem selbstverwalteten Cluster in Ihre Domain oder Sammlung zu schreiben.

   Die folgende Beispielrichtlinie für den Domänenzugriff ermöglicht es der Pipeline-Rolle, die Sie im nächsten Schritt erstellen, Daten in eine Domäne zu schreiben. Stellen Sie sicher, dass Sie das `resource` mit Ihrem eigenen ARN aktualisieren.

   JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::pipeline-account-id:role/pipeline-role"
      },
      "Action": [
        "es:DescribeDomain",
        "es:ESHttp*"
      ],
      "Resource": [
        "arn:aws:es:region:account-id:domain/domain-name"
      ]
    }
  ]
}
```

Informationen zum Erstellen einer IAM-Rolle mit den richtigen Berechtigungen für den Zugriff auf Schreibdaten für die Sammlung oder Domäne finden Sie unterthe section called “Rollen und Benutzer einrichten”.

Schritt 1: Konfigurieren Sie die Pipeline-Rolle

Nachdem Sie Ihre Pipeline-Voraussetzungen eingerichtet haben, konfigurieren Sie die Pipeline-Rolle, die Sie in Ihrer Pipeline-Konfiguration verwenden möchten, und fügen Sie der Rolle die folgenden Berechtigungen hinzu:

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SecretsManagerReadAccess",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": ["arn:aws:secretsmanager:region:account-id:secret:secret-
name"]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachNetworkInterface",
                "ec2:CreateNetworkInterface",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteNetworkInterfacePermission",
                "ec2:DetachNetworkInterface",
                "ec2:DescribeNetworkInterfaces"
            ],
            "Resource": [
                "arn:aws:ec2:*:account-id:network-interface/*",
                "arn:aws:ec2:*:account-id:subnet/*",
                "arn:aws:ec2:*:account-id:security-group/*"
            ]
        },
```

```
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:Describe*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:*:*:network-interface/*",
            "Condition": {
               "StringEquals":
                    {
                        "aws:RequestTag/OSISManaged": "true"
                    }
            }
        }
    ]
}
```

Sie müssen die oben genannten EC2 Amazon-Berechtigungen für die IAM-Rolle bereitstellen, mit der Sie die OpenSearch Ingestion-Pipeline erstellen, da die Pipeline diese Berechtigungen verwendet, um eine Netzwerkschnittstelle in Ihrer VPC zu erstellen und zu löschen. Die Pipeline kann nur über diese Netzwerkschnittstelle auf den OpenSearch Cluster zugreifen.

Schritt 2: Erstellen Sie die Pipeline

Anschließend können Sie eine OpenSearch Ingestion-Pipeline wie die folgende konfigurieren, die OpenSearch als Quelle angegeben wird.

Sie können mehrere OpenSearch Dienstdomänen als Ziele für Ihre Daten angeben. Diese Funktion ermöglicht das bedingte Routing oder die Replikation eingehender Daten in mehrere OpenSearch Dienstdomänen.

Sie können auch Daten von einem Quell OpenSearch - oder Elasticsearch-Cluster zu einer OpenSearch serverlosen VPC-Sammlung migrieren. Stellen Sie sicher, dass Sie in der Pipeline-Konfiguration eine Netzwerkzugriffsrichtlinie angeben.

```
version: "2"
opensearch-migration-pipeline:
  source:
    opensearch:
      acknowledgments: true
      host: [ "https://my-self-managed-cluster-name:9200" ]
      indices:
        include:
          - index_name_regex: "include-.*"
        exclude:
          - index_name_regex: '\..*'
      authentication:
        username: ${aws_secrets:secret:username}
        password: ${aws_secrets:secret:password}
        scheduling:
           interval: "PT2H"
           index_read_count: 3
           start_time: "2023-06-02T22:01:30.00Z"
  sink:
  - opensearch:
      hosts: ["https://search-mydomain.us-east-1.es.amazonaws.com"]
      aws:
          region: "us-east-1"
          #Uncomment the following lines if your destination is an OpenSearch
 Serverless collection
          #serverless: true
          # serverless_options:
          #     network_policy_name: "network-policy-name"
      index: "${getMetadata(\"opensearch-index\")}"
      document_id: "${getMetadata(\"opensearch-document_id\")}"
      enable_request_compression: true
      dlq:
        s3:
          bucket: "bucket-name"
          key_path_prefix: "apache-log-pipeline/logs/dlq"
          region: "us-east-1"
extension:
  aws:
    secrets:
```

```
      secret:
        secret_id: "my-opensearch-secret"
        region: "us-east-1"
        refresh_interval: PT1H
```

Sie können einen vorkonfigurierten Blueprint verwenden, um diese Pipeline zu erstellen. Weitere Informationen finden Sie unter the section called “Mit Blueprints arbeiten”.

Verwenden einer OpenSearch Ingestion-Pipeline mit Amazon Kinesis Data Streams

Sie können das Kinesis-Plug-In verwenden, um Daten von Amazon Kinesis Data Streams zu Amazon OpenSearch Service-Domains und OpenSearch serverlosen Sammlungen zu streamen. Die Pipeline ruft Datensätze von Amazon Kinesis ab OpenSearch, sendet sie an und generiert automatisch Indizes auf der Grundlage des Stream-Namens und des aktuellen Datums.

Konnektivität zu Amazon Kinesis Data Streams

Sie können OpenSearch Ingestion-Pipelines verwenden, um Daten aus Amazon Kinesis Data Streams mit öffentlicher Konfiguration zu migrieren, was bedeutet, dass der Domain-DNS-Name öffentlich aufgelöst werden kann. Richten Sie dazu eine OpenSearch Ingestion-Pipeline mit Amazon Kinesis Data Streams als Quelle und OpenSearch Service oder OpenSearch Serverless als Ziel ein. Dadurch werden Ihre Streaming-Daten von einem selbstverwalteten Quell-Cluster zu einer verwalteten Zieldomäne oder AWS-sammlung verarbeitet.

Voraussetzungen

Bevor Sie Ihre OpenSearch Ingestion-Pipeline erstellen, führen Sie die folgenden Schritte aus:

1. Erstellen Sie einen Amazon Kinesis Kinesis-Datenstream, der als Quelle dient. Der Stream sollte die Daten enthalten, die Sie in OpenSearch Service aufnehmen möchten.
2. Erstellen Sie eine OpenSearch Dienstdomäne oder eine OpenSearch serverlose Sammlung, in die Sie Daten migrieren möchten. Weitere Informationen finden Sie unter OpenSearch Dienstdomänen erstellen und Sammlungen erstellen.
3. Richten Sie die Authentifizierung für Ihren Amazon Kinesis Kinesis-Datenstrom mit AWS Secrets Manager ein. Aktivieren Sie die Rotation von Geheimnissen, indem Sie die Schritte unter AWS Secrets Manager Geheimnisse rotieren befolgen.

4. Fügen Sie Ihrer Domain eine ressourcenbasierte Richtlinie oder Ihrer Sammlung eine Datenzugriffsrichtlinie hinzu. Diese Zugriffsrichtlinien ermöglichen es OpenSearch Ingestion, Daten aus Ihrem selbstverwalteten Cluster in Ihre Domain oder Sammlung zu schreiben.

   Die folgende Beispielrichtlinie für den Domänenzugriff ermöglicht es der Pipeline-Rolle, die Sie im nächsten Schritt erstellen, Daten in eine Domäne zu schreiben. Stellen Sie sicher, dass Sie das `resource` mit Ihrem eigenen ARN aktualisieren.

   JSON

   ```
   {
     "Version": "2012-10-17",
     "Statement": [
       {
         "Effect": "Allow",
         "Principal": {
           "AWS": "arn:aws:iam::account-id:role/pipeline-role"
         },
         "Action": [
           "es:DescribeDomain",
           "es:ESHttp*"
         ],
         "Resource": [
           "arn:aws:es:region:account-id:domain/domain-name"
         ]
       }
     ]
   }
   ```

   Informationen zum Erstellen einer IAM-Rolle mit den richtigen Berechtigungen für den Zugriff auf Schreibdaten für die Sammlung oder Domäne finden Sie unterthe section called “Rollen und Benutzer einrichten”.

Schritt 1: Konfigurieren Sie die Pipeline-Rolle

Nachdem Sie die Voraussetzungen für die Amazon Kinesis Data Streams Streams-Pipeline eingerichtet haben, konfigurieren Sie die Pipeline-Rolle, die Sie in Ihrer Pipeline-Konfiguration verwenden möchten, und fügen Sie die Berechtigung zum Schreiben in eine OpenSearch Service-Domain oder eine OpenSearch Serverless-Sammlung sowie die Berechtigung zum Lesen von Geheimnissen aus Secrets Manager hinzu.

Die folgende Berechtigung ist erforderlich, um in einen Amazon S3 S3-Bucket, eine Domain und eine Sammlung zu schreiben:

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "allowReadFromStream",
            "Effect": "Allow",
            "Action": [
                "kinesis:DescribeStream",
                "kinesis:DescribeStreamConsumer",
                "kinesis:DescribeStreamSummary",
                "kinesis:GetRecords",
                "kinesis:GetShardIterator",
                "kinesis:ListShards",
                "kinesis:ListStreams",
                "kinesis:ListStreamConsumers",
                "kinesis:RegisterStreamConsumer",
                "kinesis:SubscribeToShard"
            ],
            "Resource": [
                "arn:aws:kinesis:region:account-id:stream/stream-name"
            ]
        }
    ]
}
```

Wenn die serverseitige Verschlüsselung für Streams aktiviert ist, entschlüsselt die folgende KMS-Richtlinie die Stream-Datensätze:

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "allowDecryptionOfCustomManagedKey",
```

```
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "arn:aws:kms:region:account-id:key/key-id"
        }
    ]
}
```

Damit eine Pipeline Daten in eine Domäne schreiben kann, muss die Domäne über eine Zugriffsrichtlinie auf Domänenebene verfügen, die der Pipeline-Rolle sts_role_arn den Zugriff darauf ermöglicht. Die folgende Beispielrichtlinie für den Domänenzugriff ermöglicht es der Pipeline-Rolle mit dem Namen`pipeline-role`, die Sie im vorherigen Schritt erstellt haben, Daten in die angegebene Domäne zu schreiben: `ingestion-domain`

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::account-id:role/pipeline-role"
      },
      "Action": ["es:DescribeDomain", "es:ESHttp*"],
      "Resource": "arn:aws:es:region:account-id:domain/domain-name/*"
    }
  ]
}
```

Schritt 2: Erstellen Sie die Pipeline

Anschließend können Sie eine OpenSearch Ingestion-Pipeline konfigurieren, die Amazon Kinesis als Quelle angibt. Die verfügbaren Metadatenattribute sind:

- `stream_name`: Name des Kinesis-Datenstroms, aus dem der Datensatz aufgenommen wird.
- `partition_key`: Partitionsschlüssel des Kinesis-Datenstream-Datensatzes, der aufgenommen wird.
- `sequence_number`: Sequenznummer des Kinesis-Datenstream-Datensatzes, der aufgenommen wird.

- `sub_sequence_number`: Untersequenznummer des Kinesis-Datenstream-Datensatzes, der aufgenommen wird.

Sie können mehrere OpenSearch Service-Domains als Ziele für Ihre Daten angeben. Diese Funktion ermöglicht das bedingte Routing oder die Replikation eingehender Daten in mehrere OpenSearch Dienstdomänen.

Sie können auch Daten von Amazon Kinesis zu einer OpenSearch serverlosen VPC-Sammlung migrieren. Auf der OpenSearch Ingestion-Konsole ist ein Blueprint zum Erstellen einer Pipeline verfügbar. Um eine Pipeline zu erstellen, können Sie den folgenden Blueprint verwenden. `AWS-KinesisDataStreamsPipeline`

```
version: "2"
     kinesis_data_streams_pipeline:
       source:
         kinesis_data_streams:
           acknowledgments: true
           codec:
             newline:
           streams:
             - stream_name: "<stream name>"
             - stream_name: "<stream name>"
           aws:
             region: "region"
       sink:
         - opensearch:
             hosts: [ "https://search-mydomain.region.es.amazonaws.com" ]
             index: "index_${getMetadata(\"stream-name\")}"
             document_id: "${getMetadata(\"partition_key\")}"
             aws:
               sts_role_arn: "<<arn:aws:iam::123456789012:role/Example-Role>>"
               region: "region"

               s3:
                 bucket: "dlq-bucket-name"
                 region: "region"
```

Sie können einen vorkonfigurierten Blueprint verwenden, um diese Pipeline zu erstellen. Weitere Informationen finden Sie unter the section called “Mit Blueprints arbeiten”. Weitere Konfigurationsoptionen finden Sie auch in der OpenSource-OpenSearch-Dokumentation. Weitere Informationen finden Sie unter Konfigurationsoptionen.

Datenkonsistenz

OpenSearch Die Datenaufnahme unterstützt die end-to-end Bestätigung, um die Datenbeständigkeit zu gewährleisten. Wenn die Pipeline Stream-Datensätze aus Kinesis liest, verteilt sie die Arbeit beim Lesen von Stream-Datensätzen dynamisch auf der Grundlage der mit dem Stream verknüpften Shards. Die Pipeline überprüft Streams automatisch, wenn sie nach der Aufnahme aller Datensätze in der Domain oder Sammlung eine Bestätigung erhält. OpenSearch Dadurch wird eine doppelte Verarbeitung von Stream-Datensätzen vermieden.

> **Note**
>
> Wenn Sie den Index auf der Grundlage des Stream-Namens erstellen möchten, können Sie den Index im Opensearch-Senkbereich als „index_$ {getMetadata (\“***stream_name***\“)}“ definieren.

(Optional) Empfohlene Recheneinheiten (OCUs) für die Kinesis Data Streams Streams-Pipeline konfigurieren

Beim Erstellen einer Kinesis-Quellpipeline werden mindestens 2 Recheneinheiten (OCU) empfohlen. Dadurch können die Kinesis-Datenstream-Datensätze pro Shard-Verarbeitung gleichmäßig auf die Recheneinheiten verteilt werden, wodurch ein Mechanismus mit geringer Latenz für die Aufnahme von Stream-Datensätzen gewährleistet wird.

Eine OpenSearchKinesis Datenstream-Quellpipeline kann auch so konfiguriert werden, dass Stream-Datensätze aus mehr als einem Stream aufgenommen werden. Es wird empfohlen, pro neuem Stream eine zusätzliche Recheneinheit hinzuzufügen.

> **Note**
>
> Wenn Ihre Pipeline über mehr Recheneinheiten (OCU) verfügt, als in der Gruppe von Streams, die in der Pipeline konfiguriert sind, Shards vorhanden sind, könnten einige Recheneinheiten inaktiv sein, ohne dass Stream-Datensätze pro Shard verarbeitet werden.

Nächste Schritte

Nachdem Sie Ihre Daten in eine Pipeline exportiert haben, können Sie sie von der OpenSearch Service-Domain abfragen, die als Senke für die Pipeline konfiguriert ist. Die folgenden Ressourcen können Ihnen den Einstieg erleichtern:

- Beobachtbarkeit
- the section called “Trace Analytics”
- the section called “Piped Processing Language”

Verwenden einer OpenSearch Ingestion-Pipeline mit AWS Lambda

Verwenden Sie den AWS Lambda Prozessor, um Daten aus beliebigen Quellen oder Zielen, die von OpenSearch Ingestion unterstützt werden, mithilfe von benutzerdefiniertem Code anzureichern. Mit dem Lambda-Prozessor können Sie Ihre eigenen Datentransformationen oder -anreicherungen anwenden und die verarbeiteten Ereignisse dann zur weiteren Verarbeitung an Ihre Pipeline zurücksenden. Dieser Prozessor ermöglicht eine maßgeschneiderte Datenverarbeitung und gibt Ihnen die volle Kontrolle darüber, wie Daten manipuliert werden, bevor sie die Pipeline durchlaufen.

> **Note**
>
> Die maximale Nutzlastgröße für ein einzelnes Ereignis, das von einem Lambda-Prozessor verarbeitet wird, beträgt 5 MB. Darüber hinaus unterstützt der Lambda-Prozessor nur Antworten im JSON-Array-Format.

Voraussetzungen

Bevor Sie eine Pipeline mit einem Lambda-Prozessor erstellen, erstellen Sie die folgenden Ressourcen:

- Eine AWS Lambda Funktion, die Ihre Quelldaten anreichert und transformiert. Anweisungen finden Sie unter Erstellen Sie Ihre erste Lambda-Funktion.
- Eine OpenSearch Dienstdomäne oder eine OpenSearch serverlose Sammlung, die als Pipeline-Senke fungiert. Weitere Informationen erhalten Sie unter the section called “ OpenSearch Dienstdomänen erstellen” und the section called “Erstellen von Sammlungen”.

- Eine Pipeline-Rolle, die Berechtigungen zum Schreiben in die Domäne oder Sammlungssenke beinhaltet. Weitere Informationen finden Sie unter the section called “Rolle „Pipeline“”.

  Die Pipeline-Rolle benötigt außerdem eine angehängte Berechtigungsrichtlinie, die es ihr ermöglicht, die in der Pipeline-Konfiguration angegebene Lambda-Funktion aufzurufen. Zum Beispiel:

  JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "allowinvokeFunction",
            "Effect": "Allow",
            "Action": [
                "lambda:invokeFunction",
                "lambda:InvokeAsync",
                "lambda:ListFunctions"
            ],
            "Resource": "arn:aws:lambda:region:account-id:function:function-
name"

        }
    ]
}
```

Erstellen Sie eine Pipeline

Um sie AWS Lambda als Prozessor zu verwenden, konfigurieren Sie eine OpenSearch Ingestion-Pipeline und geben Sie `aws_lambda` sie als Prozessor an. Sie können auch den AWS Lambda benutzerdefinierten Enrichment-Blueprint verwenden, um die Pipeline zu erstellen. Weitere Informationen finden Sie unter the section called “Mit Blueprints arbeiten”.

Die folgende Beispielpipeline empfängt Daten aus einer HTTP-Quelle, reichert sie mithilfe eines Datenprozessors und des Prozessors an und nimmt die AWS Lambda verarbeiteten Daten in eine Domain auf. OpenSearch

```
version: "2"
lambda-processor-pipeline:
  source:
```

```
    http:
      path: "/${pipelineName}/logs"
  processor:
      - date:
        destination: "@timestamp"
        from_time_received: true
    - aws_lambda:
        function_name: "my-lambda-function"

        tags_on_failure: ["lambda_failure"]
        batch:
            key_name: "events"
        aws:
          region: region
  sink:
    - opensearch:
        hosts: [ "https://search-mydomain.us-east-1es.amazonaws.com" ]
        index: "table-index"
        aws:
          region: "region"
          serverless: false
```

Die folgende AWS Lambda Beispielfunktion transformiert eingehende Daten, indem sie jedem Element im bereitgestellten Ereignisarray ein neues Schlüssel-Wert-Paar (`"transformed": "true"`) hinzufügt und dann die geänderte Version zurücksendet.

```
import json

def lambda_handler(event, context):
    input_array = event.get('events', [])
    output = []
    for input in input_array:
        input["transformed"] = "true";
        output.append(input)

    return output
```

Stapelverarbeitung

Pipelines senden gebündelte Ereignisse an den Lambda-Prozessor und passen die Batchgröße dynamisch an, um sicherzustellen, dass sie unter dem 5-MB-Limit bleibt.

Im Folgenden finden Sie ein Beispiel für einen Pipeline-Batch:

```
batch:
    key_name: "events"

input_arrary = event.get('events', [])
```

> **Note**
>
> Wenn Sie eine Pipeline erstellen, stellen Sie sicher, dass die `key_name` Option in der Lambda-Prozessorkonfiguration mit dem Ereignisschlüssel im Lambda-Handler übereinstimmt.

Bedingte Filterung

Mit der bedingten Filterung können Sie steuern, wann Ihr AWS Lambda Prozessor die Lambda-Funktion auf der Grundlage bestimmter Bedingungen in Ereignisdaten aufruft. Dies ist besonders nützlich, wenn Sie bestimmte Ereignistypen selektiv verarbeiten und andere ignorieren möchten.

Die folgende Beispielkonfiguration verwendet bedingte Filterung:

```
processors:
  - aws_lambda:
      function_name: "my-lambda-function"
      aws:
        region: "region"
      lambda_when: "/sourceIp == 10.10.10.10"
```

Migrieren von Daten zwischen Domains und Sammlungen mithilfe von Amazon OpenSearch Ingestion

Sie können OpenSearch Ingestion-Pipelines verwenden, um Daten zwischen Amazon OpenSearch Service-Domains oder OpenSearch serverlosen VPC-Sammlungen zu migrieren. Dazu richten Sie eine Pipeline ein, in der Sie eine Domain oder Sammlung als Quelle und eine andere Domain oder Sammlung als Senke konfigurieren. Dadurch werden Ihre Daten effektiv von einer Domain oder Sammlung zur anderen migriert.

Um Daten zu migrieren, benötigen Sie die folgenden Ressourcen:

- Eine OpenSearch Quelldienstdomäne oder eine OpenSearch serverlose VPC-Sammlung. Diese Domain oder Sammlung enthält die Daten, die Sie migrieren möchten. Wenn Sie eine Domain verwenden, muss sie OpenSearch Version 1.0 oder höher oder Elasticsearch Version 7.4 oder höher ausführen. Die Domain muss außerdem über eine Zugriffsrichtlinie verfügen, die Ihrer Pipeline-Rolle die entsprechenden Berechtigungen gewährt.
- Eine separate Domain oder VPC-Sammlung, in die Sie Ihre Daten migrieren möchten. Diese Domain oder Sammlung fungiert als Pipeline-Senke.
- Eine Pipeline-Rolle, die OpenSearch Ingestion zum Lesen und Schreiben in Ihre Sammlung oder Domain verwendet. Sie nehmen den Amazon-Ressourcennamen (ARN) dieser Rolle in Ihre Pipeline-Konfiguration auf. Weitere Informationen finden Sie in den folgenden Ressourcen:
  - the section called “Pipelines Zugriff auf Domains gewähren”
  - the section called “Pipelines Zugriff auf Sammlungen gewähren”

Themen

- Einschränkungen
- OpenSearch Dienst als Quelle
- Angabe mehrerer OpenSearch Service-Domain-Senken
- Migrieren von Daten zu einer OpenSearch serverlosen VPC-Sammlung

Einschränkungen

Die folgenden Einschränkungen gelten, wenn Sie OpenSearch Service-Domains oder OpenSearch Serverless-Sammlungen als Senken kennzeichnen:

- Eine Pipeline kann nicht in mehr als eine VPC-Domäne schreiben.
- Sie können nur Daten zu oder aus OpenSearch serverlosen Sammlungen migrieren, die VPC-Zugriff verwenden. Öffentliche Sammlungen werden nicht unterstützt.
- Sie können keine Kombination aus VPC und öffentlichen Domänen in einer einzigen Pipeline-Konfiguration angeben.
- In einer einzigen Pipeline-Konfiguration können Sie maximal 20 Senken verwenden, die keine Pipeline sind.
- Sie können in einer einzigen Pipeline-Konfiguration maximal drei verschiedene AWS-Regionen Senken angeben.

- Bei einer Pipeline mit mehreren Senken kann es im Laufe der Zeit zu einer Verringerung der Verarbeitungsgeschwindigkeit kommen, wenn eine der Senken zu lange ausgefallen ist oder nicht über genügend Kapazität für den Empfang eingehender Daten verfügt.

OpenSearch Dienst als Quelle

Aus der Domäne oder Sammlung, die Sie als Quelle angeben, werden die Daten migriert.

Eine Pipeline-Rolle in IAM erstellen

Um Ihre OpenSearch Ingestion-Pipeline zu erstellen, müssen Sie zunächst eine Pipeline-Rolle erstellen, um Lese- und Schreibzugriff zwischen Domänen oder Sammlungen zu gewähren. Führen Sie dazu die folgenden Schritte aus:

1. Erstellen Sie eine neue Berechtigungsrichtlinie in IAM, um sie an die Pipeline-Rolle anzuhängen. Stellen Sie sicher, dass Sie Berechtigungen zum Lesen von der Quelle und zum Schreiben in die Senke zulassen. Weitere Informationen zum Einrichten von IAM-Pipelineberechtigungen für OpenSearch Dienstdomänen finden Sie unter the section called “Pipelines Zugriff auf Domains gewähren” undthe section called “Pipelines Zugriff auf Sammlungen gewähren”.
2. Geben Sie innerhalb der Pipeline-Rolle die folgenden Berechtigungen an, um aus der Quelle zu lesen:

   JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":"es:ESHttpGet",
         "Resource":[
            "arn:aws:es:region:account-id:domain/domain-name/",
            "arn:aws:es:region:account-id:domain/domain-name/_cat/indices",
            "arn:aws:es:region:account-id:domain/domain-name/_search",
            "arn:aws:es:region:account-id:domain/domain-name/_search/scroll",
            "arn:aws:es:region:account-id:domain/domain-name/*/_search"
         ]
      },
      {
         "Effect":"Allow",
```

```
            "Action":"es:ESHttpPost",
            "Resource":[
               "arn:aws:es:region:account-id:domain/domain-name/*/_search/
point_in_time",
               "arn:aws:es:region:account-id:domain/domain-name/*/_search/scroll"
            ]
         },
         {
            "Effect":"Allow",
            "Action":"es:ESHttpDelete",
            "Resource":[
               "arn:aws:es:region:account-id:domain/domain-name/_search/
point_in_time",
               "arn:aws:es:region:account-id:domain/domain-name/_search/scroll"
            ]
         }
      ]
}
```

Eine Pipeline erstellen

Nachdem Sie die Richtlinie an die Pipeline-Rolle angehängt haben, verwenden Sie den AWSOpenSearchDataMigrationPipelineMigrations-Blueprint, um die Pipeline zu erstellen. Dieser Blueprint enthält eine Standardkonfiguration für die Migration von Daten zwischen OpenSearch Dienstdomänen oder Sammlungen. Weitere Informationen finden Sie unter the section called “Mit Blueprints arbeiten”.

> **Note**
>
> OpenSearch Die Aufnahme verwendet Ihre Quelldomänenversion und -verteilung, um zu bestimmen, welcher Mechanismus für die Migration verwendet werden soll. Einige Versionen unterstützen diese Option. `point_in_time` OpenSearch Serverless verwendet die `search_after` Option, weil sie `point_in_time` oder `scroll` nicht unterstützt.

Während des Migrationsprozesses werden möglicherweise gerade neue Indizes erstellt, oder Dokumente werden während der Migration aktualisiert. Aus diesem Grund müssen Sie möglicherweise entweder einen einzelnen Scan oder mehrere Scans Ihrer Domainindexdaten durchführen, um neue oder aktualisierte Daten zu erhalten.

Geben Sie die Anzahl der auszuführenden Scans an, indem Sie das `index_read_count` und `interval` in der Pipeline-Konfiguration konfigurieren. Das folgende Beispiel zeigt, wie mehrere Scans durchgeführt werden:

```
scheduling:
    interval: "PT2H"
    index_read_count: 3
    start_time: "2023-06-02T22:01:30.00Z"
```

OpenSearch Ingestion verwendet die folgende Konfiguration, um sicherzustellen, dass Ihre Daten in denselben Index geschrieben werden und dieselbe Dokument-ID beibehalten wird:

```
index: "${getMetadata(\"opensearch-index\")}"
document_id: "${getMetadata(\"opensearch-document_id\")}"
```

Angabe mehrerer OpenSearch Service-Domain-Senken

Sie können mehrere öffentliche OpenSearch Dienstdomänen als Ziele für Ihre Daten angeben. Sie können diese Funktion verwenden, um bedingtes Routing durchzuführen oder eingehende Daten in mehrere OpenSearch Dienstdomänen zu replizieren. Sie können bis zu 10 verschiedene öffentliche OpenSearch Dienstdomänen als Senken angeben.

Im folgenden Beispiel werden eingehende Daten bedingt an verschiedene OpenSearch Dienstdomänen weitergeleitet:

```
...
  route:
    - 2xx_status: "/response >= 200 and /response < 300"
    - 5xx_status: "/response >= 500 and /response < 600"
  sink:
    - opensearch:
        hosts: [ "https://search-response-2xx.region.es.amazonaws.com" ]
        aws:
          region: "us-east-1"
        index: "response-2xx"
        routes:
          - 2xx_status
    - opensearch:
        hosts: [ "https://search-response-5xx.region.es.amazonaws.com" ]
        aws:
```

```
          region: "us-east-1"
        index: "response-5xx"
        routes:
          - 5xx_status
```

Migrieren von Daten zu einer OpenSearch serverlosen VPC-Sammlung

Sie können OpenSearch Ingestion verwenden, um Daten von einer OpenSearch Quell-Servicedomäne oder einer OpenSearch serverlosen Sammlung zu einer VPC-Sammelsenke zu migrieren. Sie müssen in der Pipeline-Konfiguration eine Netzwerkzugriffsrichtlinie angeben. Weitere Informationen zur Datenaufnahme in OpenSearch serverlose VPC-Sammlungen finden Sie unter. the section called “Tutorial: Daten in eine Sammlung aufnehmen”

So migrieren Sie Daten zu einer VPC-Sammlung

1. Erstellen Sie eine OpenSearch serverlose Sammlung. Detaillierte Anweisungen finden Sie unter the section called “Tutorial: Daten in eine Sammlung aufnehmen”.
2. Erstellen Sie eine Netzwerkrichtlinie für die Sammlung, die den VPC-Zugriff sowohl auf den Sammlungsendpunkt als auch auf den Dashboards-Endpunkt festlegt. Detaillierte Anweisungen finden Sie unter the section called “Netzwerkzugriff”.
3. Erstellen Sie die Pipeline-Rolle, falls Sie noch keine haben. Detaillierte Anweisungen finden Sie unter the section called “Rolle „Pipeline“”.
4. Erstellen Sie die Pipeline. Detaillierte Anweisungen finden Sie unter the section called “Mit Blueprints arbeiten”.

Verwenden von AWS SDKs zur Interaktion mit Amazon OpenSearch Ingestion

Dieser Abschnitt enthält ein Beispiel für die Verwendung von für AWS SDKs die Interaktion mit Amazon OpenSearch Ingestion. Das Codebeispiel zeigt, wie Sie eine Domain und eine Pipeline erstellen und dann Daten in die Pipeline aufnehmen.

Themen

- Python

Python

Das folgende Beispielskript verwendet die AWS SDK für Python (Boto3), um eine IAM-Pipeline-Rolle, eine Domäne, in die Daten geschrieben werden, und eine Pipeline, über die Daten aufgenommen werden, zu erstellen. Anschließend nimmt es mithilfe der HTTP-Bibliothek eine Beispielprotokolldatei in die Pipeline auf`requests`.

Führen Sie die folgenden Befehle aus, um die erforderlichen Abhängigkeiten zu installieren:

```
pip install boto3
pip install botocore
pip install requests
pip install requests-auth-aws-sigv4
```

Ersetzen Sie innerhalb des Skripts alle Instanzen von *account-id* durch Ihre AWS-Konto ID.

```
import boto3
import botocore
from botocore.config import Config
import requests
from requests_auth_aws_sigv4 import AWSSigV4
import time

# Build the client using the default credential configuration.
# You can use the CLI and run 'aws configure' to set access key, secret
# key, and default region.

opensearch = boto3.client('opensearch', config=my_config)
iam = boto3.client('iam', config=my_config)
osis = boto3.client('osis', config=my_config)

domainName = 'test-domain'  # The name of the domain
pipelineName = 'test-pipeline' # The name of the pipeline

def createPipelineRole(iam, domainName):
    """Creates the pipeline role"""
    response = iam.create_policy(
        PolicyName='pipeline-policy',
        PolicyDocument=f'{{\"Version\":\"2012-10-17\",\"Statement\":[{{\"Effect\":
\"Allow\",\"Action\":\"es:DescribeDomain\",\"Resource\":\"arn:aws:es:us-east-1:account-
id:domain\/{domainName}\"}},{{\"Effect\":\"Allow\",\"Action\":\"es:ESHttp*\",\"Resource
\":\"arn:aws:es:us-east-1:account-id:domain\/{domainName}\/*\"}}]}}'
```

```
    )
    policyarn = response['Policy']['Arn']

    response = iam.create_role(
        RoleName='PipelineRole',
        AssumeRolePolicyDocument='{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect
\":\"Allow\",\"Principal\":{\"Service\":\"osis-pipelines.amazonaws.com\"},\"Action\":
\"sts:AssumeRole\"}]}'
    )
    rolename=response['Role']['RoleName']

    response = iam.attach_role_policy(
        RoleName=rolename,
        PolicyArn=policyarn
    )

    print('Creating pipeline role...')
    time.sleep(10)
    print('Role created: ' + rolename)

def createDomain(opensearch, domainName):
    """Creates a domain to ingest data into"""
    response = opensearch.create_domain(
        DomainName=domainName,
        EngineVersion='OpenSearch_2.3',
        ClusterConfig={
            'InstanceType': 't2.small.search',
            'InstanceCount': 5,
            'DedicatedMasterEnabled': True,
            'DedicatedMasterType': 't2.small.search',
            'DedicatedMasterCount': 3
        },
        # Many instance types require EBS storage.
        EBSOptions={
            'EBSEnabled': True,
            'VolumeType': 'gp2',
            'VolumeSize': 10
        },
        AccessPolicies=f'{{\"Version\":\"2012-10-17\",\"Statement\":[{{\"Effect
\":\"Allow\",\"Principal\":{{\"AWS\":\"arn:aws:iam::account-id:role\/PipelineRole
\"}},\"Action\":\"es:*\",\"Resource\":\"arn:aws:es:us-east-1:account-id:domain\/
{domainName}\/*\"}}]}}',
        NodeToNodeEncryptionOptions={
            'Enabled': True
```

```
        }
    )
    return(response)

def waitForDomainProcessing(opensearch, domainName):
    """Waits for the domain to be active"""
    try:
        response = opensearch.describe_domain(
            DomainName=domainName
        )
        # Every 30 seconds, check whether the domain is processing.
        while 'Endpoint' not in response['DomainStatus']:
            print('Creating domain...')
            time.sleep(60)
            response = opensearch.describe_domain(
                DomainName=domainName)

        # Once we exit the loop, the domain is ready for ingestion.
        endpoint = response['DomainStatus']['Endpoint']
        print('Domain endpoint ready to receive data: ' + endpoint)
        createPipeline(osis, endpoint)

    except botocore.exceptions.ClientError as error:
        if error.response['Error']['Code'] == 'ResourceNotFoundException':
            print('Domain not found.')
        else:
            raise error

def createPipeline(osis, endpoint):
    """Creates a pipeline using the domain and pipeline role"""
    try:
        definition = f'version: \"2\"\nlog-pipeline:\n  source:\n    http:\n      path:
 \"/${{pipelineName}}/logs\"\n  processor:\n    - date:\n        from_time_received:
 true\n        destination: \"@timestamp\"\n  sink:\n    - opensearch:\n        hosts:
 [ \"https://{endpoint}\" ]\n        index: \"application_logs\"\n        aws:\n
   region: \"us-east-1\"'
        response = osis.create_pipeline(
            PipelineName=pipelineName,
            MinUnits=4,
            MaxUnits=9,
            PipelineConfigurationBody=definition,
            PipelineRoleArn="arn:aws:iam::account-id:role/PipelineRole"
        )
```

```
        response = osis.get_pipeline(
                PipelineName=pipelineName
        )

        # Every 30 seconds, check whether the pipeline is active.
        while response['Pipeline']['Status'] == 'CREATING':
            print('Creating pipeline...')
            time.sleep(30)
            response = osis.get_pipeline(
                PipelineName=pipelineName)

        # Once we exit the loop, the pipeline is ready for ingestion.
        ingestionEndpoint = response['Pipeline']['IngestEndpointUrls'][0]
        print('Pipeline ready to ingest data at endpoint: ' + ingestionEndpoint)
        ingestData(ingestionEndpoint)

    except botocore.exceptions.ClientError as error:
        if error.response['Error']['Code'] == 'ResourceAlreadyExistsException':
            print('Pipeline already exists.')
            response = osis.get_pipeline(
                PipelineName=pipelineName
            )
            ingestionEndpoint = response['Pipeline']['IngestEndpointUrls'][0]
            ingestData(ingestionEndpoint)
        else:
            raise error


def ingestData(ingestionEndpoint):
    """Ingests a sample log file into the pipeline"""
    endpoint = 'https://' + ingestionEndpoint
    r = requests.request('POST', f'{endpoint}/log-pipeline/logs',

 data='[{"time":"2014-08-11T11:40:13+00:00","remote_addr":"122.226.223.69","status":"404","requ
 http://www.k2proxy.com//hello.html HTTP/1.1","http_user_agent":"Mozilla/4.0
 (compatible; WOW64; SLCC2;)"}]',
    auth=AWSSigV4('osis'))
    print('Ingesting sample log file into pipeline')
    print('Response: ' + r.text)

def main():
    createPipelineRole(iam, domainName)
    createDomain(opensearch, domainName)
    waitForDomainProcessing(opensearch, domainName)
```

```
if __name__ == "__main__":
    main()
```

Sicherheit bei Amazon OpenSearch Ingestion

Cloud-Sicherheit hat AWS höchste Priorität. Als AWS Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame Verantwortung von Ihnen AWS und Ihnen. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS Dienste in der AWS Cloud ausführt. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Auditoren von Drittanbietern testen und überprüfen die Effektivität unserer Sicherheitsmaßnahmen im Rahmen der AWS -Compliance-Programme regelmäßig.
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Dienst, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Verwendung von OpenSearch Ingestion anwenden können. In den folgenden Themen erfahren Sie, wie Sie OpenSearch Ingestion konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Außerdem erfahren Sie, wie Sie andere AWS Dienste nutzen können, die Sie bei der Überwachung und Sicherung Ihrer OpenSearch Ingestion-Ressourcen unterstützen.

Themen

- Konfiguration des VPC-Zugriffs für Amazon OpenSearch Ingestion-Pipelines
- Identity and Access Management für Amazon OpenSearch Ingestion
- Protokollieren von Amazon OpenSearch Ingestion-API-Aufrufen mit AWS CloudTrail

Konfiguration des VPC-Zugriffs für Amazon OpenSearch Ingestion-Pipelines

Sie können über einen Schnittstellen-VPC-Endpunkt auf Ihre Amazon OpenSearch Ingestion-Pipeline zugreifen. Eine VPC ist ein virtuelles Netzwerk, das speziell für Ihr AWS-Konto ausgelegt ist. Es ist von anderen virtuellen Netzwerken in der AWS Cloud getrennt. Der Zugriff auf eine Pipeline über einen VPC-Endpunkt ermöglicht eine sichere Kommunikation zwischen OpenSearch Ingestion und anderen Services innerhalb der VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung benötigt wird. Der gesamte Datenverkehr bleibt in der AWS -Cloud geschützt.

OpenSearch Ingestion stellt diese private Verbindung her, indem ein Schnittstellen-Endpunkt erstellt wird, der von unterstützt wird. AWS PrivateLink Wir erstellen eine Endpunktnetzwerkschnittstelle in jedem Subnetz, das Sie bei der Pipeline angeben. Hierbei handelt es sich um vom Anforderer verwaltete Netzwerkschnittstellen, die als Eingangspunkt für den Datenverkehr dienen, der für die Ingestion-Peline bestimmt ist OpenSearch . Sie können die Schnittstellen-Endpunkte auch selbst erstellen und verwalten.

Mit einer VPC können Sie den Datenfluss durch Ihre OpenSearch Ingestion-Pipelines innerhalb der Grenzen der VPC erzwingen, anstatt über das öffentliche Internet. Pipelines, die sich nicht in einer VPC befinden, senden und empfangen Daten über öffentlich zugängliche Endpunkte und das Internet.

Eine Pipeline mit VPC-Zugriff kann in öffentliche Domänen oder OpenSearch VPC-Dienstdomänen sowie in öffentliche oder serverlose OpenSearch VPC-Sammlungen schreiben.

Themen

- Überlegungen
- Einschränkungen
- Voraussetzungen
- Konfigurieren des VPC-Zugriffs für eine Pipeline
- Selbstverwaltet VPC Endpunkte
- Service-verknüpfte Rolle für den VPC-Zugriff

Überlegungen

Berücksichtigen Sie Folgendes, wenn Sie den VPC-Zugriff für eine Pipeline konfigurieren.

- Eine Pipeline muss sich nicht in derselben VPC wie ihre Senke befinden. Sie müssen auch keine Verbindung zwischen den beiden VPCs herstellen. OpenSearch Ingestion kümmert sich darum, sie für Sie zu verbinden.
- Sie können nur eine VPC für Ihre Pipeline angeben.
- Im Gegensatz zu öffentlichen Pipelines muss sich eine VPC-Pipeline in derselben AWS-Region Domäne oder Sammelsenke befinden, in die sie schreibt.
- Sie können eine Pipeline in einem, zwei oder drei Subnetzen Ihrer VPC bereitstellen. Die Subnetze sind auf dieselben Availability Zones verteilt, in denen Ihre OpenSearch Ingestion-Recheneinheiten () OCUs bereitgestellt werden.
- Wenn Sie nur eine Pipeline in einem Subnetz bereitstellen und die Availability Zone ausfällt, können Sie keine Daten aufnehmen. Um eine hohe Verfügbarkeit zu gewährleisten, empfehlen wir, Pipelines mit zwei oder drei Subnetzen zu konfigurieren.
- Die Angabe einer Sicherheitsgruppe ist optional. Wenn Sie keine Sicherheitsgruppe angeben, verwendet OpenSearch Ingestion die Standardsicherheitsgruppe, die in der VPC angegeben ist.

Einschränkungen

Pipelines mit VPC-Zugriff haben folgende Einschränkungen.

- Sie können die Netzwerkkonfiguration einer Pipeline nicht mehr ändern, nachdem Sie sie erstellt haben. Wenn Sie eine Pipeline innerhalb einer VPC starten, können Sie sie später nicht in einen öffentlichen Endpunkt ändern und umgekehrt.
- Sie können Ihre Pipeline entweder mit einem Schnittstellen-VPC-Endpunkt oder einem öffentlichen Endpunkt starten, aber Sie können nicht beides tun. Sie müssen sich beim Erstellen einer Pipeline für eine Option entscheiden.
- Nachdem Sie eine Pipeline mit VPC-Zugriff bereitgestellt haben, kann sie nicht in eine andere VPC verlagert werden, und Sie können auch ihre Subnetze oder Sicherheitsgruppeneinstellungen nicht ändern.
- Wenn Ihre Pipeline in eine Domain oder Sammlungssenke schreibt, die VPC-Zugriff verwendet, können Sie nicht später zurückkehren und die Senke (VPC oder öffentlich) ändern, nachdem die Pipeline erstellt wurde. Sie müssen die Pipeline mit einer neuen Senke löschen und neu erstellen. Sie können immer noch von einer öffentlichen Senke zu einer Senke mit VPC-Zugriff wechseln.
- Sie können keinen kontenübergreifenden Aufnahmezugriff auf VPC-Pipelines gewähren.

Voraussetzungen

Bevor Sie eine Pipeline mit VPC-Zugriff bereitstellen können, müssen Sie die folgenden Schritte ausführen:

- Erstellen einer VPC

  Sie können zum Erstellen der VPC die Amazon VPC-Konsole, die AWS CLI oder eine Option verwenden. AWS SDKs Weitere Informationen finden Sie unter Arbeiten mit VPCs im Amazon VPC-Benutzerhandbuch. Wenn bereits eine VPC vorhanden ist, können Sie diesen Schritt überspringen.
- Reservieren von IP-Adressen

  OpenSearch Ingestion fügt dann in jedem elastic network interface, das Sie beim Erstellen der Pipeline angeben, eine ENI hinzu. Jeder Netzwerkschnittstelle ist eine IP-Adresse zugewiesen. Sie müssen eine IP-Adresse pro Subnetz für die Netzwerkschnittstellen reservieren.

Konfigurieren des VPC-Zugriffs für eine Pipeline

Sie können den VPC-Zugriff für eine Pipeline in der OpenSearch Servicekonsole oder mithilfe der AWS CLI aktivieren.

Konsole

Sie konfigurieren den VPC-Zugriff während der Pipelineerstellung. Wählen Sie unter Quellnetzwerkoptionen die Option VPC-Zugriff aus und konfigurieren Sie die folgenden Einstellungen:

Einstellung	Beschreibung
Endpunktv erwaltung	Wählen Sie aus, ob Sie Ihre VPC-Endpoints selbst erstellen möchten oder ob Sie sie von OpenSearch Ingestion für Sie erstellen lassen möchten.
VPC	Wählen Sie für die Virtual Private Cloud (VPC) die ID, die Sie verwenden möchten. Die VPC und die Pipeline müssen sich im selben AWS-Region befinden.
Subnets	Wählen Sie unter Subnetz ein oder mehrere Subnetze aus. OpenSearch Service fügt dann den Subnetzen einen VPC-Endpunkt und Elastic-Network-Schnittstellen (ENIs) hinzu.

Einstellung	Beschreibung
Sicherheitsgruppen	Wählen Sie eine oder mehrere VPC-Sicherheitsgruppen, die es Ihrer erforderlichen Anwendung ermöglichen, die Pipeline über OpenSearch die von der Pipeline bereitgestellten Ports (80 oder 443) und Protokolle (HTTP oder HTTPs) zu erreichen.
VPC-Anhangsoptionen	Wenn Ihre Quelle eine VPC-übergreifende Kommunikation erfordert, z. B. Amazon DocumentDB, Self-Managed oder Confluent Kafka OpenSearch, erstellt OpenSearch Ingestion Elastic Network Interfaces (ENIs) in den Subnetzen, die Sie angeben, um eine Verbindung zu diesen Quellen herzustellen. OpenSearch Ingestion verwendet in jeder Availability Zone, um die angegebenen Quellen zu erreichen. ENIs Die Option An VPC anhängen verbindet die VPC der OpenSearch Aufnahmedatenebene mit Ihrer angegebenen VPC. Wählen Sie eine CIDR-Reservierung für die verwaltete VPC aus, um die Netzwerkschnittstelle bereitzustellen.

CLI

Um den VPC-Zugriff mit dem zu konfigurieren AWS CLI, geben Sie den `--vpc-options` Parameter an:

```
aws osis create-pipeline \
  --pipeline-name vpc-pipeline \
  --min-units 4 \
  --max-units 10 \
  --vpc-options
 SecurityGroupIds={sg-12345678,sg-9012345},SubnetIds=subnet-1212234567834asdf \
  --pipeline-configuration-body "file://pipeline-config.yaml"
```

Selbstverwaltet VPC Endpunkte

Wenn Sie eine Pipeline erstellen, können Sie Endpoint Management verwenden, um eine Pipeline mit selbstverwalteten Endpunkten oder dienstverwalteten Endpunkten zu erstellen. Endpoint Management ist optional und verwendet standardmäßig Endgeräte, die von Ingestion verwaltet werden. OpenSearch

Informationen zum Erstellen einer Pipeline mit einem selbstverwalteten VPC-Endpunkt in der AWS Management Console finden Sie unter Pipelines mit der OpenSearch Servicekonsole erstellen. Um eine Pipeline mit einem selbstverwalteten VPC-Endpunkt in der zu erstellen AWS CLI, können Sie den `--vpc-options` Parameter im Befehl create-pipeline verwenden:

```
--vpc-options SubnetIds=subnet-abcdef01234567890,VpcEndpointManagement=CUSTOMER
```

Sie können einen Endpunkt für Ihre Pipeline selbst erstellen, wenn Sie Ihren Endpunktservice angeben. Um Ihren Endpunktdienst zu finden, verwenden Sie den Befehl get-pipeline, der eine Antwort ähnlich der folgenden zurückgibt:

```
"vpcEndpointService" : "com.amazonaws.osis.us-east-1.pipeline-
id-1234567890abcdef1234567890",
"vpcEndpoints" : [
  {
    "vpcId" : "vpc-1234567890abcdef0",
    "vpcOptions" : {
      "subnetIds" : [ "subnet-abcdef01234567890", "subnet-021345abcdef6789" ],
      "vpcEndpointManagement" : "CUSTOMER"
    }
  }
```

Verwenden Sie die Antwort `vpcEndpointService` von der Antwort, um einen VPC-Endpunkt mit dem AWS Management Console oder AWS CLI zu erstellen.

Wenn Sie selbstverwaltete VPC-Endpoints verwenden, müssen Sie die DNS-Attribute `enableDnsSupport` und `enableDnsHostnames` in Ihrer VPC aktivieren. Beachten Sie, dass Sie, wenn Sie eine Pipeline mit einem selbstverwalteten Endpunkt haben, den Sie beenden und neu starten, den VPC-Endpunkt in Ihrem Konto neu erstellen müssen.

Service-verknüpfte Rolle für den VPC-Zugriff

Eine Service-verknüpfte Rolle ist ein spezieller Typ der IAM-Rolle zum Übertragen von Berechtigungen an einen Service, damit dieser Ressourcen für Sie erstellen und verwalten kann. Wenn Sie sich für einen Service-verwalteten VPC-Endpunkt entscheiden, benötigt OpenSearch Ingestion eine Service-verknüpfte Rolle, die aufgerufen wird, AWSServiceRoleForAmazonOpenSearchIngestionServiceum auf die VPC zuzugreifen, den Pipeline-Endpunkt zu erstellen und Netzwerkschnittstellen in ein Subnetz der VPC einzufügen.

Wenn Sie sich für einen selbstverwalteten VPC-Endpunkt entscheiden, erfordert OpenSearch Ingestion eine serviceverknüpfte Rolle namens. AWSServiceRoleForOpensearchIngestionSelfManagedVpce Weitere Informationen zu diesen Rollen, ihren Berechtigungen und wie Sie sie löschen können, finden Sie unter. the section called “Rolle bei der Pipeline-Erstellung”

OpenSearch Die Aufnahme erstellt die Rolle automatisch, wenn Sie eine Aufnahme-Pipeline erstellen. Damit diese automatische Erstellung erfolgreich ist, muss der Benutzer, der die erste Pipeline in einem Konto erstellt, über Berechtigungen für die Aktion verfügen. `iam:CreateServiceLinkedRole` Weitere Informationen finden Sie unter Berechtigungen von Service-verknüpften Rollen im IAM-Benutzerhandbuch. Sie können die Rolle in der AWS Identity and Access Management (IAM-) Konsole anzeigen, nachdem sie erstellt wurde.

Identity and Access Management für Amazon OpenSearch Ingestion

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf Ressourcen sicher zu kontrollieren. AWS IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Ingestion-Ressourcen zu verwenden OpenSearch . IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Themen

- Identitätsbasierte Richtlinien für die Datenerfassung OpenSearch
- Richtlinienmaßnahmen für Ingestion OpenSearch
- Richtlinienressourcen für Ingestion OpenSearch
- Schlüssel zu den Richtlinienbedingungen für Amazon OpenSearch Ingestion
- ABAC mit Ingestion OpenSearch
- Temporäre Anmeldeinformationen mit Ingestion verwenden OpenSearch
- Mit Diensten verknüpfte Rollen für Ingestion OpenSearch
- Beispiele für identitätsbasierte Richtlinien für Ingestion OpenSearch

Identitätsbasierte Richtlinien für die Datenerfassung OpenSearch

Unterstützt Richtlinien auf Identitätsbasis: Ja

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern,

welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Beispiele für identitätsbasierte Richtlinien für Ingestion OpenSearch

Beispiele für identitätsbasierte Richtlinien zur Datenerfassung finden OpenSearch Sie unter. the section called “Beispiele für identitätsbasierte Richtlinien”

Richtlinienmaßnahmen für Ingestion OpenSearch

Unterstützt Richtlinienaktionen: Ja

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie der zugehörige AWS API-Vorgang. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keinen passenden API-Vorgang gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Bei Richtlinienaktionen in OpenSearch Ingestion wird vor der Aktion das folgende Präfix verwendet:

```
osis
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

```
"Action": [
      "osis:action1",
      "osis:action2"
```

```
        ]
```

Sie können mehrere Aktionen mit Platzhalterzeichen (*) angeben. Beispielsweise können Sie alle Aktionen festlegen, die mit dem Wort `List` beginnen, einschließlich der folgenden Aktion:

```
"Action": "osis:List*"
```

Beispiele für identitätsbasierte Richtlinien OpenSearch bei Ingestion finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Serverless OpenSearch

Richtlinienressourcen für Ingestion OpenSearch

Unterstützt Richtlinienressourcen: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Anweisungen müssen entweder ein – `Resource`oder ein `NotResource`-Element enthalten. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

```
"Resource": "*"
```

Schlüssel zu den Richtlinienbedingungen für Amazon OpenSearch Ingestion

Unterstützt dienstspezifische Richtlinien-Bedingungsschlüssel: Nein

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition` block) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte

Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen AND-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, AWS wertet die Bedingung mithilfe einer logischen OR Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter IAM-Richtlinienelemente: Variablen und Tags im IAM-Benutzerhandbuch.

AWS unterstützt globale Bedingungsschlüssel und dienstspezifische Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

Eine Liste der OpenSearch Ingestion-Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für Amazon OpenSearch Ingestion in der Service Authorization Reference. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Von Amazon OpenSearch Ingestion definierte Aktionen.

ABAC mit Ingestion OpenSearch

Unterstützt ABAC (Tags in Richtlinien): Ja

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In werden AWS diese Attribute als Tags bezeichnet. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und an viele AWS Ressourcen anhängen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt von ABAC. Anschließend entwerfen Sie ABAC-Richtlinien, um Operationen zuzulassen, wenn das Tag des Prinzipals mit dem Tag der Ressource übereinstimmt, auf die sie zugreifen möchten.

ABAC ist in Umgebungen hilfreich, die schnell wachsen, und unterstützt Sie in Situationen, in denen die Richtlinienverwaltung mühsam wird.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, oder Bedingung `aws:TagKeys` verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu ABAC finden Sie unter Definieren von Berechtigungen mit ABAC-Autorisierung im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe Attributbasierte Zugriffskontrolle (ABAC) verwenden im IAM-Benutzerhandbuch.

Weitere Informationen zum Taggen von OpenSearch Ingestion-Ressourcen finden Sie unter. the section called “Markieren von Pipelines”

Temporäre Anmeldeinformationen mit Ingestion verwenden OpenSearch

Unterstützt temporäre Anmeldeinformationen: Ja

Einige funktionieren AWS-Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich Informationen, die mit temporären Anmeldeinformationen AWS-Services funktionieren AWS-Services , finden Sie im IAM-Benutzerhandbuch unter Diese Option funktioniert mit IAM.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS Management Console Methode als einem Benutzernamen und einem Passwort bei der Anmeldung anmelden. Wenn Sie beispielsweise AWS über den Single Sign-On-Link (SSO) Ihres Unternehmens darauf zugreifen, werden bei diesem Vorgang automatisch temporäre Anmeldeinformationen erstellt. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Wechseln von Rollen finden Sie unter Wechseln von einer Benutzerrolle zu einer IAM-Rolle (Konsole) im IAM-Benutzerhandbuch.

Mithilfe der AWS API AWS CLI oder können Sie temporäre Anmeldeinformationen manuell erstellen. Sie können diese temporären Anmeldeinformationen dann für den Zugriff verwenden AWS. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen in IAM.

Mit Diensten verknüpfte Rollen für Ingestion OpenSearch

Unterstützt dienstbezogene Rollen: Ja

Eine serviceverknüpfte Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen.

Dienstbezogene Rollen werden in Ihrem Dienst angezeigt AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

OpenSearch Bei der Aufnahme wird eine dienstbezogene Rolle mit dem Namen verwendet. `AWSServiceRoleForAmazonOpenSearchIngestionService` Die angegebene serviceverknüpfte Rolle `AWSServiceRoleForOpensearchIngestionSelfManagedVpce` ist auch für Pipelines mit selbstverwalteten VPC-Endpunkten verfügbar. Einzelheiten zum Erstellen und Verwalten von serviceverknüpften OpenSearch Ingestion-Rollen finden Sie unter. the section called “Rolle bei der Pipeline-Erstellung”

Beispiele für identitätsbasierte Richtlinien für Ingestion OpenSearch

Standardmäßig sind Benutzer und Rollen nicht berechtigt, Ingestion-Ressourcen zu erstellen oder zu ändern. OpenSearch Sie können auch keine Aufgaben mithilfe der AWS Management Console, AWS Command Line Interface (AWS CLI) oder AWS API ausführen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von IAM-Richtlinien (Konsole) im IAM-Benutzerhandbuch.

Einzelheiten zu den von Amazon OpenSearch Ingestion definierten Aktionen und Ressourcentypen, einschließlich des Formats ARNs für die einzelnen Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon OpenSearch Ingestion in der Service Authorization Reference.

Themen

- Bewährte Methoden für Richtlinien
- Ingestion in der Konsole verwenden OpenSearch
- Verwaltung von OpenSearch Ingestion-Pipelines
- Daten in eine OpenSearch Ingestion-Pipeline aufnehmen

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien sind sehr leistungsfähig. Sie bestimmen, ob jemand OpenSearch Ingestion-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

Identitätsbasierte Richtlinien legen fest, ob jemand OpenSearch Ingestion-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Erste Schritte mit AWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um damit zu beginnen, Ihren Benutzern und Workloads Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien oder AWS -verwaltete Richtlinien für Auftrags-Funktionen im IAM-Benutzerhandbuch.
- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. AWS CloudFormation B. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue

und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung mit IAM Access Analyzer im IAM-Benutzerhandbuch.

- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Sicherer API-Zugriff mit MFA im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Ingestion in der Konsole verwenden OpenSearch

Um über die OpenSearch Servicekonsole auf OpenSearch Ingestion zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Informationen zu den OpenSearch Ingestion-Ressourcen in Ihrem Konto aufzulisten und einzusehen. AWS Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (wie IAM-Rollen) mit dieser Richtlinie.

Sie müssen Benutzern, die nur die API AWS CLI oder die API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. AWS Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die der API-Operation entsprechen, die Sie ausführen möchten.

Die folgende Richtlinie ermöglicht es einem Benutzer, über die OpenSearch Servicekonsole auf OpenSearch Ingestion zuzugreifen:

JSON

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

```
                "osis:ListPipelines",
                "osis:GetPipeline",
                "osis:ListPipelineBlueprints",
                "osis:GetPipelineBlueprint",
                "osis:GetPipelineChangeProgress"
            ]
        }
    ]
}
```

Alternativ können Sie die the section called “AmazonOpenSearchIngestionReadOnlyAccess” AWS verwaltete Richtlinie verwenden, die nur Lesezugriff auf alle OpenSearch Ingestion-Ressourcen für einen gewährt. AWS-Konto

Verwaltung von OpenSearch Ingestion-Pipelines

Diese Richtlinie ist ein Beispiel für eine „Pipeline-Admin“ -Richtlinie, die es einem Benutzer ermöglicht, Amazon OpenSearch Ingestion-Pipelines zu verwalten und zu verwalten. Der Benutzer kann Pipelines erstellen, anzeigen und löschen.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Resource": "arn:aws:osis:region:123456789012:pipeline/*",
            "Action": [
                "osis:CreatePipeline",
                "osis:DeletePipeline",
                "osis:UpdatePipeline",
                "osis:ValidatePipeline",
                "osis:StartPipeline",
                "osis:StopPipeline"
            ],
            "Effect": "Allow"
        },
        {
            "Resource": "*",
            "Action": [
                "osis:ListPipelines",
```

```
                "osis:GetPipeline",
                "osis:ListPipelineBlueprints",
                "osis:GetPipelineBlueprint",
                "osis:GetPipelineChangeProgress"
            ],
            "Effect": "Allow"
        }
    ]
}
```

Daten in eine OpenSearch Ingestion-Pipeline aufnehmen

Diese Beispielrichtlinie ermöglicht es einem Benutzer oder einer anderen Entität, Daten in eine Amazon OpenSearch Ingestion-Pipeline in ihrem Konto aufzunehmen. Der Benutzer kann die Pipelines nicht ändern.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Resource": "arn:aws:osis:region:123456789012:pipeline/*",
            "Action": [
                "osis:Ingest"
            ],
            "Effect": "Allow"
        }
    ]
}
```

Protokollieren von Amazon OpenSearch Ingestion-API-Aufrufen mit AWS CloudTrail

Amazon OpenSearch Ingestion ist in einen Service mit integriert AWS CloudTrail, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einem AWS -Service in OpenSearch Amazon EKS durchgeführten Aktionen bietet.

CloudTrail erfasst alle API-Aufrufe für OpenSearch Ingestion als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe aus dem OpenSearch -Bereich der OpenSearch Servicekonsole und Code-Aufrufe der OpenSearch -API-Vorgänge.

Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen Amazon-S3-Bucket, einschließlich Ereignisse für die OpenSearch Aufnahme aktivieren. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse in der CloudTrail -Konsole trotzdem in Ereignisverlauf anzeigen.

Mit den von CloudTrail gesammelten Informationen können Sie die an gestellte Anfrage OpenSearch , die IP-Adresse, von der die Anfrage gestellt wurde, den Zeitpunkt der Anfrage und zusätzliche Details bestimmen.

Weitere Informationen CloudTrail dazu finden Sie im AWS CloudTrail Benutzerhandbuch.

OpenSearch Informationen zur Einnahme finden Sie in CloudTrail

CloudTrail wird AWS-Konto beim Erstellen Ihres für Sie aktiviert. Wenn eine Aktivität in OpenSearch Ingestion auftritt, wird diese Aktivität in einem CloudTrail Ereignis zusammen mit anderen Ereignissen des AWS -Service in Ereignisverlauf protokolliert. Sie können in Ihrem AWS-Konto die neusten Ereignisse anzeigen, suchen und herunterladen. Weitere Informationen finden Sie unter Anzeigen von Ereignissen mit dem CloudTrail -Ereignisverlauf.

Erstellen Sie einen Trail zur laufenden Aufzeichnung der Ereignisse im -Konto AWS-Konto, einschließlich der Ereignisse im Zusammenhang mit OpenSearch der Einnahme. Ein Trail ermöglicht CloudTrail die Bereitstellung von Protokolldateien in einem Amazon-S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen-Regionen.

Der Trail protokolliert Ereignisse aus allen Regionen in der AWS -Partition und stellt die Protokolldateien in dem Amazon S3 S3-Bucket bereit, den Sie angeben. Darüber hinaus können Sie andere AWS -Services konfigurieren, um die in den CloudTrail -Protokollen erfassten Ereignisdaten weiter zu analysieren und entsprechend zu agieren. Weitere Informationen finden Sie hier:

- Übersicht zum Erstellen eines Trails
- CloudTrail unterstützte Dienste und Integrationen
- Konfigurieren von Amazon SNS SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail -Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail -Protokolldateien aus mehreren Konten

Alle OpenSearch Ingestion-Aktionen werden von der Ingestion-API-Referenz protokolliert CloudTrail und sind in OpenSearch dieser dokumentiert. Zum Beispiel werden durch Aufrufe der `CreateCollection`-, `ListCollections`- und `DeleteCollection`-Aktionen Einträge in den CloudTrail -Protokolldateien generiert.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen helfen Ihnen beim Bestimmen der Folgenden Elemente:

- Ob die Anfrage mit Root- oder AWS Identity and Access Management (IAM) -Benutzer-Anmeldeinformationen ausgeführt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anforderung aus einem anderen AWS -Service gesendet wurde

Weitere Informationen finden Sie unter CloudTrail -Element userIdentity.

Grundlagen zu OpenSearch -Protokolldateieinträgen

Ein Trail ist eine Konfiguration, durch die Ereignisse als Protokolldateien an den von Ihnen angegebenen Amazon-S3-Bucket übermittelt werden. CloudTrail -Protokolldateien können einen oder mehrere Einträge enthalten.

Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar. Es enthält unter anderem Informationen über die angeforderte Aktion, etwaige Anforderungsparameter und das Datum und die Uhrzeit der Aktion. CloudTrail Protokolldateien sind kein geordnetes Stacktrace der öffentlichen API-Aufrufe und erscheinen daher nicht in einer bestimmten Reihenfolge.

Das folgende Beispiel zeigt einen CloudTrail -Protokolleintrag, der die `DeletePipeline` Aktion demonstriert.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn":"arn:aws:iam::123456789012:user/test-user",
        "accountId": "123456789012",
        "accessKeyId": "access-key",
        "sessionContext": {
            "sessionIssuer": {
```

```
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/Admin",
                "accountId": "123456789012",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-04-21T16:48:33Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-04-21T16:49:22Z",
    "eventSource": "osis.amazonaws.com",
    "eventName": "UpdatePipeline",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "123.456.789.012",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/112.0.0.0 Safari/537.36",
    "requestParameters": {
        "pipelineName": "my-pipeline",
        "pipelineConfigurationBody": "version: \"2\"\nlog-pipeline:\n  source:\n
 http:\n        path: \"/test/logs\"\n  processor:\n    - grok:\n        match:\n
        log: [ '%{COMMONAPACHELOG}' ]\n    - date:\n        from_time_received: true
\n        destination: \"@timestamp\"\n  sink:\n    - opensearch:\n        hosts:
 [ \"https://search-b5zd22mwxhggheqpj5ftslgyle.us-west-2.es.amazonaws.com\" ]\n
  index: \"apache_logs2\"\n        aws_sts_role_arn: \"arn:aws:iam::709387180454:role/
canary-bootstrap-OsisRole-J1BARLD26QKN\"\n        aws_region: \"us-west-2\"\n
 aws_sigv4: true\n"
    },
    "responseElements": {
        "pipeline": {
            "pipelineName": "my-pipeline",sourceIPAddress
            "pipelineArn": "arn:aws:osis:us-west-2:123456789012:pipeline/my-pipeline",
            "minUnits": 1,
            "maxUnits": 1,
            "status": "UPDATING",
            "statusReason": {
                "description": "An update was triggered for the pipeline. It is still
 available to ingest data."
            },
            "pipelineConfigurationBody": "version: \"2\"\nlog-pipeline:\n  source:\n
    http:\n        path: \"/test/logs\"\n  processor:\n    - grok:\n        match:
```

```
\n          log: [ '%{COMMONAPACHELOG}' ]\n    - date:\n        from_time_received:
 true\n        destination: \"@timestamp\"\n  sink:\n    - opensearch:\n        hosts:
 [ \"https://search-b5zd22mwxhggheqpj5ftslgyle.us-west-2.es.amazonaws.com\" ]\n
  index: \"apache_logs2\"\n        aws_sts_role_arn: \"arn:aws:iam::709387180454:role/
canary-bootstrap-OsisRole-J1BARLD26QKN\"\n        aws_region: \"us-west-2\"\n
 aws_sigv4: true\n",
            "createdAt": "Mar 29, 2023 1:03:44 PM",
            "lastUpdatedAt": "Apr 21, 2023 9:49:21 AM",
            "ingestEndpointUrls": [
                "my-pipeline-tu33ldsgdltgv7x7tjqiudvf7m.us-west-2.osis.amazonaws.com"
            ]
        }
    },
    "requestID": "12345678-1234-1234-1234-987654321098",
    "eventID": "12345678-1234-1234-1234-987654321098",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "709387180454",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "osis.us-west-2.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}
```


Kennzeichnen von Amazon OpenSearch Ingestion-Pipelines

Mit Tags können Sie einer OpenSearch Amazon-Ingestion-Pipeline beliebige Informationen zuweisen, damit Sie diese Informationen kategorisieren und filtern können. Ein Tag ist ein Metadaten-Etikett, das von Ihnen oder von einer AWS -Ressource AWS zugewiesen wird. Jedes Tag besteht aus einem Schlüssel und einem Wert. Für Tags, die Sie zuweisen, definieren Sie einen Schlüssel und einen Wert. So können Sie beispielsweise den Schlüssel als `stage` und den Wert für eine Ressource als `test` definieren.

Tags sind für folgende Aktivitäten nützlich:

- Identifizieren und Organisieren Ihrer AWS -Ressourcen. Viele AWS -Services unterstützen das Markieren mit Tags (kurz: Tagging). So können Ressourcen aus verschiedenen Services

denselben Tag zuweisen, um anzugeben, dass die Ressourcen verbunden sind. Sie können beispielsweise dasselbe Tag einer OpenSearch Ingestion-Pipeline und einer OpenSearch Amazon-Service-Domäne zuweisen.

- Überwachen von AWS -Kosten. Sie aktivieren diese Tags im AWS Fakturierung und Kostenmanagement -Dashboard. AWS verwendet die Tags zur Kategorisierung Ihrer Kosten und zur Bereitstellung eines monatlichen Kostenzuordnungsberichts für Sie. Weitere Informationen finden Sie unter Verwendung von Kostenzuordnungs-Tags im AWS Billing -Benutzerhandbuch.
- Schränkt den Zugriff auf Pipelines mithilfe einer attributbasierten Zugriffskontrolle ein. Weitere Informationen finden Sie unter Zugriffssteuerung auf der Grundlage von Tag-Schlüsseln im IAM-Benutzerhandbuch.

Bei OpenSearch Ingestion ist die primäre Ressource eine Pipeline. Sie können die OpenSearch Servicekonsole, die AWS CLI, OpenSearch Ingestion oder die verwenden APIs, AWS SDKs um einer Pipeline Tags hinzuzufügen, zu verwalten und zu entfernen.

Themen

- Erforderliche Berechtigungen
- Arbeiten mit Tags (Konsole)
- Arbeiten mit Tags (AWS CLI)

Erforderliche Berechtigungen

OpenSearch Ingestion verwendet die folgenden AWS Identity and Access Management Access Analyzer (IAM-) Berechtigungen für das Taggen von Pipelines:

- `osis:TagResource`
- `osis:ListTagsForResource`
- `osis:UntagResource`

Weitere Informationen zu den einzelnen Berechtigungen finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für OpenSearch Ingestion in der Service Authorization Reference.

Arbeiten mit Tags (Konsole)

Die Konsole ist die einfachste Möglichkeit, eine Pipeline zu markieren.

Um ein Tag zu erstellen

1. Melden Sie sich zu https://console.aws.amazon.com/aos/Hause bei der Amazon OpenSearch Service-Konsole an.
2. Wählen Sie im linken Navigationsbereich Pipelines.
3. Wählen Sie die Pipeline aus, zu der Sie Tags hinzufügen möchten und gehen Sie zur Registerkarte Tags.
4. Wählen Sie Verwalten und neues Tag hinzufügen.
5. Geben Sie einen Tag-Schlüssel und einen optionalen Wert ein.
6. Wählen Sie Speichern.

Um ein Tag zu löschen, führen Sie die gleichen Schritte aus und wählen Sie Entfernen auf der Seite Tags verwalten.

Weitere Informationen zur Verwendung der Konsole für die Arbeit mit Tags finden Sie unter Tag Editor im AWS Handbuch „Erste Schritte“ der Managementkonsole.

Arbeiten mit Tags (AWS CLI)

Um eine Pipeline mit dem zu AWS CLI taggen, senden Sie eine `TagResource` Anfrage:

```
aws osis tag-resource
  --arn arn:aws:osis:us-east-1:123456789012:pipeline/my-pipeline
  --tags Key=service,Value=osis Key=source,Value=otel
```

Entfernen Sie Tags mit dem `UntagResource` folgenden Befehl aus einer Pipeline:

```
aws osis untag-resource
  --arn arn:aws:osis:us-east-1:123456789012:pipeline/my-pipeline
  --tag-keys service
```

Zeigen Sie die vorhandenen Tags für eine Pipeline mit dem `ListTagsForResource` folgenden Befehl an:

```
aws osis list-tags-for-resource
  --arn arn:aws:osis:us-east-1:123456789012:pipeline/my-pipeline
```

Protokollierung und Überwachung von Amazon OpenSearch Ingestion mit Amazon CloudWatch

Amazon OpenSearch Ingestion veröffentlicht Metriken und Protokolle auf Amazon. CloudWatch

Themen

- Überwachen der Pipeline-Protokolle
- Überwachen der Pipeline

Überwachen der Pipeline-Protokolle

Sie können die Protokollierung für Amazon OpenSearch Ingestion-Pipelines aktivieren, um Fehler- und Warnmeldungen anzuzeigen, die während Pipeline-Vorgängen und Aufnahmeaktivitäten ausgelöst wurden. OpenSearch Ingestion veröffentlicht alle Protokolle in Amazon CloudWatch Logs. CloudWatch Mithilfe von Protokollen können Sie Informationen in den Protokolldateien überwachen und Sie benachrichtigen, wenn bestimmte Schwellenwerte erreicht werden. Sie können Ihre Protokolldaten auch in einem sehr robusten Speicher archivieren. Weitere Informationen finden Sie im Amazon CloudWatch Logs-Benutzerhandbuch.

Protokolle von OpenSearch Ingestion können auf eine fehlgeschlagene Verarbeitung von Anfragen, Authentifizierungsfehler von der Quelle bis zur Senke und andere Warnungen hinweisen, die bei der Fehlerbehebung hilfreich sein können. OpenSearch Ingestion verwendet für seine Protokolle die ProtokollebenenINFO,, undWARN. ERROR FATAL Wir empfehlen, die Protokollveröffentlichung für alle Pipelines zu aktivieren.

Erforderliche Berechtigungen

So aktivieren Sie OpenSearch Ingestion, um Protokolle an CloudWatch Protokolle zu senden. Sie müssen als Benutzer angemeldet sein, der über bestimmte IAM-Berechtigungen verfügt.

Sie benötigen die folgenden CloudWatch Logs-Berechtigungen, um Ressourcen für die Protokollzustellung zu erstellen und zu aktualisieren:

```
{a
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Effect": "Allow",
            "Resource": "*",
            "Action": [
                "logs:CreateLogDelivery",
                "logs:PutResourcePolicy",
                "logs:UpdateLogDelivery",
                "logs:DeleteLogDelivery",
                "logs:DescribeResourcePolicies",
                "logs:GetLogDelivery",
                "logs:ListLogDeliveries"
            ]
        }
    ]
}
```

Aktivieren der Protokollveröffentlichung

Sie können die Protokollveröffentlichung in vorhandenen Pipelines oder beim Erstellen einer Pipeline aktivieren. Anweisungen zum Aktivieren der Protokollveröffentlichung während der Pipelineerstellung finden Sie unterthe section called “Pipelines erstellen”.

Konsole

So aktivieren Sie die Veröffentlichung von Protokollen in einer vorhandenen Pipeline

1. Melden Sie sich zu https://console.aws.amazon.com/aos/Hause bei der Amazon OpenSearch Service-Konsole an.
2. Klicken Sie im linken Navigationsbereich auf Pipelines.
3. Öffnen Sie die Pipeline, für die Sie Protokolle aktivieren möchten, und wählen Sie dann Aktionen, Optionen zur Protokollveröffentlichung bearbeiten aus.
4. Aktivieren Sie „In CloudWatch Protokollen veröffentlichen“.
5. Erstellen Sie entweder eine neue Protokollgruppe oder wählen Sie eine bestehende. Wir empfehlen, den Namen als Pfad zu formatieren, z. `/aws/vendedlogs/OpenSearchIngestion/pipeline-name/audit-logs` B. Dieses Format erleichtert die Anwendung einer CloudWatch Zugriffsrichtlinie, die allen Protokollgruppen unter einem bestimmten Pfad Berechtigungen gewährt, z. `/aws/vendedlogs/OpenSearchIngestion` B.

> **Important**
>
> Sie müssen das Präfix `vendedlogs` in den Namen der Protokollgruppe aufnehmen, andernfalls schlägt die Erstellung fehl.

6. Wählen Sie Speichern.

CLI

Um die Veröffentlichung von Protokollen mithilfe von zu aktivieren AWS CLI, senden Sie die folgende Anfrage:

```
aws osis update-pipeline \
  --pipeline-name my-pipeline \
  --log-publishing-options  IsLoggingEnabled=true,CloudWatchLogDestination={LogGroup="/
aws/vendedlogs/OpenSearchIngestion/pipeline-name"}
```

Überwachen der Pipeline

Sie können Amazon OpenSearch Ingestion-Pipelines mit Amazon überwachen CloudWatch, das Rohdaten erfasst und in lesbare Kennzahlen in nahezu Echtzeit verarbeitet. Diese Statistiken werden 15 Monate gespeichert, damit Sie auf Verlaufsinformationen zugreifen können und einen besseren Überblick darüber erhalten, wie Ihre Webanwendung oder der Service ausgeführt werden. Sie können auch Alarme einrichten, die auf bestimmte Grenzwerte achten und Benachrichtigungen senden oder Aktivitäten auslösen, wenn diese Grenzwerte erreicht werden. Weitere Informationen finden Sie im CloudWatch Amazon-Benutzerhandbuch.

Die OpenSearch Ingestion-Konsole zeigt eine Reihe von Diagrammen an, die auf den unformatierten Daten aus CloudWatch der Registerkarte Performance für jede Pipeline basieren.

OpenSearch Ingestion meldet Metriken der meisten unterstützten Plugins. Wenn bestimmte Plugins unten keine eigene Tabelle haben, bedeutet das, dass sie keine Plugin-spezifischen Metriken melden. Pipeline-Metriken werden im `AWS/OSIS` Namespace veröffentlicht.

Themen

- Häufige -Metriken
- Puffer-Metriken

- Signature V4-Metriken
- Metriken für begrenzte Blockierungspuffer
- Quellmetriken von Otel Trace
- Hotel-Metriken, Quellmetriken
- HTTP-Metriken
- S3-Metriken
- Gesamtmetriken
- Datumsmetriken
- Metriken von Lambda
- Grok-Metriken
- Otel Trace Rohmetriken
- Metriken zu Hotel-Trace-Gruppen
- Zustandsmetriken zu Service Map
- OpenSearch Metriken
- System- und Metriken

Häufige -Metriken

Die folgenden Metriken gelten für alle Prozessoren und Senken.

Jeder Metrik wird der Name der Subpipeline und der Name des Plugins im Format < *sub_pipeline_name* >< >< > *plugin* vorangestellt. *metric_name* Der vollständige Name der `recordsIn.count` Metrik für eine Sub-Pipeline würde beispielsweise lauten `my-pipeline` und der Datumsprozessor lauten. `my-pipeline.date.recordsIn.count`

Metric	Beschreibung
`recordsIn.count`	Der Eingang von Datensätzen in eine Pipeline-Komponente. Diese Metrik gilt für Prozessoren und Senken. Relevante Statistiken: Summe Abmessung: `PipelineName`

Metric	Beschreibung
`recordsOut.count`	Der Ausgang von Datensätzen aus einer Pipeline-Komponente. Diese Metrik gilt für Prozessoren und Quellen. Relevante Statistiken: Summe Abmessung: `PipelineName`
`timeElapsed.count`	Eine Anzahl von Datenpunkten, die während der Ausführung einer Pipeline-Komponente aufgezeichnet wurden. Diese Metrik gilt für Prozessoren und Senken. Relevante Statistiken: Summe Abmessung: `PipelineName`
`timeElapsed.sum`	Die Gesamtzeit, die während der Ausführung einer Pipeline-Komponente verstrichen ist. Diese Metrik gilt für Prozessoren und Senken in Millisekunden. Relevante Statistiken: Summe Abmessung: `PipelineName`
`timeElapsed.max`	Die maximale Zeit, die während der Ausführung einer Pipeline-Komponente verstrichen ist. Diese Metrik gilt für Prozessoren und Senken in Millisekunden. Relevante Statistiken: Maximum Abmessung: `PipelineName`

Puffer-Metriken

Die folgenden Metriken gelten für den standardmäßigen Bounded Blocking Buffer, den OpenSearch Ingestion automatisch für alle Pipelines konfiguriert.

Jeder Metrik wird der Name der Subpipeline und der Name des Puffers im Format **< >< >** vorangestellt. *`sub_pipeline_name buffer_name metric_name`* Der vollständige Name der `recordsWritten.count` Metrik für eine Sub-Pipeline würde beispielsweise lauten. `my-pipeline` `my-pipeline.BlockingBuffer.recordsWritten.count`

Metric	Beschreibung
`recordsWritten.count`	Die Anzahl der Datensätze, die in einen Puffer geschrieb en wurden. Relevante Statistiken: Summe Dimension: `PipelineName`
`recordsRead.count`	Die Anzahl der Datensätze, die aus einem Puffer gelesen wurden. Relevante Statistiken: Summe Dimension: `PipelineName`
`recordsInFlight.value`	Die Anzahl der ungeprüften Datensätze, die aus einem Puffer gelesen wurden. Relevante Statistiken: Durchschnitt Dimension: `PipelineName`
`recordsInBuffer.value`	Die Anzahl der Datensätze, die sich derzeit in einem Puffer befinden. Relevante Statistiken: Durchschnitt Dimension: `PipelineName`
`recordsProcessed.count`	Die Anzahl der Datensätze, die aus einem Puffer gelesen und von einer Pipeline verarbeitet wurden. Relevante Statistiken: Summe Abmessung: `PipelineName`

Metric	Beschreibung
`recordsWriteFailed.count`	Die Anzahl der Datensätze, die die Pipeline nicht in die Senke schreiben konnte. Relevante Statistiken: Summe Abmessung: `PipelineName`
`writeTimeElapsed.count`	Eine Anzahl von Datenpunkten, die beim Schreiben in einen Puffer aufgezeichnet wurden. Relevante Statistiken: Summe Abmessung: `PipelineName`
`writeTimeElapsed.sum`	Die Gesamtzeit, die beim Schreiben in einen Puffer vergangen ist, in Millisekunden. Relevante Statistiken: Summe Abmessung: `PipelineName`
`writeTimeElapsed.max`	Die maximale Zeit, die beim Schreiben in einen Puffer verstrichen ist, in Millisekunden. Relevante Statistiken: Maximum Abmessung: `PipelineName`
`writeTimeouts.count`	Die Anzahl der Schreib-Timeouts in einen Puffer. Relevante Statistiken: Summe Dimension: `PipelineName`
`readTimeElapsed.count`	Eine Anzahl von Datenpunkten, die beim Lesen aus einem Puffer aufgezeichnet wurden. Relevante Statistiken: Summe Abmessung: `PipelineName`

Metric	Beschreibung
`readTimeElapsed.sum`	Die Gesamtzeit, die beim Lesen aus einem Puffer vergangen ist, in Millisekunden. Relevante Statistiken: Summe Abmessung: `PipelineName`
`readTimeElapsed.max`	Die maximale Zeit, die beim Lesen aus einem Puffer verstrichen ist, in Millisekunden. Relevante Statistiken: Maximum Abmessung: `PipelineName`
`checkpointTimeElapsed.count`	Eine Anzahl von Datenpunkten, die beim Checkpointing aufgezeichnet wurden. Relevante Statistiken: Summe Abmessung: `PipelineName`
`checkpointTimeElapsed.sum`	Die Gesamtzeit, die beim Checkpoint verstrichen ist, in Millisekunden. Relevante Statistiken: Summe Abmessung: `PipelineName`
`checkpointTimeElapsed.max`	Die maximale Zeit, die beim Checkpoint verstrichen ist, in Millisekunden. Relevante Statistiken: Maximum Abmessung: `PipelineName`

Signature V4-Metriken

Die folgenden Metriken gelten für den Aufnahmeendpunkt einer Pipeline und sind den Quell-Plugins (`httpotel_trace`, und`otel_metrics`) zugeordnet. Alle Anfragen an den Aufnahmeendpunkt

müssen mit Signature Version 4 signiert werden. Diese Metriken können Ihnen helfen, Autorisierungsprobleme beim Herstellen einer Verbindung zu Ihrer Pipeline zu identifizieren oder zu bestätigen, dass Sie sich erfolgreich authentifizieren.

Jeder Metrik wird der Name und der Sub-Pipeline vorangestellt. `osis_sigv4_auth` Beispiel, *`sub_pipeline_name`*`.osis_sigv4_auth.httpAuthSuccess.count`.

Metric	Beschreibung
`httpAuthSuccess.count`	Die Anzahl der erfolgreichen Signature V4-Anfragen an die Pipeline. Relevante Statistiken: Summe Dimension: `PipelineName`
`httpAuthFailure.count`	Die Anzahl der fehlgeschlagenen Signature V4-Anfragen an die Pipeline. Relevante Statistiken: Summe Abmessung: `PipelineName`
`httpAuthServerError.count`	Die Anzahl der Signature V4-Anfragen an die Pipeline, die Serverfehler zurückgegeben haben. Relevante Statistiken: Summe Dimension: `PipelineName`

Metriken für begrenzte Blockierungspuffer

Die folgenden Metriken gelten für den begrenzten Blockierpuffer. Jeder Metrik wird der Sub-Pipeline-Name und vorangestellt. `BlockingBuffer` Beispiel, *`sub_pipeline_name`*`.BlockingBuffer.bufferUsage.value`.

Metric	Beschreibung
`bufferUsage.value`	Prozentuale Nutzung von, `buffer_size` basierend auf der Anzahl der Datensätze im Puffer. `buffer_size` steht für die maximale Anzahl von Datensätzen, die in den Puffer geschrieben wurden, sowie für Datensätze, die noch nicht überprüft wurden. Relevante Statistiken: Durchschnitt Dimension: `PipelineName`

Quellmetriken von Otel Trace

Die folgenden Metriken gelten für die OTel Trace-Quelle. Jeder Metrik wird der Sub-Pipeline-Name und vorangestellt. `otel_trace_source` Beispiel, *`sub_pipeline_name`*`.otel_trace_source.requestTimeouts.count`.

Metric	Beschreibung
`requestTimeouts.count`	Die Anzahl der Anfragen, die das Zeitlimit überschritten haben. Relevante Statistiken: Summe Dimension: `PipelineName`
`requestsReceived.count`	Die Anzahl der vom Plugin empfangenen Anfragen. Relevante Statistiken: Summe Abmessung: `PipelineName`
`successRequests.count`	Die Anzahl der Anfragen, die vom Plugin erfolgreich verarbeitet wurden. Relevante Statistiken: Summe Abmessung: `PipelineName`

Metric	Beschreibung
`badRequests.count`	Die Anzahl der Anfragen mit einem ungültigen Format, die vom Plugin verarbeitet wurden. Relevante Statistiken: Summe Abmessung: `PipelineName`
`requestsTooLarge.count`	Die Anzahl der Anfragen, bei denen die Anzahl der Spans im Inhalt größer ist als die Pufferkapazität. Relevante Statistiken: Summe Dimension: `PipelineName`
`internalServerError.count`	Die Anzahl der Anfragen, die vom Plugin mit einem benutzerdefinierten Ausnahmetyp verarbeitet wurden. Relevante Statistiken: Summe Dimension: `PipelineName`
`requestProcessDuration.count`	Eine Anzahl von Datenpunkten, die bei der Verarbeitung von Anfragen durch das Plugin aufgezeichnet wurden. Relevante Statistiken: Summe Abmessung: `PipelineName`
`requestProcessDuration.sum`	Die Gesamtlatenz der vom Plugin verarbeiteten Anfragen in Millisekunden. Relevante Statistiken: Summe Abmessung: `PipelineName`

Metric	Beschreibung
`requestProcessDuration.max`	Die maximale Latenz der vom Plugin verarbeiteten Anfragen in Millisekunden. Relevante Statistiken: Maximum Abmessung: `PipelineName`
`payloadSize.count`	Zählt die Verteilung der Nutzlastgrößen eingehender Anfragen in Byte. Relevante Statistiken: Summe Abmessung: `PipelineName`
`payloadSize.sum`	Die Gesamtverteilung der Nutzlastgrößen eingehender Anfragen in Byte. Relevante Statistiken: Summe Abmessung: `PipelineName`
`payloadSize.max`	Die maximale Verteilung der Nutzlastgrößen eingehender Anfragen in Byte. Relevante Statistiken: Maximum Abmessung: `PipelineName`

Hotel-Metriken, Quellmetriken

Die folgenden Metriken gelten für die Quelle der OTel Metriken. Jeder Metrik wird der Name und der Sub-Pipeline vorangestellt. `otel_metrics_source` Beispiel, *`sub_pipeline_name`*`.otel_metrics_source.requestTimeouts.count`.

Metric	Beschreibung
`requestTimeouts.count`	Die Gesamtanzahl der Anfragen an das Plugin, die das Zeitlimit überschritten haben.

Metric	Beschreibung
	Relevante Statistiken: Summe Dimension: `PipelineName`
`requestsReceived.count`	Die Gesamtzahl der vom Plugin empfangenen Anfragen. Relevante Statistiken: Summe Dimension: `PipelineName`
`successRequests.count`	Die Anzahl der Anfragen, die vom Plugin erfolgreich verarbeitet wurden (200 Antwortstatuscode). Relevante Statistiken: Summe Abmessung: `PipelineName`
`requestProcessDuration.count`	Zählt die Latenz der vom Plugin verarbeiteten Anfragen in Sekunden. Relevante Statistiken: Summe Abmessung: `PipelineName`
`requestProcessDuration.sum`	Die Gesamtlatenz der vom Plugin verarbeiteten Anfragen in Millisekunden. Relevante Statistiken: Summe Abmessung: `PipelineName`
`requestProcessDuration.max`	Die maximale Latenz der vom Plugin verarbeiteten Anfragen in Millisekunden. Relevante Statistiken: Maximum Abmessung: `PipelineName`

Metric	Beschreibung
`payloadSize.count`	Zählt die Verteilung der Nutzlastgrößen eingehender Anfragen in Byte. Relevante Statistiken: Summe Abmessung: `PipelineName`
`payloadSize.sum`	Die Gesamtverteilung der Nutzlastgrößen eingehender Anfragen in Byte. Relevante Statistiken: Summe Abmessung: `PipelineName`
`payloadSize.max`	Die maximale Verteilung der Nutzlastgrößen eingehender Anfragen in Byte. Relevante Statistiken: Maximum Abmessung: `PipelineName`

HTTP-Metriken

Die folgenden Metriken gelten für die HTTP-Quelle. Jeder Metrik wird der Sub-Pipeline-Name und vorangestellt. `http` Beispiel, *`sub_pipeline_name`*`.http.requestsReceived.count`.

Metric	Beschreibung
`requestsReceived.count`	Die Anzahl der vom `/log/ingest` -Endpunkt empfangenen Anforderungen. Relevante Statistiken: Summe Dimension: `PipelineName`
`requestsRejected.count`	Die Anzahl der vom Plugin abgelehnten Anfragen (429 Antwortstatuscode).

Metric	Beschreibung
	Relevante Statistiken: Summe Abmessung: `PipelineName`
`successRequests.count`	Die Anzahl der Anfragen, die vom Plugin erfolgreich verarbeitet wurden (200 Antwortstatuscode). Relevante Statistiken: Summe Abmessung: `PipelineName`
`badRequests.count`	Die Anzahl der Anfragen mit ungültigem Inhaltstyp oder Format (400 Antwortstatuscode), die vom Plugin verarbeit et wurden. Relevante Statistiken: Summe Dimension: `PipelineName`
`requestTimeouts.count`	Die Anzahl der Anfragen, bei denen im HTTP-Quellserver ein Timeout auftritt (415 Antwortstatuscode). Relevante Statistiken: Summe Dimension: `PipelineName`
`requestsTooLarge.count`	Die Anzahl der Anfragen, bei denen die Größe der Ereignisse im Inhalt größer ist als die Pufferkapazität (413 Antwortstatuscode). Relevante Statistiken: Summe Dimension: `PipelineName`

Metric	Beschreibung
`internalServerError.count`	Die Anzahl der Anfragen, die vom Plugin mit einem benutzerdefinierten Ausnahmetyp (500 Antwortstatuscode) verarbeitet wurden. Relevante Statistiken: Summe Dimension: `PipelineName`
`requestProcessDuration.count`	Zählt die Latenz der vom Plugin verarbeiteten Anfragen in Sekunden. Relevante Statistiken: Summe Abmessung: `PipelineName`
`requestProcessDuration.sum`	Die Gesamtlatenz der vom Plugin verarbeiteten Anfragen in Millisekunden. Relevante Statistiken: Summe Abmessung: `PipelineName`
`requestProcessDuration.max`	Die maximale Latenz der vom Plugin verarbeiteten Anfragen in Millisekunden. Relevante Statistiken: Maximum Abmessung: `PipelineName`
`payloadSize.count`	Zählt die Verteilung der Nutzlastgrößen eingehender Anfragen in Byte. Relevante Statistiken: Summe Abmessung: `PipelineName`

Metric	Beschreibung
`payloadSize.sum`	Die Gesamtverteilung der Nutzlastgrößen eingehender Anfragen in Byte. Relevante Statistiken: Summe Abmessung: `PipelineName`
`payloadSize.max`	Die maximale Verteilung der Nutzlastgrößen eingehender Anfragen in Byte. Relevante Statistiken: Maximum Abmessung: `PipelineName`

S3-Metriken

Die folgenden Metriken gelten für die S3-Quelle. Jeder Metrik wird der Name der Subpipeline und vorangestellt. `s3` Beispiel, *`sub_pipeline_name`*`.s3.s3ObjectsFailed.count`.

Metric	Beschreibung
`s3ObjectsFailed.count`	Die Gesamtzahl der S3-Objekte, die das Plugin nicht lesen konnte. Relevante Statistiken: Summe Abmessung: `PipelineName`
`s3ObjectsNotFound.count`	Die Anzahl der S3-Objekte, die das Plugin aufgrund eines `Not Found` Fehlers von S3 nicht lesen konnte. Diese Metriken werden ebenfalls auf die `s3ObjectsFailed` Metrik angerechnet. Relevante Statistiken: Summe Dimension: `PipelineName`

Metric	Beschreibung
`s3ObjectsAccessDenied.count`	Die Anzahl der S3-Objekte, die das Plugin aufgrund eines `Access Denied` `Forbidden` Oder-Fehlers von S3 nicht lesen konnte. Diese Metriken werden ebenfalls auf die `s3ObjectsFailed` Metrik angerechnet. Relevante Statistiken: Summe Dimension: `PipelineName`
`s3ObjectReadTimeElapsed.count`	Die Zeit, die das Plugin benötigt, um eine GET-Anfrage für ein S3-Objekt auszuführen, es zu analysieren und Ereignisse in den Puffer zu schreiben. Relevante Statistiken: Summe Abmessung: `PipelineName`
`s3ObjectReadTimeElapsed.sum`	Die Gesamtzeit in Millisekunden, die das Plugin benötigt, um eine GET-Anfrage für ein S3-Objekt auszuführen, es zu analysieren und Ereignisse in den Puffer zu schreiben. Relevante Statistiken: Summe Abmessung: `PipelineName`
`s3ObjectReadTimeElapsed.max`	Die maximale Zeit in Millisekunden, die das Plugin benötigt, um eine GET-Anfrage für ein S3-Objekt auszuführen, es zu analysieren und Ereignisse in den Puffer zu schreiben. Relevante Statistiken: Maximum Abmessung: `PipelineName`
`s3ObjectSizeBytes.count`	Die Anzahl der Verteilung der S3-Objektgrößen in Byte. Relevante Statistiken: Summe Abmessung: `PipelineName`

Metric	Beschreibung
`s3ObjectSizeBytes.sum`	Die Gesamtverteilung der S3-Objektgrößen in Byte. Relevante Statistiken: Summe Dimension: `PipelineName`
`s3ObjectSizeBytes.max`	Die maximale Verteilung der S3-Objektgrößen in Byte. Relevante Statistiken: Maximum Dimension: `PipelineName`
`s3ObjectProcessedBytes.count`	Die Anzahl der vom Plugin verarbeiteten S3-Objekte in Byte. Relevante Statistiken: Summe Abmessung: `PipelineName`
`s3ObjectProcessedBytes.sum`	Die Gesamtverteilung der vom Plugin verarbeiteten S3-Objekte in Byte. Relevante Statistiken: Summe Abmessung: `PipelineName`
`s3ObjectProcessedBytes.max`	Die maximale Verteilung der vom Plugin verarbeiteten S3-Objekte in Byte. Relevante Statistiken: Maximum Abmessung: `PipelineName`
`s3ObjectsEvents.count`	Die Anzahl der vom Plugin empfangenen S3-Ereignisse. Relevante Statistiken: Summe Abmessung: `PipelineName`

Metric	Beschreibung
`s3ObjectsEvents.sum`	Die Gesamtverteilung der vom Plugin empfangenen S3-Ereignisse. Relevante Statistiken: Summe Abmessung: `PipelineName`
`s3ObjectsEvents.max`	Die maximale Verteilung der vom Plugin empfangenen S3-Ereignisse. Relevante Statistiken: Maximum Abmessung: `PipelineName`
`sqsMessageDelay.count`	Eine Anzahl von Datenpunkten, die aufgezeichnet wurden, während S3 einen Zeitpunkt des Ereignisses von der Erstellung eines Objekts bis zu dem Zeitpunkt aufzeichnet, zu dem es vollständig analysiert wurde. Relevante Statistiken: Summe Abmessung: `PipelineName`
`sqsMessageDelay.sum`	Die Gesamtzeit in Millisekunden zwischen dem Zeitpunkt , zu dem S3 ein Ereignis für die Erstellung eines Objekts aufzeichnet, und dem Zeitpunkt, zu dem es vollständig analysiert wurde. Relevante Statistiken: Summe Abmessung: `PipelineName`

Metric	Beschreibung
`sqsMessageDelay.max`	Die maximale Zeitspanne zwischen dem Zeitpunkt, zu dem S3 ein Ereignis für die Erstellung eines Objekts aufzeichn et, und dem Zeitpunkt, zu dem es vollständig analysiert wurde, in Millisekunden. Relevante Statistiken: Maximum Abmessung: `PipelineName`
`s3ObjectsSucceeded.count`	Die Anzahl der S3-Objekte, die das Plugin erfolgreich gelesen hat. Relevante Statistiken: Summe Abmessung: `PipelineName`
`sqsMessagesReceived.count`	Die Anzahl der Amazon SQS SQS-Nachrichten, die das Plugin aus der Warteschlange empfangen hat. Relevante Statistiken: Summe Abmessung: `PipelineName`
`sqsMessagesDeleted.count`	Die Anzahl der Amazon SQS SQS-Nachrichten, die durch das Plugin aus der Warteschlange gelöscht wurden. Relevante Statistiken: Summe Abmessung: `PipelineName`
`sqsMessagesFailed.count`	Die Anzahl der Amazon SQS SQS-Nachrichten, die das Plugin nicht analysieren konnte. Relevante Statistiken: Summe Abmessung: `PipelineName`

Gesamtmetriken

Die folgenden Metriken gelten für den Aggregate-Prozessor. Jeder Metrik wird der Sub-Pipeline-Name und vorangestellt. `aggregate` Beispiel, *`sub_pipeline_name`*`.aggregate.actionHandleEventsOut.count`.

Metric	Beschreibung
`actionHandleEventsOut.count`	Die Anzahl der Ereignisse, die vom `handleEvent` Aufruf zur konfigurierten Aktion zurückgegeben wurden. Relevante Statistiken: Summe Abmessung: `PipelineName`
`actionHandleEventsDropped.count`	Die Anzahl der Ereignisse, die vom `handleEvent` Aufruf zur konfigurierten Aktion zurückgegeben wurden. Relevante Statistiken: Summe Abmessung: `PipelineName`
`actionHandleEventsProcessingErrors.count`	Die Anzahl der Aufrufe `handleEvent` für die konfiguri erte Aktion, die zu einem Fehler geführt haben. Relevante Statistiken: Summe Abmessung: `PipelineName`
`actionConcludeGroupEventsOut.count`	Die Anzahl der Ereignisse, die vom `concludeGroup` Aufruf zur konfigurierten Aktion zurückgegeben wurden. Relevante Statistiken: Summe Abmessung: `PipelineName`
`actionConcludeGroupEventsDropped.count`	Die Anzahl der Ereignisse, die beim `condludeGroup` Aufruf der konfigurierten Aktion nicht zurückgegeben wurden. Relevante Statistiken: Summe

Metric	Beschreibung
	Abmessung: `PipelineName`
`actionConcludeGroupEventsProcessingErrors.count`	Die Anzahl der Aufrufe `concludeGroup` für die konfigurierte Aktion, die zu einem Fehler geführt haben. Relevante Statistiken: Summe Abmessung: `PipelineName`
`currentAggregateGroups.value`	Die aktuelle Anzahl von Gruppen. Diese Anzeige nimmt ab, wenn Gruppen geschlossen werden, und nimmt zu, wenn ein Ereignis die Erstellung einer neuen Gruppe einleitet. Relevante Statistiken: Durchschnitt Dimension: `PipelineName`

Datumsmetriken

Die folgenden Metriken gelten für den Datumsprozessor. Jeder Metrik wird der Name und der Subpipeline vorangestellt. `date` Beispiel, *`sub_pipeline_name`*`.date.dateProcessingMatchSuccess.count`.

Metric	Beschreibung
`dateProcessingMatchSuccess.count`	Die Anzahl der Datensätze, die mindestens einem der in der `match` Konfigurationsoption angegebenen Muster entsprechen. Relevante Statistiken: Summe Dimension: `PipelineName`
`dateProcessingMatchFailure.count`	Die Anzahl der Datensätze, die keinem der in der `match` Konfigurationsoption angegebenen Muster entsprachen. Relevante Statistiken: Summe

Metric	Beschreibung
	Dimension: `PipelineName`

Metriken von Lambda

Die folgenden Metriken gelten für den AWS LambdaProzessor. Jeder Metrik wird der Sub-Pipeline-Name und vorangestellt. `lambda` Beispiel, *`sub_pipeline_name`*`.lambda.recordsSuccessfullySentToLambda.count`.

Metric	Beschreibung
`recordsSuccessfullySentToLambda.count`	Die Anzahl der Datensätze, die von der Lambda-Funktion erfolgreich verarbeitet wurden. Relevante Statistiken: Summe Abmessung: `PipelineName`
`recordsFailedToSendToLambda.count`	Die Anzahl der Datensätze, die nicht an die Lambda-Funktion gesendet wurden. Relevante Statistiken: Summe Abmessung: `PipelineName`
`lambdaFunctionLatency.avg` `lambdaFunctionLatency.max`	Die Latenz von Lambda-Funktionsaufrufen. Relevante Statistiken: Durchschnitt und Maximum Dimension: `PipelineName`
`numberOfRequestsSucceeded.count`	Die Gesamtzahl der erfolgreichen Lambda-Aufrufanforderungen. Relevante Statistiken: Summe Dimension: `PipelineName`

Metric	Beschreibung
`numberOfRequestsFailed.count`	Die Gesamtzahl der fehlgeschlagenen Lambda-Aufrufanforderungen. Relevante Statistiken: Summe Dimension: `PipelineName`
`requestPayloadSize.avg`	Die Größe der an Lambda gesendeten Anforderungsnutzlasten. Relevante Statistiken: Durchschnitt Dimension: `PipelineName`
`responsePayloadSize.avg`	Die Größe der Antwortnutzlasten, die von Lambda empfangen wurden. Relevante Statistiken: Durchschnitt Dimension: `PipelineName`

Grok-Metriken

Die folgenden Metriken gelten für den Grok-Prozessor. Jeder Metrik wird der Sub-Pipeline-Name und vorangestellt. `grok` Beispiel, *`sub_pipeline_name`*`.grok.grokProcessingMatch.count`.

Metric	Beschreibung
`grokProcessingMatch.count`	Die Anzahl der Datensätze, bei denen mindestens eine Musterübereinstimmung mit der `match` Konfigurationsoption gefunden wurde. Relevante Statistiken: Summe Abmessung: `PipelineName`
`grokProcessingMismatch.count`	Die Anzahl der Datensätze, die keinem der in der `match` Konfigurationsoption angegebenen Muster entsprachen.

Metric	Beschreibung
	Relevante Statistiken: Summe Dimension: `PipelineName`
`grokProcessingErrors.count`	Die Anzahl der Fehler bei der Verarbeitung von Datensätzen. Relevante Statistiken: Summe Dimension: `PipelineName`
`grokProcessingTimeouts.count`	Die Anzahl der Datensätze, die beim Abgleich das Zeitlimit überschritten haben. Relevante Statistiken: Summe Dimension: `PipelineName`
`grokProcessingTime.count`	Eine Anzahl von Datenpunkten, die aufgezeichnet wurden, während ein einzelner Datensatz mit Mustern aus der `match` Konfigurationsoption übereinstimmt. Relevante Statistiken: Summe Dimension: `PipelineName`
`grokProcessingTime.sum`	Die Gesamtzeit, die jeder einzelne Datensatz benötigt, um ihn mit den Mustern aus der `match` Konfigurationsoption abzugleichen, in Millisekunden. Relevante Statistiken: Summe Dimension: `PipelineName`

Metric	Beschreibung
`grokProcessingTime.max`	Die maximale Zeit in Millisekunden, die jeder einzelne Datensatz benötigt, um ihn mit den Mustern aus der `match` Konfigurationsoption abzugleichen. Relevante Statistiken: Maximum Abmessung: `PipelineName`

Otel Trace Rohmetriken

Die folgenden Metriken gelten für den OTel Trace Raw-Prozessor. Jeder Metrik wird der Sub-Pipeline-Name und vorangestellt. `otel_trace_raw` Beispiel, *`sub_pipeline_name`*`.otel_trace_raw.traceGroupCacheCount.value`.

Metric	Beschreibung
`traceGroupCacheCount.value`	Die Anzahl der Trace-Gruppen im Trace-Gruppen-Cache. Relevante Statistiken: Summe Dimension: `PipelineName`
`spanSetCount.value`	Die Anzahl der Span-Sets in der Span-Set-Sammlung. Relevante Statistiken: Summe Dimension: `PipelineName`

Metriken zu Hotel-Trace-Gruppen

Die folgenden Metriken gelten für den OTel Trace-Gruppenprozessor. Jeder Metrik wird der Sub-Pipeline-Name und vorangestellt. `otel_trace_group` Beispiel, *`sub_pipeline_name`*`.otel_trace_group.recordsInMissingTraceGroup.count`.

Metric	Beschreibung
`recordsInMissingTraceGroup.count`	Die Anzahl der Eingangsdatensätze, bei denen Trace-Gruppenfelder fehlen. Relevante Statistiken: Summe Dimension: `PipelineName`
`recordsOutFixedTraceGroup.count`	Die Anzahl der Ausgangsdatensätze mit Trace-Gruppenfeldern, die erfolgreich gefüllt wurden. Relevante Statistiken: Summe Dimension: `PipelineName`
`recordsOutMissingTraceGroup.count`	Die Anzahl der Ausgangsdatensätze, bei denen Trace-Gruppenfelder fehlen. Relevante Statistiken: Summe Dimension: `PipelineName`

Zustandsmetriken zu Service Map

Die folgenden Metriken gelten für den zustandsbehafteten Service-MAP-Prozessor. Jeder Metrik wird der Sub-Pipeline-Name und vorangestellt. `service-map-stateful` Beispiel, *`sub_pipeline_name`*`.service-map-stateful.spansDbSize.count`.

Metric	Beschreibung
`spansDbSize.value`	Die speicherinternen Bytegrößen von Spans in MapDB für die aktuelle und vorherige Fensterdauer. Relevante Statistiken: Durchschnitt Dimension: `PipelineName`

Metric	Beschreibung
`traceGroupDbSize.value`	Die speicherinternen Bytegrößen der Trace-Gruppen in MapDB für die aktuelle und vorherige Fensterdauer. Relevante Statistiken: Durchschnitt Dimension: `PipelineName`
`spansDbCount.value`	Die Anzahl der Zeitspannen in MapDB über die aktuelle und vorherige Fensterdauer. Relevante Statistiken: Summe Abmessung: `PipelineName`
`traceGroupDbCount.value`	Die Anzahl der Trace-Gruppen in MapDB für die aktuelle und vorherige Fensterdauer. Relevante Statistiken: Summe Dimension: `PipelineName`
`relationshipCount.value`	Die Anzahl der Beziehungen, die während der aktuellen und vorherigen Fensterdauer gespeichert wurden. Relevante Statistiken: Summe Dimension: `PipelineName`

OpenSearch Metriken

Die folgenden Kennzahlen gelten für die OpenSearchSpüle. Jeder Metrik wird der Name und der Subpipeline vorangestellt. `opensearch` Beispiel, *`sub_pipeline_name`*`.opensearch.bulkRequestErrors.count`.

Metric	Beschreibung
`bulkRequestErrors.count`	Die Gesamtzahl der Fehler, die beim Senden von Massenanfragen aufgetreten sind.

Metric	Beschreibung
	Relevante Statistiken: Summe Dimension: `PipelineName`
`documentsSuccess.count`	Die Anzahl der Dokumente, die erfolgreich per Sammelanforderung an den OpenSearch Service gesendet wurden, einschließlich Wiederholungen. Relevante Statistiken: Summe Abmessung: `PipelineName`
`documentsSuccessFirstAttempt.count`	Die Anzahl der Dokumente, die beim ersten Versuch erfolgreich per Sammelanforderung an den OpenSearch Service gesendet wurden. Relevante Statistiken: Summe Abmessung: `PipelineName`
`documentErrors.count`	Die Anzahl der Dokumente, die im Rahmen von Massenanfragen nicht gesendet werden konnten. Relevante Statistiken: Summe Abmessung: `PipelineName`
`bulkRequestFailed.count`	Die Anzahl der fehlgeschlagenen Massenanforderungen. Relevante Statistiken: Summe Dimension: `PipelineName`
`bulkRequestNumberOfRetries.count`	Die Anzahl der Wiederholungen fehlgeschlagener Massenanforderungen. Relevante Statistiken: Summe Dimension: `PipelineName`

Metric	Beschreibung
`bulkBadRequestErrors.count`	Die Anzahl der `Bad Request` Fehler, die beim Senden von Massenanfragen aufgetreten sind. Relevante Statistiken: Summe Abmessung: `PipelineName`
`bulkRequestNotAllowedErrors.count`	Die Anzahl der `Request Not Allowed` Fehler, die beim Senden von Massenanfragen aufgetreten sind. Relevante Statistiken: Summe Abmessung: `PipelineName`
`bulkRequestInvalidInputErrors.count`	Die Anzahl der `Invalid Input` Fehler, die beim Senden von Massenanfragen aufgetreten sind. Relevante Statistiken: Summe Abmessung: `PipelineName`
`bulkRequestNotFoundErrors.count`	Die Anzahl der `Request Not Found` Fehler, die beim Senden von Massenanfragen aufgetreten sind. Relevante Statistiken: Summe Abmessung: `PipelineName`
`bulkRequestTimeoutErrors.count`	Die Anzahl der `Request Timeout` Fehler, die beim Senden von Massenanfragen aufgetreten sind. Relevante Statistiken: Summe Abmessung: `PipelineName`

Metric	Beschreibung
`bulkRequestServerErrors.count`	Die Anzahl der `Server Error` Fehler, die beim Senden von Massenanfragen aufgetreten sind. Relevante Statistiken: Summe Abmessung: `PipelineName`
`bulkRequestSizeBytes.count`	Zählt die Verteilung der Nutzlastgrößen von Massenanfragen in Byte. Relevante Statistiken: Summe Abmessung: `PipelineName`
`bulkRequestSizeBytes.sum`	Die Gesamtverteilung der Nutzlastgrößen von Massenanfragen in Byte. Relevante Statistiken: Summe Dimension: `PipelineName`
`bulkRequestSizeBytes.max`	Die maximale Verteilung der Nutzlastgrößen von Massenanfragen in Byte. Relevante Statistiken: Maximum Abmessung: `PipelineName`
`bulkRequestLatency.count`	Eine Anzahl von Datenpunkten, die aufgezeichnet wurden, während Anfragen an das Plugin gesendet werden, einschließlich Wiederholungsversuchen. Relevante Statistiken: Summe Abmessung: `PipelineName`

Metric	Beschreibung
`bulkRequestLatency.sum`	Die Gesamtlatenz der an das Plugin gesendeten Anfragen, einschließlich Wiederholungen, in Millisekunden. Relevante Statistiken: Summe Abmessung: `PipelineName`
`bulkRequestLatency.max`	Die maximale Latenz von Anfragen, die an das Plugin gesendet werden, einschließlich Wiederholungen, in Millisekunden. Relevante Statistiken: Maximum Abmessung: `PipelineName`
`s3.dlqS3RecordsSuccess.count`	Die Anzahl der Datensätze, die erfolgreich an die S3-Warteschlange für unzustellbare Briefe gesendet wurden. Relevante Statistiken: Summe Abmessung: `PipelineName`
`s3.dlqS3RecordsFailed.count`	Die Anzahl der Ressourcen, die nicht an die S3-Warteschlange für unzustellbare Briefe gesendet werden konnten. Relevante Statistiken: Summe Abmessung: `PipelineName`
`s3.dlqS3RequestSuccess.count`	Die Anzahl der erfolgreichen Anfragen an die S3-Warteschlange für unzustellbare Briefe. Relevante Statistiken: Summe Abmessung: `PipelineName`

Metric	Beschreibung
`s3.dlqS3RequestFailed.count`	Die Anzahl der fehlgeschlagenen Anfragen an die S3-Warteschlange für unzustellbare Briefe. Relevante Statistiken: Summe Abmessung: `PipelineName`
`s3.dlqS3RequestLatency.count`	Eine Anzahl von Datenpunkten, die aufgezeichnet wurden, während Anfragen an die S3-Warteschlange für unzustellbare Briefe gesendet wurden, einschließlich Wiederholungsversuchen. Relevante Statistiken: Summe Abmessung: `PipelineName`
`s3.dlqS3RequestLatency.sum`	Die Gesamtlatenz von Anfragen, die an die S3-Warteschlange für unzustellbare Briefe gesendet wurden, einschließlich Wiederholungen, in Millisekunden. Relevante Statistiken: Summe Abmessung: `PipelineName`
`s3.dlqS3RequestLatency.max`	Die maximale Latenz von Anfragen, die an die S3-Warteschlange für unzustellbare Briefe gesendet werden, einschließlich Wiederholungen, in Millisekunden. Relevante Statistiken: Maximum Abmessung: `PipelineName`
`s3.dlqS3RequestSizeBytes.count`	Zählt die Verteilung der Nutzlastgrößen von Anfragen an die S3-Warteschlange mit unerlaubten Briefen in Byte. Relevante Statistiken: Summe Abmessung: `PipelineName`

Metric	Beschreibung
`s3.dlqS3RequestSizeBytes.sum`	Die Gesamtverteilung der Nutzlastgrößen von Anfragen an die S3-Warteschlange mit unerlaubten Briefen in Byte. Relevante Statistiken: Summe Dimension: `PipelineName`
`s3.dlqS3RequestSizeBytes.max`	Die maximale Verteilung der Nutzlastgrößen von Anfragen an die S3-Warteschlange mit unerlaubten Briefen in Byte. Relevante Statistiken: Maximum Abmessung: `PipelineName`

System- und Metriken

Die folgenden -Metriken gelten für das gesamte OpenSearch Aufnahmesystem. Diesen Metriken ist nichts vorangestellt.

Metrik	Beschreibung
`system.cpu.usage.value`	Der Prozentsatz der verfügbaren CPU-Auslastung für alle Datenknoten. Relevante Statistiken: Durchschnitt Dimension:`PipelineName` ,`area`, `id`
`system.cpu.count.value`	Die Gesamtmenge der CPU-Auslastung für alle Datenknoten. Relevante Statistiken: Durchschnitt Dimension:`PipelineName` ,`area`, `id`
`jvm.memory.max.value`	Die maximale Speichermenge, die für die Speicherverwaltung verwendet werden kann, in Byte.

Metrik	Beschreibung
	Relevante Statistiken: Durchschnitt Dimension:`PipelineName ,area, id`
`jvm.memory.used.value`	Die Gesamtmenge des Arbeitsspeichers in Byte. Relevante Statistiken: Durchschnitt Größe: 1`PipelineName` , 2`area`, 1 `id` Zeichen
`jvm.memory.committed.value`	Die Speichermenge, die für die Verwendung durch die Java Virtual Machine (JVM) zugeteilt ist (in Byte). Relevante Statistiken: Durchschnitt Dimension:`PipelineName ,area, id`
`computeUnits`	Die Anzahl der Ingestion OpenSearch Compute Units (Ingestion OCUs), die von einer Pipeline verwendet werden. Relevante Statistiken: Maximum, Summe, Durchschnitt Dimension: `PipelineName`

Bewährte Methoden für Amazon OpenSearch Ingestion

Dieses Thema enthält bewährte Methoden für die Erstellung und Verwaltung von OpenSearch Amazon-Ingestion-Pipelines sowie allgemeine Richtlinien, die für viele Anwendungsfälle gelten. Jede Workload ist einzigartig und weist einzigartige Merkmale auf, sodass keine generische Empfehlung für jeden Anwendungsfall genau richtig ist.

Themen

- Allgemeine bewährte Methoden
- Empfohlene CloudWatch Alarme

Allgemeine bewährte Methoden

Die folgenden allgemeinen bewährten Methoden gelten für die Erstellung und Verwaltung von Pipelines.

- Um eine hohe Verfügbarkeit sicherzustellen, konfigurieren Sie VPC-Pipelines mit zwei oder drei Subnetzen. Wenn Sie eine Pipeline nur in einem Subnetz bereitstellen und die Availability Zone ausfällt, können Sie keine Daten aufnehmen.
- Wir empfehlen, die Anzahl der Sub-Pipelines innerhalb jeder Pipeline auf 5 oder weniger zu beschränken.
- Wenn Sie das S3-Quell-Plugin verwenden, verwenden Sie S3-Dateien mit gleichmäßiger Größe, um eine optimale Leistung zu erzielen.
- Wenn Sie das S3-Quell-Plugin verwenden, fügen Sie für eine optimale Leistung 30 Sekunden zusätzliches Sichtbarkeits-Timeout pro 0,25 GB Dateigröße im S3-Bucket hinzu.
- Fügen Sie Ihrer Pipeline-Konfiguration eine Warteschlange (Dead-Letter Queue, DLQ) hinzu, damit Sie fehlgeschlagene Ereignisse auslagern und sie für Analysen zugänglich machen können. Wenn Ihre Senken Daten aufgrund falscher Zuordnungen oder anderer Probleme zurückweisen, können Sie die Daten an den DLQ weiterleiten, um das Problem zu beheben und zu beheben.

Empfohlene CloudWatch Alarme

CloudWatch Alarme führen eine Aktion aus, wenn eine CloudWatch Metrik einen bestimmten Wert für einen bestimmten Zeitraum überschreitet. Möglicherweise möchten Sie Ihnen eine E-Mail AWS senden, wenn Ihr Cluster-Integritätsstatus `red` länger als eine Minute andauert. Dieser Abschnitt enthält einige empfohlene Alarme für Amazon OpenSearch Ingestion und angemessene Reaktionen darauf.

Weitere Informationen zur Konfiguration von Alarmen finden Sie unter CloudWatchAmazon-Alarme erstellen im CloudWatch Amazon-Benutzerhandbuch.

Alarm	Problem
`computeUnits` Der Höchstwert ist = der `maxUnits` für 15 Minuten konfigurierte	Die Pipeline hat die maximale Kapazität erreicht und muss möglicher weise `maxUnits` aktualisiert werden. Erhöhen Sie die maximale Kapazität Ihrer Pipeline

Alarm	Problem
Wert, 3 aufeinand erfolgende Male	
`opensearc h.documen tErrors.c ount` Summe ist = *`{sub_pipe line_name }`* `.opensear ch.record sIn.count` Summe für 1 Minute, 1 Mal hintereinander	Die Pipeline kann nicht in die OpenSearch Senke schreiben. Überprüfen Sie die Pipeline-Berechtigungen und stellen Sie sicher, dass die Domain oder Sammlung fehlerfrei ist. Sie können auch die Dead-Letter-Wartes chlange (DLQ) auf fehlgeschlagene Ereignisse überprüfen, sofern sie konfiguriert ist.
`bulkReque stLatency .max` Max ist >= x für 1 Minute, 1 Mal hintereinander	Die Pipeline weist beim Senden von Daten an die OpenSearch Senke eine hohe Latenz auf. Dies ist wahrscheinlich auf eine zu geringe Größe der Senke oder auf eine schlechte Sharding-Strategie zurückzuführen, wodurch die Senke ins Hintertreffen gerät. Eine anhaltend hohe Latenz kann sich auf die Leistung der Pipeline auswirken und wird wahrschei nlich zu einem Gegendruck auf die Clients führen.
`httpAuthF ailure.co unt` Summe >= 1 für 1 Minute, 1 Mal hintereinander	Aufnahmeanfragen werden nicht authentifiziert. Vergewissern Sie sich, dass auf allen Clients die Authentifizierung mit Signature Version 4 korrekt aktiviert ist.
`system.cp u.usage.v alue` Durchschnitt >= 80% für 15 Minuten, 3 Mal hintereinander	Eine anhaltend hohe CPU-Auslastung kann problematisch sein. Erwägen Sie, die maximale Kapazität für die Pipeline zu erhöhen.

Alarm	Problem
`bufferUsage.value` Durchschnitt >= 80% für 15 Minuten, 3 Mal hintereinander	Eine anhaltend hohe Puffernutzung kann problematisch sein. Erwägen Sie, die maximale Kapazität für die Pipeline zu erhöhen.

Andere Alarme, die Sie in Betracht ziehen könnten

Erwägen Sie, die folgenden Alarme zu konfigurieren, je nachdem, welche OpenSearch Amazon-Ingestion-Funktionen Sie regelmäßig verwenden.

Alarm	Problem
`dynamodb.exportJobFailure.count` Summe 1	Der Versuch, einen Export zu Amazon S3 auszulösen, ist fehlgeschlagen.
`opensearch.EndtoEndLatency.avg` Durchschnitt > X für 15 Minuten, 4 aufeinanderfolgende Male	Der `EndtoEndLatency` ist höher als gewünscht für das Lesen aus DynamoDB-Streams. Dies kann durch einen unterskalierten OpenSearch Cluster oder eine maximale Pipeline-OCU-Kapazität verursacht werden, die für den WCU-Durchsatz in der DynamoDB-Tabelle zu niedrig ist. `EndtoEndLatency` wird nach einem Export höher sein, sollte aber im Laufe der Zeit abnehmen, wenn es sich an die neuesten DynamoDB-Streams anpasst.
`dynamodb.changeEventsProcessed.count` Summe == 0 für X Minuten	Es werden keine Datensätze aus DynamoDB-Streams gesammelt. Dies könnte daran liegen, dass in der Tabelle keine Aktivität vorhanden ist oder dass ein Problem beim Zugriff auf DynamoDB-Streams aufgetreten ist.
`opensearch.s3.dlqS3RecordsS`	Es wird eine größere Anzahl von Datensätzen an den DLQ gesendet als an die Senke. OpenSearch Überprüfen Sie die Metriken des OpenSearch Sink-Plug-ins, um die Ursache zu untersuchen und zu ermitteln.

Alarm	Problem
`uccess.co unt` Summe >= `opensearc h.documen tSuccess.count` Summe für 1 Minute, 1 Mal hintereinander	
`grok.grok Processin gTimeouts .count` sum = RecordsIn.Count Summe für 1 Minute, 5 Mal hintereinander	Bei allen Daten tritt ein Timeout auf, während der Grok-Prozessor versucht, ein Muster zu finden. Dies wirkt sich wahrscheinlich auf die Leistung aus und verlangsamt Ihre Pipeline. Erwägen Sie, Ihre Muster anzupassen, um Timeouts zu reduzieren.
`grok.grok Processin gErrors.c ount` Summe ist >= 1 für 1 Minute, 1 Mal hintereinander	Der Grok-Prozessor kann die Muster nicht mit den Daten in der Pipeline abgleichen, was zu Fehlern führt. Überprüfen Sie Ihre Daten und die Grok-Plug-in-Konfigurationen, um sicherzustellen, dass der Musterabg leich erwartet wird.
`grok.grok Processin gMismatch .count` sum = RecordsIn.Count Summe für 1 Minute, 5 Mal hintereinander	Der Grok-Prozessor kann den Daten in der Pipeline keine Muster zuordnen. Überprüfen Sie Ihre Daten und die Grok-Plug-in-Konfi gurationen, um sicherzustellen, dass der Musterabgleich erwartet wird.

Alarm	Problem
`date.dateProcessingMatchFailure.count` sum = RecordsIn.Count die Summe für 1 Minute, 5 aufeinanderfolgende Male	Der Datumsprozessor kann den Daten in der Pipeline keine Muster zuordnen. Überprüfen Sie Ihre Daten- und Date-Plugin-Konfigurationen, um sicherzustellen, dass das Muster erwartet wird.
`s3.s3ObjectsFailed.count` Summe >= 1 für 1 Minute, 1 Mal hintereinander	Dieses Problem tritt entweder auf, weil das S3-Objekt nicht existiert oder die Pipeline nicht über ausreichende Rechte verfügt. Überprüfen Sie die `s3ObjectsNotFound.count` und `s3ObjectsAccessDenied.count` -Metriken, um die Ursache zu ermitteln. Vergewissern Sie sich, dass das S3-Objekt vorhanden ist, und/oder aktualisieren Sie die Berechtigungen.
`s3.sqsMessagesFailed.count` Summe >= 1 für 1 Minute, 1 Mal hintereinander	Das S3-Plugin konnte eine Amazon SQS SQS-Nachricht nicht verarbeiten. Wenn Sie in Ihrer SQS-Warteschlange eine DLQ aktiviert haben, überprüfen Sie die fehlgeschlagene Nachricht. Die Warteschlange empfängt möglicherweise ungültige Daten, die die Pipeline zu verarbeiten versucht.
`http.badRequests.count` Summe >= 1 für 1 Minute, 1 Mal hintereinander	Der Client sendet eine fehlerhafte Anfrage. Vergewissern Sie sich, dass alle Clients die richtige Payload senden.
`http.requestsTooLarge.count` Summe >= 1 für 1 Minute, 1 Mal hintereinander	Anfragen vom HTTP-Quell-Plugin enthalten zu viele Daten, wodurch die Pufferkapazität überschritten wird. Passen Sie die Batchgröße für Ihre Kunden an.

Alarm	Problem
`http.internalServerError.count` Summe >= 0 für 1 Minute, 1 Mal hintereinander	Das HTTP-Quell-Plugin hat Probleme beim Empfang von Ereignissen.
`http.requestTimeouts.count` Summe >= 0 für 1 Minute, 1 Mal hintereinander	Quell-Timeouts sind wahrscheinlich das Ergebnis einer unzureichenden Bereitstellung der Pipeline. Erwägen Sie, die Pipeline `maxUnits` zu erweitern, um die zusätzliche Arbeitslast zu bewältigen.
`otel_trace.badRequests.count` Summe >= 1 für 1 Minute, 1 Mal hintereinander	Der Client sendet eine fehlerhafte Anfrage. Vergewissern Sie sich, dass alle Clients die richtige Payload senden.
`otel_trace.requestsTooLarge.count` Summe >= 1 für 1 Minute, 1 Mal hintereinander	Anfragen vom Otel Trace-Quell-Plugin enthalten zu viele Daten, wodurch die Pufferkapazität überschritten wird. Passen Sie die Batchgröße für Ihre Kunden an.
`otel_trace.internalServerError.count` Summe >= 0 für 1 Minute, 1 Mal hintereinander	Das Quell-Plugin von Otel Trace hat Probleme beim Empfang von Ereignissen.

Alarm	Problem
`otel_trace.requestTimeouts.count` Summe **>=** 0 für 1 Minute, 1 Mal hintereinander	Quell-Timeouts sind wahrscheinlich das Ergebnis einer unzureichenden Bereitstellung der Pipeline. Erwägen Sie, die Pipeline `maxUnits` zu erweitern, um die zusätzliche Arbeitslast zu bewältigen.
`otel_metrics.requestTimeouts.count` Summe **>=** 0 für 1 Minute, 1 Mal hintereinander	Quell-Timeouts sind wahrscheinlich das Ergebnis einer unzureichenden Bereitstellung der Pipeline. Erwägen Sie, die Pipeline `maxUnits` zu erweitern, um die zusätzliche Arbeitslast zu bewältigen.

Amazon OpenSearch Serverlos

Amazon OpenSearch Serverless ist eine On-Demand-Konfiguration mit auto-scaling für Amazon OpenSearch Service. Im Gegensatz zu bereitgestellten OpenSearch Domains, die ein manuelles Kapazitätsmanagement erfordern, skaliert eine OpenSearch serverlose Erfassung die Rechenressourcen automatisch entsprechend den Anforderungen Ihrer Anwendung.

OpenSearch Serverless bietet eine kostengünstige Lösung für Workloads, die selten, intermittierend oder unvorhersehbar sind. Es optimiert die Kosten, indem die Rechenkapazität automatisch auf der Grundlage der Nutzung Ihrer Anwendung skaliert wird. Serverlose Sammlungen verwenden dasselbe verteilte und hochverfügbare Speichervolumen mit hoher Kapazität wie bereitgestellte OpenSearch Dienstdomänen.

OpenSearch Serverlose Sammlungen sind immer verschlüsselt. Sie können den Verschlüsselungsschlüssel auswählen, aber Sie können die Verschlüsselung nicht deaktivieren. Weitere Informationen finden Sie unter the section called “Verschlüsselung”.

Vorteile

OpenSearch Serverless bietet die folgenden Vorteile:

- Einfacher als bereitgestellt — OpenSearch Serverless macht die Verwaltung von OpenSearch Clustern und Kapazitäten weitgehend überflüssig. Es skaliert und optimiert Ihre Cluster automatisch und kümmert sich um die Lebenszyklusverwaltung von Shards und Indizes. Es verwaltet auch Service-Software-Updates und OpenSearch Versions-Upgrades. Alle Updates und Upgrades sind unterbrechungsfrei.
- Kostengünstig — Wenn Sie OpenSearch Serverless verwenden, zahlen Sie nur für die Ressourcen, die Sie verbrauchen. Dadurch entfällt die Notwendigkeit einer Vorabbereitstellung und Überbereitstellung für Spitzenlasten.
- Hochverfügbar — OpenSearch Serverless unterstützt Produktionsworkloads mit Redundanz zum Schutz vor Ausfällen der Availability Zone und Infrastrukturausfällen.
- Skalierbar — OpenSearch Serverless skaliert Ressourcen automatisch, um gleichbleibend hohe Datenaufnahmeraten und Antwortzeiten bei Abfragen aufrechtzuerhalten.

Was ist Amazon OpenSearch Serverless?

Amazon OpenSearch Serverless ist eine serverlose On-Demand-Option für Amazon OpenSearch Service, die die betriebliche Komplexität der Bereitstellung, Konfiguration und Optimierung von Clustern überflüssig macht. OpenSearch Es ist ideal für Unternehmen, die es vorziehen, ihre Cluster nicht selbst zu verwalten, oder die nicht über die speziellen Ressourcen und das Fachwissen verfügen, um umfangreiche Bereitstellungen zu betreiben. Mit OpenSearch Serverless können Sie große Datenmengen durchsuchen und analysieren, ohne die zugrunde liegende Infrastruktur verwalten zu müssen.

Eine OpenSearch serverlose Sammlung ist eine Gruppe von OpenSearch Indizes, die zusammenarbeiten, um eine bestimmte Arbeitslast oder einen bestimmten Anwendungsfall zu unterstützen. Sammlungen vereinfachen den Betrieb im Vergleich zu selbstverwalteten OpenSearch Clustern, die eine manuelle Bereitstellung erfordern.

Sammlungen verwenden denselben verteilten und hochverfügbaren Speicher mit hoher Kapazität wie bereitgestellte OpenSearch Dienstdomänen, reduzieren jedoch die Komplexität weiter, da die manuelle Konfiguration und Optimierung entfällt. Daten innerhalb einer Sammlung werden bei der Übertragung verschlüsselt. OpenSearch Serverless unterstützt auch OpenSearch Dashboards und bietet so eine Schnittstelle für die Datenanalyse.

Derzeit wird für serverlose Sammlungen die Version 2.0.x ausgeführt OpenSearch . Wenn neue Versionen veröffentlicht werden, aktualisiert OpenSearch Serverless Sammlungen automatisch, um neue Funktionen, Bugfixes und Leistungsverbesserungen zu integrieren.

OpenSearch Serverless unterstützt dieselben Ingest- und Abfrage-API-Operationen wie die OpenSearch Open-Source-Suite, sodass Sie Ihre vorhandenen Clients und Anwendungen weiterhin verwenden können. Ihre Clients müssen mit OpenSearch 2.x kompatibel sein, um mit Serverless arbeiten zu können. OpenSearch Weitere Informationen finden Sie unter the section called “Erfassung von Daten in Sammlungen”.

Themen

- Anwendungsfälle für Serverless OpenSearch
- Funktionsweise
- Auswahl eines Sammlungstyps
- Preisgestaltung
- Unterstützt AWS-Regionen

- Einschränkungen
- Vergleich von OpenSearch Service und Serverless OpenSearch

Anwendungsfälle für Serverless OpenSearch

OpenSearch Serverless unterstützt zwei Hauptanwendungsfälle:

- Protokollanalyse – Das Segment Protokollanalyse befasst sich mit der Analyse großer Mengen an halbstrukturierten, maschinell generierten Zeitreihendaten, um Einblicke in das Betriebs- und Benutzerverhalten zu erhalten.
- Volltextsuche – Das Segment der Volltextsuche unterstützt Anwendungen in Ihren internen Netzwerken (Content-Management-Systeme, Rechtsdokumente) und mit dem Internet verbundene Anwendungen, wie z. B. die Inhaltssuche von E-Commerce-Websites.

Wenn Sie eine Sammlung erstellen, wählen Sie einen dieser Anwendungsfälle aus. Weitere Informationen finden Sie unter the section called “Auswahl eines Sammlungstyps”.

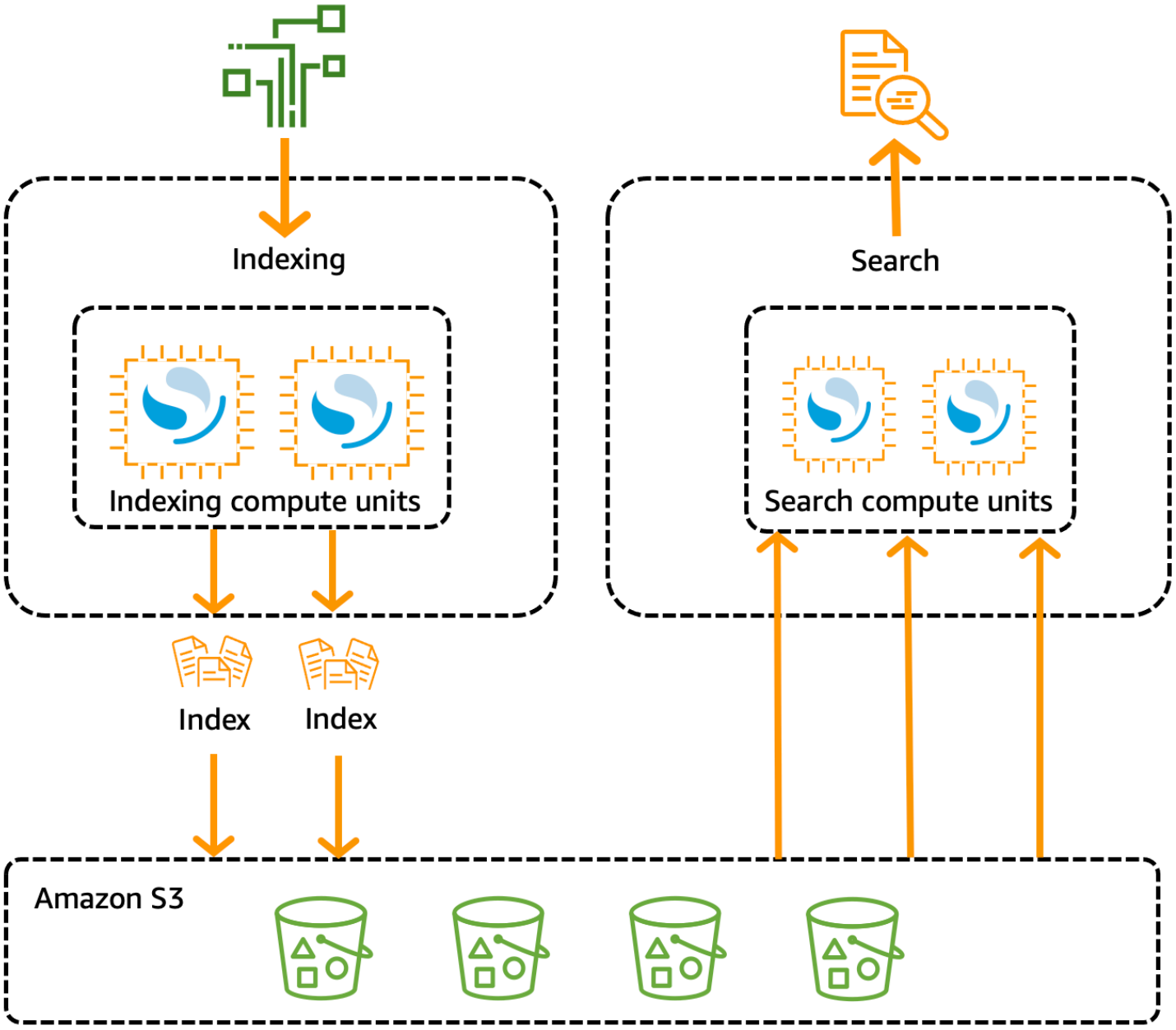
Funktionsweise

Herkömmliche OpenSearch Cluster verfügen über einen einzigen Satz von Instances, die sowohl Indizierungs- als auch Suchvorgänge ausführen, und der Indexspeicher ist eng mit der Rechenkapazität verknüpft. Im Gegensatz dazu verwendet OpenSearch Serverless eine cloudnative Architektur, die die Indexierungskomponenten (Ingest) von den Such- (Abfrage-) Komponenten trennt, wobei Amazon S3 der primäre Datenspeicher für Indizes ist.

Diese entkoppelte Architektur ermöglicht es Ihnen, Such- und Indizierungsfunktionen unabhängig voneinander und unabhängig von den indizierten Daten in S3 zu skalieren. Die Architektur bietet auch eine Isolierung für Aufnahme- und Abfragevorgänge, so dass sie ohne Ressourcenkonflikte gleichzeitig ausgeführt werden können.

Wenn Sie Daten in eine Sammlung schreiben, verteilt OpenSearch Serverless sie an die Recheneinheiten für die Indexierung. Die indizierenden Recheneinheiten nehmen die eingehenden Daten auf und verschieben die Indizes zu S3. Wenn Sie eine Suche nach den Sammlungsdaten durchführen, leitet OpenSearch Serverless Anfragen an die Recheneinheiten für die Suche weiter, die die abgefragten Daten enthalten. Die Recheneinheiten für die Suche laden die indizierten Daten direkt von S3 herunter (wenn sie nicht bereits lokal zwischengespeichert sind), führen Suchvorgänge aus und führen Aggregationen durch.

Das folgende Image veranschaulicht diese entkoppelte Architektur:



OpenSearch Serverlose Rechenkapazität für Datenaufnahme, Suche und Abfrage wird in Recheneinheiten () gemessen. OpenSearch OCUs Jede OCU ist eine Kombination aus 6 GB Speicher und entsprechender virtueller CPU (vCPU) und erstellt eine Daten-Pipeline zu Amazon S3. Jede OCU enthält ausreichend flüchtigen Hot-Speicher für 120 GiB Indexdaten.

Wenn Sie Ihre erste Sammlung erstellen, instanziiert OpenSearch Serverless zwei OCUs — eine für die Indizierung und eine für die Suche. Um eine hohe Verfügbarkeit zu gewährleisten, wird auch eine Reihe von Standby-Knoten in einer anderen Availability Zone gestartet. Zu Entwicklungs- und Testzwecken können Sie die Einstellung Redundanz aktivieren für eine Sammlung

deaktivieren, wodurch die beiden Standby-Replikate entfernt und nur zwei instanziiert werden. OCUs Standardmäßig sind die redundanten aktiven Replikate aktiviert, was bedeutet, dass insgesamt vier für die erste Sammlung in einem Konto instanziiert OCUs werden.

Diese sind auch dann OCUs vorhanden, wenn auf keinem Sammlungsendpunkt eine Aktivität stattfindet. Alle nachfolgenden Sammlungen haben diese OCUs gemeinsam. Wenn Sie weitere Sammlungen in demselben Konto erstellen, fügt OpenSearch Serverless nur dann zusätzliche OCUs für die Suche und Aufnahme hinzu, wenn dies zur Unterstützung der Sammlungen erforderlich ist, und zwar entsprechend den von Ihnen angegebenen Kapazitätsgrenzen. Die Kapazität wird mit sinkender Computernutzung wieder herunterskaliert.

Informationen darüber, wie Ihnen diese in Rechnung gestellt werden OCUs, finden Sie unterthe section called “Preisgestaltung”.

Auswahl eines Sammlungstyps

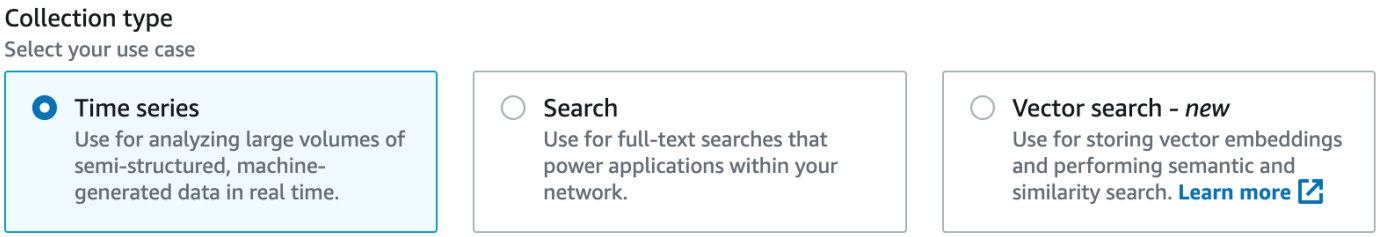
OpenSearch Serverless unterstützt drei primäre Erfassungstypen:

Zeitreihen — Das Segment der Protokollanalysen, das große Mengen halbstrukturierter, maschinengenerierter Daten in Echtzeit analysiert und so Einblicke in Betrieb, Sicherheit, Benutzerverhalten und Unternehmensleistung bietet.

Suche — Volltextsuche, die Anwendungen innerhalb interner Netzwerke, wie Content-Management-Systeme und Ablagen für juristische Dokumente, sowie Internetanwendungen wie E-Commerce-Sitesuche und Content-Discovery ermöglicht.

Vektorsuche — Die semantische Suche nach Vektor-Einbettungen vereinfacht die Verwaltung von Vektordaten und ermöglicht durch maschinelles Lernen (ML) erweiterte Sucherlebnisse. Es unterstützt generative KI-Anwendungen wie Chatbots, persönliche Assistenten und Betrugserkennung.

Sie wählen einen Sammlungstyp aus, wenn Sie zum ersten Mal eine Sammlung erstellen:



Der ausgewählte Sammlungstyp hängt von der Art der Daten ab, die Sie in die Sammlung aufnehmen möchten, und davon, wie Sie diese abfragen möchten. Sie können den Sammlungstyp nach dem Erstellen nicht mehr ändern.

Die Sammlungstypen weisen die folgenden bemerkenswerten Unterschiede auf:

- Bei Such - und Vektorsuchsammlungen werden alle Daten im Hot-Storage gespeichert, um schnelle Antwortzeiten bei Abfragen zu gewährleisten. Zeitreihen-Sammlungen verwenden eine Kombination aus Hot- und Warm-Speicher, wobei die aktuellsten Daten im Hot-Speicher aufbewahrt werden, um die Reaktionszeiten bei Abfragen für Daten mit häufigerem Zugriff zu optimieren.
- Bei Sammlungen mit Zeitreihen und Vektorsuche können Sie weder anhand einer benutzerdefinierten Dokument-ID indexieren noch anhand von Upsert-Anfragen aktualisieren. Dieser Vorgang ist Suchanwendungsfällen vorbehalten. Sie können stattdessen anhand der Dokument-ID aktualisieren. Weitere Informationen finden Sie unter the section called “Unterstützte OpenSearch API-Operationen und -Berechtigungen”.
- Für Such - und Zeitreihensammlungen können Sie keine Indizes vom Typ k-NN verwenden.

Preisgestaltung

AWS berechnet Ihnen die folgenden OpenSearch serverlosen Komponenten:

- Datenerfassungsleistung
- Such- und Abfrageleistung
- In Amazon S3 verbleibender Speicher

Die OCU wird stündlich mit einer Genauigkeit pro Sekunde abgerechnet. In Ihrem Kontoauszug finden Sie einen Eintrag für die Berechnung in OCU-Stunden mit einer Bezeichnung für Datenaufnahme und einer Bezeichnung für Suche. AWS stellt Ihnen auch monatlich die in Amazon S3 gespeicherten Daten in Rechnung. Für die Nutzung von OpenSearch Dashboards fallen keine Gebühren an.

Ihnen werden mindestens 2 (0,5 OCU x 2) für die Aufnahme und 1 OCU OCUs (0,5 OCU x 2) für die Suche in Rechnung gestellt, wenn Sie eine Sammlung erstellen und redundante aktive Replikate aktivieren. Ihnen wird mindestens 1 OCU (0,5 OCU x 2) für die erste Sammlung in Ihrem Konto in Rechnung gestellt, wenn Sie redundante aktive Replikate deaktivieren. Alle nachfolgenden Sammlungen können diese gemeinsam nutzen. OCUs

OpenSearch Serverless fügt je nach OCUs Rechenleistung und Speicherplatz, die zur Unterstützung Ihrer Sammlungen benötigt werden, schrittweise um 1 OCU hinzu. Sie können eine maximale Anzahl von OCUs für Ihr Konto konfigurieren, um die Kosten zu kontrollieren.

> **Note**
>
> Sammlungen, die einzigartig sind, AWS KMS keys können nicht OCUs mit anderen Sammlungen geteilt werden.

OpenSearch Serverlose Versuche, die minimal erforderlichen Ressourcen zu verwenden, um wechselnden Workloads Rechnung zu tragen. Die Anzahl der zu einem beliebigen Zeitpunkt OCUs bereitgestellten Dateien kann variieren und ist nicht exakt. Im Laufe der Zeit wird der von OpenSearch Serverless verwendete Algorithmus weiter verbessert, um die Systemnutzung besser zu minimieren.

Vollständige Preisinformationen finden Sie unter Amazon OpenSearch Service-Preise.

Unterstützt AWS-Regionen

OpenSearch Serverless ist in einer Teilmenge verfügbar AWS-Regionen , in der der OpenSearch Service verfügbar ist. Eine Liste der unterstützten Regionen finden Sie unter Amazon OpenSearch Service-Endpunkte und Kontingente in der Allgemeine AWS-Referenz.

Einschränkungen

OpenSearch Serverless hat die folgenden Einschränkungen:

- Einige OpenSearch API-Operationen werden nicht unterstützt. Siehe the section called “Unterstützte OpenSearch API-Operationen und -Berechtigungen”.
- Einige OpenSearch Plugins werden nicht unterstützt. Siehe the section called “Unterstützte OpenSearch Plugins”.
- Derzeit gibt es keine Möglichkeit, Ihre Daten automatisch von einer verwalteten OpenSearch Dienstdomäne zu einer serverlosen Sammlung zu migrieren. Sie müssen Ihre Daten von einer Domain zu einer Sammlung neu indizieren.
- Kontoübergreifender Zugriff auf Sammlungen wird nicht unterstützt. Sie können Sammlungen von anderen Konten nicht in Ihre Verschlüsselungs- oder Datenzugriffsrichtlinien aufnehmen.
- Benutzerdefinierte OpenSearch Plug-ins werden nicht unterstützt.

- Sie können keine Snapshots von OpenSearch serverlosen Sammlungen erstellen oder wiederherstellen.
- Regionsübergreifende Suche und Replikation werden nicht unterstützt.
- Die Anzahl der Serverless-Ressourcen, die Sie in einem einzigen Konto und einer Region haben können, ist begrenzt. Siehe OpenSearch Serverlose Kontingente.
- Das Aktualisierungsintervall für Indizes in Vektorsuchsammlungen beträgt ungefähr 60 Sekunden. Das Aktualisierungsintervall für Indizes in Such- und Zeitreihensammlungen beträgt ungefähr 10 Sekunden.
- Die Anzahl der Shards, die Anzahl der Intervalle und das Aktualisierungsintervall können nicht geändert werden und werden von Serverless verwaltet. OpenSearch Die Sharding-Strategie basiert auf der Art der Erfassung und dem Datenverkehr. Beispielsweise skaliert eine Zeitreihen-Sammlung primäre Shards auf der Grundlage von Engpässen im Schreibdatenverkehr.
- Geodatenfunktionen, die in OpenSearch Versionen bis 2.1 verfügbar sind, werden unterstützt.

Vergleich von OpenSearch Service und Serverless OpenSearch

Bei OpenSearch Serverless unterscheiden sich einige Konzepte und Funktionen von den entsprechenden Funktionen für eine bereitgestellte Service-Domain OpenSearch . Ein wichtiger Unterschied besteht beispielsweise darin, dass OpenSearch Serverless nicht über das Konzept eines Clusters oder Knotens verfügt.

In der folgenden Tabelle wird beschrieben, wie sich wichtige Funktionen und Konzepte in OpenSearch Serverless von den entsprechenden Funktionen in einer bereitgestellten OpenSearch Dienstdomäne unterscheiden.

Funktion	OpenSearch Dienst	OpenSearch Serverlos
Domains im Vergleich zu Sammlungen	Indizes werden in Domänen gespeichert, bei denen es sich um vorab bereitgestellte OpenSearch Cluster handelt. Weitere Informationen finden Sie unter Erstellen und Verwalten von Domains.	Indizes werden in Sammlungen gespeicherte, bei denen es sich um logische Gruppierungen von Indizes handelt, die einen bestimmten Workload oder Anwendungsfall darstellen. Weitere Informationen finden Sie unter the section called “Verwalten von Sammlungen”.

Funktion	OpenSearch Dienst	OpenSearch Serverlos
Knotentypen und Kapazitätsverwaltung	Sie erstellen einen Cluster mit Knotentypen, die Ihren Kosten- und Leistungsspezifikationen entsprechen. Sie müssen Ihren eigenen Speicherbedarf berechnen und einen Instance-Typ für Ihre Domain auswählen. Weitere Informationen finden Sie unter the section called “Größenanpassung von Domains”.	OpenSearch Serverless skaliert automatisch und stellt zusätzliche Recheneinheiten für Ihr Konto auf der Grundlage Ihrer Kapazitätsnutzung bereit. Weitere Informationen finden Sie unter the section called “Verwalten von Kapazitätsgrenzen”.
Fakturierung	Sie zahlen für jede Nutzungsstunde einer EC2 Instance und für die Gesamtgröße aller EBS-Speichervolumes, die Ihren Instances zugeordnet sind. Weitere Informationen finden Sie unter the section called “Preisgestaltung”.	Die Rechenleistung für die Datenerfassung, die Rechenleistung für Suche und Abfrage sowie der in S3 beibehaltene Speicherplatz werden Ihnen in OCU-Stunden in Rechnung gestellt. Weitere Informationen finden Sie unter the section called “Preisgestaltung”.
Verschlüsselung	Die Verschlüsselung im Ruhezustand ist für Domains optional. Weitere Informationen finden Sie unter the section called “Verschlüsselung im Ruhezustand”.	Die Verschlüsselung im Ruhezustand ist für Sammlungen erforderlich. Weitere Informationen finden Sie unter the section called “Verschlüsselung”.

Funktion	OpenSearch Dienst	OpenSearch Serverlos
Datenzugriffskontrolle	Der Zugriff auf die Daten innerhalb von Domains wird durch IAM-Richtlinien und eine differenzierte Zugriffskontrolle bestimmt.	Der Zugriff auf Daten innerhalb von Sammlungen wird durch Datenzugriffsrichtlinien bestimmt.
Unterstützte Operationen OpenSearch	OpenSearch Der Service unterstützt eine Teilmenge aller OpenSearch API-Operationen. Weitere Informationen finden Sie unter the section called “Unterstützte Vorgänge”.	OpenSearch Serverless unterstützt eine andere Teilmenge von OpenSearch API-Vorgängen. Weitere Informationen finden Sie unter the section called “Unterstützte Vorgänge und Plugins”.
Anmeldung für Dashboards	Melden Sie sich mit einem Benutzernamen und einem Passwort an. Weitere Informationen finden Sie unter the section called “Als Masterbenutzer auf OpenSearch Dashboards zugreifen”.	Wenn Sie in der AWS Konsole angemeldet sind und zu Ihrer Dashboard-URL navigieren, melden Sie sich automatisch an. Weitere Informationen finden Sie unter the section called “Zugriff auf OpenSearch Dashboards”.
APIs	Interagieren Sie mithilfe der OpenSearch Service-API-Operationen programmgesteuert mit dem OpenSearch Service.	Interagieren Sie programmgesteuert mit OpenSearch Serverless mithilfe der Serverless-API-Operationen. OpenSearch

Funktion	OpenSearch Dienst	OpenSearch Serverlos
Netzwerkzugriff	Die Netzwerkeinstellungen für eine Domain gelten sowohl für den Domain-Endpunkt als auch für den Dashboard -Endpunkt. OpenSearch Der Netzwerkzugriff für beide ist eng gekoppelt.	Die Netzwerkeinstellungen für den Domain-Endpunkt und den OpenSearch Dashboard -Endpunkt sind entkoppelt. Sie können sich dafür entscheiden, den Netzwerkzugriff für Dashboards nicht zu konfigurieren. OpenSearch Weitere Informationen finden Sie unter the section called “Netzwerkzugriff”.
Signieren von Anforderungen	Verwenden Sie die REST-Clients auf OpenSearch hoher und niedriger Ebene, um Anfragen zu signieren. Geben Sie den Service-Namen als `es` an.	Derzeit unterstützt OpenSearch Serverless eine Untergruppe von Clients, die OpenSearch Service unterstützt. Geben Sie beim Signieren von Anfragen den Service-Namen als `aoss` an. Der `x-amz-content-sha256` -Header ist erforderlich. Weitere Informationen finden Sie unter the section called “Andere Kunden”.
OpenSearch Versionsupgrades	Sie aktualisieren Ihre Domains manuell, sobald neue Versionen von OpenSearch verfügbar sind. Sie sind dafür verantwortlich, dass Ihre Domain die Upgrade-Voraussetzungen erfüllt und dass Sie alle grundlegenden Änderungen vorgenommen haben.	OpenSearch Serverless aktualisiert Ihre Sammlungen automatisch auf neue OpenSearch Versionen. Upgrades werden nicht unbedingt durchgeführt, sobald eine neue Version verfügbar ist.
Service-Software-Updates	Sie wenden Service-Software-Updates manuell auf Ihre Domain an, sobald sie verfügbar sind.	OpenSearch Serverless aktualisiert Ihre Sammlungen automatisch, um die neuesten Bugfixes, Funktionen und Leistungsverbesserungen zu nutzen.

Funktion	OpenSearch Dienst	OpenSearch Serverlos
VPC-Zugriff	Sie können Ihre Domain innerhalb einer VPC bereitstellen. Sie können auch zusätzlich vom OpenSearch Service verwaltete VPC-Endpunkte für den Zugriff auf die Domain erstellen.	Sie erstellen einen oder OpenSearch mehrere serverlos verwaltete VPC-Endpoints für Ihr Konto. Anschließend nehmen Sie diese Endpunkte in die Netzwerkrichtlinien auf.
SAML-Authentifizierung	Sie aktivieren die SAML-Authentifizierung auf Domain-Basis. Weitere Informationen finden Sie unter the section called “SAML-Authentifizierung für OpenSearch Dashboards ”.	Sie konfigurieren einen oder mehrere SAML-Anbieter auf Kontoebene und schließen dann den zugehörigen Benutzer und die zugehörige Gruppe in die Datenzugriffsrichtlinien ein. IDs Weitere Informationen finden Sie unter the section called “SAML-Authentifizierung”.
Transport Layer Security (TLS)	OpenSearch Der Service unterstützt TLS 1.2, es wird jedoch empfohlen, TLS 1.3 zu verwenden.	OpenSearch Serverless unterstützt TLS 1.2, es wird jedoch empfohlen, TLS 1.3 zu verwenden.

Tutorial: Erste Schritte mit Amazon OpenSearch Serverless

Dieses Tutorial führt Sie durch die grundlegenden Schritte, um eine Amazon OpenSearch Serverless-Suchsammlung schnell zum Laufen zu bringen. Eine Suchsammlung ermöglicht es Ihnen, Anwendungen in Ihren internen Netzwerken und mit dem Internet verbundene Anwendungen wie die Suche nach E-Commerce-Websites und die Inhaltssuche zu unterstützen.

Informationen zur Verwendung einer Vektorsuchsammlung finden Sie unter. the section called “Arbeiten mit Sammlungen für die Vektorsuche” Ausführlichere Informationen zur Verwendung von Sammlungen finden Sie unter the section called “Verwalten von Sammlungen” und den anderen Themen in diesem Handbuch.

In diesem Tutorial führen Sie die folgenden Schritte durch:

1. Konfigurieren von Berechtigungen
2. Erstellen einer Sammlung
3. Hochladen und Suchen von Daten
4. Löschen der Sammlung

> **Note**
>
> Wir empfehlen, dass Sie für Ihre nur ASCII-Zeichen verwenden. `IndexName` Wenn Sie für Ihre keine ASCII-Zeichen verwenden`IndexName`, werden die eingegebenen CloudWatch Messwerte `IndexName` in ein URL-codiertes Format für Nicht-ASCII-Zeichen konvertiert.

Schritt 1: Konfigurieren von Berechtigungen

Um dieses Tutorial abzuschließen und OpenSearch Serverless im Allgemeinen verwenden zu können, müssen Sie über die richtigen IAM-Berechtigungen verfügen. In diesem Tutorial werden Sie eine Sammlung erstellen, Daten hochladen und suchen und die Sammlung anschließend löschen.

Ihr Benutzer oder Ihre Rolle muss über eine angefügte identitätsbasierte Richtlinie mit den folgenden Mindestberechtigungen verfügen:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "aoss:CreateCollection",
        "aoss:ListCollections",
        "aoss:BatchGetCollection",
        "aoss:DeleteCollection",
        "aoss:CreateAccessPolicy",
        "aoss:ListAccessPolicies",
        "aoss:UpdateAccessPolicy",
        "aoss:CreateSecurityPolicy",
        "aoss:GetSecurityPolicy",
        "aoss:UpdateSecurityPolicy",
        "iam:ListUsers",
```

```
        "iam:ListRoles"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Weitere Informationen zu OpenSearch Serverless IAM-Berechtigungen finden Sie unter. the section called “Identitäts- und Zugriffsverwaltung”

Schritt 2: Erstellen einer Sammlung

Eine Sammlung ist eine Gruppe von OpenSearch Indizes, die zusammenarbeiten, um eine bestimmte Arbeitslast oder einen bestimmten Anwendungsfall zu unterstützen.

Um eine OpenSearch serverlose Sammlung zu erstellen

1. Öffnen Sie die Amazon OpenSearch Service-Konsole zu https://console.aws.amazon.com/aos/Hause.
2. Wählen Sie im linken Navigationsbereich Collections (Sammlungen) und wählen Sie Create collection (Sammlung erstellen) aus.
3. Benennen Sie die Sammlung movies (Filme).
4. Wählen Sie für den Sammlungstyp Search (Suche) aus. Weitere Informationen finden Sie unter Auswahl eines Sammlungstyps.
5. Wählen Sie unter Sicherheit die Option Standard Create aus.
6. Wählen Sie unter Verschlüsselung die Option Verwenden aus AWS-eigener Schlüssel. Dies ist der AWS KMS key , den OpenSearch Serverless verwendet, um Ihre Daten zu verschlüsseln.
7. Konfigurieren Sie unter Network (Netzwerk) die Netzwerkeinstellungen für die Sammlung.
   - Wählen Sie für den Zugriffstyp Public (Öffentlich) aus.
   - Wählen Sie als Ressourcentyp sowohl Zugriff auf OpenSearch Endpunkte aktivieren als auch Zugriff auf Dashboards aktivieren aus. OpenSearch Da Sie Daten mithilfe von OpenSearch Dashboards hochladen und suchen, müssen Sie beide aktivieren.
8. Wählen Sie Weiter aus.
9. Richten Sie unter Configure data access (Datenzugriff konfigurieren) die Zugriffseinstellungen für die Sammlung ein. Datenzugriffsrichtlinien ermöglichen Benutzern und Rollen den Zugriff auf

die Daten innerhalb einer Sammlung. In diesem Tutorial erteilen wir einem einzelnen Benutzer die Berechtigungen, die zum Indizieren und Durchsuchen von Daten in der Filme-Sammlung erforderlich sind.

Erstellen Sie eine einzelne Regel, die den Zugriff auf die Filme-Sammlung ermöglicht. Nennen Sie die Regel Movies collection access (Zugriff auf Filme-Sammlung).

10. Wählen Sie Principals, IAM-Benutzer und -Rollen hinzufügen und wählen Sie den Benutzer oder die Rolle aus, mit der Sie sich bei OpenSearch Dashboards anmelden und Daten indexieren möchten. Wählen Sie Speichern.
11. Wählen Sie unter Index permissions (Indexberechtigungen) alle Berechtigungen aus.
12. Wählen Sie Weiter aus.
13. Wählen Sie für die Zugriffsrichtlinieneinstellungen die Option Create a new data access policy (Neue Datenzugriffsrichtlinie erstellen) aus und nennen Sie die Richtlinie movies (Filme).
14. Wählen Sie Weiter aus.
15. Überprüfen Sie Ihre Sammlungseinstellungen und wählen Sie Submit (Senden) aus. Warten Sie einige Minuten, bis der Sammlungsstatus `Active` erreicht ist.

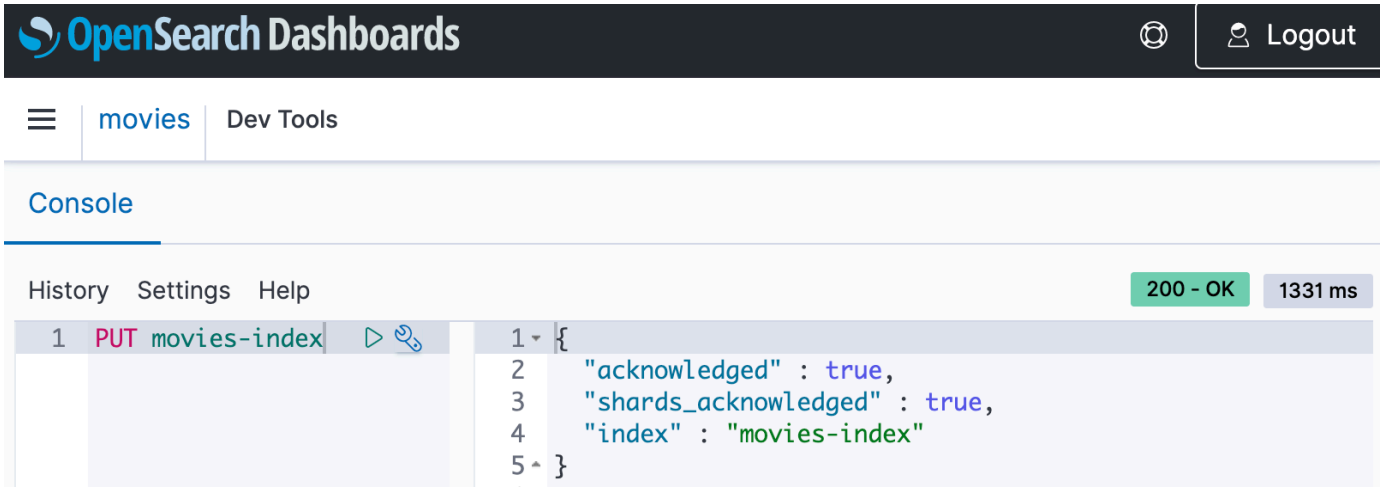
Schritt 3: Daten hochladen und suchen

Sie können Daten mit Postman oder cURL in eine OpenSearch serverlose Sammlung hochladen. Der Kürze halber verwenden diese Beispiele Dev Tools in der Dashboards-Konsole. OpenSearch

So indizieren und durchsuchen Sie Daten in der Filme-Sammlung

1. Wählen Sie im linken Navigationsbereich Collections (Sammlungen) und wählen Sie die movies (Filme)-Sammlung aus, um ihre Detailseite zu öffnen.
2. Wählen Sie die OpenSearch Dashboard-URL für die Sammlung aus. Die URL nimmt das Format `https://dashboards.{region}.aoss.amazonaws.com/_login/?collectionId={collection-id}` an.
3. Öffnen Sie in OpenSearch Dashboards den linken Navigationsbereich und wählen Sie Dev Tools aus.
4. Um einen einzelnen Index mit dem Namen movies-index zu erstellen, senden Sie die folgende Anfrage:

```
PUT movies-index
```



5. Um ein einzelnes Dokument in movies-index zu indizieren, senden Sie die folgende Anfrage:

```
PUT movies-index/_doc/1
{
  "title": "Shawshank Redemption",
  "genre": "Drama",
  "year": 1994
}
```

6. Um Daten in OpenSearch Dashboards zu suchen, müssen Sie mindestens ein Indexmuster konfigurieren. OpenSearch verwendet diese Muster, um zu identifizieren, welche Indizes Sie analysieren möchten. Öffnen Sie den linken Navigationsbereich, wählen Sie Stack-Verwaltung, wählen Sie Indexmuster und anschließend die Option Indexmuster erstellen aus. Geben Sie für dieses Tutorial Filme ein.
7. Wählen Sie Nächster Schritt aus und klicken Sie auf Indexmuster erstellen. Nachdem das Muster erstellt wurde, können Sie die verschiedenen Dokumentfelder anzeigen, z. B. `title` und `genre`.
8. Um mit der Suche nach Ihren Daten zu beginnen, öffnen Sie erneut den linken Navigationsbereich und wählen Sie Discover (Entdecken) aus, oder verwenden Sie die Such-API in Dev Tools.

Schritt 4: Sammlung löschen

Da die Filme-Sammlung zu Testzwecken dient, sollten Sie sie löschen, wenn Sie mit dem Experimentieren fertig sind.

Um eine OpenSearch serverlose Sammlung zu löschen

1. Gehen Sie zurück zur Amazon OpenSearch Service-Konsole.
2. Wählen Sie im linken Navigationsbereich Collections (Sammlungen) und anschließend die movies (Filme)-Samlung aus.
3. Wählen Sie Löschen und bestätigen Sie das Löschen.

Nächste Schritte

Da Sie nun wissen, wie Sie eine Sammlung erstellen und Daten indizieren, möchten Sie vielleicht einige der folgenden Übungen ausprobieren:

- Weitere erweiterte Optionen zum Erstellen einer Sammlung finden Sie hier. Weitere Informationen finden Sie unter the section called “Verwalten von Sammlungen”.
- Erfahren Sie, wie Sie Sicherheitsrichtlinien konfigurieren, um die Sammlungssicherheit in großem Umfang zu verwalten. Weitere Informationen finden Sie unter the section called “Sicherheit bei Serverless OpenSearch ”.
- Entdecken Sie andere Möglichkeiten, Daten in Sammlungen zu indizieren. Weitere Informationen finden Sie unter the section called “Erfassung von Daten in Sammlungen”.

Amazon OpenSearch Serverless-Sammlungen erstellen und verwalten

Sie können Amazon OpenSearch Serverless-Sammlungen mithilfe der Konsole, der AWS CLI and-API AWS SDKs, der und und AWS CloudFormation erstellen.

Themen

- Verwaltung von Amazon OpenSearch Serverless-Sammlungen
- Arbeiten mit Sammlungen für die Vektorsuche
- Verwenden von Datenlebenszyklusrichtlinien mit Amazon OpenSearch Serverless
- Verwenden von AWS SDKs für die Interaktion mit Amazon OpenSearch Serverless
- Verwenden AWS CloudFormation , um Amazon OpenSearch Serverless-Sammlungen zu erstellen

Verwaltung von Amazon OpenSearch Serverless-Sammlungen

Eine Sammlung in Amazon OpenSearch Serverless ist eine logische Gruppierung von einem oder mehreren Indizes, die eine Analyse-Workload darstellen. OpenSearch Serverless verwaltet und optimiert die Sammlung automatisch und erfordert nur minimale manuelle Eingaben.

Themen

- Erforderliche Berechtigungen
- Erstellen von Sammlungen
- Zugriff auf OpenSearch Dashboards
- Anzeigen von Sammlungen
- Löschen von Sammlungen

Erforderliche Berechtigungen

OpenSearch Serverless verwendet die folgenden AWS Identity and Access Management (IAM) -Berechtigungen zum Erstellen und Verwalten von Sammlungen. Sie können IAM-Bedingungen festlegen, um Benutzer auf bestimmte Sammlungen zu beschränken.

- `aoss:CreateCollection` – Erstellt Sie eine Sammlung.
- `aoss:ListCollections` – Listet Sammlungen im aktuellen Konto auf.
- `aoss:BatchGetCollection` – Ruft Details zu einer oder mehreren Sammlungen ab.
- `aoss:UpdateCollection` – Ändert eine Sammlung.
- `aoss:DeleteCollection` – Löscht eine Sammlung.

Das folgende Beispiel für eine identitätsbasierte Zugriffsrichtlinie stellt die Mindestberechtigungen bereit, die ein Benutzer benötigt, um eine einzelne Sammlung mit dem Namen `Logs` zu verwalten:

```
[
   {
      "Sid":"Allows managing logs collections",
      "Effect":"Allow",
      "Action":[
         "aoss:CreateCollection",
         "aoss:ListCollections",
         "aoss:BatchGetCollection",
         "aoss:UpdateCollection",
```

```
            "aoss:DeleteCollection",
            "aoss:CreateAccessPolicy",
            "aoss:CreateSecurityPolicy"
         ],
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "aoss:collection":"Logs"
            }
         }
      }
]
```

`aoss:CreateAccessPolicy` und `aoss:CreateSecurityPolicy` sind enthalten, da Verschlüsselungs-, Netzwerk- und Datenzugriffsrichtlinien erforderlich sind, damit eine Sammlung ordnungsgemäß funktioniert. Weitere Informationen finden Sie unter the section called “Identitäts- und Zugriffsverwaltung”.

> **Note**
>
> Wenn Sie die erste Sammlung in Ihrem Konto erstellen, benötigen Sie auch die `iam:CreateServiceLinkedRole`-Berechtigung. Weitere Informationen finden Sie unter the section called “Rolle bei der Sammlungserstellung”.

Erstellen von Sammlungen

Sie können die Konsole oder das verwenden AWS CLI , um eine Serverless-Sammlung zu erstellen. In diesen Schritten wird beschrieben, wie Sie eine Suche oder eine Zeitreihensammlung erstellen. Informationen zum Erstellen einer Vektorsuchsammlung finden Sie unterthe section called “Arbeiten mit Sammlungen für die Vektorsuche”.

Eine Sammlung erstellen (Konsole)

So erstellen Sie eine Sammlung mithilfe der Konsole

1. Navigieren Sie zu der Amazon OpenSearch Service-Konsole zu https://console.aws.amazon.com/aos/Hause/.
2. Erweitern Sie im linken Navigationsbereich Serverless und wählen Sie Collections (Sammlungen) aus.

3. Wählen Sie Create Connection (Verbindung erstellen) aus.
4. Geben Sie einen Namen und eine Beschreibung für die Sammlung an. Der Name muss die folgenden Kriterien erfüllen:

   - Ist für Ihr Konto und eindeutig AWS-Region
   - Beginnt mit einem Kleinbuchstaben
   - Enthält zwischen 3 und 32 Zeichen
   - Enthält nur Kleinbuchstaben a–z, die Zahlen 0–9 und den Bindestrich (-)
5. Auswahl eines Sammlungstyps:

   - Time series (Zeitreihen) – Segment der Protokollanalyse, das sich auf die Analyse großer Mengen halbstrukturierter, maschinell generierter Daten konzentriert. In Hot-Indizes werden mindestens 24 Stunden an Daten gespeichert, der Rest verbleibt im Warm-Speicher.
   - Search (Suche) – Volltextsuche, die Anwendungen in Ihren internen Netzwerken und Anwendungen mit Internetzugriff unterstützt. Alle Suchdaten werden im Hot-Speicher gespeichert, um schnelle Antwortzeiten auf Abfragen zu stellen.
   - Vektorsuche — Semantische Suche nach Vektoreinbettungen, die die Verwaltung von Vektordaten vereinfacht. Unterstützt erweiterte Sucherlebnisse mit maschinellem Lernen (ML) und generative KI-Anwendungen wie Chatbots, persönliche Assistenten und Betrugserkennung.

   Weitere Informationen finden Sie unter the section called “Auswahl eines Sammlungstyps”.
6. Wählen Sie als Bereitstellungstyp die Redundanzeinstellung für Ihre Sammlung aus. Standardmäßig ist jede Sammlung redundant, was bedeutet, dass die OpenSearch Recheneinheiten für Indexierung und Suche (OCUs) jeweils ihre eigenen Standby-Replikate in einer anderen Availability Zone haben. Zu Entwicklungs- und Testzwecken können Sie die Redundanz deaktivieren, wodurch die Anzahl der Redundanz OCUs in Ihrer Sammlung auf zwei reduziert wird. Weitere Informationen finden Sie unter the section called “Funktionsweise”.
7. Wählen Sie aus Sicherheitsgründen die Option Standard create aus.
8. Wählen Sie für Encryption (Verschlüsselung) einen AWS KMS -Schlüssel, mit dem Sie Ihre Daten verschlüsseln möchten. OpenSearch Serverless benachrichtigt Sie, wenn der von Ihnen eingegebene Sammlungsname mit einem Muster übereinstimmt, das in einer Verschlüsselungsrichtlinie definiert ist. Sie können diese Übereinstimmung beibehalten oder mit eindeutigen Verschlüsselungseinstellungen überschreiben. Weitere Informationen finden Sie unter the section called “Verschlüsselung”.

9. Konfigurieren Sie für Network access settings (Netzwerkzugriffseinstellungen) den Netzwerkzugriff für die Sammlung.

   - Wählen Sie als Zugriffstyp öffentlich oder privat aus.

     Wenn Sie privat wählen, geben Sie an, welche VPC-Endpoints auf die AWS-Services Sammlung zugreifen können.

     - VPC-Endpunkte für den Zugriff — Geben Sie einen oder mehrere VPC-Endpunkte an, um den Zugriff zuzulassen. Informationen zum Erstellen eines VPC-Endpunkts finden Sie unter the section called “VPC-Endpunkte”.
     - AWS-Service privater Zugriff — Wählen Sie einen oder mehrere unterstützte Dienste aus, auf die Sie zugreifen möchten.
   - Wählen Sie für Resource type (Ressourcentyp) aus, ob Benutzer über ihren OpenSearchEndpunkt (um API-Aufrufe über cURL, Postman usw. zu tätigen), über den Dashboards -Endpunkt (um mit Visualisierungen zu funktionieren und API-Aufrufe über die Konsole zu tätigen), über den OpenSearch Dashboards -Endpunkt (um mit Visualisierungen zu funktionieren und API-Aufrufe über die Konsole zu tätigen), oder über beide zugegriffen werden kann.

     > **Note**
     >
     > AWS-Service Der private Zugriff gilt nur für den Endpunkt, nicht für den OpenSearch Dashboards-Endpunkt. OpenSearch

   OpenSearch Serverless benachrichtigt Sie, wenn der von Ihnen eingegebene Sammlungsname mit einem Muster übereinstimmt, das in einer Netzwerkrichtlinie definiert ist. Sie können diese Übereinstimmung beibehalten oder mit benutzerdefinierten Netzwerkeinstellungen überschreiben. Weitere Informationen finden Sie unter the section called “Netzwerkzugriff”.

10. (Optional) Fügen Sie der Sammlung ein oder mehrere Tags hinzu. Weitere Informationen finden Sie unter the section called “Markieren von Sammlungen”.
11. Wählen Sie Weiter aus.
12. Konfigurieren Sie Datenzugriffsregeln für die Sammlung, die festlegen, wer auf die Daten innerhalb der Sammlung zugreifen kann. Für jede Regel, die Sie erstellen, führen Sie die folgenden Schritte aus:

- Wählen Sie Add principals (Prinzipale hinzufügen) und wählen Sie eine oder mehrere IAM-Rollen oder SAML users and groups (SAML-Benutzer und -Gruppen) aus, denen Sie Datenzugriff gewähren möchten.
- Unter Grant permissions (Berechtigungen gewähren) wählen Sie die Alias-, Vorlagen- und Indexberechtigungen aus, um die zugehörigen Prinzipale zu erteilen. Eine vollständige Liste der Berechtigungen und des von ihnen gewährten Zugriffs finden Sie unter the section called “Unterstützte OpenSearch API-Operationen und -Berechtigungen”.

OpenSearch Serverless benachrichtigt Sie, wenn der von Ihnen eingegebene Sammlungsname mit einem Muster übereinstimmt, das in einer Datenzugriffsrichtlinie definiert ist. Sie können diese Übereinstimmung beibehalten oder mit eindeutigen Datenzugriffseinstellungen überschreiben. Weitere Informationen finden Sie unter the section called “Datenzugriffskontrolle”.

13. Wählen Sie Weiter aus.
14. Wählen Sie für Data access policy settings (Einstellungen für die Datenzugriffsrichtlinie) aus, was mit den Regeln geschehen soll, die Sie gerade erstellt haben. Sie können sie entweder verwenden, um eine neue Datenzugriffsrichtlinie zu erstellen, oder sie zu einer vorhandenen Richtlinie hinzufügen.
15. Wählen Sie Weiter aus.
16. Überprüfen Sie Ihre Sammlungskonfiguration und wählen Sie Submit (Senden) aus.

Der Sammlungsstatus ändert sich in`Creating`, OpenSearch wenn Serverless die Sammlung erstellt.

Eine Sammlung erstellen (CLI)

Bevor Sie eine Sammlung mit dem erstellen AWS CLI, müssen Sie über eine Verschlüsselungsrichtlinie mit einem Ressourcenmuster verfügen, das dem beabsichtigten Namen der Sammlung entspricht. Wenn Sie beispielsweise Ihre Sammlungs-Protokollanwendung benennen möchten, können Sie eine Verschlüsselungsrichtlinie wie die folgende erstellen:

```
aws opensearchserverless create-security-policy \
  --name logs-policy \
  --type encryption --policy "{\"Rules\":[{\"ResourceType\":\"collection\",\"Resource
\":[\"collection\/logs-application\"]}],\"AWSOwnedKey\":true}"
```

Wenn Sie die Richtlinie für weitere Sammlungen verwenden möchten, können Sie die Regel breiter fassen, wie z. B. `collection/logs*` oder `collection/*`.

Außerdem müssen Sie Netzwerkeinstellungen für die Sammlung in Form einer Netzwerkrichtlinie konfigurieren. Unter Verwendung des vorherigen Beispiels für die Protokollanwendung könnten Sie die folgende Netzwerkrichtlinie erstellen:

```
aws opensearchserverless create-security-policy \
  --name logs-policy \
  --type network --policy "[{\"Description\":\"Public access for logs collection
\",\"Rules\":[{\"ResourceType\":\"dashboard\",\"Resource\":[\"collection\/logs-
application\"]},{\"ResourceType\":\"collection\",\"Resource\":[\"collection\/logs-
application\"]}],\"AllowFromPublic\":true}]"
```

> **Note**
>
> Sie können Netzwerkrichtlinien erstellen, nachdem Sie eine Sammlung erstellt haben. Wir empfehlen jedoch, dies vorher zu tun.

Um eine Sammlung zu erstellen, senden Sie eine CreateCollectionAnfrage:

```
aws opensearchserverless create-collection --name "logs-application" --type SEARCH --
description "A collection for storing log data"
```

Geben Sie für `type` entweder `SEARCH` oder `TIMESERIES` an. Weitere Informationen finden Sie unter the section called “Auswahl eines Sammlungstyps”.

Beispielantwort

```
{
    "createCollectionDetail": {
        "id": "07tjusf2h91cunochc",
        "name": "books",
        "description":"A collection for storing log data",
        "status": "CREATING",
        "type": "SEARCH",
        "kmsKeyArn": "auto",
        "arn": "arn:aws:aoss:us-east-1:123456789012:collection/07tjusf2h91cunochc",
        "createdDate": 1665952577473
    }
}
```

Wenn Sie in der Anfrage keinen Sammlungstyp angeben, wird standardmäßig `TIMESERIES` verwendet. Wenn Ihre Sammlung mit einem AWS-eigener Schlüssel verschlüsselt ist, handelt es sich bei `kmsKeyArn` um `auto` und nicht um einen ARN.

> **Important**
>
> Nachdem Sie eine Sammlung erstellt haben, können Sie nicht darauf zugreifen, es sei denn, sie entspricht einer Datenzugriffsrichtlinie. Anweisungen zum Erstellen von Datenzugriffsrichtlinien finden Sie unter the section called “Datenzugriffskontrolle”.

Zugriff auf OpenSearch Dashboards

Nachdem Sie eine Sammlung mit dem erstellt haben AWS Management Console,, können Sie zur OpenSearch Dashboards-URL der Sammlung navigieren. Sie finden die Dashboards -URL, indem Sie im linken Navigationsbereich Collections (Sammlungen) auswählen und die Sammlung auswählen, um ihre Detailseite zu öffnen. Die URL nimmt das Format `https://dashboards.us-east-1.aoss.amazonaws.com/_login/?collectionId=07tjusf2h91cunochc` an. Sobald Sie zur URL navigieren, melden Sie sich automatisch bei Dashboards an.

Wenn Sie die OpenSearch Dashboard-URL bereits verfügbar haben, aber nicht auf der sind AWS Management Console, wird beim Aufrufen der Dashboard-URL über den Browser zur Konsole weitergeleitet. Sobald Sie Ihre AWS Anmeldeinformationen eingegeben haben, melden Sie sich automatisch bei Dashboards an. Informationen zum Zugriff auf Sammlungen für SAML finden Sie unter Zugreifen auf OpenSearch Dashboards mit SAML.

Das Timeout der OpenSearch Dashboard-Konsole beträgt eine Stunde und ist nicht konfigurierbar.

> **Note**
>
> Am 10. Mai 2023 OpenSearch wurde ein gemeinsamer globaler Endpunkt für OpenSearch Dashboards eingeführt. Sie können jetzt im Browser mit einer URL, die das Format annimmt, zu OpenSearch Dashboards navigieren. `https://dashboards.us-east-1.aoss.amazonaws.com/_login/?collectionId=07tjusf2h91cunochc` Um die Abwärtskompatibilität zu gewährleisten, werden wir die bestehenden sammlungsspezifischen OpenSearch Dashboard-Endpunkte weiterhin mit diesem Format unterstützen. `https://07tjusf2h91cunochc.us-east-1.aoss.amazonaws.com/_dashboards`

Anzeigen von Sammlungen

Sie können die vorhandenen Sammlungen in Ihrem AWS-Konto auf der Registerkarte Sammlungen der OpenSearch Amazon-Servicekonsole anzeigen.

Um Sammlungen zusammen mit ihren aufzulisten IDs, senden Sie eine ListCollectionsAnfrage.

```
aws opensearchserverless list-collections
```

Beispielantwort

```
{
   "collectionSummaries":[
      {
         "arn":"arn:aws:aoss:us-east-1:123456789012:collection/07tjusf2h91cunochc",
         "id":"07tjusf2h91cunochc",
         "name":"my-collection",
         "status":"CREATING"
      }
   ]
}
```

Um die Suchergebnisse einzuschränken, verwenden Sie Sammlungsfilter. Diese Anfrage filtert die Antwort auf Sammlungen im `ACTIVE`-Zustand:

```
aws opensearchserverless list-collections --collection-filters '{ "status": "ACTIVE" }'
```

Um detailliertere Informationen zu einer oder mehreren Sammlungen zu erhalten, einschließlich des OpenSearch Endpunkts und des OpenSearch Dashboards-Endpunkts, senden Sie eine BatchGetCollectionAnfrage:

```
aws opensearchserverless batch-get-collection --ids ["07tjusf2h91cunochc",
 "1iu5usc4rame"]
```

> **Note**
>
> Sie können `--names` oder `--ids` in die Anfrage aufnehmen, aber nicht beides.

Beispielantwort

```
{
   "collectionDetails":[
      {
         "id": "07tjusf2h91cunochc",
         "name": "my-collection",
         "status": "ACTIVE",
         "type": "SEARCH",
         "description": "",
         "arn": "arn:aws:aoss:us-east-1:123456789012:collection/07tjusf2h91cunochc",
         "kmsKeyArn": "arn:aws:kms:us-
east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab",
         "createdDate": 1667446262828,
         "lastModifiedDate": 1667446300769,
         "collectionEndpoint": "https://07tjusf2h91cunochc.us-
east-1.aoss.amazonaws.com",
         "dashboardEndpoint": "https://07tjusf2h91cunochc.us-east-1.aoss.amazonaws.com/
_dashboards"
      },
      {
         "id": "178ukvtg3i82dvopdid",
         "name": "another-collection",
         "status": "ACTIVE",
         "type": "TIMESERIES",
         "description": "",
         "arn": "arn:aws:aoss:us-east-1:123456789012:collection/178ukvtg3i82dvopdid",
         "kmsKeyArn": "arn:aws:kms:us-
east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab",
         "createdDate": 1667446262828,
         "lastModifiedDate": 1667446300769,
         "collectionEndpoint": "https://178ukvtg3i82dvopdid.us-
east-1.aoss.amazonaws.com",
         "dashboardEndpoint": "https://178ukvtg3i82dvopdid.us-
east-1.aoss.amazonaws.com/_dashboards"
      }
   ],
   "collectionErrorDetails":[]
}
```


Löschen von Sammlungen

Beim Löschen einer Sammlung werden alle Daten und Indizes in der Sammlung gelöscht. Sie können Sammlungen nicht wiederherstellen, nachdem Sie diese gelöscht haben.

So löschen Sie eine Sammlung über die Konsole

1. Wählen Sie im Bereich Collections (Sammlungen) der OpenSearch Amazon-Service-Konsole die Sammlung aus, die Sie löschen möchten.
2. Wählen Sie Löschen und bestätigen Sie das Löschen.

Um eine Sammlung mit dem zu löschen AWS CLI, senden Sie eine DeleteCollectionAnfrage:

```
aws opensearchserverless delete-collection --id 07tjusf2h91cunochc
```

Beispielantwort

```
{
   "deleteCollectionDetail":{
      "id":"07tjusf2h91cunochc",
      "name":"my-collection",
      "status":"DELETING"
   }
}
```

Arbeiten mit Sammlungen für die Vektorsuche

Der Sammlungstyp der Vektorsuche in OpenSearch Serverless bietet eine skalierbare und leistungsstarke Funktion zur Ähnlichkeitssuche. Es macht es Ihnen leicht, moderne, erweiterte Sucherlebnisse für maschinelles Lernen (ML) und Anwendungen für generative künstliche Intelligenz (KI) zu entwickeln, ohne die zugrunde liegende Vektordatenbankinfrastruktur verwalten zu müssen.

Zu den Anwendungsfällen für Vektorsuchsammlungen gehören Bildersuchen, Dokumentensuchen, Musikabruf, Produktempfehlungen, Videosuchen, standortbezogene Suchen, Betrugserkennung und Anomalieerkennung.

Da die Vektor-Engine für OpenSearch Serverless auf der Suchfunktion k-Nearest Neighbor (k-NN) basiert OpenSearch, erhalten Sie dieselbe Funktionalität mit der Einfachheit einer serverlosen Umgebung. Die Engine unterstützt die k-NN-Plug-in-API. Mit diesen Vorgängen können Sie Volltextsuche, erweiterte Filterung, Aggregationen, Geodatenabfragen, verschachtelte Abfragen zum schnelleren Abrufen von Daten und verbesserte Suchergebnisse nutzen.

Die Vektor-Engine bietet Entfernungsmetriken wie euklidische Entfernung, Kosinusähnlichkeit und Punktproduktähnlichkeit und kann 16.000 Dimensionen aufnehmen. Sie können Felder

mit verschiedenen Datentypen für Metadaten wie Zahlen, Boolesche Werte, Datumsangaben, Stichwörter und Geopunkte speichern. Sie können auch Felder mit Text für beschreibende Informationen speichern, um gespeicherten Vektoren mehr Kontext zu verleihen. Durch die gemeinsame Zuordnung der Datentypen wird die Komplexität reduziert, die Wartbarkeit erhöht und Datenduplizierungen, Probleme mit der Versionskompatibilität und Lizenzprobleme vermieden.

> **Note**
>
> Amazon OpenSearch Serverless unterstützt die skalare 16-Bit-Quantisierung von Faiss, mit der Konvertierungen zwischen 32-Bit-Floating- und 16-Bit-Vektoren durchgeführt werden können. Weitere Informationen finden Sie unter Faiss-16-Bit-Skalarquantisierung. Sie können auch binäre Vektoren verwenden, um die Speicherkosten zu senken. Weitere Informationen finden Sie unter Binäre Vektoren.

Erste Schritte mit Sammlungen für die Vektorsuche

In diesem Tutorial führen Sie die folgenden Schritte aus, um Vektoreinbettungen in Echtzeit zu speichern, zu suchen und abzurufen:

1. Konfigurieren von Berechtigungen
2. Erstellen einer Sammlung
3. Hochladen und Suchen von Daten
4. Löschen der Sammlung

Schritt 1: Konfigurieren von Berechtigungen

Um dieses Tutorial abzuschließen (und OpenSearch Serverless im Allgemeinen zu verwenden), benötigen Sie die richtigen AWS Identity and Access Management (IAM-) Berechtigungen. In diesem Tutorial erstellen Sie eine Sammlung, laden Daten hoch und suchen sie und löschen dann die Sammlung.

Ihr Benutzer oder Ihre Rolle muss über eine angefügte identitätsbasierte Richtlinie mit den folgenden Mindestberechtigungen verfügen:

JSON

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "aoss:CreateCollection",
        "aoss:ListCollections",
        "aoss:BatchGetCollection",
        "aoss:DeleteCollection",
        "aoss:CreateAccessPolicy",
        "aoss:ListAccessPolicies",
        "aoss:UpdateAccessPolicy",
        "aoss:CreateSecurityPolicy",
        "iam:ListUsers",
        "iam:ListRoles"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Weitere Informationen zu OpenSearch serverlosen IAM-Berechtigungen finden Sie unter. the section called “Identitäts- und Zugriffsverwaltung”

Schritt 2: Erstellen einer Sammlung

Eine Sammlung ist eine Gruppe von OpenSearch Indizes, die zusammenarbeiten, um eine bestimmte Arbeitslast oder einen bestimmten Anwendungsfall zu unterstützen.

Um eine OpenSearch serverlose Sammlung zu erstellen

1. Öffnen Sie die Amazon OpenSearch Service-Konsole zu https://console.aws.amazon.com/aos/Hause.
2. Wählen Sie im linken Navigationsbereich Collections (Sammlungen) und wählen Sie Create collection (Sammlung erstellen) aus.
3. Nennen Sie das Sammelgehäuse.
4. Wählen Sie als Sammlungstyp die Option Vektorsuche aus. Weitere Informationen finden Sie unter the section called “Auswahl eines Sammlungstyps”.
5. Deaktivieren Sie unter Bereitstellungstyp die Option Redundanz aktivieren (aktive Replikate). Dadurch wird eine Sammlung im Entwicklungs- oder Testmodus erstellt und die Anzahl der

OpenSearch Recheneinheiten (OCUs) in Ihrer Sammlung auf zwei reduziert. Wenn Sie in diesem Tutorial eine Produktionsumgebung erstellen möchten, lassen Sie das Kontrollkästchen aktiviert.

6. Wählen Sie unter Sicherheit die Option Einfach erstellen aus, um Ihre Sicherheitskonfiguration zu optimieren. Alle Daten in der Vector Engine werden bei der Übertragung und im Ruhezustand standardmäßig verschlüsselt. Die Vektor-Engine unterstützt detaillierte IAM-Berechtigungen, sodass Sie definieren können, wer Verschlüsselungen, Netzwerke, Sammlungen und Indizes erstellen, aktualisieren und löschen darf.
7. Wählen Sie Weiter aus.
8. Überprüfen Sie Ihre Sammlungseinstellungen und wählen Sie Submit (Senden) aus. Warten Sie einige Minuten, bis der Sammlungsstatus `Active` erreicht ist.

Schritt 3: Daten hochladen und suchen

Ein Index ist eine Sammlung von Dokumenten mit einem gemeinsamen Datenschema, das es Ihnen ermöglicht, Ihre Vektoreinbettungen und andere Felder zu speichern, zu suchen und abzurufen. Sie können Daten erstellen und in Indizes in einer OpenSearch serverlosen Sammlung hochladen, indem Sie die Dev Tools-Konsole in OpenSearch Dashboards oder ein HTTP-Tool wie Postman oder awscurl verwenden. In diesem Tutorial werden Dev Tools verwendet.

So indizieren und durchsuchen Sie Daten in der Filme-Sammlung

1. Um einen einzelnen Index für Ihre neue Sammlung zu erstellen, senden Sie die folgende Anfrage an die Dev Tools-Konsole. Standardmäßig wird dadurch ein Index mit einer `nmslib` Engine und einer euklidischen Distanz erstellt.

```
PUT housing-index
{
   "settings": {
      "index.knn": true
   },
   "mappings": {
      "properties": {
         "housing-vector": {
            "type": "knn_vector",
            "dimension": 3
         },
         "title": {
            "type": "text"
```

```
         },
         "price": {
            "type": "long"
         },
         "location": {
            "type": "geo_point"
         }
      }
   }
}
```

2. Um ein einzelnes Dokument in den Housing-Index zu indexieren, senden Sie die folgende Anfrage:

```
POST housing-index/_doc
{
  "housing-vector": [
    10,
    20,
    30
  ],
  "title": "2 bedroom in downtown Seattle",
  "price": "2800",
  "location": "47.71, 122.00"
}
```

3. Um nach Immobilien zu suchen, die denen in Ihrem Index ähnlich sind, senden Sie die folgende Abfrage:

```
GET housing-index/_search
{
    "size": 5,
    "query": {
        "knn": {
            "housing-vector": {
                "vector": [
                    10,
                    20,
                    30
                ],
                "k": 5
            }
        }
```

```
    }
}
```

Schritt 4: Sammlung löschen

Da die Wohnungssammlung zu Testzwecken dient, sollten Sie sie unbedingt löschen, wenn Sie mit dem Experimentieren fertig sind.

Um eine OpenSearch serverlose Sammlung zu löschen

1. Gehen Sie zurück zur Amazon OpenSearch Service-Konsole.
2. Wählen Sie im linken Navigationsbereich Sammlungen und dann die Eigenschaftensammlung aus.
3. Wählen Sie Löschen und bestätigen Sie den Löschvorgang.

Gefilterte Suche

Sie können Filter verwenden, um Ihre semantischen Suchergebnisse zu verfeinern. Um einen Index zu erstellen und eine gefilterte Suche in Ihren Dokumenten durchzuführen, ersetzen Sie die folgenden Anweisungen anstelle von Daten hochladen und suchen aus dem vorherigen Tutorial. Die anderen Schritte bleiben gleich. Weitere Informationen zu Filtern finden Sie unter k-NN-Suche mit Filtern.

So indizieren und durchsuchen Sie Daten in der Filme-Sammlung

1. Um einen einzelnen Index für Ihre Sammlung zu erstellen, senden Sie die folgende Anfrage in der Dev Tools-Konsole:

```
PUT housing-index-filtered
{
  "settings": {
    "index.knn": true
  },
  "mappings": {
    "properties": {
      "housing-vector": {
        "type": "knn_vector",
        "dimension": 3,
        "method": {
```

```
          "engine": "faiss",
          "name": "hnsw"
        }
      },
      "title": {
        "type": "text"
      },
      "price": {
        "type": "long"
      },
      "location": {
        "type": "geo_point"
      }
    }
  }
}
```

2. Um ein einzelnes Dokument zu indexieren housing-index-filtered, senden Sie die folgende Anfrage:

```
POST housing-index-filtered/_doc
{
  "housing-vector": [
    10,
    20,
    30
  ],
  "title": "2 bedroom in downtown Seattle",
  "price": "2800",
  "location": "47.71, 122.00"
}
```

3. Um nach Ihren Daten nach einer Wohnung in Seattle zu einem bestimmten Preis und in einer bestimmten Entfernung von einem geografischen Punkt zu suchen, senden Sie die folgende Anfrage:

```
GET housing-index-filtered/_search
{
  "size": 5,
  "query": {
    "knn": {
      "housing-vector": {
        "vector": [
```

```
          0.1,
          0.2,
          0.3
        ],
        "k": 5,
        "filter": {
          "bool": {
            "must": [
              {
                "query_string": {
                  "query": "Find me 2 bedroom apartment in Seattle under $3000 ",
                  "fields": [
                    "title"
                  ]
                }
              },
              {
                "range": {
                  "price": {
                    "lte": 3000
                  }
                }
              },
              {
                "geo_distance": {
                  "distance": "100miles",
                  "location": {
                    "lat": 48,
                    "lon": 121
                  }
                }
              }
            ]
          }
        }
      }
    }
  }
}
```

Workloads im Milliardenbereich

Vektorsuchsammlungen unterstützen Workloads mit Milliarden von Vektoren. Sie müssen zu Skalierungszwecken keine Neuindizierung durchführen, da Auto Scaling dies für Sie erledigt. Wenn Sie über Millionen von Vektoren (oder mehr) mit einer hohen Anzahl von Dimensionen verfügen und mehr als 200 benötigen OCUs, wenden Sie sich an den AWS Support, um die maximale Anzahl an OpenSearch Recheneinheiten (OCUs) für Ihr Konto zu erhöhen.

Einschränkungen

Für Sammlungen der Vektorsuche gelten die folgenden Einschränkungen:

- Sammlungen für die Vektorsuche unterstützen die Apache Lucene ANN-Engine nicht.
- Sammlungen mit Vektorsuche unterstützen nur den HNSW-Algorithmus mit Faiss und nicht IVF und IVFQ.
- Sammlungen für die Vektorsuche unterstützen die API-Operationen Warmup, Statistik und Modelltraining nicht.
- Sammlungen für die Vektorsuche unterstützen keine Inline- oder gespeicherten Skripts.
- Informationen zur Indexanzahl sind in den Sammlungen AWS Management Console für die Vektorsuche nicht verfügbar.
- Das Aktualisierungsintervall für Indizes für Vektorsuchsammlungen beträgt 60 Sekunden.

Nächste Schritte

Da Sie nun wissen, wie Sie eine Vektorsuchsammlung erstellen und Daten indexieren, möchten Sie vielleicht einige der folgenden Übungen ausprobieren:

- Verwenden Sie den OpenSearch Python-Client, um mit Vektorsuchsammlungen zu arbeiten. Sehen Sie sich dieses Tutorial unter an GitHub.
- Verwenden Sie den OpenSearch Java-Client, um mit Vektorsuchsammlungen zu arbeiten. Sehen Sie sich dieses Tutorial unter an GitHub.
- Für LangChain die Verwendung OpenSearch als Vektorspeicher eingerichtet. LangChain ist ein Open-Source-Framework für die Entwicklung von Anwendungen, die auf Sprachmodellen basieren. Weitere Informationen finden Sie in der LangChain -Dokumentation.

Verwenden von Datenlebenszyklusrichtlinien mit Amazon OpenSearch Serverless

Eine Datenlebenszyklusrichtlinie in Amazon OpenSearch Serverless definiert, wie lange OpenSearch Serverless Daten in einer Zeitreihenerfassung aufbewahrt. Sie können beispielsweise eine Richtlinie festlegen, nach der Protokolldaten 30 Tage lang aufbewahrt werden, bevor OpenSearch Serverless sie löscht.

Sie können für jeden Index innerhalb jeder Zeitreihensammlung in Ihrem eine separate Richtlinie konfigurieren. AWS-Konto OpenSearch Serverless bewahrt Dokumente mindestens für die Dauer auf, die Sie in der Richtlinie angeben. Anschließend werden die Dokumente automatisch nach bestem Wissen und Gewissen gelöscht, in der Regel innerhalb von 48 Stunden oder innerhalb von 10% der Aufbewahrungsfrist, je nachdem, welcher Zeitraum länger ist.

Nur Zeitreihenerfassungen unterstützen Richtlinien für den Datenlebenszyklus. Sammlungen mit Such- und Vektorsuche tun dies nicht.

Themen

- Richtlinien für den Datenlebenszyklus
- Erforderliche Berechtigungen
- Vorrang der Richtlinie
- Richtliniensyntax
- Erstellung von Richtlinien für den Datenlebenszyklus
- Aktualisierung der Richtlinien für den Datenlebenszyklus
- Löschen von Datenlebenszyklus-Richtlinien

Richtlinien für den Datenlebenszyklus

In einer Datenlebenszyklus-Richtlinie geben Sie eine Reihe von Regeln an. Mit der Datenlebenszyklus-Richtlinie können Sie die Aufbewahrungsdauer von Daten verwalten, die Indizes oder Sammlungen zugeordnet sind, die diesen Regeln entsprechen. Diese Regeln definieren den Aufbewahrungszeitraum für Daten in einem Index oder einer Gruppe von Indizes. Jede Regel besteht aus einem Ressourcentyp (`index`), einem Aufbewahrungszeitraum und einer Liste von Ressourcen (Indizes), für die der Aufbewahrungszeitraum gilt.

Sie definieren den Aufbewahrungszeitraum mit einem der folgenden Formate:

- `"MinIndexRetention": "24h"`— OpenSearch Serverless speichert Indexdaten für den angegebenen Zeitraum in Stunden oder Tagen. Sie können für diesen Zeitraum einen Zeitraum von `24h` bis `3650d` festlegen.
- `"NoMinIndexRetention": true`— OpenSearch Serverless speichert Indexdaten auf unbestimmte Zeit.

In der folgenden Beispielrichtlinie legt die erste Regel eine Aufbewahrungsfrist von 15 Tagen für alle Indizes innerhalb der Sammlung fest. `marketing` Die zweite Regel legt fest, dass für alle Indexnamen, die mit `log` in der `finance` Sammlung beginnen, keine Aufbewahrungsfrist festgelegt ist und dass sie auf unbestimmte Zeit aufbewahrt werden.

```
{
   "lifeCyclePolicyDetail": {
      "type": "retention",
      "name": "my-policy",
      "policyVersion": "MTY4ODI0NTM2OTk1N18x",
      "policy": {
         "Rules": [
            {
            "ResourceType":"index",
            "Resource":[
               "index/marketing/*"
            ],
            "MinIndexRetention": "15d"
         },
         {
            "ResourceType":"index",
            "Resource":[
               "index/finance/log*"
            ],
            "NoMinIndexRetention": true
         }
         ]
      },
      "createdDate": 1688245369957,
      "lastModifiedDate": 1688245369957
   }
}
```

In der folgenden Beispiel-Richtlinienregel speichert OpenSearch Serverless die Daten in allen Indizes für alle Sammlungen innerhalb des Kontos auf unbestimmte Zeit.

```
{
   "Rules": [
      {
         "ResourceType": "index",
         "Resource": [
            "index/*/*"
         ]
      }
   ],
   "NoMinIndexRetention": true
}
```

Erforderliche Berechtigungen

Lifecycle-Richtlinien für OpenSearch Serverless verwenden die folgenden AWS Identity and Access Management (IAM-) Berechtigungen. Sie können IAM-Bedingungen angeben, um Benutzer auf Datenlebenszyklus-Richtlinien zu beschränken, die bestimmten Sammlungen und Indizes zugeordnet sind.

- `aoss:CreateLifecyclePolicy`— Erstellen Sie eine Datenlebenszyklus-Richtlinie.
- `aoss:ListLifecyclePolicies`— Listet alle Datenlebenszyklus-Richtlinien im aktuellen Konto auf.
- `aoss:BatchGetLifecyclePolicy`— Zeigen Sie eine Datenlebenszyklus-Richtlinie an, die einem Konto- oder Richtliniennamen zugeordnet ist.
- `aoss:BatchGetEffectiveLifecyclePolicy`— Eine Datenlebenszyklus-Richtlinie für eine bestimmte Ressource anzeigen (`index`ist die einzige unterstützte Ressource).
- `aoss:UpdateLifecyclePolicy`— Ändern Sie eine bestimmte Datenlebenszyklus-Richtlinie und ändern Sie deren Aufbewahrungseinstellung oder Ressource.
- `aoss:DeleteLifecyclePolicy`— Löscht eine Datenlebenszyklus-Richtlinie.

Die folgende identitätsbasierte Zugriffsrichtlinie ermöglicht es einem Benutzer, alle Datenlebenszyklusrichtlinien einzusehen und Richtlinien anhand des Ressourcenmusters zu aktualisieren: `collection/application-logs`

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "aoss:UpdateLifecyclePolicy"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aoss:collection": "application-logs"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "aoss:ListLifecyclePolicies",
                "aoss:BatchGetLifecyclePolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

Vorrang der Richtlinie

Es kann Situationen geben, in denen sich die Richtlinienregeln für den Datenlebenszyklus innerhalb oder zwischen Richtlinien überschneiden. In diesem Fall überschreibt eine Regel mit einem spezifischeren Ressourcennamen oder einem spezifischeren Muster für einen Index eine Regel mit einem allgemeineren Ressourcennamen oder Muster für alle Indizes, die beiden Regeln gemeinsam sind.

In der folgenden Richtlinie gelten beispielsweise zwei Regeln für einen Index. `index/sales/logstash` In diesem Fall hat die zweite Regel Vorrang, da sie `index/sales/log*` am längsten entsprich`index/sales/logstash`. Daher legt OpenSearch Serverless keine Aufbewahrungsfrist für den Index fest.

```
{
      "Rules":[
         {
            "ResourceType":"index",
            "Resource":[
               "index/sales/*",
            ],
            "MinIndexRetention": "15d"
         },
         {
            "ResourceType":"index",
            "Resource":[
               "index/sales/log*",
            ],
            "NoMinIndexRetention": true
         }
      ]
   }
```

Richtliniensyntax

Geben Sie eine oder mehrere Regeln an. Diese Regeln definieren die Datenlebenszykluseinstellungen für Ihre OpenSearch Serverless-Indizes.

Jede Regel enthält die folgenden Elemente. Sie können `NoMinIndexRetention` in jeder Regel entweder `MinIndexRetention` oder angeben, aber nicht beides.

Element	Beschreibung
Ressourcentyp	Der Ressourcentyp, für den die Regel gilt. Die einzige unterstützte Option für Datenlebe nszyklus-Richtlinien ist`index`.
Ressource	Eine Liste von and/or Mustern mit Ressource nnamen. Muster bestehen aus einem Präfix und einem Platzhalter (*), sodass die zugehörigen Berechtigungen auf mehrere Ressourcen angewendet werden können. Beispiel, `index/`*`<collection-name|p attern>`* `/`*`<index-name|pattern>`* .

Element	Beschreibung
MinIndexRetention	Der Mindestzeitraum in Tagen (d) oder Stunden (h) für die Aufbewahrung des Dokuments im Index. Die Untergrenze ist `24h` und die Obergrenze ist`3650d`.
NoMinIndexRetention	Wenn`true`, OpenSearch Serverless speichert Dokumente auf unbestimmte Zeit.

Im folgenden Beispiel gilt die erste Regel für alle Indizes unter dem `autoparts-inventory` Muster (`index/autoparts-inventory/*`) und erfordert, dass Daten mindestens 20 Tage lang aufbewahrt werden, bevor Aktionen wie Löschen oder Archivieren ausgeführt werden können.

Die zweite Regel zielt auf Indizes ab, die dem `auto*/gear` Muster (`index/auto*/gear`) entsprechen, und legt eine Mindestaufbewahrungsdauer von 24 Stunden fest.

Die dritte Regel gilt speziell für den `tires` Index und hat keine Mindestaufbewahrungsdauer. Das bedeutet, dass Daten in diesem Index sofort oder auf der Grundlage anderer Kriterien gelöscht oder archiviert werden können. Diese Regeln helfen bei der Verwaltung der Aufbewahrung von Indexdaten mit unterschiedlichen Aufbewahrungszeiten oder ohne Aufbewahrungsbeschränkungen.

```
{
  "Rules": [
    {
      "ResourceType": "index",
      "Resource": [
        "index/autoparts-inventory/*"
      ],
      "MinIndexRetention": "20d"
    },
    {
      "ResourceType": "index",
      "Resource": [
        "index/auto*/gear"
      ],
      "MinIndexRetention": "24h"
    },
    {
      "ResourceType": "index",
```

```
      "Resource": [
        "index/autoparts-inventory/tires"
      ],
      "NoMinIndexRetention": true
    }
  ]
}
```

Erstellung von Richtlinien für den Datenlebenszyklus

Um eine Datenlebenszyklus-Richtlinie zu erstellen, definieren Sie Regeln, die die Aufbewahrung und Löschung Ihrer Daten auf der Grundlage bestimmter Kriterien regeln.

Konsole

Um eine Datenlebenszyklus-Richtlinie zu erstellen

1. Melden Sie sich zu https://console.aws.amazon.com/aos/Hause bei der Amazon OpenSearch Service-Konsole an.
2. Wählen Sie im linken Navigationsbereich die Option Data Lifecycle Policies aus.
3. Wählen Sie Datenlebenszyklus-Richtlinie erstellen aus.
4. Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
5. Wählen Sie unter Datenlebenszyklus die Option Hinzufügen und wählen Sie die Sammlungen und Indizes für die Richtlinie aus.

   Wählen Sie zunächst die Sammlungen aus, zu denen die Indizes gehören. Wählen Sie dann entweder den Index aus der Liste aus oder geben Sie ein Indexmuster ein. Um alle Sammlungen als Quellen auszuwählen, geben Sie ein Sternchen (*) ein.
6. Für die Datenaufbewahrung können Sie entweder wählen, ob die Daten auf unbestimmte Zeit aufbewahrt werden sollen, oder die Option Unbegrenzt (niemals löschen) deaktivieren und einen Zeitraum angeben, nach dem OpenSearch Serverless die Daten automatisch aus Amazon S3 löscht.
7. Wählen Sie Speichern und dann Erstellen.

AWS CLI

Um eine Datenlebenszyklus-Richtlinie mit dem zu erstellen AWS CLI, verwenden Sie den create-lifecycle-policyBefehl mit den folgenden Optionen:

- `--name`— Der Name der Richtlinie.
- `--type`— Die Art der Richtlinie. Derzeit ist der einzig verfügbare Wert`retention`.
- `--policy`— Die Datenlebenszyklus-Richtlinie. Dieser Parameter akzeptiert sowohl Inline-Richtlinien als auch JSON-Dateien. Sie müssen Inline-Richtlinien als JSON-Escape-Zeichenfolge codieren. Verwenden Sie das Format`--policy file://my-policy.json`, um die Richtlinie in einer Datei bereitzustellen.

Example

```
aws opensearchserverless create-lifecycle-policy \
  --name my-policy \
  --type retention \
  --policy "{\"Rules\":[{\"ResourceType\":\"index\",\"Resource\":[\"index/autoparts-
inventory/*\"],\"MinIndexRetention\": \"81d\"},{\"ResourceType\":\"index\",\"Resource
\":[\"index/sales/orders*\"],\"NoMinIndexRetention\":true}]}"
```

Aktualisierung der Richtlinien für den Datenlebenszyklus

Um eine Datenlebenszyklus-Richtlinie zu aktualisieren, können Sie bestehende Regeln ändern, um Änderungen Ihrer Anforderungen an die Aufbewahrung oder Löschung von Daten widerzuspiegeln. Auf diese Weise können Sie Ihre Richtlinien an die sich ändernden Anforderungen an das Datenmanagement anpassen.

Zwischen der Aktualisierung der Richtlinie und dem Beginn der Durchsetzung der neuen Aufbewahrungsfristen durch OpenSearch Serverless kann es zu einer Verzögerung von einigen Minuten kommen.

Konsole

Um eine Datenlebenszyklus-Richtlinie zu aktualisieren

1. Melden Sie sich zu https://console.aws.amazon.com/aos/Hause bei der Amazon OpenSearch Service-Konsole an.
2. Wählen Sie im linken Navigationsbereich die Option Data Lifecycle Policies aus.
3. Wählen Sie die Datenlebenszyklus-Richtlinie aus, die Sie aktualisieren möchten, und klicken Sie dann auf Bearbeiten.
4. Ändern Sie die Richtlinie mit dem visuellen Editor oder dem JSON-Editor.
5. Wählen Sie Speichern.

AWS CLI

Verwenden Sie den update-lifecycle-policyBefehl AWS CLI, um eine Datenlebenszyklus-Richtlinie mithilfe von zu aktualisieren.

Sie müssen den `--policy-version` Parameter in die Anfrage aufnehmen. Sie können die Richtlinienversion mithilfe der list-lifecycle-policies- oder batch-get-lifecycle-policy-Befehle abrufen. Wir empfehlen, die neueste Richtlinienversion einzubeziehen, um zu verhindern, dass Änderungen, die von anderen vorgenommen wurden, versehentlich überschrieben werden.

Mit der folgenden Anfrage wird eine Datenlebenszyklus-Richtlinie mit einem neuen JSON-Richtliniendokument aktualisiert.

Example

```
aws opensearchserverless update-lifecycle-policy \
  --name my-policy \
  --type retention \
  --policy-version MTY2MzY5MTY1MDA3Ml8x \
  --policy file://my-new-policy.json
```

Löschen von Datenlebenszyklus-Richtlinien

Wenn Sie eine Datenlebenszyklus-Richtlinie löschen, OpenSearch erzwingt Serverless sie nicht mehr für übereinstimmende Indizes.

Konsole

Um eine Datenlebenszyklus-Richtlinie zu löschen

1. Melden Sie sich zu https://console.aws.amazon.com/aos/Hause bei der Amazon OpenSearch Service-Konsole an.
2. Wählen Sie im linken Navigationsbereich die Option Data Lifecycle Policies aus.
3. Wählen Sie die Richtlinie aus, die Sie löschen möchten, wählen Sie dann Löschen und bestätigen Sie den Löschvorgang.

AWS CLI

Verwenden Sie den delete-lifecycle-policyBefehl AWS CLI, um eine Datenlebenszyklus-Richtlinie mithilfe von zu löschen.

Example

```
aws opensearchserverless delete-lifecycle-policy \
  --name my-policy \
  --type retention
```

Verwenden von AWS SDKs für die Interaktion mit Amazon OpenSearch Serverless

Dieser Abschnitt enthält Beispiele für die Verwendung des AWS SDKs zur Interaktion mit Amazon OpenSearch Serverless. Diese Codebeispiele zeigen, wie Sicherheitsrichtlinien und Sammlungen erstellt und Sammlungen abgefragt werden.

> **Note**
>
> Wir sind gerade dabei, diese Codebeispiele zu erstellen. Wenn Sie ein Codebeispiel (Java, Go, etc.) beitragen möchten, öffnen Sie direkt im GitHub Repository eine Pull-Anfrage.

Themen

- Python
- JavaScript

Python

Das folgende Beispielskript verwendet das AWS SDK für Python (Boto3) sowie den opensearch-py-Client für Python, um Verschlüsselungs-, Netzwerk- und Datenzugriffsrichtlinien zu erstellen, eine passende Sammlung zu erstellen und einige Beispieldaten zu indizieren.

Führen Sie die folgenden Befehle aus, um die erforderlichen Abhängigkeiten zu installieren:

```
pip install opensearch-py
pip install boto3
pip install botocore
pip install requests-aws4auth
```

Ersetzen Sie innerhalb des Skripts das `Principal`-Element durch den Amazon-Ressourcennamen (ARN) des Benutzers oder der Rolle, die die Anfrage signiert. Optional können Sie auch das `region` ändern.

```
from opensearchpy import OpenSearch, RequestsHttpConnection
from requests_aws4auth import AWS4Auth
import boto3
import botocore
import time

# Build the client using the default credential configuration.
# You can use the CLI and run 'aws configure' to set access key, secret
# key, and default region.

client = boto3.client('opensearchserverless')
service = 'aoss'
region = 'us-east-1'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key,
                   region, service, session_token=credentials.token)


def createEncryptionPolicy(client):
    """Creates an encryption policy that matches all collections beginning with tv-"""
    try:
        response = client.create_security_policy(
            description='Encryption policy for TV collections',
            name='tv-policy',
            policy="""
                {
                    \"Rules\":[
                        {
                            \"ResourceType\":\"collection\",
                            \"Resource\":[
                                \"collection\/tv-*\"
                            ]
                        }
                    ],
                    \"AWSOwnedKey\":true
                }
                """,
            type='encryption'
        )
```

```
        print('\nEncryption policy created:')
        print(response)
    except botocore.exceptions.ClientError as error:
        if error.response['Error']['Code'] == 'ConflictException':
            print(
                '[ConflictException] The policy name or rules conflict with an existing
 policy.')
        else:
            raise error


def createNetworkPolicy(client):
    """Creates a network policy that matches all collections beginning with tv-"""
    try:
        response = client.create_security_policy(
            description='Network policy for TV collections',
            name='tv-policy',
            policy="""
                [{
                    \"Description\":\"Public access for TV collection\",
                    \"Rules\":[
                        {
                            \"ResourceType\":\"dashboard\",
                            \"Resource\":[\"collection\/tv-*\"]
                        },
                        {
                            \"ResourceType\":\"collection\",
                            \"Resource\":[\"collection\/tv-*\"]
                        }
                    ],
                    \"AllowFromPublic\":true
                }]
                """,
            type='network'
        )
        print('\nNetwork policy created:')
        print(response)
    except botocore.exceptions.ClientError as error:
        if error.response['Error']['Code'] == 'ConflictException':
            print(
                '[ConflictException] A network policy with this name already exists.')
        else:
            raise error
```

```
def createAccessPolicy(client):
    """Creates a data access policy that matches all collections beginning with tv-"""
    try:
        response = client.create_access_policy(
            description='Data access policy for TV collections',
            name='tv-policy',
            policy="""
                [{
                    \"Rules\":[
                        {
                            \"Resource\":[
                                \"index\/tv-*\/*\"
                            ],
                            \"Permission\":[
                                \"aoss:CreateIndex\",
                                \"aoss:DeleteIndex\",
                                \"aoss:UpdateIndex\",
                                \"aoss:DescribeIndex\",
                                \"aoss:ReadDocument\",
                                \"aoss:WriteDocument\"
                            ],
                            \"ResourceType\": \"index\"
                        },
                        {
                            \"Resource\":[
                                \"collection\/tv-*\"
                            ],
                            \"Permission\":[
                                \"aoss:CreateCollectionItems\"
                            ],
                            \"ResourceType\": \"collection\"
                        }
                    ],
                    \"Principal\":[
                        \"arn:aws:iam::123456789012:role\/Admin\"
                    ]
                }]
                """,
            type='data'
        )
        print('\nAccess policy created:')
        print(response)
    except botocore.exceptions.ClientError as error:
```

```
        if error.response['Error']['Code'] == 'ConflictException':
            print(
                '[ConflictException] An access policy with this name already exists.')
        else:
            raise error


def createCollection(client):
    """Creates a collection"""
    try:
        response = client.create_collection(
            name='tv-sitcoms',
            type='SEARCH'
        )
        return(response)
    except botocore.exceptions.ClientError as error:
        if error.response['Error']['Code'] == 'ConflictException':
            print(
                '[ConflictException] A collection with this name already exists. Try
 another name.')
        else:
            raise error


def waitForCollectionCreation(client):
    """Waits for the collection to become active"""
    response = client.batch_get_collection(
        names=['tv-sitcoms'])
    # Periodically check collection status
    while (response['collectionDetails'][0]['status']) == 'CREATING':
        print('Creating collection...')
        time.sleep(30)
        response = client.batch_get_collection(
            names=['tv-sitcoms'])
    print('\nCollection successfully created:')
    print(response["collectionDetails"])
    # Extract the collection endpoint from the response
    host = (response['collectionDetails'][0]['collectionEndpoint'])
    final_host = host.replace("https://", "")
    indexData(final_host)


def indexData(host):
    """Create an index and add some sample data"""
```

```
    # Build the OpenSearch client
    client = OpenSearch(
        hosts=[{'host': host, 'port': 443}],
        http_auth=awsauth,
        use_ssl=True,
        verify_certs=True,
        connection_class=RequestsHttpConnection,
        timeout=300
    )
    # It can take up to a minute for data access rules to be enforced
    time.sleep(45)

    # Create index
    response = client.indices.create('sitcoms-eighties')
    print('\nCreating index:')
    print(response)

    # Add a document to the index.
    response = client.index(
        index='sitcoms-eighties',
        body={
            'title': 'Seinfeld',
            'creator': 'Larry David',
            'year': 1989
        },
        id='1',
    )
    print('\nDocument added:')
    print(response)


def main():
    createEncryptionPolicy(client)
    createNetworkPolicy(client)
    createAccessPolicy(client)
    createCollection(client)
    waitForCollectionCreation(client)


if __name__ == "__main__":
    main()
```

JavaScript

Das folgende Beispielskript verwendet das SDK für JavaScript in Node.js sowie den opensearch-js -Client für JavaScript, um Verschlüsselungs-, Netzwerk- und Datenzugriffsrichtlinien zu erstellen, eine passende Sammlung zu erstellen, einen Index zu erstellen und einige Beispieldaten zu indizieren.

Führen Sie die folgenden Befehle aus, um die erforderlichen Abhängigkeiten zu installieren:

```
npm i aws-sdk
npm i aws4
npm i @opensearch-project/opensearch
```

Ersetzen Sie innerhalb des Skripts das `Principal`-Element durch den Amazon-Ressourcennamen (ARN) des Benutzers oder der Rolle, die die Anfrage signiert. Optional können Sie auch das `region` ändern.

```
var AWS = require('aws-sdk');
var aws4 = require('aws4');
var {
    Client,
    Connection
} = require("@opensearch-project/opensearch");
var {
    OpenSearchServerlessClient,
    CreateSecurityPolicyCommand,
    CreateAccessPolicyCommand,
    CreateCollectionCommand,
    BatchGetCollectionCommand
} = require("@aws-sdk/client-opensearchserverless");
var client = new OpenSearchServerlessClient();

async function execute() {
    await createEncryptionPolicy(client)
    await createNetworkPolicy(client)
    await createAccessPolicy(client)
    await createCollection(client)
    await waitForCollectionCreation(client)
}

async function createEncryptionPolicy(client) {
    // Creates an encryption policy that matches all collections beginning with 'tv-'
    try {
```

```
        var command = new CreateSecurityPolicyCommand({
            description: 'Encryption policy for TV collections',
            name: 'tv-policy',
            type: 'encryption',
            policy: " \
        { \
            \"Rules\":[ \
                { \
                    \"ResourceType\":\"collection\", \
                    \"Resource\":[ \
                        \"collection\/tv-*\" \
                    ] \
                } \
            ], \
            \"AWSOwnedKey\":true \
        }"
        });
        const response = await client.send(command);
        console.log("Encryption policy created:");
        console.log(response['securityPolicyDetail']);
    } catch (error) {
        if (error.name === 'ConflictException') {
            console.log('[ConflictException] The policy name or rules conflict with an
 existing policy.');
        } else
            console.error(error);
    };
}

async function createNetworkPolicy(client) {
    // Creates a network policy that matches all collections beginning with 'tv-'
    try {
        var command = new CreateSecurityPolicyCommand({
            description: 'Network policy for TV collections',
            name: 'tv-policy',
            type: 'network',
            policy: " \
            [{ \
                \"Description\":\"Public access for television collection\", \
                \"Rules\":[ \
                    { \
                        \"ResourceType\":\"dashboard\", \
                        \"Resource\":[\"collection\/tv-*\"] \
                    }, \
```

```
                    { \
                        \"ResourceType\":\"collection\", \
                        \"Resource\":[\"collection\/tv-*\"] \
                    } \
                ], \
                \"AllowFromPublic\":true \
            }]"
        });
        const response = await client.send(command);
        console.log("Network policy created:");
        console.log(response['securityPolicyDetail']);
    } catch (error) {
        if (error.name === 'ConflictException') {
            console.log('[ConflictException] A network policy with that name already
 exists.');
        } else
            console.error(error);
    };
}

async function createAccessPolicy(client) {
    // Creates a data access policy that matches all collections beginning with 'tv-'
    try {
        var command = new CreateAccessPolicyCommand({
            description: 'Data access policy for TV collections',
            name: 'tv-policy',
            type: 'data',
            policy: " \
            [{ \
                \"Rules\":[ \
                    { \
                        \"Resource\":[ \
                            \"index\/tv-*\/*\" \
                        ], \
                        \"Permission\":[ \
                            \"aoss:CreateIndex\", \
                            \"aoss:DeleteIndex\", \
                            \"aoss:UpdateIndex\", \
                            \"aoss:DescribeIndex\", \
                            \"aoss:ReadDocument\", \
                            \"aoss:WriteDocument\" \
                        ], \
                        \"ResourceType\": \"index\" \
                    }, \
```

```
                    { \
                        \"Resource\":[ \
                            \"collection\/tv-*\" \
                        ], \
                        \"Permission\":[ \
                            \"aoss:CreateCollectionItems\" \
                        ], \
                        \"ResourceType\": \"collection\" \
                    } \
                ], \
                \"Principal\":[ \
                    \"arn:aws:iam::123456789012:role\/Admin\" \
                ] \
            }]"
        });
        const response = await client.send(command);
        console.log("Access policy created:");
        console.log(response['accessPolicyDetail']);
    } catch (error) {
        if (error.name === 'ConflictException') {
            console.log('[ConflictException] An access policy with that name already
 exists.');
        } else
            console.error(error);
    };
}

async function createCollection(client) {
    // Creates a collection to hold TV sitcoms indexes
    try {
        var command = new CreateCollectionCommand({
            name: 'tv-sitcoms',
            type: 'SEARCH'
        });
        const response = await client.send(command);
        return (response)
    } catch (error) {
        if (error.name === 'ConflictException') {
            console.log('[ConflictException] A collection with this name already
 exists. Try another name.');
        } else
            console.error(error);
    };
}
```

```
async function waitForCollectionCreation(client) {
    // Waits for the collection to become active
    try {
        var command = new BatchGetCollectionCommand({
            names: ['tv-sitcoms']
        });
        var response = await client.send(command);
        while (response.collectionDetails[0]['status'] == 'CREATING') {
            console.log('Creating collection...')
            await sleep(30000) // Wait for 30 seconds, then check the status again
            function sleep(ms) {
                return new Promise((resolve) => {
                    setTimeout(resolve, ms);
                });
            }
            var response = await client.send(command);
        }
        console.log('Collection successfully created:');
        console.log(response['collectionDetails']);
        // Extract the collection endpoint from the response
        var host = (response.collectionDetails[0]['collectionEndpoint'])
        // Pass collection endpoint to index document request
        indexDocument(host)
    } catch (error) {
        console.error(error);
    };
}

async function indexDocument(host) {

    var client = new Client({
        node: host,
        Connection: class extends Connection {
            buildRequestObject(params) {
                var request = super.buildRequestObject(params)
                request.service = 'aoss';
                request.region = 'us-east-1'; // e.g. us-east-1
                var body = request.body;
                request.body = undefined;
                delete request.headers['content-length'];
                request.headers['x-amz-content-sha256'] = 'UNSIGNED-PAYLOAD';
                request = aws4.sign(request, AWS.config.credentials);
                request.body = body;
```

```
                return request
            }
        }
    });

    // Create an index
    try {
        var index_name = "sitcoms-eighties";

        var response = await client.indices.create({
            index: index_name
        });

        console.log("Creating index:");
        console.log(response.body);

        // Add a document to the index
        var document = "{ \"title\": \"Seinfeld\", \"creator\": \"Larry David\", \"year
\": \"1989\" }\n";

        var response = await client.index({
            index: index_name,
            body: document
        });

        console.log("Adding document:");
        console.log(response.body);
    } catch (error) {
        console.error(error);
    };
}

execute()
```

Verwenden AWS CloudFormation , um Amazon OpenSearch Serverless-Sammlungen zu erstellen

Sie können verwenden AWS CloudFormation , um OpenSearch Amazon-Serverless-Ressourcen wie Sammlungen, Sicherheitsrichtlinien und VPC-Endpunkte zu erstellen. Die umfassende CloudFormation Referenz zu OpenSearch Serverless finden Sie unter Amazon OpenSearch Serverless im AWS CloudFormation Benutzerhandbuch.

Die folgende CloudFormation Beispielvorlage erstellt eine einfache Datenzugriffsrichtlinie, Netzwerkrichtlinie und Sicherheitsrichtlinie sowie eine passende Sammlung. Es ist eine gute Möglichkeit, die Ausführung von Amazon OpenSearch Serverless schnell zu beginnen und die notwendigen Elemente zum Erstellen und Verwenden einer Sammlung bereitzustellen.

> **Important**
>
> In diesem Beispiel wird der öffentliche Netzwerkzugriff verwendet, was für Produktionsworkloads nicht empfohlen wird. Wir empfehlen die Verwendung des VPC-Zugriffs, um Ihre Sammlungen zu schützen. Weitere Informationen erhalten Sie unter AWS::OpenSearchServerless::VpcEndpoint und the section called “VPC-Endpunkte”.

```
AWSTemplateFormatVersion: 2010-09-09
Description: 'Amazon OpenSearch Serverless template to create an IAM user, encryption
 policy, data access policy and collection'
Resources:
  IAMUSer:
    Type: 'AWS::IAM::User'
    Properties:
      UserName:  aossadmin
  DataAccessPolicy:
    Type: 'AWS::OpenSearchServerless::AccessPolicy'
    Properties:
      Name: quickstart-access-policy
      Type: data
      Description: Access policy for quickstart collection
      Policy: !Sub >-
        [{"Description":"Access for cfn user","Rules":
[{"ResourceType":"index","Resource":["index/*/*"],"Permission":["aoss:*"]},
        {"ResourceType":"collection","Resource":["collection/quickstart"],"Permission":
["aoss:*"]}],
        "Principal":["arn:aws:iam::${AWS::AccountId}:user/aossadmin"]}]
  NetworkPolicy:
    Type: 'AWS::OpenSearchServerless::SecurityPolicy'
    Properties:
      Name: quickstart-network-policy
      Type: network
      Description: Network policy for quickstart collection
      Policy: >-
```

```
        [{"Rules":[{"ResourceType":"collection","Resource":["collection/
quickstart"]}, {"ResourceType":"dashboard","Resource":["collection/
quickstart"]}],"AllowFromPublic":true}]
  EncryptionPolicy:
    Type: 'AWS::OpenSearchServerless::SecurityPolicy'
    Properties:
      Name: quickstart-security-policy
      Type: encryption
      Description: Encryption policy for quickstart collection
      Policy: >-
        {"Rules":[{"ResourceType":"collection","Resource":["collection/
quickstart"]}],"AWSOwnedKey":true}
  Collection:
    Type: 'AWS::OpenSearchServerless::Collection'
    Properties:
      Name: quickstart
      Type: TIMESERIES
      Description: Collection to holds timeseries data
    DependsOn: EncryptionPolicy
Outputs:
  IAMUser:
    Value: !Ref IAMUSer
  DashboardURL:
    Value: !GetAtt Collection.DashboardEndpoint
  CollectionARN:
    Value: !GetAtt Collection.Arn
```

Verwaltung von Kapazitätsgrenzen für Amazon OpenSearch Serverless

Mit Amazon OpenSearch Serverless müssen Sie die Kapazität nicht selbst verwalten. OpenSearch Serverless skaliert die Rechenkapazität für Ihr Konto automatisch auf der Grundlage der aktuellen Arbeitslast. Serverlose Rechenkapazität wird in OpenSearch Recheneinheiten () OCUs gemessen. Jede OCU ist eine Kombination aus 6 GB Speicher und entsprechender virtueller CPU (vCPU) und erstellt eine Daten-Pipeline zu Amazon S3. Weitere Informationen zur entkoppelten Architektur in OpenSearch Serverless finden Sie unter. the section called “Funktionsweise”

Wenn Sie Ihre erste Sammlung erstellen, instanziiert OpenSearch OCUs Serverless auf der Grundlage Ihrer Redundanzeinstellungen. Standardmäßig sind redundante aktive Replikate aktiviert, was bedeutet, dass insgesamt vier instanziiert OCUs werden (zwei für die Indizierung und zwei

für die Suche), um eine hohe Verfügbarkeit mit Standby-Knoten in einer anderen Availability Zone sicherzustellen. Zu Entwicklungs- und Testzwecken können Sie die Einstellung Redundanz aktivieren für eine Sammlung deaktivieren, wodurch die Standby-Replikate entfernt und nur zwei OCUs (eines für die Indizierung und eines für die Suche) instanziiert werden. Diese sind OCUs immer vorhanden, auch wenn keine Indizierungs- oder Suchaktivitäten stattfinden. Alle nachfolgenden Sammlungen können diese gemeinsam nutzen OCUs (mit Ausnahme von Sammlungen mit eindeutigen AWS KMS Schlüsseln, die ihren eigenen Satz von Schlüsseln instanziieren). OCUs Bei Bedarf skaliert OpenSearch Serverless automatisch und fügt weitere hinzu, wenn Ihre Indexierungs OCUs - und Suchnutzung zunimmt. Wenn der Verkehr auf Ihrem Erfassungsendpunkt abnimmt, wird die Kapazität wieder auf die für Ihre Datengröße OCUs erforderliche Mindestanzahl herunterskaliert. Für die Suche und die Erfassung von Zeitreihen ist die Anzahl der im Leerlauf OCUs erforderlichen Daten proportional zur Datengröße und Indexanzahl. Bei Vektoren hängt dies sowohl vom Arbeitsspeicher (RAM) zum Speichern von Vektorgrafiken als auch vom Festplattenspeicher zum Speichern von Indizes ab. Wenn Sie sich nicht im Ruhezustand befinden, berücksichtigen die OCU-Anforderungen beide Faktoren.

Vektorsammlungen speichern Indexdaten im lokalen OCU-Speicher. Die OCU-RAM-Grenzwerte werden schneller erreicht als die OCU-Festplattenlimits, was dazu führt, dass Vektorsammlungen durch den RAM-Speicherplatz eingeschränkt werden. Es wird höchstens auf 1 OCU [0,5 OCU x 2] für die Indizierung und 1 OCU [0,5 OCU x 2] für die Suche herunterskaliert. Bei der Skalierung wird auch die Anzahl der Shards berücksichtigt, die für Ihre Sammlung oder Ihren Index benötigt werden. Jede OCU kann eine bestimmte Anzahl von Shards unterstützen. Die Anzahl der Indizes sollte proportional zur Anzahl der Shards sein. Die Gesamtzahl der OCUs benötigten Basen entspricht der maximal benötigten Daten-, Speicher- und Shard-Menge. Weitere Informationen finden Sie im AWS Big Data-Blog OpenSearch unter kostengünstige Suchfunktionen von Amazon Serverless in beliebiger Größenordnung.

Bei Sammlungen von Such - und Vektorsuchen werden alle Daten in Hot-Indizes gespeichert, um schnelle Antwortzeiten bei Abfragen zu gewährleisten. Zeitreihenerfassungen verwenden eine Kombination aus heißem und warmem Speicher, wobei die neuesten Daten im Hot-Storage aufbewahrt werden, um die Antwortzeiten bei Abfragen für Daten, auf die häufiger zugegriffen wird, zu optimieren. Weitere Informationen finden Sie unter the section called “Auswahl eines Sammlungstyps”.

> **Note**
>
> Eine Vektorsuchsammlung kann nicht OCUs mit Such - und Zeitreihensammlungen gemeinsam genutzt werden, selbst wenn die Vektorsuchsammlung denselben KMS-

Schlüssel wie die Such - oder Zeitreihensammlungen verwendet. Für Ihre erste Vektorsammlung OCUs wird ein neuer Satz von erstellt. Die Vektorsammlungen werden OCUs von denselben KMS-Schlüsselsammlungen gemeinsam genutzt.

Um die Kapazität Ihrer Sammlungen zu verwalten und die Kosten zu kontrollieren, können Sie die maximale Indexierungs- und Suchkapazität für das aktuelle Konto und die Region insgesamt angeben. OpenSearch Serverless skaliert Ihre Sammlungsressourcen automatisch auf der Grundlage dieser Spezifikationen.

Da die Indizierungs- und Suchkapazität separat skaliert werden, geben Sie für beide Limits auf Kontoebene an:

- Maximale Indexkapazität — OpenSearch Serverless kann die Indexierungskapazität auf bis zu diese Anzahl von erhöhen. OCUs
- Maximale Suchkapazität — OpenSearch Serverless kann die Suchkapazität auf bis zu diese Anzahl von erhöhen. OCUs

Note

Derzeit gelten Kapazitätseinstellungen nur auf Kontoebene. Sie können keine Kapazitätsgrenzen pro Sammlung konfigurieren.

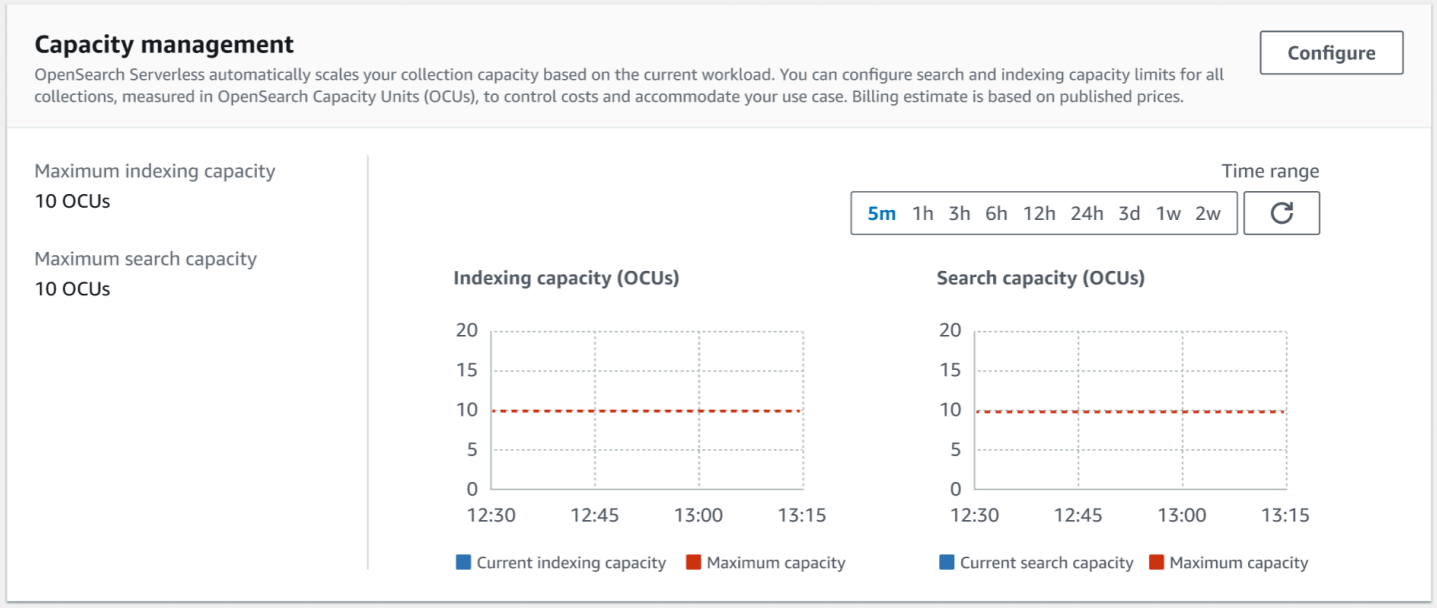
Ihr Ziel sollte es sein, sicherzustellen, dass die maximale Kapazität hoch genug ist, um Spitzen im Workload zu bewältigen. Basierend auf Ihren Einstellungen skaliert OpenSearch Serverless automatisch die Anzahl der Dateien, damit Ihre Sammlungen den Arbeitsaufwand OCUs für Indexierung und Suche verarbeiten können.

Themen

- Konfigurieren von Kapazitätseinstellungen
- Maximale Kapazitätsgrenzen
- Überwachung der Kapazitätsnutzung

Konfigurieren von Kapazitätseinstellungen

Um die Kapazitätseinstellungen in der OpenSearch Serverless-Konsole zu konfigurieren, erweitern Sie Serverless im linken Navigationsbereich und wählen Sie Dashboard aus. Geben Sie unter Capacity management (Kapazitätsverwaltung) die maximale Indizierungs- und Suchkapazität an:



Um die Kapazität mit dem zu konfigurieren AWS CLI, senden Sie eine UpdateAccountSettingsAnfrage:

```
aws opensearchserverless update-account-settings \
    --capacity-limits '{ "maxIndexingCapacityInOCU": 8,"maxSearchCapacityInOCU": 9 }'
```

Maximale Kapazitätsgrenzen

Die maximale Gesamtzahl von Indizes, die eine Sammlung enthalten kann, beträgt 1000. Für alle drei Arten von Sammlungen beträgt die standardmäßige maximale OCU-Kapazität 10 für die Indizierung und 10 OCUs OCUs für die Suche. Die für ein Konto zulässige Mindestkapazität ist 1 OCU [0,5 OCU x 2] für die Indexierung und 1 OCU [0,5 OCU x 2] für die Suche. Für alle Sammlungen beträgt die maximal zulässige Kapazität 1.700 für die Indexierung und 1.700 OCUs für die Suche. OCUs Sie können die OCU-Anzahl so konfigurieren, dass sie eine beliebige Zahl von 1 bis zur maximal zulässigen Kapazität ist, und zwar in Vielfachen von 2.

Jede OCU verfügt über ausreichend kurzlebigen Hot-Speicher für 120 GiB Indexdaten. OpenSearch Serverless unterstützt bis zu 1 TiB an Daten pro Index in Such - und Vektorsuchsammlungen und 100

TiB an heißen Daten pro Index in einer Zeitreihensammlung. Bei Zeitreihen-Sammlungen können Sie immer noch mehr Daten aufnehmen, die dann als warme Daten in S3 gespeichert werden können.

Eine Liste aller Kontingente finden Sie unter OpenSearch Serverlose Kontingente.

Überwachung der Kapazitätsnutzung

Sie können die Metriken `Search0CU` und die CloudWatch Kennzahlen `Indexing0CU` auf Kontoebene überwachen, um zu verstehen, wie Ihre Sammlungen skalieren. Wir empfehlen Ihnen, Warnungen zu konfigurieren, um sich benachrichtigen zu lassen wenn sich Ihr Konto einem Schwellenwert für kapazitätsbezogene Metriken nähert. So können Sie Ihre Kapazitätseinstellungen entsprechend anpassen.

Sie können diese Metriken auch verwenden, um festzustellen, ob Ihre Einstellungen für die maximale Kapazität angemessen sind oder ob Sie diese anpassen müssen. Analysieren Sie diese Metriken, um Ihre Bemühungen auf die Optimierung der Effizienz Ihrer Sammlungen zu konzentrieren. Weitere Informationen zu den Metriken, an die OpenSearch Serverless sendet, finden Sie CloudWatch unter. the section called “Überwachen von OpenSearch Serverless-Management”

Erfassung von Daten in OpenSearch Amazon-Serverless-Sammlungen

Diese Abschnitte enthalten Details zu den unterstützten Erfassungspipelines für die Datenerfassung in Amazon-Serverless-Sammlungen. OpenSearch Sie behandeln auch einige der Clients, die Sie zur Interaktion mit den OpenSearch API-Operationen verwenden können. Ihre Clients sollten mit OpenSearch 2.x kompatibel sein, um eine Integration mit OpenSearch Serverless zu ermöglichen.

Themen

- Erforderliche Mindestberechtigungen
- OpenSearch Verschlucken
- Fluent Bit
- Amazon Data Firehose
- Go
- Java
- JavaScript

- Logstash
- Python
- Ruby
- Signieren von HTTP-Anforderungen mit anderen Clients

Erforderliche Mindestberechtigungen

Um Daten in eine OpenSearch Serverless-Sammlung aufzunehmen, müssen dem Prinzipal, der die Daten schreibt, die folgenden Mindestberechtigungen in einer Datenzugriffsrichtlinie zugewiesen werden:

```
[
   {
      "Rules":[
         {
            "ResourceType":"index",
            "Resource":[
               "index/target-collection/logs"
            ],
            "Permission":[
               "aoss:CreateIndex",
               "aoss:WriteDocument",
               "aoss:UpdateIndex"
            ]
         }
      ],
      "Principal":[
         "arn:aws:iam::123456789012:user/my-user"
      ]
   }
]
```

Die Berechtigungen können umfassender sein, wenn Sie in zusätzliche Indizes schreiben möchten. Anstatt beispielsweise einen einzelnen Zielindex anzugeben, können Sie die Berechtigung für alle Indizes (index/ *target-collection* /*) oder eine Teilmenge von Indizes (index//) erteilen. *target-collection logs**

Eine Referenz aller verfügbaren OpenSearch API-Operationen und der zugehörigen Berechtigungen finden Sie unterthe section called “Unterstützte Vorgänge und Plugins”.

OpenSearch Verschlucken

Anstatt einen Drittanbieter-Client zu verwenden, um Daten direkt an eine OpenSearch serverlose Sammlung zu senden, können Sie Amazon OpenSearch Ingestion verwenden. Sie konfigurieren Ihre Datenproduzenten zum Senden von Daten an OpenSearch Ingestion. Die Daten werden dann automatisch an die angegebene Sammlung geliefert. Sie können OpenSearch Ingestion auch so konfigurieren, dass die Daten vor der Bereitstellung transformiert werden. Weitere Informationen finden Sie unter OpenSearch Einnahme durch Amazon.

Eine OpenSearch Ingestion-Pipeline benötigt die Berechtigung, in eine OpenSearch serverlose Sammlung zu schreiben, die als Senke konfiguriert ist. Diese Berechtigungen umfassen die Möglichkeit, die Sammlung zu beschreiben und HTTP-Anforderungen an sie zu senden. Anweisungen zur Verwendung von OpenSearch Ingestion zum Hinzufügen von Daten zu einer Sammlung finden Sie unter. the section called “Pipelines Zugriff auf Sammlungen gewähren”

Informationen zu den ersten Schritten mit OpenSearch Ingestion finden Sie unter. the section called “Tutorial: Daten in eine Sammlung aufnehmen”

Fluent Bit

Sie können AWS für Fluent-Bit-Image und das OpenSearch Ausgabe-Plugin verwenden, um Daten in OpenSearch Serverless-Sammlungen aufzunehmen.

> **Note**
>
> Sie benötigen Version 2.30.0 oder höher von AWS für Fluent-Bit-Images, um in Serverless integrieren zu können. OpenSearch

Beispielkonfiguration:

Dieser Beispielausgabeabschnitt der Konfigurationsdatei zeigt, wie eine OpenSearch Serverless-Sammlung als Ziel verwendet wird. Die wichtige Ergänzung ist der `AWS_Service_Name`-Parameter, der `aoss` ist. `Host` ist der Sammlungsendpunkt.

```
[OUTPUT]
    Name  opensearch
    Match *
    Host  collection-endpoint.us-west-2.aoss.amazonaws.com
    Port  443
```

```
    Index  my_index
    Trace_Error On
    Trace_Output On
    AWS_Auth On
    AWS_Region <region>
    AWS_Service_Name aoss
    tls     On
    Suppress_Type_Name On
```

Amazon Data Firehose

Firehose unterstützt OpenSearch Serverless als Zustellziel. Anweisungen zum Senden von Daten an OpenSearch Serverless finden Sie unter Erstellen eines Kinesis-Data-Firehose-Bereitstellungsstreams und Auswahl von OpenSearch Serverless als Ihr Ziel im Entwicklerhandbuch fürAmazon Data Firehose.

Die IAM-Rolle, die Sie Firehose für die Bereitstellung zur Verfügung stellen, muss in einer Datenzugriffsrichtlinie mit der `aoss:WriteDocument` Mindestberechtigung für die Zielsammlung angegeben werden, und Sie benötigen ein zuvor vorhandenes Index, an das Sie Daten senden. Weitere Informationen finden Sie unter the section called “Erforderliche Mindestberechtigungen”.

Bevor Sie Daten an OpenSearch Serverless senden, müssen Sie möglicherweise Transformationen an den Daten durchführen. Weitere Informationen über die Verwendung von Lambda-Funktionen zur Ausführung dieser Aufgabe finden Sie unter Amazon Kinesis Data Firehose Datentransformation im selben Handbuch.

Go

Der folgende Beispielcode verwendet den opensearch-go -Client für Go, um eine sichere Verbindung zur angegebenen OpenSearch Serverless-Sammlung herzustellen und einen einzelnen Index zu erstellen. Sie müssen Werte für `region` und `host` angeben.

```
package main

import (
  "context"
  "log"
  "strings"
  "github.com/aws/aws-sdk-go-v2/aws"
  "github.com/aws/aws-sdk-go-v2/config"
  opensearch "github.com/opensearch-project/opensearch-go/v2"
```

```
  opensearchapi "github.com/opensearch-project/opensearch-go/v2/opensearchapi"
  requestsigner "github.com/opensearch-project/opensearch-go/v2/signer/awsv2"
)

const endpoint = "" // serverless collection endpoint

func main() {
 ctx := context.Background()

 awsCfg, err := config.LoadDefaultConfig(ctx,
  config.WithRegion("<AWS_REGION>"),
  config.WithCredentialsProvider(
   getCredentialProvider("<AWS_ACCESS_KEY>", "<AWS_SECRET_ACCESS_KEY>",
 "<AWS_SESSION_TOKEN>"),
  ),
 )
 if err != nil {
  log.Fatal(err) // don't log.fatal in a production-ready app
 }

 // create an AWS request Signer and load AWS configuration using default config folder
 or env vars.
 signer, err := requestsigner.NewSignerWithService(awsCfg, "aoss") // "aoss" for Amazon
 OpenSearch Serverless
 if err != nil {
  log.Fatal(err) // don't log.fatal in a production-ready app
 }

 // create an opensearch client and use the request-signer
 client, err := opensearch.NewClient(opensearch.Config{
  Addresses: []string{endpoint},
  Signer:    signer,
 })
 if err != nil {
  log.Fatal("client creation err", err)
 }

 indexName := "go-test-index"

  // define index mapping
 mapping := strings.NewReader(`{
  "settings": {
    "index": {
         "number_of_shards": 4
```

```
          }
        }
  }`)

 // create an index
 createIndex := opensearchapi.IndicesCreateRequest{
  Index: indexName,
    Body: mapping,
 }
 createIndexResponse, err := createIndex.Do(context.Background(), client)
 if err != nil {
  log.Println("Error ", err.Error())
  log.Println("failed to create index ", err)
  log.Fatal("create response body read err", err)
 }
 log.Println(createIndexResponse)

 // delete the index
 deleteIndex := opensearchapi.IndicesDeleteRequest{
  Index: []string{indexName},
 }

 deleteIndexResponse, err := deleteIndex.Do(context.Background(), client)
 if err != nil {
  log.Println("failed to delete index ", err)
  log.Fatal("delete index response body read err", err)
 }
 log.Println("deleting index", deleteIndexResponse)
}

func getCredentialProvider(accessKey, secretAccessKey, token string)
 aws.CredentialsProviderFunc {
 return func(ctx context.Context) (aws.Credentials, error) {
  c := &aws.Credentials{
   AccessKeyID:     accessKey,
   SecretAccessKey: secretAccessKey,
   SessionToken:    token,
  }
  return *c, nil
 }
}
```

Java

Der folgende Beispielcode verwendet den opensearch-java -Client für Java, um eine sichere Verbindung zur angegebenen OpenSearch Serverless-Sammlung herzustellen und einen einzelnen Index zu erstellen. Sie müssen Werte für `region` und `host` angeben.

Der wichtige Unterschied zu OpenSearch Service- Domains ist der Service-Name (`aoss`anstelle von`es`).

```
// import OpenSearchClient to establish connection to OpenSearch Serverless collection
import org.opensearch.client.opensearch.OpenSearchClient;

SdkHttpClient httpClient = ApacheHttpClient.builder().build();
// create an opensearch client and use the request-signer
OpenSearchClient client = new OpenSearchClient(
    new AwsSdk2Transport(
        httpClient,
        "...us-west-2.aoss.amazonaws.com", // serverless collection endpoint
        "aoss" // signing service name
        Region.US_WEST_2, // signing service region
        AwsSdk2TransportOptions.builder().build()
    )
);

String index = "sample-index";

// create an index
CreateIndexRequest createIndexRequest = new
 CreateIndexRequest.Builder().index(index).build();
CreateIndexResponse createIndexResponse = client.indices().create(createIndexRequest);
System.out.println("Create index reponse: " + createIndexResponse);

// delete the index
DeleteIndexRequest deleteIndexRequest = new
 DeleteIndexRequest.Builder().index(index).build();
DeleteIndexResponse deleteIndexResponse = client.indices().delete(deleteIndexRequest);
System.out.println("Delete index reponse: " + deleteIndexResponse);

httpClient.close();
```

Der folgende Beispielcode stellt erneut eine sichere Verbindung her und durchsucht dann einen Index.

```
import org.opensearch.client.opensearch.OpenSearchClient;
>>>>>>> aoss-slr-update

SdkHttpClient httpClient = ApacheHttpClient.builder().build();

OpenSearchClient client = new OpenSearchClient(
    new AwsSdk2Transport(
        httpClient,
        "...us-west-2.aoss.amazonaws.com", // serverless collection endpoint
        "aoss" // signing service name
        Region.US_WEST_2, // signing service region
        AwsSdk2TransportOptions.builder().build()
    )
);

Response response = client.generic()
    .execute(
        Requests.builder()
            .endpoint("/" + "users" + "/_search?typed_keys=true")
            .method("GET")
            .json("{"
                + "    \"query\": {"
                + "        \"match_all\": {}"
                + "    }"
                + "}")
            .build());

httpClient.close();
```

JavaScript

Der folgende Beispielcode verwendet den opensearch-js -Client, JavaScript um eine sichere Verbindung zur angegebenen OpenSearch Serverless-Sammlung herzustellen, einen einzelnen Index zu erstellen, ein Dokument hinzuzufügen und den Index zu löschen. Sie müssen Werte für `node` und `region` angeben.

Der wichtige Unterschied zu OpenSearch Service- Domains ist der Service-Name (`aoss`anstelle von`es`).

Version 3

In diesem Beispiel wird die Version 3 des SDK für JavaScript in Node.js verwendet.

```
const { defaultProvider } = require('@aws-sdk/credential-provider-node');
const { Client } = require('@opensearch-project/opensearch');
const { AwsSigv4Signer } = require('@opensearch-project/opensearch/aws');

async function main() {
    // create an opensearch client and use the request-signer
    const client = new Client({
        ...AwsSigv4Signer({
            region: 'us-west-2',
            service: 'aoss',
            getCredentials: () => {
                const credentialsProvider = defaultProvider();
                return credentialsProvider();
            },
        }),
        node: '' # // serverless collection endpoint
    });

    const index = 'movies';

    // create index if it doesn't already exist
    if (!(await client.indices.exists({ index })).body) {
        console.log((await client.indices.create({ index })).body);
    }

    // add a document to the index
    const document = { foo: 'bar' };
    const response = await client.index({
        id: '1',
        index: index,
        body: document,
    });
    console.log(response.body);

    // delete the index
    console.log((await client.indices.delete({ index })).body);
}

main();
```

Version 2

In diesem Beispiel wird Version 2 des SDK für JavaScript in Node.js verwendet.

```
const AWS = require('aws-sdk');
const { Client } = require('@opensearch-project/opensearch');
const { AwsSigv4Signer } = require('@opensearch-project/opensearch/aws');

async function main() {
    // create an opensearch client and use the request-signer
    const client = new Client({
        ...AwsSigv4Signer({
            region: 'us-west-2',
            service: 'aoss',
            getCredentials: () =>
                new Promise((resolve, reject) => {
                    AWS.config.getCredentials((err, credentials) => {
                        if (err) {
                            reject(err);
                        } else {
                            resolve(credentials);
                        }
                    });
                }),
        }),
        node: '' # // serverless collection endpoint
    });

    const index = 'movies';

    // create index if it doesn't already exist
    if (!(await client.indices.exists({ index })).body) {
        console.log((await client.indices.create({
            index
        })).body);
    }

    // add a document to the index
    const document = {
        foo: 'bar'
    };
    const response = await client.index({
        id: '1',
        index: index,
        body: document,
    });
    console.log(response.body);
```

```
    // delete the index
    console.log((await client.indices.delete({ index })).body);
}

main();
```

Logstash

Sie können das OpenSearch Logstash-Plugin verwenden, um Logs in OpenSearch serverlosen Sammlungen zu veröffentlichen.

So verwenden Sie Logstash zum Senden von Daten an Serverless OpenSearch

1. Installieren Sie Version 2.0.0 oder höher des logstash-output-opensearchPlugins mit Docker oder Linux.

   Docker

   Docker hostet die Logstash-OSS-Software mit dem vorinstallierten OpenSearch Ausgabe-Plugin: opensearchproject/ -output-plugin. logstash-oss-with-opensearch Sie können das Image wie jedes andere Image abrufen:

   ```
   docker pull opensearchproject/logstash-oss-with-opensearch-output-plugin:latest
   ```

   Linux

   Installieren Sie zunächst die neueste Version von Logstash, falls Sie dies noch nicht getan haben. Installieren Sie anschließend Version 2.0.0 des Ausgabe-Plugins:

   ```
   cd logstash-8.5.0/
   bin/logstash-plugin install --version 2.0.0 logstash-output-opensearch
   ```

   Wenn das Plugin bereits installiert ist, aktualisieren Sie es auf die neueste Version:

   ```
   bin/logstash-plugin update logstash-output-opensearch
   ```

Ab Version 2.0.0 des Plugins verwendet das AWS -SDK Version 3. Wenn Sie eine Logstash-Version vor 8.4.0 verwenden, müssen Sie alle vorinstallierten AWS -Plugins entfernen und das Plugin installieren: `logstash-integration-aws`

```
/usr/share/logstash/bin/logstash-plugin remove logstash-input-s3
/usr/share/logstash/bin/logstash-plugin remove logstash-input-sqs
/usr/share/logstash/bin/logstash-plugin remove logstash-output-s3
/usr/share/logstash/bin/logstash-plugin remove logstash-output-sns
/usr/share/logstash/bin/logstash-plugin remove logstash-output-sqs
/usr/share/logstash/bin/logstash-plugin remove logstash-output-cloudwatch

/usr/share/logstash/bin/logstash-plugin install --version 0.1.0.pre logstash-
integration-aws
```

2. Damit das OpenSearch Ausgabe-Plugin mit OpenSearch Serverless funktioniert, müssen Sie die folgenden Änderungen am `opensearch` Ausgabebereich von logstash.conf vornehmen:

   - Geben Sie `aoss` als `service_name` unter `auth_type` an.
   - Geben Sie Ihren Sammlungsendpunkt für `hosts` an.
   - Fügen Sie die Parameter `default_server_major_version` und `legacy_template` hinzu. Diese Parameter sind erforderlich, damit das Plugin mit OpenSearch Serverless funktioniert.

```
output {
  opensearch {
    hosts => "collection-endpoint:443"
    auth_type => {
      ...
      service_name => 'aoss'
    }
    default_server_major_version => 2
    legacy_template => false
  }
}
```

Diese Beispielkonfigurationsdatei übernimmt ihre Eingabe von Dateien in einem S3-Bucket und sendet sie an eine OpenSearch Serverless-Sammlung:

```
input {
```

```
  s3  {
    bucket => "my-s3-bucket"
    region => "us-east-1"
  }
}

output {
  opensearch {
    ecs_compatibility => disabled
    hosts => "https://my-collection-endpoint.us-east-1.aoss.amazonaws.com:443"
    index => my-index
    auth_type => {
      type => 'aws_iam'
      aws_access_key_id => 'your-access-key'
      aws_secret_access_key => 'your-secret-key'
      region => 'us-east-1'
      service_name => 'aoss'
    }
    default_server_major_version => 2
    legacy_template => false
  }
}
```

3. Führen Sie dann Logstash mit der neuen Konfiguration aus, um das Plugin zu testen:

```
bin/logstash -f config/test-plugin.conf
```

Python

Der folgende Beispielcode verwendet den opensearch-py -Client für Python, um eine sichere Verbindung zur angegebenen OpenSearch Serverless-Sammlung herzustellen, einen einzelnen Index zu erstellen und diesen Index zu durchsuchen. Sie müssen Werte für `region` und `host` angeben.

Der wichtige Unterschied zu OpenSearch Service- Domains ist der Service-Name (`aoss`anstelle von`es`).

```
from opensearchpy import OpenSearch, RequestsHttpConnection, AWSV4SignerAuth
import boto3

host = ''  # serverless collection endpoint, without https://
```

```
region = ''  # e.g. us-east-1

service = 'aoss'
credentials = boto3.Session().get_credentials()
auth = AWSV4SignerAuth(credentials, region, service)

# create an opensearch client and use the request-signer
client = OpenSearch(
    hosts=[{'host': host, 'port': 443}],
    http_auth=auth,
    use_ssl=True,
    verify_certs=True,
    connection_class=RequestsHttpConnection,
    pool_maxsize=20,
)

# create an index
index_name = 'books-index'
create_response = client.indices.create(
    index_name
)

print('\nCreating index:')
print(create_response)

# index a document
document = {
  'title': 'The Green Mile',
  'director': 'Stephen King',
  'year': '1996'
}

response = client.index(
    index = 'books-index',
    body = document,
    id = '1'
)


# delete the index
delete_response = client.indices.delete(
    index_name
)
```

```
print('\nDeleting index:')
print(delete_response)
```

Ruby

Das `opensearch-aws-sigv4` Gem bietet OpenSearch standardmäßig Zugriff auf Serverless zusammen mit OpenSearch Service. Es hat alle Funktionen des opensearch-ruby-Clients, da es von diesem Gem abhängig ist.

Geben Sie bei der Instanziierung des Sigv4-Signers `aoss` als Servicenamen an:

```
require 'opensearch-aws-sigv4'
require 'aws-sigv4'

signer = Aws::Sigv4::Signer.new(service: 'aoss',
                                region: 'us-west-2',
                                access_key_id: 'key_id',
                                secret_access_key: 'secret')

# create an opensearch client and use the request-signer
client = OpenSearch::Aws::Sigv4Client.new(
  { host: 'https://your.amz-opensearch-serverless.endpoint',
    log: true },
  signer)

# create an index
index = 'prime'
client.indices.create(index: index)

# insert data
client.index(index: index, id: '1', body: { name: 'Amazon Echo',
                                            msrp: '5999',
                                            year: 2011 })

# query the index
client.search(body: { query: { match: { name: 'Echo' } } })

# delete index entry
client.delete(index: index, id: '1')

# delete the index
client.indices.delete(index: index)
```

Signieren von HTTP-Anforderungen mit anderen Clients

Beim Signieren von Anforderungen an OpenSearch Serverless-Sammlungen gelten die folgenden Anforderungen, wenn Sie HTTP-Anforderungen mit anderen Clients erstellen:

- Sie müssen den Service-Namen als `aoss` angeben.
- Der `x-amz-content-sha256`-Header ist für alle Anforderungen der AWS Signature Version 4 erforderlich. Es stellt einen Hash der Anforderungsnutzlast bereit. Wenn eine Anforderungsnutzlast vorhanden ist, legen Sie den Wert auf den kryptografischen Hash des Secure Hash Algorithm (SHA256SHA) fest. Wenn keine Anforderungsnutzlast vorhanden ist, setzen Sie den Wert auf `e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855`, was der Hash einer leeren Zeichenfolge ist.

Themen

- Indizierung mit cURL
- Indexierung mit Postman

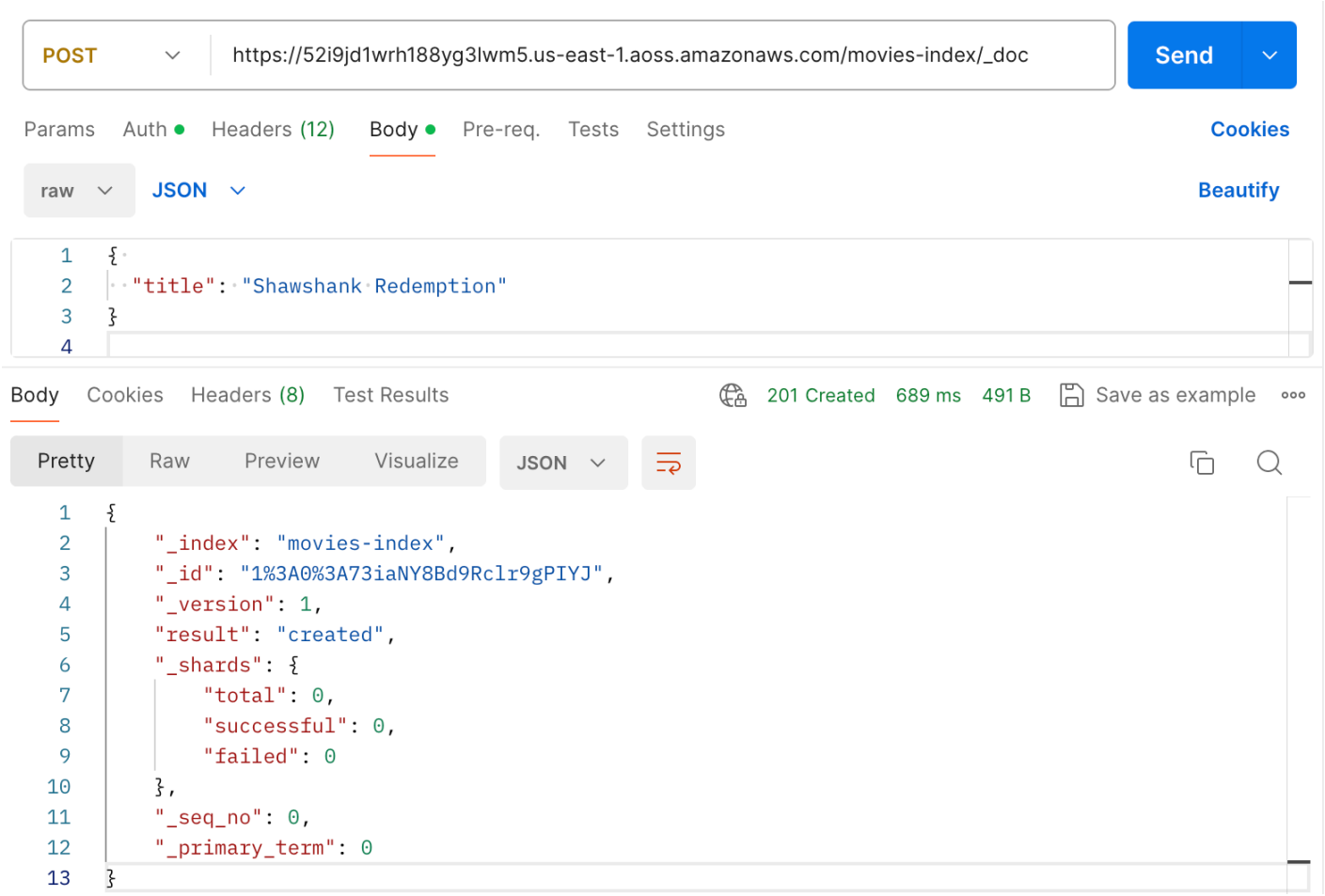
Indizierung mit cURL

Die folgende Beispielanforderung verwendet die Client URL Request Library (cURL), um ein einzelnes Dokument an einen Index zu senden, der `movies-index` innerhalb einer Sammlung benannt ist:

```
curl -XPOST \
    --user "$AWS_ACCESS_KEY_ID":"$AWS_SECRET_ACCESS_KEY" \
    --aws-sigv4 "aws:amz:us-east-1:aoss" \
    --header "x-amz-content-sha256: $REQUEST_PAYLOAD_SHA_HASH" \
    --header "x-amz-security-token: $AWS_SESSION_TOKEN" \
    "https://my-collection-endpoint.us-east-1.aoss.amazonaws.com/movies-index/_doc" \
    -H "Content-Type: application/json" -d '{"title": "Shawshank Redemption"}'
```

Indexierung mit Postman

In der folgenden Abbildung sehen Sie, wie eine Anfrage an eine Sammlung mithilfe von Postman gesendet wird. Anweisungen zur Authentifizierung finden Sie unter Workflow zur Authentifizierung mit AWS Signatur in Postman.



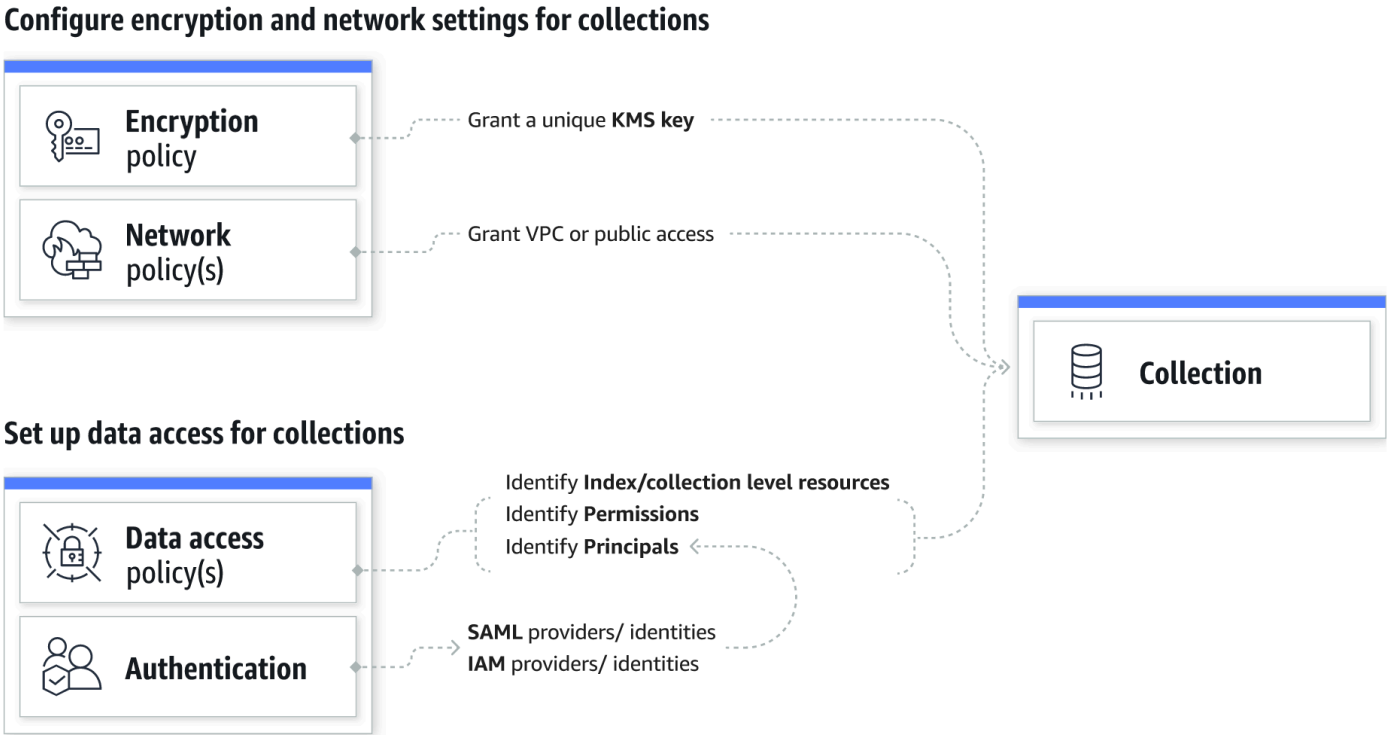
Überblick über die Sicherheit in Amazon OpenSearch Serverless

Die Sicherheit in Amazon OpenSearch Serverless unterscheidet sich in folgenden Punkten grundlegend von der Sicherheit in Amazon OpenSearch Service:

Funktion	OpenSearch Service	OpenSearch Serverlos
Datenzugr iffskontrolle	Der Datenzugriff wird durch IAM-Richt linien und eine differenzierte Zugangsko ntrolle festgelegt.	Der Datenzugriff wird durch Datenzugriffsrichtlinien festgeleg t.
Verschlüsselung im Ruhezustand	Die Verschlüsselung im Ruhezustand ist für Domains optional.	Die Verschlüsselung im Ruhezustand ist für Sammlunge n erforderlich.

Funktion	OpenSearch Service	OpenSearch Serverlos
Einrichtung und Verwaltung der Sicherheit	Sie müssen Netzwerk, Verschlüsselung und Datenzugriff für jede Domain einzeln konfigurieren.	Sie können Sicherheitsrichtli nien verwenden, um Sicherhei tseinstellungen für mehrere Sammlungen in großem Umfang zu verwalten.

Das folgende Diagramm veranschaulicht die Sicherheitskomponenten, aus denen eine funktionale Sammlung besteht. Eine Sammlung muss über einen zugewiesenen Verschlüsselungsschlüssel, Netzwerkzugriffseinstellungen und eine passende Datenzugriffsrichtlinie verfügen, die ihren Ressourcen Berechtigungen gewährt.



Themen

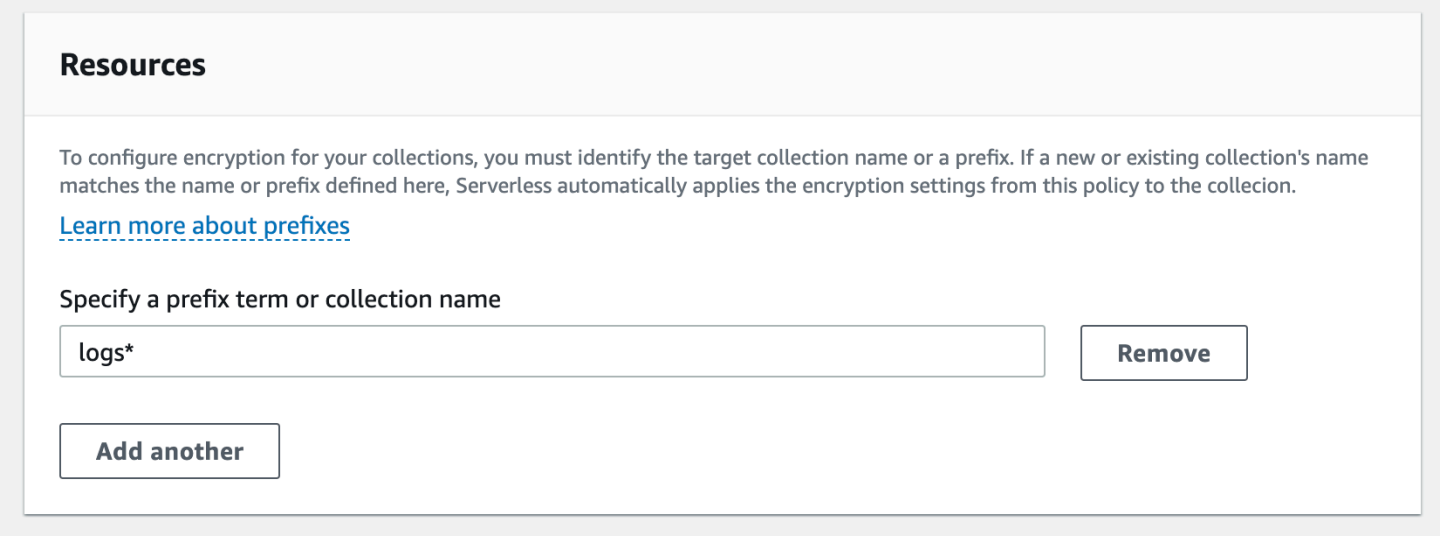
- Verschlüsselungsrichtlinien
- Netzwerkrichtlinien
- Daten-Zugriffsrichtlinien
- IAM und SAML-Authentifizierung
- Sicherheit der Infrastruktur

- Erste Schritte mit der Sicherheit in Amazon OpenSearch Serverless
- Identity and Access Management für Amazon OpenSearch Serverless
- Verschlüsselung in Amazon OpenSearch Serverless
- Netzwerkzugriff für Amazon OpenSearch Serverless
- Datenzugriffskontrolle für Amazon OpenSearch Serverless
- Greifen Sie über einen Schnittstellenendpunkt auf Amazon OpenSearch Serverless zu ()AWS PrivateLink
- SAML-Authentifizierung für Amazon Serverless OpenSearch
- Compliance-Validierung für Amazon OpenSearch Serverless

Verschlüsselungsrichtlinien

Verschlüsselungsrichtlinien definieren, ob Ihre Sammlungen mit einem AWS-eigener Schlüssel oder einem vom Kunden verwalteten Schlüssel verschlüsselt werden. Verschlüsselungsrichtlinien bestehen aus zwei Komponenten: einem Ressourcenmuster und einem Verschlüsselungsschlüssel. Das Ressourcenmuster legt fest, für welche Sammlung oder Sammlungen die Richtlinie gilt. Der Verschlüsselungsschlüssel legt fest, wie die zugehörigen Sammlungen gesichert werden.

Um eine Richtlinie auf mehrere Sammlungen anzuwenden, fügen Sie der Richtlinienregel ein Platzhalterzeichen (*) hinzu. Die folgende Richtlinie gilt beispielsweise für alle Sammlungen, deren Namen mit „logs“ beginnen.



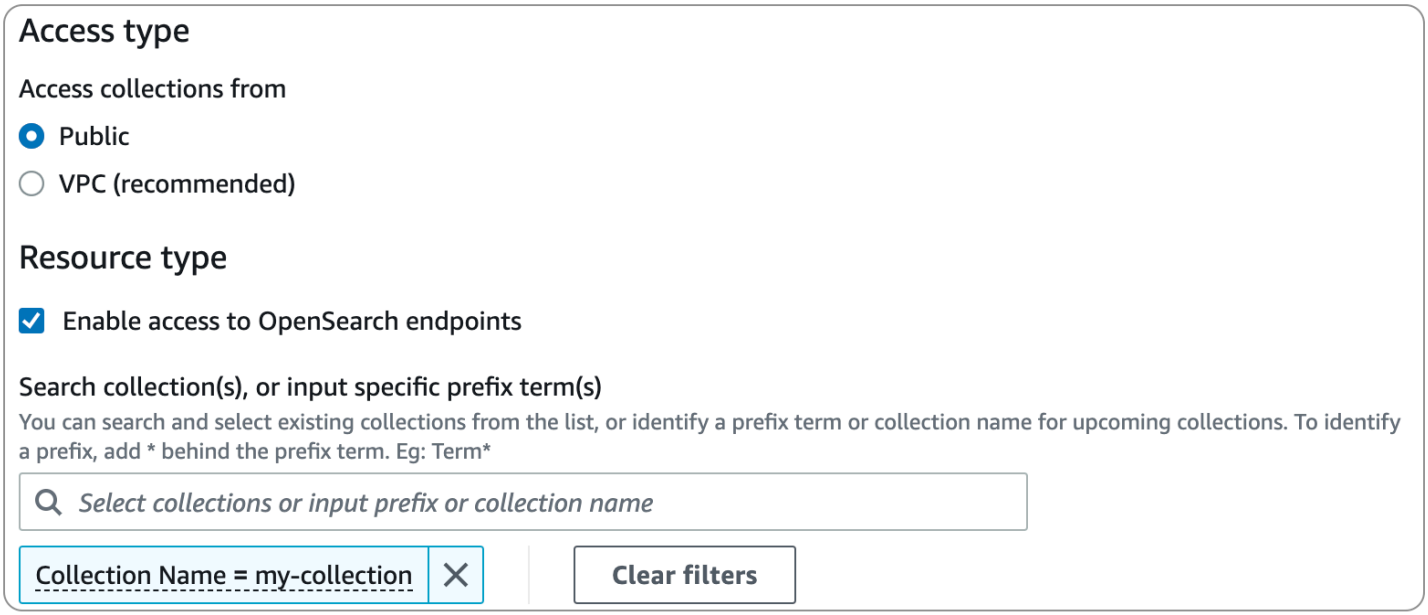
Verschlüsselungsrichtlinien optimieren den Prozess der Erstellung und Verwaltung von Sammlungen, insbesondere wenn Sie dies programmgesteuert tun. Sie können eine Sammlung erstellen,

indem Sie einfach einen Namen angeben. Bei der Erstellung wird dieser automatisch ein Verschlüsselungsschlüssel zugewiesen.

Netzwerkrichtlinien

Netzwerkrichtlinien definieren, ob Ihre Sammlungen privat oder über das Internet von öffentlichen Netzwerken aus zugänglich sind. Auf private Sammlungen kann über OpenSearch serverlos verwaltete VPC-Endpunkte oder über spezifische Endpunkte AWS-Services wie Amazon Bedrock über privaten Zugriff zugegriffen werden.AWS-Service Genau wie Verschlüsselungsrichtlinien können auch Netzwerkrichtlinien für mehrere Sammlungen gelten, so dass Sie den Netzwerkzugriff für viele Sammlungen in großem Umfang verwalten können.

Netzwerkrichtlinien bestehen aus zwei Komponenten: einem Zugriffstyp und einem Ressourcentyp. Der Zugriffstyp kann entweder öffentlich oder privat sein. Der Ressourcentyp bestimmt, ob der von Ihnen gewählte Zugriff für den Sammlungsendpunkt, den OpenSearch Dashboards-Endpunkt oder für beide gilt.



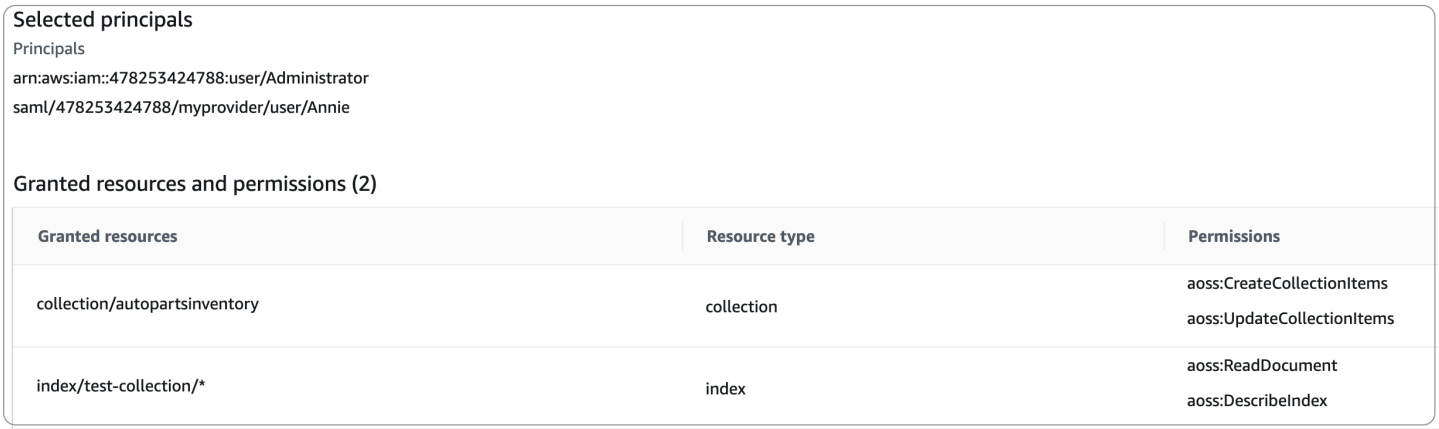
Wenn Sie den VPC-Zugriff innerhalb einer Netzwerkrichtlinie konfigurieren möchten, müssen Sie zunächst einen oder OpenSearch mehrere serverlos verwaltete VPC-Endpoints erstellen. Mit diesen Endpunkten können Sie wie in Ihrer VPC auf OpenSearch Serverless zugreifen, ohne ein Internet-Gateway, ein NAT-Gerät, eine VPN-Verbindung oder eine Verbindung verwenden zu müssen. AWS Direct Connect

Der private Zugriff auf AWS-Services kann nur für den Endpunkt der Sammlung gelten, nicht für den OpenSearch Endpunkt der OpenSearch Dashboards. AWS-Services kann kein Zugriff auf OpenSearch Dashboards gewährt werden.

Daten-Zugriffsrichtlinien

Datenzugriffsrichtlinien definieren, wie Ihre Benutzer auf die Daten in Ihren Sammlungen zugreifen. Datenzugriffsrichtlinien unterstützen Sie bei der Verwaltung von Sammlungen in großem Umfang, indem sie automatisch Zugriffsberechtigungen für Sammlungen und Indizes zuweisen, die einem bestimmten Muster übereinstimmen. Mehrere Richtlinien können für eine einzelne Ressource gelten.

Datenzugriffsrichtlinien bestehen aus einer Reihe von Regeln mit jeweils drei Komponenten: einem Ressourcentyp, gewährte Ressourcen und einer Reihe von Berechtigungen. Der Ressourcentyp kann eine Sammlung oder ein Index sein. Bei den gewährten Ressourcen kann es sich um collection/ index Namen oder Muster mit einem Platzhalter (*) handeln. Die Liste der Berechtigungen gibt an, auf welche OpenSearch API-Operationen die Richtlinie Zugriff gewährt. Darüber hinaus enthält die Richtlinie eine Liste von Prinzipalen, die die IAM-Rollen, -Benutzer und SAML-Identitäten angeben, denen Zugriff gewährt werden soll.



Weitere Informationen zum Format einer Datenzugriffsrichtlinie finden Sie in der Richtliniensyntax.

Bevor Sie eine Datenzugriffsrichtlinie erstellen, müssen Sie über eine oder mehrere IAM-Rollen oder -Benutzer oder SAML-Identitäten verfügen, auf die Sie in der Richtlinie Zugriff gewähren können. Einzelheiten finden Sie im nächsten Abschnitt.

> **Note**
>
> Wenn Sie für Ihre Sammlung vom öffentlichen zum privaten Zugriff wechseln, wird die Registerkarte „Indizes“ in der OpenSearch Serverless Collection Console entfernt.

IAM und SAML-Authentifizierung

IAM-Prinzipale und SAML-Identitäten sind eine der Bausteine einer Datenzugriffsrichtlinie. Innerhalb der `principal`-Anweisung einer Zugriffsrichtlinie können Sie IAM-Rollen, IAM-Benutzer und SAML-Identitäten angeben. Diesen Prinzipalen werden dann die Berechtigungen gewährt, die Sie in den zugeordneten Richtlinienregeln angeben.

```
[
   {
      "Rules":[
         {
            "ResourceType":"index",
            "Resource":[
               "index/marketing/orders*"
            ],
            "Permission":[
               "aoss:*"
            ]
         }
      ],
      "Principal":[
         "arn:aws:iam::123456789012:user/Dale",
         "arn:aws:iam::123456789012:role/RegulatoryCompliance",
         "saml/123456789012/myprovider/user/Annie"
      ]
   }
]
```

Sie konfigurieren die SAML-Authentifizierung direkt in Serverless. OpenSearch Weitere Informationen finden Sie unter the section called “SAML-Authentifizierung”.

Sicherheit der Infrastruktur

Amazon OpenSearch Serverless ist durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter AWS Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS Umgebung unter Verwendung der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf Amazon OpenSearch Serverless zuzugreifen. Clients müssen Transport Layer Security (TLS) unterstützen. Wir benötigen

TLS 1.2 und empfehlen TLS 1.3. Eine Liste der unterstützten Verschlüsselungen für TLS 1.3 finden Sie unter TLS-Protokolle und Chiffren in der Elastic Load Balancing Balancing-Dokumentation.

Darüber hinaus müssen Sie Anfragen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signieren, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

Erste Schritte mit der Sicherheit in Amazon OpenSearch Serverless

Die folgenden Tutorials helfen Ihnen bei den ersten Schritten mit Amazon OpenSearch Serverless. In beiden Tutorials werden die gleichen grundlegenden Schritte ausgeführt, aber eines verwendet die Konsole, während das andere die AWS CLI verwendet.

Beachten Sie, dass die Anwendungsfälle in diesen Tutorials vereinfacht sind. Die Netzwerk- und Sicherheitsrichtlinien sind relativ offen. Bei Produktions-Workloads empfehlen wir, robustere Sicherheitsfunktionen wie SAML-Authentifizierung, VPC-Zugriff und restriktive Datenzugriffsrichtlinien zu konfigurieren.

Themen

- Tutorial: Erste Schritte mit der Sicherheit in Amazon OpenSearch Serverless (Konsole)
- Tutorial: Erste Schritte mit der Sicherheit in Amazon OpenSearch Serverless (CLI)

Tutorial: Erste Schritte mit der Sicherheit in Amazon OpenSearch Serverless (Konsole)

Dieses Tutorial führt Sie durch die grundlegenden Schritte zur Erstellung und Verwaltung von Sicherheitsrichtlinien mithilfe der Amazon OpenSearch Serverless-Konsole.

In diesem Tutorial führen Sie die folgenden Schritte aus:

1. Konfigurieren von Berechtigungen
2. Erstellen einer Verschlüsselungsrichtlinie
3. Eine Netzwerkrichtlinie erstellen
4. Konfigurieren einer Datenzugriffsrichtlinie
5. Erstellen einer Sammlung
6. Hochladen und Suchen von Daten

Dieses Tutorial führt Sie durch die Einrichtung einer Sammlung mithilfe von. AWS Management Console Dieselben Schritte mit dem AWS CLI finden Sie unterthe section called “Tutorial: Erste Schritte mit Sicherheit (CLI)”.

Schritt 1: Konfigurieren von Berechtigungen

> **Note**
>
> Sie können diesen Schritt überspringen, wenn Sie bereits eine umfassendere identitätsbasierte Richtlinie verwenden, z. B. `Action":"aoss:*"` oder `Action":"*"`. In Produktionsumgebungen empfehlen wir jedoch, dem Prinzipal der geringsten Berechtigung zu folgen und nur die für die Ausführung einer Aufgabe erforderlichen Mindestberechtigungen zuzuweisen.

Um dieses Tutorial und OpenSearch Serverless im Allgemeinen verwenden zu können, müssen Sie über die richtigen IAM-Berechtigungen verfügen. Ihr Benutzer oder Ihre Rolle muss über eine angefügte identitätsbasierte Richtlinie mit den folgenden Mindestberechtigungen verfügen:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "aoss:ListCollections",
        "aoss:BatchGetCollection",
        "aoss:CreateCollection",
        "aoss:CreateSecurityPolicy",
        "aoss:GetSecurityPolicy",
        "aoss:ListSecurityPolicies",
        "aoss:CreateAccessPolicy",
        "aoss:GetAccessPolicy",
        "aoss:ListAccessPolicies"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
```

```
}
```

Eine vollständige Liste der OpenSearch Serverless-Berechtigungen finden Sie unterthe section called “Identitäts- und Zugriffsverwaltung”.

Schritt 2: Erstellen einer Verschlüsselungsrichtlinie

Verschlüsselungsrichtlinien geben den AWS KMS Schlüssel an, den OpenSearch Serverless zum Verschlüsseln der Sammlung verwendet. Sie können Sammlungen mit einem Von AWS verwalteter Schlüssel oder einem anderen Schlüssel verschlüsseln. Der Einfachheit halber verschlüsseln wir in diesem Tutorial unsere Sammlung mit einem Von AWS verwalteter Schlüssel.

So erstellen Sie eine Verschlüsselungsrichtlinie

1. Öffnen Sie die Amazon OpenSearch Service-Konsole zu https://console.aws.amazon.com/aos/Hause.
2. Erweitern Sie im linken Navigationsbereich Serverless und wählen Sie Encryption policies (Verschlüsselungsrichtlinien).
3. Wählen Sie Create encryption policy (Verschlüsselungsrichtlinie erstellen).
4. Benennen Sie die Richtlinie books-policy (Bücher-Richtlinie). Geben Sie als Beschreibung Encryption policy for books collection (Verschlüsselungsrichtlinie für die Bücher-Sammlung) ein.
5. Geben Sie unter Resources (Ressourcen) den Namen books (Bücher) ein, den Sie Ihrer Sammlung geben werden. Wenn Sie die Richtlinie weiter fassen möchten, können Sie ein Sternchen (`books*`) einfügen, damit die Richtlinie für alle Sammlungen gilt, die mit dem Wort „Bücher“ beginnen.
6. Lassen Sie für Verschlüsselung die Option AWS Eigenen Schlüssel verwenden aktiviert.
7. Wählen Sie Erstellen aus.

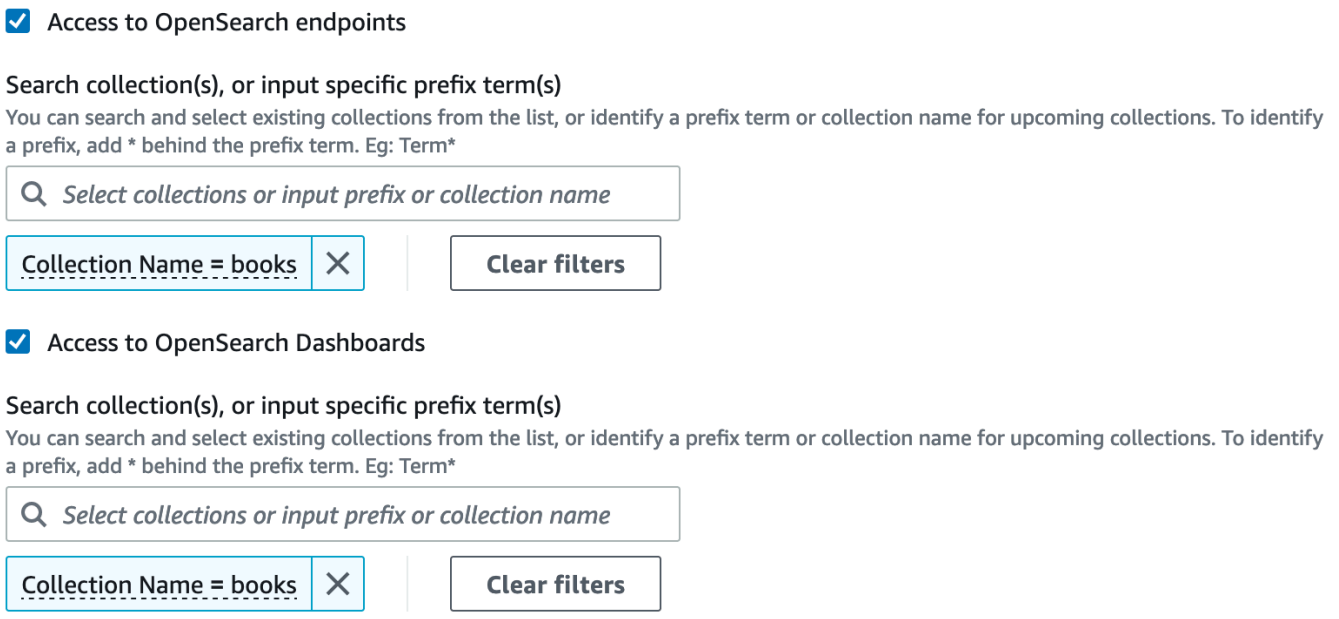
Schritt 3: Erstellen Sie eine Netzwerkrichtlinie

Netzwerkrichtlinien bestimmen, ob auf Ihre Sammlung über das Internet von öffentlichen Netzwerken aus zugegriffen werden kann oder ob der Zugriff über serverlos verwaltete OpenSearch VPC-Endpunkte erfolgen muss. In diesem Tutorial konfigurieren wir den öffentlichen Zugriff.

So erstellen Sie eine Netzwerkrichtlinie

1. Wählen Sie im linken Navigationsbereich Network policies (Netzwerkrichtlinien) und dann Create network policy (Netzwerkrichtlinie erstellen) aus.
2. Benennen Sie die Richtlinie books-policy (Bücher-Richtlinie). Geben Sie als Beschreibung Network policy for books collection (Netzwerkrichtlinie für Bücher-Sammlung) ein.
3. Benennen Sie unter Rule 1 (Regel 1) die Regel Public access for books collection (Öffentlicher Zugriff für Bücher-Sammlung).
4. Der Einfachheit halber konfigurieren wir in diesem Tutorial den öffentlichen Zugriff für die Bücher-Sammlung. Wählen Sie für den Zugriffstyp Public (Öffentlich) aus.
5. Wir werden über Dashboards auf die Sammlung zugreifen. OpenSearch Dazu müssen Sie den Netzwerkzugriff für Dashboards und den OpenSearch Endpunkt konfigurieren, da Dashboards sonst nicht funktionieren.

   Aktivieren Sie für den Ressourcentyp sowohl Zugriff auf OpenSearch Endpunkte als auch Zugriff auf Dashboards. OpenSearch
6. Geben Sie in beiden Eingabefeldern Collection Name = books (Sammlungsname = Bücher) ein. Diese Einstellung schränkt die Richtlinie so ein, dass sie nur für eine einzelne Sammlung gilt (`books`). Ihre Regel sollte folgendermaßen aussehen:



7. Wählen Sie Erstellen aus.

Schritt 4: Erstellen Sie eine Datenzugriffsrichtlinie

Ihre Sammlungsdaten sind erst dann zugänglich, wenn Sie den Zugriff auf die Daten konfigurieren. Datenzugriffsrichtlinien sind von der identitätsbasierten IAM-Richtlinie, die Sie in Schritt 1 konfiguriert haben, getrennt. Diese ermöglichen den Benutzern den Zugriff auf die tatsächlichen Daten innerhalb einer Sammlung.

In diesem Tutorial gewähren wir einem einzelnen Benutzer die Berechtigungen, die zum Indizieren von Daten in der Bücher-Sammlung erforderlich sind.

So erstellen Sie eine Datenzugriffsrichtlinie

1. Wählen Sie im linken Navigationsbereich Data access policies (Datenzugriffsrichtlinien) und anschließend Create access policy (Zugriffsrichtlinie erstellen) aus.
2. Benennen Sie die Richtlinie books-policy (Bücher-Richtlinie). Geben Sie als Beschreibung Data access policy for books collection (Datenzugriffsrichtlinie für die Bücher-Sammlung) ein.
3. Wählen Sie JSON als Methode zur Richtliniendefinition aus und fügen Sie die folgende Richtlinie in den JSON-Editor ein.

   Ersetzen Sie den Haupt-ARN durch den ARN des Kontos, mit dem Sie sich bei OpenSearch Dashboards anmelden und Daten indexieren.

```
[
   {
      "Rules":[
         {
            "ResourceType":"index",
            "Resource":[
               "index/books/*"
            ],
            "Permission":[
               "aoss:CreateIndex",
               "aoss:DescribeIndex",
               "aoss:ReadDocument",
               "aoss:WriteDocument",
               "aoss:UpdateIndex",
               "aoss:DeleteIndex"
            ]
         }
      ],
      "Principal":[
```

```
            "arn:aws:iam::123456789012:user/my-user"
        ]
    }
]
```

Diese Richtlinie gewährt einem einzelnen Benutzer die Mindestberechtigungen, die erforderlich sind, um einen Index in der Bücher-Sammlung zu erstellen, einige Daten zu indizieren und danach zu suchen.

4. Wählen Sie Erstellen aus.

Schritt 5: Erstellen Sie eine Sammlung

Nachdem Sie die Verschlüsselungs- und Netzwerkrichtlinien konfiguriert haben, können Sie eine passende Sammlung erstellen und die Sicherheitseinstellungen werden automatisch darauf angewendet.

Um eine OpenSearch serverlose Sammlung zu erstellen

1. Wählen Sie im linken Navigationsbereich Collections (Sammlungen) und wählen Sie Create collection (Sammlung erstellen) aus.
2. Benennen Sie die Sammlung books (Bücher).
3. Wählen Sie als Sammlungstyp Search (Suchen) aus.
4. Unter Verschlüsselung werden Sie von OpenSearch Serverless darüber informiert, dass der Name der Sammlung der `books-policy` Verschlüsselungsrichtlinie entspricht.
5. Unter Netzwerkzugriffseinstellungen informiert Sie OpenSearch Serverless darüber, dass der Name der Sammlung der `books-policy` Netzwerkrichtlinie entspricht.
6. Wählen Sie Weiter aus.
7. Unter Optionen für Datenzugriffsrichtlinien informiert Sie OpenSearch Serverless darüber, dass der Name der Sammlung der `books-policy` Datenzugriffsrichtlinie entspricht.
8. Wählen Sie Weiter aus.
9. Überprüfen Sie die Sammlungskonfiguration und wählen Sie Submit (Senden) aus. Die Initialisierung von Sammlungen dauert in der Regel weniger als eine Minute.

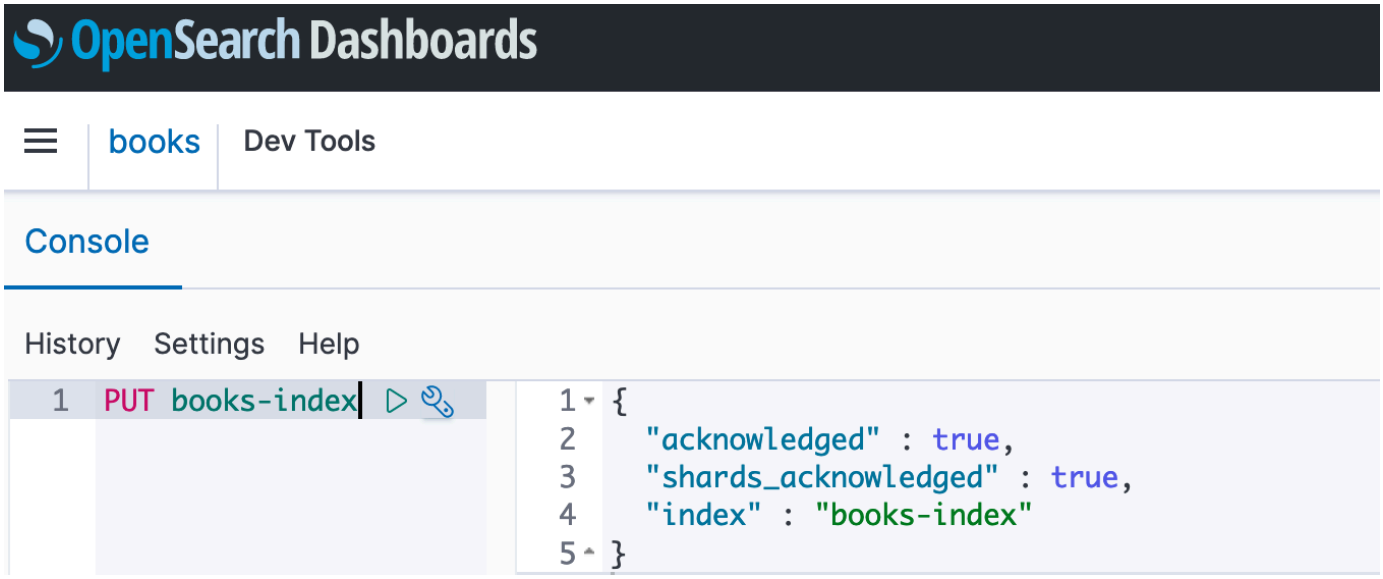
Schritt 6: Hochladen und Suchen von Daten

Sie können Daten mit Postman oder Curl in eine OpenSearch serverlose Sammlung hochladen. Der Kürze halber verwenden diese Beispiele Dev Tools in der Dashboards-Konsole. OpenSearch

So indizieren und suchen Sie Daten in einer Sammlung

1. Wählen Sie im linken Navigationsbereich Collections (Sammlungen) und dann die Bücher-Sammlung aus, um die Detailseite zu öffnen.
2. Wählen Sie die OpenSearch Dashboard-URL für die Sammlung aus. Die URL nimmt das Format `https://collection-id.us-east-1.aoss.amazonaws.com/_dashboards` an.
3. Melden Sie sich mit den AWS Zugriffs- und Geheimschlüsseln für den Principal, die Sie in Ihrer Datenzugriffsrichtlinie angegeben haben, bei OpenSearch Dashboards an.
4. Öffnen Sie in OpenSearch Dashboards das linke Navigationsmenü und wählen Sie Dev Tools aus.
5. Führen Sie den folgenden Befehl aus, um einen einzelnen Index mit dem Namen books-index zu erstellen:

```
PUT books-index
```



6. Führen Sie den folgenden Befehl aus, um ein einzelnes Dokument in books-index zu indizieren:

```
PUT books-index/_doc/1
{
  "title": "The Shining",
```

```
  "author": "Stephen King",
  "year": 1977
}
```

7. Um Daten in OpenSearch Dashboards zu suchen, müssen Sie mindestens ein Indexmuster konfigurieren. OpenSearch verwendet diese Muster, um zu identifizieren, welche Indizes Sie analysieren möchten. Öffnen Sie das Dashboards-Hauptmenü, wählen Sie Stack-Management, wählen Sie Indexmuster und dann Indexmuster erstellen. Geben Sie für dieses Tutorial books-index ein.
8. Wählen Sie Nächster Schritt aus und klicken Sie auf Indexmuster erstellen. Nachdem das Muster erstellt wurde, können Sie die verschiedenen Dokumentfelder anzeigen, z. B. `author` und `title`.
9. Um mit der Suche nach Ihren Daten zu beginnen, öffnen Sie erneut das Hauptmenü und wählen Sie Discover (Erkunden) oder verwenden Sie die Such-API.

Tutorial: Erste Schritte mit der Sicherheit in Amazon OpenSearch Serverless (CLI)

Dieses Tutorial führt Sie durch die im Tutorial Erste Schritte der Konsole zum Thema Sicherheit beschriebenen Schritte, verwendet jedoch die Servicekonsole AWS CLI und nicht die OpenSearch Service-Konsole.

In diesem Tutorial führen Sie die folgenden Schritte durch:

1. Erstellen Sie eine IAM-Berechtigungsrichtlinie
2. Ordnen Sie die IAM-Richtlinie einer IAM-Rolle zu
3. Eine Verschlüsselungsrichtlinie erstellen
4. Eine Netzwerkrichtlinie erstellen
5. Eine Sammlung erstellen
6. Konfigurieren einer Datenzugriffsrichtlinie
7. Rufen Sie den Sammlungsendpunkt ab
8. Laden Sie Daten auf Ihre Verbindung hoch
9. Suchen Sie nach Daten in Ihrer Sammlung

Das Ziel dieses Tutorials besteht darin, eine einzelne OpenSearch serverlose Sammlung mit relativ einfachen Verschlüsselungs-, Netzwerk- und Datenzugriffseinstellungen einzurichten. Beispielsweise

konfigurieren wir den öffentlichen Netzwerkzugriff, eine Von AWS verwalteter Schlüssel für die Verschlüsselung und eine vereinfachte Datenzugriffsrichtlinie, die einem einzelnen Benutzer nur minimale Berechtigungen gewährt.

Erwägen Sie in einem Produktionsumgebung die Implementierung einer robusteren Konfiguration, einschließlich SAML-Authentifizierung, eines benutzerdefinierten Verschlüsselungsschlüssels und VPC-Zugriff.

Um mit Sicherheitsrichtlinien in OpenSearch Serverless zu beginnen

1.
> **Note**
>
> Sie können diesen Schritt überspringen, wenn Sie bereits eine umfassendere identitätsbasierte Richtlinie verwenden, z. B. `Action":"aoss:*"` oder `Action":"*"`. In Produktionsumgebungen empfehlen wir jedoch, dem Prinzipal der geringsten Berechtigung zu folgen und nur die für die Ausführung einer Aufgabe erforderlichen Mindestberechtigungen zuzuweisen.

   Erstellen Sie zunächst eine AWS Identity and Access Management Richtlinie mit den erforderlichen Mindestberechtigungen, um die Schritte in diesem Tutorial auszuführen. Wir werden die Richtlinie `TutorialPolicy` nennen:

```
aws iam create-policy \
  --policy-name TutorialPolicy \
  --policy-document "{\"Version\": \"2012-10-17\",\"Statement\":
 [{\"Action\": [\"aoss:ListCollections\",\"aoss:BatchGetCollection\",
\"aoss:CreateCollection\",\"aoss:CreateSecurityPolicy\",\"aoss:GetSecurityPolicy\",
\"aoss:ListSecurityPolicies\",\"aoss:CreateAccessPolicy\",\"aoss:GetAccessPolicy\",
\"aoss:ListAccessPolicies\"],\"Effect\": \"Allow\",\"Resource\": \"*\"}]}"
```

   Beispielantwort

```
{
    "Policy": {
        "PolicyName": "TutorialPolicy",
        "PolicyId": "ANPAW6WRAECKG6QJWUV7U",
        "Arn": "arn:aws:iam::123456789012:policy/TutorialPolicy",
        "Path": "/",
        "DefaultVersionId": "v1",
```

```
        "AttachmentCount": 0,
        "PermissionsBoundaryUsageCount": 0,
        "IsAttachable": true,
        "CreateDate": "2022-10-16T20:57:18+00:00",
        "UpdateDate": "2022-10-16T20:57:18+00:00"
    }
}
```

2. Fügen Sie `TutorialPolicy` der IAM-Rolle an, die die Daten in der Sammlung indizieren und durchsuchen wird. Wir benennen den Benutzer `TutorialRole`:

```
aws iam attach-role-policy \
  --role-name TutorialRole \
  --policy-arn arn:aws:iam::123456789012:policy/TutorialPolicy
```

3. Bevor Sie eine Sammlung erstellen, müssen Sie eine Verschlüsselungsrichtlinie erstellen, die ein AWS-eigener Schlüssel der in einem späteren Schritt erstellten Bücher-Sammlung zuweist.

   Senden Sie die folgende Anfrage, um eine Verschlüsselungsrichtlinie für die Bücher-Sammlung zu erstellen:

```
aws opensearchserverless create-security-policy \
  --name books-policy \
  --type encryption --policy "{\"Rules\":[{\"ResourceType\":\"collection\",
\"Resource\":[\"collection\/books\"]}],\"AWSOwnedKey\":true}"
```

   Beispielantwort

```
{
    "securityPolicyDetail": {
        "type": "encryption",
        "name": "books-policy",
        "policyVersion": "MTY2OTI0MDAwNTk5MF8x",
        "policy": {
            "Rules": [
                {
                    "Resource": [
                        "collection/books"
                    ],
                    "ResourceType": "collection"
                }
            ],
```

```
            "AWSOwnedKey": true
        },
        "createdDate": 1669240005990,
        "lastModifiedDate": 1669240005990
    }
}
```

4. Erstellen Sie eine Netzwerkrichtlinie, die öffentlichen Zugriff auf die Bücher-Sammlung gewährt:

```
aws opensearchserverless create-security-policy --name books-policy --type network
 \
  --policy "[{\"Description\":\"Public access for books collection\",\"Rules
\":[{\"ResourceType\":\"dashboard\",\"Resource\":[\"collection\/books\"]},
{\"ResourceType\":\"collection\",\"Resource\":[\"collection\/books\"]}],
\"AllowFromPublic\":true}]"
```

Beispielantwort

```
{
    "securityPolicyDetail": {
        "type": "network",
        "name": "books-policy",
        "policyVersion": "MTY2OTI0MDI1Njk1NV8x",
        "policy": [
            {
                "Rules": [
                    {
                        "Resource": [
                            "collection/books"
                        ],
                        "ResourceType": "dashboard"
                    },
                    {
                        "Resource": [
                            "collection/books"
                        ],
                        "ResourceType": "collection"
                    }
                ],
                "AllowFromPublic": true,
                "Description": "Public access for books collection"
            }
        ],
```

```
        "createdDate": 1669240256955,
        "lastModifiedDate": 1669240256955
    }
}
```

5. Erstellen Sie die Bücher-Sammlung:

```
aws opensearchserverless create-collection --name books --type SEARCH
```

Beispielantwort

```
{
    "createCollectionDetail": {
        "id": "8kw362bpwg4gx9b2f6e0",
        "name": "books",
        "status": "CREATING",
        "type": "SEARCH",
        "arn": "arn:aws:aoss:us-
east-1:123456789012:collection/8kw362bpwg4gx9b2f6e0",
        "kmsKeyArn": "auto",
        "createdDate": 1669240325037,
        "lastModifiedDate": 1669240325037
    }
}
```

6. Erstellen Sie eine Datenzugriffsrichtlinie, die die Mindestberechtigungen zum Indizieren und Suchen von Daten in der Bücher-Sammlung bereitstellt. Ersetzen Sie den Prinzipal-ARN durch den ARN von `TutorialRole` aus Schritt 1:

```
aws opensearchserverless create-access-policy \
  --name books-policy \
  --type data \
  --policy "[{\"Rules\":[{\"ResourceType\":\"index\",\"Resource\":
[\"index\/books\/books-index\"],\"Permission\":[\"aoss:CreateIndex
\",\"aoss:DescribeIndex\",\"aoss:ReadDocument\",\"aoss:WriteDocument
\",\"aoss:UpdateIndex\",\"aoss:DeleteIndex\"]}],\"Principal\":
[\"arn:aws:iam::123456789012:role\/TutorialRole\"]}]"
```

Beispielantwort

```
{
    "accessPolicyDetail": {
```

```
        "type": "data",
        "name": "books-policy",
        "policyVersion": "MTY2OTI0MDM5NDY1M18x",
        "policy": [
            {
                "Rules": [
                    {
                        "Resource": [
                            "index/books/books-index"
                        ],
                        "Permission": [
                            "aoss:CreateIndex",
                            "aoss:DescribeIndex",
                            "aoss:ReadDocument",
                            "aoss:WriteDocument",
                            "aoss:UpdateDocument",
                            "aoss:DeleteDocument"
                        ],
                        "ResourceType": "index"
                    }
                ],
                "Principal": [
                    "arn:aws:iam::123456789012:role/TutorialRole"
                ]
            }
        ],
        "createdDate": 1669240394653,
        "lastModifiedDate": 1669240394653
    }
}
```

`TutorialRole` sollte nun in der Lage sein, Dokumente in der Bücher-Sammlung zu indizieren und zu durchsuchen.

7. Um Aufrufe an die OpenSearch API zu tätigen, benötigen Sie den Sammlungsendpunkt. Senden Sie die folgende Anfrage, um den `collectionEndpoint`-Parameter abzurufen:

```
aws opensearchserverless batch-get-collection --names books
```

Beispielantwort

```
{
```

```
    "collectionDetails": [
        {
            "id": "8kw362bpwg4gx9b2f6e0",
            "name": "books",
            "status": "ACTIVE",
            "type": "SEARCH",
            "description": "",
            "arn": "arn:aws:aoss:us-
east-1:123456789012:collection/8kw362bpwg4gx9b2f6e0",
            "createdDate": 1665765327107,
            "collectionEndpoint": "https://8kw362bpwg4gx9b2f6e0.us-
east-1.aoss.amazonaws.com",
            "dashboardEndpoint": "https://8kw362bpwg4gx9b2f6e0.us-
east-1.aoss.amazonaws.com/_dashboards"
        }
    ],
    "collectionErrorDetails": []
}
```

> **Note**
>
> Sie können den Sammlungsendpunkt erst sehen, wenn sich der Sammlungsstatus zu `ACTIVE` ändert. Möglicherweise müssen Sie mehrere Aufrufe durchführen, um den Status zu überprüfen, bis die Sammlung erfolgreich erstellt wurde.

8. Verwenden Sie ein HTTP-Tool wie Postman oder curl, um Daten in der Bücher-Sammlung zu indizieren. Wir erstellen einen Index mit dem Namen books-index und fügen ein einzelnes Dokument hinzu.

   Senden Sie die folgende Anforderung mit den Anmeldeinformationen für `TutorialRole` an den Sammlungsendpunkt, den Sie im vorherigen Schritt abgerufen haben.

```
PUT https://8kw362bpwg4gx9b2f6e0.us-east-1.aoss.amazonaws.com/books-index/_doc/1
{
  "title": "The Shining",
  "author": "Stephen King",
  "year": 1977
}
```

   Beispielantwort

```
{
  "_index" : "books-index",
  "_id" : "1",
  "_version" : 1,
  "result" : "created",
  "_shards" : {
    "total" : 0,
    "successful" : 0,
    "failed" : 0
  },
  "_seq_no" : 0,
  "_primary_term" : 0
}
```

9. Verwenden Sie die Such-API, um mit der Suche nach Daten in Ihrer Sammlung zu beginnen. Die folgende Abfrage führt eine einfache Suche durch:

```
GET https://8kw362bpwg4gx9b2f6e0.us-east-1.aoss.amazonaws.com/books-index/_search
```

Beispielantwort

```
{
    "took": 405,
    "timed_out": false,
    "_shards": {
        "total": 6,
        "successful": 6,
        "skipped": 0,
        "failed": 0
    },
    "hits": {
        "total": {
            "value": 2,
            "relation": "eq"
        },
        "max_score": 1.0,
        "hits": [
            {
                "_index": "books-index:0::3xJq14MBUaOS0wL26UU9:0",
                "_id": "F_bt4oMBLle5pYmm5q4T",
                "_score": 1.0,
```

```
                "_source": {
                    "title": "The Shining",
                    "author": "Stephen King",
                    "year": 1977
                }
            }
        ]
    }
}
```

Identity and Access Management für Amazon OpenSearch Serverless

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf Ressourcen sicher zu kontrollieren. AWS IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um serverlose Ressourcen zu verwenden OpenSearch . IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Themen

- Identitätsbasierte Richtlinien für Serverless OpenSearch
- Richtlinienaktionen für Serverless OpenSearch
- Richtlinienressourcen für Serverless OpenSearch
- Schlüssel für Richtlinienbedingungen für Amazon OpenSearch Serverless
- ABAC mit Serverless OpenSearch
- Temporäre Anmeldeinformationen mit Serverless verwenden OpenSearch
- Mit Diensten verknüpfte Rollen für Serverless OpenSearch
- Weitere Richtlinientypen
- Beispiele für identitätsbasierte Richtlinien für Serverless OpenSearch
- IAM Identity Center-Unterstützung für Amazon Serverless OpenSearch

Identitätsbasierte Richtlinien für Serverless OpenSearch

Unterstützt Richtlinien auf Identitätsbasis: Ja

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern,

welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Beispiele für identitätsbasierte Richtlinien für Serverless OpenSearch

Beispiele für identitätsbasierte Richtlinien OpenSearch ohne Server finden Sie unter. the section called “Beispiele für identitätsbasierte Richtlinien”

Richtlinienaktionen für Serverless OpenSearch

Unterstützt Richtlinienaktionen: Ja

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie der zugehörige AWS API-Vorgang. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keinen passenden API-Vorgang gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Bei Richtlinienaktionen in OpenSearch Serverless wird vor der Aktion das folgende Präfix verwendet:

```
aoss
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

```
"Action": [
      "aoss:action1",
      "aoss:action2"
         ]
```

Sie können mehrere Aktionen mit Platzhalterzeichen (*) angeben. Beispielsweise können Sie alle Aktionen festlegen, die mit dem Wort `Describe` beginnen, einschließlich der folgenden Aktion:

```
"Action": "aoss:List*"
```

Beispiele für identitätsbasierte OpenSearch Richtlinien ohne Server finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Serverless OpenSearch

Richtlinienressourcen für Serverless OpenSearch

Unterstützt Richtlinienressourcen: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Anweisungen müssen entweder ein – `Resource`oder ein `NotResource`-Element enthalten. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

```
"Resource": "*"
```

Schlüssel für Richtlinienbedingungen für Amazon OpenSearch Serverless

Unterstützt servicespezifische Richtlinienbedingungsschlüssel: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition` block) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen `AND`-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, AWS wertet die Bedingung mithilfe einer logischen `OR` Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter IAM-Richtlinienelemente: Variablen und Tags im IAM-Benutzerhandbuch.

AWS unterstützt globale Bedingungsschlüssel und dienstspezifische Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

Neben der attributebasierten Zugriffskontrolle (ABAC) unterstützt OpenSearch Serverless die folgenden Bedingungsschlüssel:

- `aoss:collection`
- `aoss:CollectionId`
- `aoss:index`

Sie können diese Bedingungsschlüssel auch beim Bereitstellen von Berechtigungen für Zugriffsrichtlinien und Sicherheitsrichtlinien verwenden. Zum Beispiel:

```
[
   {
      "Effect":"Allow",
      "Action":[
         "aoss:CreateAccessPolicy",
         "aoss:CreateSecurityPolicy"
      ],
      "Resource":"*",
      "Condition":{
         "StringLike":{
            "aoss:collection":"log"
         }
      }
   }
]
```

In diesem Beispiel gilt die Bedingung für Richtlinien, die Regeln enthalten, die mit einem Sammlungsnamen oder -muster übereinstimmen. Die Bedingungen haben das folgende Verhalten:

- `StringEquals` – Gilt für Richtlinien mit Regeln, die die exakte Ressourcenzeichenfolge „log“ (d. h. `collection/log`) enthalten.
- `StringLike` – Gilt für Richtlinien mit Regeln, die eine Ressourcenzeichenfolge enthalten, die die Zeichenfolge „log“ enthält (d. h. `collection/log`, aber auch `collection/logs-application` oder `collection/applogs123`).

> **Note**
>
> Bedingungsschlüssel für Sammlungen gelten nicht auf der Indexebene. In der obigen Richtlinie würde die Bedingung beispielsweise nicht auf eine Zugriffs- oder Sicherheitsrichtlinie gelten, die die Ressourcenzeichenfolge `index/logs-application/*` enthält.

Eine Liste der OpenSearch Serverless-Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für Amazon OpenSearch Serverless in der Service Authorization Reference. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Von Amazon OpenSearch Serverless definierte Aktionen.

ABAC mit Serverless OpenSearch

Unterstützt ABAC (Tags in Richtlinien): Ja

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In AWS werden diese Attribute als Tags bezeichnet. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und an viele AWS Ressourcen anhängen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt von ABAC. Anschließend entwerfen Sie ABAC-Richtlinien, um Operationen zuzulassen, wenn das Tag des Prinzipals mit dem Tag der Ressource übereinstimmt, auf die sie zugreifen möchten.

ABAC ist in Umgebungen hilfreich, die schnell wachsen, und unterstützt Sie in Situationen, in denen die Richtlinienverwaltung mühsam wird.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, oder Bedingung `aws:TagKeys` verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu ABAC finden Sie unter Definieren von Berechtigungen mit ABAC-Autorisierung im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe Attributbasierte Zugriffskontrolle (ABAC) verwenden im IAM-Benutzerhandbuch.

Weitere Informationen zum Taggen OpenSearch serverloser Ressourcen finden Sie unter. the section called “Markieren von Sammlungen”

Temporäre Anmeldeinformationen mit Serverless verwenden OpenSearch

Unterstützt temporäre Anmeldeinformationen: Ja

Einige funktionieren AWS-Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich Informationen, die mit temporären Anmeldeinformationen AWS-Services funktionieren AWS-Services , finden Sie im IAM-Benutzerhandbuch unter Diese Option funktioniert mit IAM.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS Management Console Methode als einem Benutzernamen und einem Passwort anmelden. Wenn Sie beispielsweise AWS über den Single Sign-On-Link (SSO) Ihres Unternehmens darauf zugreifen, werden bei diesem Vorgang automatisch temporäre Anmeldeinformationen erstellt. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Wechseln von Rollen finden Sie unter Wechseln von einer Benutzerrolle zu einer IAM-Rolle (Konsole) im IAM-Benutzerhandbuch.

Mithilfe der AWS API AWS CLI oder können Sie temporäre Anmeldeinformationen manuell erstellen. Sie können diese temporären Anmeldeinformationen dann für den Zugriff verwenden AWS. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen in IAM.

Mit Diensten verknüpfte Rollen für Serverless OpenSearch

Unterstützt dienstverknüpfte Rollen: Ja

Eine serviceverknüpfte Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen.

Dienstbezogene Rollen werden in Ihrem Dienst angezeigt AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Einzelheiten zum Erstellen und Verwalten OpenSearch serverloser dienstbezogener Rollen finden Sie unter. the section called “Rolle bei der Sammlungserstellung”

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger verbreitete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- Dienststeuerungsrichtlinien (SCPs) — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen. AWS Organizations AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer AWS Konten, die Ihrem Unternehmen gehören. Wenn Sie alle Funktionen in einer Organisation aktivieren, können Sie Richtlinien zur Servicesteuerung (SCPs) auf einige oder alle Ihre Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen AWS Root-Benutzer. Weitere Informationen zu Organizations und SCPs finden Sie unter Richtlinien zur Servicesteuerung im AWS Organizations Benutzerhandbuch.
- Ressourcenkontrollrichtlinien (RCPs) — RCPs sind JSON-Richtlinien, mit denen Sie die maximal verfügbaren Berechtigungen für Ressourcen in Ihren Konten festlegen können, ohne die IAM-Richtlinien aktualisieren zu müssen, die jeder Ressource zugeordnet sind, deren Eigentümer Sie sind. Das RCP schränkt die Berechtigungen für Ressourcen in Mitgliedskonten ein und kann sich auf die effektiven Berechtigungen für Identitäten auswirken, einschließlich des Root-Benutzers des AWS Kontos, unabhängig davon, ob diese zu Ihrer Organisation gehören. Weitere Informationen zu Organizations sowie RCPs eine Liste der unterstützten AWS RCPs Dienste finden Sie unter Resource Control Policies (RCPs) im AWS Organizations Benutzerhandbuch.

Beispiele für identitätsbasierte Richtlinien für Serverless OpenSearch

Standardmäßig sind Benutzer und Rollen nicht berechtigt, serverlose Ressourcen zu erstellen oder zu ändern OpenSearch . Sie können auch keine Aufgaben mithilfe der AWS Management Console, AWS Command Line Interface (AWS CLI) oder AWS API ausführen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von IAM-Richtlinien (Konsole) im IAM-Benutzerhandbuch.

Einzelheiten zu den von Amazon OpenSearch Serverless definierten Aktionen und Ressourcentypen, einschließlich des Formats ARNs für die einzelnen Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon OpenSearch Serverless in der Service Authorization Reference.

Themen

- Bewährte Methoden für Richtlinien
- Serverless in der Konsole verwenden OpenSearch
- Verwaltung serverloser Sammlungen OpenSearch
- Serverlose Sammlungen anzeigen OpenSearch
- OpenSearchAPI-Operationen verwenden
- ABAC für API-Operationen OpenSearch

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien sind sehr leistungsfähig. Sie bestimmen, ob jemand OpenSearch Serverless-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

Identitätsbasierte Richtlinien legen fest, ob jemand OpenSearch serverlose Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um Ihren Benutzern und Workloads zunächst Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien oder AWS -verwaltete Richtlinien für Auftrags-Funktionen im IAM-Benutzerhandbuch.

- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. AWS CloudFormation B. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung mit IAM Access Analyzer im IAM-Benutzerhandbuch.
- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Sicherer API-Zugriff mit MFA im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Serverless in der Konsole verwenden OpenSearch

Um über die OpenSearch Servicekonsole auf OpenSearch Serverless zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den OpenSearch Serverless-Ressourcen in Ihrem AWS Konto aufzulisten

und einzusehen. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (wie IAM-Rollen) mit dieser Richtlinie.

Sie müssen Benutzern, die nur die API AWS CLI oder die AWS API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die der API-Operation entsprechen, die Sie ausführen möchten.

Die folgende Richtlinie ermöglicht einem Benutzer den Zugriff auf OpenSearch Serverless innerhalb der OpenSearch Servicekonsole:

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Resource": "*",
            "Effect": "Allow",
            "Action": [
                "aoss:ListCollections",
                "aoss:BatchGetCollection",
                "aoss:ListAccessPolicies",
                "aoss:ListSecurityConfigs",
                "aoss:ListSecurityPolicies",
                "aoss:ListTagsForResource",
                "aoss:ListVpcEndpoints",
                "aoss:GetAccessPolicy",
                "aoss:GetAccountSettings",
                "aoss:GetSecurityConfig",
                "aoss:GetSecurityPolicy"
            ]
        }
    ]
}
```

Verwaltung serverloser Sammlungen OpenSearch

Diese Richtlinie ist ein Beispiel für eine „Sammlungsadministrator“ -Richtlinie, die es einem Benutzer ermöglicht, Amazon OpenSearch Serverless-Sammlungen zu verwalten und zu verwalten. Der Benutzer kann Sammlungen erstellen, anzeigen und löschen.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Resource": "arn:aws:aoss:region:123456789012:collection/*",
            "Action": [
                "aoss:CreateCollection",
                "aoss:DeleteCollection",
                "aoss:UpdateCollection"
            ],
            "Effect": "Allow"
        },
        {
            "Resource": "*",
            "Action": [
                "aoss:BatchGetCollection",
                "aoss:ListCollections",
                "aoss:CreateAccessPolicy",
                "aoss:CreateSecurityPolicy"
            ],
            "Effect": "Allow"
        }
    ]
}
```

Serverlose Sammlungen anzeigen OpenSearch

Diese Beispielrichtlinie ermöglicht es einem Benutzer, Details für alle Amazon OpenSearch Serverless-Sammlungen in seinem Konto einzusehen. Der Benutzer kann die Sammlungen oder die zugeordneten Sicherheitsrichtlinien nicht ändern.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Resource": "*",
```

```
            "Action": [
                "aoss:ListAccessPolicies",
                "aoss:ListCollections",
                "aoss:ListSecurityPolicies",
                "aoss:ListTagsForResource",
                "aoss:BatchGetCollection"
            ],
            "Effect": "Allow"
        }
    ]
}
```

OpenSearchAPI-Operationen verwenden

API-Operationen auf Datenebene bestehen aus den Funktionen, die Sie in OpenSearch Serverless verwenden, um Echtzeitwerte aus dem Dienst abzuleiten. API-Operationen auf der Kontrollebene bestehen aus den Funktionen, mit denen Sie die Umgebung einrichten.

Um über den Browser auf Amazon OpenSearch Serverless Data Plane APIs und OpenSearch Dashboards zuzugreifen, müssen Sie zwei IAM-Berechtigungen für Sammelressourcen hinzufügen. Diese Berechtigungen sind und. `aoss:APIAccessAll` `aoss:DashboardsAccessAll`

> **Note**
>
> Ab dem 10. Mai 2023 benötigt OpenSearch Serverless diese beiden neuen IAM-Berechtigungen für Sammlungsressourcen. Die `aoss:APIAccessAll` Berechtigung ermöglicht den Zugriff auf die Datenebene, und die `aoss:DashboardsAccessAll` Berechtigung ermöglicht OpenSearch Dashboards vom Browser aus. Wenn die beiden neuen IAM-Berechtigungen nicht hinzugefügt werden, wird ein 403-Fehler angezeigt.

Diese Beispielrichtlinie ermöglicht es einem Benutzer, auf die Datenebene APIs für eine bestimmte Sammlung in seinem Konto zuzugreifen und auf OpenSearch Dashboards für alle Sammlungen in seinem Konto zuzugreifen.

JSON

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
         {
            "Effect": "Allow",
            "Action": "aoss:APIAccessAll",
            "Resource": "arn:aws:aoss:region:account-id:collection/collection-id"
        },
        {
            "Effect": "Allow",
            "Action": "aoss:DashboardsAccessAll",
            "Resource": "arn:aws:aoss:region:account-id:dashboards/default"
        }
    ]
}
```

Beides `aoss:APIAccessAll` und `aoss:DashboardsAccessAll` gewährt volle IAM-Berechtigungen für die Sammlungsressourcen, während die Dashboard-Berechtigung auch Zugriff auf Dashboards gewährt OpenSearch . Jede Berechtigung funktioniert unabhängig voneinander, sodass eine ausdrückliche Verweigerung `aoss:APIAccessAll` nicht den `aoss:DashboardsAccessAll` Zugriff auf die Ressourcen, einschließlich der Entwicklungstools, blockiert. Das Gleiche gilt für die Option „Ablehnen`aoss:DashboardsAccessAll`“. OpenSearch Serverless unterstützt die folgenden globalen Bedingungsschlüssel:

- `aws:CalledVia`
- `aws:CalledViaAWSService`
- `aws:CalledViaFirst`
- `aws:CalledViaLast`
- `aws:CurrentTime`
- `aws:EpochTime`
- `aws:PrincipalAccount`
- `aws:PrincipalArn`
- `aws:PrincipallsAWSService`
- `aws:PrincipalOrgID`
- `aws:PrincipalOrgPaths`
- `aws:PrincipalType`
- `aws:PrincipalServiceName`

- aws:PrincipalServiceNamesList
- aws:ResourceAccount
- aws:ResourceOrgID
- aws:ResourceOrgPaths
- aws:RequestedRegion
- aws:ResourceTag
- aws:SourceIp
- aws:SourceVpce
- aws:SourceVpc
- aws:userid
- aws:username

Im Folgenden finden Sie ein Beispiel für die Verwendung aws:SourceIp im Bedingungsblock in der IAM-Richtlinie Ihres Prinzipals für Aufrufe auf Datenebene:

```
"Condition": {
    "IpAddress": {
         "aws:SourceIp": "203.0.113.0"
    }
}
```

Im Folgenden finden Sie ein Beispiel für die Verwendung aws:SourceVpc im Bedingungsblock in der IAM-Richtlinie Ihres Prinzipals für Datenebenenanrufe:

```
"Condition": {
    "StringEquals": {
        "aws:SourceVpc": "vpc-0fdd2445d8EXAMPLE"
    }
}
```

Darüber hinaus wird Unterstützung für die folgenden OpenSearch serverlosen Schlüssel angeboten:

- aoss:CollectionId
- aoss:collection

Im Folgenden finden Sie ein Beispiel für die Verwendung `aoss:collection` im Bedingungsblock in der IAM-Richtlinie Ihres Prinzipals für Aufrufe auf Datenebene:

```
"Condition": {
    "StringLike": {
         "aoss:collection": "log-*"
    }
}
```

ABAC für API-Operationen OpenSearch

Mit identitätsbasierten Richtlinien können Sie Tags verwenden, um den Zugriff auf die Amazon OpenSearch Serverless-Datenebene zu kontrollieren. APIs Die folgende Richtlinie ist ein Beispiel dafür, dass verbundene Principals auf die Datenebene zugreifen können, APIs wenn die Sammlung über das Tag verfügt: `team:devops`

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "aoss:APIAccessAll",
            "Resource": "arn:aws:aoss:region:account-id:collection/collection-
id",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/team": "devops"
                }
            }
        }
    ]
}
```

Die folgende Richtlinie ist ein Beispiel dafür, verbundenen Prinzipalen den Zugriff auf Datenebene APIs und Dashboards zu verweigern, wenn die Sammlung über das Tag verfügt: `environment:production`

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "aoss:APIAccessAll",
                "aoss:DashboardsAccessAll",
            ],
            "Resource": "arn:aws:aoss:region:account-id:collection/collection-id",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/environment": "production"
                }
            }
        }
    ]
}
```

Amazon OpenSearch Serverless unterstützt `RequestTag` keine `TagKeys` globalen Bedingungsschlüssel für die Datenebene APIs.

IAM Identity Center-Unterstützung für Amazon Serverless OpenSearch

IAM Identity Center-Unterstützung für Amazon Serverless OpenSearch

Sie können IAM Identity Center-Prinzipale (Benutzer und Gruppen) verwenden, um über Amazon Applications auf Amazon OpenSearch Serverless-Daten zuzugreifen. OpenSearch Um die IAM Identity Center-Unterstützung für Amazon OpenSearch Serverless zu aktivieren, müssen Sie die Verwendung von IAM Identity Center aktivieren. Weitere Informationen dazu finden Sie unter Was ist IAM Identity Center?

Nachdem die IAM Identity Center-Instance erstellt wurde, muss der Administrator des Kundenkontos eine IAM Identity Center-Anwendung für den Amazon OpenSearch Serverless-Service erstellen. Dies kann durch Aufrufen von: erfolgen. CreateSecurityConfig Der Administrator des Kundenkontos kann angeben, welche Attribute für die Autorisierung der Anfrage verwendet werden. Die verwendeten Standardattribute sind und `UserId` `GroupId`.

Die IAM Identity Center-Integration für Amazon OpenSearch Serverless verwendet die folgenden AWS IAM Identity Center (IAM) -Berechtigungen:

- `aoss:CreateSecurityConfig`— Erstellen Sie einen IAM Identity Center-Anbieter
- `aoss:ListSecurityConfig`— Listet alle IAM Identity Center-Anbieter im aktuellen Konto auf.

- `aoss:GetSecurityConfig`— IAM Identity Center-Anbieterinformationen anzeigen.
- `aoss:UpdateSecurityConfig`— Ändern Sie eine bestimmte IAM Identity Center-Konfiguration
- `aoss:DeleteSecurityConfig`— Löscht einen IAM Identity Center-Anbieter.

Die folgende identitätsbasierte Zugriffsrichtlinie kann zur Verwaltung aller IAM Identity Center-Konfigurationen verwendet werden:

JSON

```
{
"Version": "2012-10-17",
    "Statement": [
        {
"Action": [
                "aoss:CreateSecurityConfig",
                "aoss:DeleteSecurityConfig",
                "aoss:GetSecurityConfig",
                "aoss:UpdateSecurityConfig",
                "aoss:ListSecurityConfigs"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

> **Note**
>
> Das `Resource` Element muss ein Platzhalter sein.

Einen IAM Identity Center-Anbieter (Konsole) erstellen

Sie können einen IAM Identity Center-Anbieter erstellen, um die Authentifizierung mit OpenSearch der Anwendung zu ermöglichen. Gehen Sie wie folgt vor, um die IAM Identity Center-Authentifizierung für OpenSearch Dashboards zu aktivieren:

1. Melden Sie sich bei der Amazon OpenSearch Service-Konsole an.

2. Erweitern Sie im linken Navigationsbereich Serverless und wählen Sie Authentifizierung aus.
3. Wählen Sie IAM Identity Center-Authentifizierung.
4. Wählen Sie Bearbeiten
5. Markieren Sie das Kästchen neben Mit IAM Identity Center authentifizieren.
6. Wählen Sie den Benutzer- und Gruppenattributschlüssel aus dem Dropdownmenü aus. Benutzerattribute werden verwendet, um Benutzer auf der Grundlage von `UserName` `UserId`, und zu autorisieren. `Email` Gruppenattribute werden verwendet, um Benutzer auf `GroupName` der Grundlage von und zu authentifizieren. `GroupId`
7. Wählen Sie die IAM Identity Center-Instanz aus.
8. Wählen Sie Speichern

Der IAM Identity Center-Anbieter wird erstellt ()AWS CLI

Verwenden Sie den folgenden Befehl, um einen IAM Identity Center-Anbieter mithilfe von AWS Command Line Interface (AWS CLI) zu erstellen:

```
aws opensearchserverless create-security-config \
--region us-east-2 \
--name "iamidentitycenter-config" \
--description "description" \
--type "iamidentitycenter" \
--iam-identity-center-options '{
    "instanceArn": "arn:aws:sso:::instance/ssoins-99199c99e99ee999",
    "userAttribute": "UserName",
    "groupAttribute": "GroupId"
}'
```

Nachdem ein IAM Identity Center aktiviert wurde, können Kunden nur Benutzer- und Gruppenattribute ändern.

```
aws opensearchserverless update-security-config \
--region us-east-1 \
--id <id_from_list_security_configs> \
--config-version <config_version_from_get_security_config> \
--iam-identity-center-options-updates '{
    "userAttribute": "UserId",
    "groupAttribute": "GroupId"
}'
```

Verwenden Sie den folgenden Befehl, um den IAM Identity Center-Anbieter mithilfe von anzuzeigen: AWS Command Line Interface

```
aws opensearchserverless list-security-configs --type iamidentitycenter
```

Löschen eines IAM Identity Center-Anbieters

IAM Identity Center bietet zwei Instanzen von Anbietern, eine für Ihr Organisationskonto und eine für Ihr Mitgliedskonto. Wenn Sie Ihre IAM Identity Center-Instanz ändern müssen, müssen Sie Ihre Sicherheitskonfiguration über die `DeleteSecurityConfig` API löschen und mithilfe der neuen IAM Identity Center-Instanz eine neue Sicherheitskonfiguration erstellen. Der folgende Befehl kann verwendet werden, um einen IAM Identity Center-Anbieter zu löschen:

```
aws opensearchserverless delete-security-config \
--region us-east-1 \
--id <id_from_list_security_configs>
```

Gewähren Sie dem IAM Identity Center Zugriff auf Sammlungsdaten

Nachdem Ihr IAM Identity Center-Anbieter aktiviert wurde, können Sie die Zugriffsrichtlinie für Sammlungsdaten so aktualisieren, dass sie IAM Identity Center-Prinzipale einbezieht. Die IAM Identity Center-Prinzipale müssen im folgenden Format aktualisiert werden:

```
[
   {
"Rules":[
       ...
      ],
      "Principal":[
         "iamidentitycenter/<iamidentitycenter-instance-id>/user/<UserName>",
         "iamidentitycenter/<iamidentitycenter-instance-id>/group/<GroupId>"
      ]
   }
]
```

> **Note**
>
> Amazon OpenSearch Serverless unterstützt nur eine IAM Identity Center-Instance für alle Kundensammlungen und kann bis zu 100 Gruppen für einen einzelnen Benutzer unterstützen. Wenn Sie versuchen, mehr als die zulässige Anzahl von Instances zu

verwenden, kommt es zu Inkonsistenzen bei der Autorisierungsverarbeitung Ihrer Datenzugriffsrichtlinie und Sie erhalten eine `403` Fehlermeldung.

Sie können Zugriff auf Sammlungen, Indizes oder beides gewähren. Wenn Sie möchten, dass verschiedene Benutzer unterschiedliche Berechtigungen haben, müssen Sie mehrere Regeln erstellen. Eine Liste der verfügbaren Berechtigungen finden Sie unter Identity and Access Management in Amazon OpenSearch Service. Informationen zum Formatieren einer Zugriffsrichtlinie finden Sie unter SAML-Identitäten Zugriff auf Sammlungsdaten gewähren.

IAM Identity Center bietet zwei Instanzen von Anbietern, eine für Ihr Organisationskonto und eine für Ihr Mitgliedskonto. Wenn Sie Ihre IAM Identity Center-Instanz ändern müssen, müssen Sie Ihre Sicherheitskonfiguration über die `DeleteSecurityConfig` API löschen und mithilfe der neuen IAM Identity Center-Instanz eine neue Sicherheitskonfiguration erstellen. Der folgende Befehl kann verwendet werden, um einen IAM Identity Center-Anbieter zu löschen:

```
aws opensearchserverless delete-security-config \
--region us-east-1 \
--id <id_from_list_security_configs>
```

Verschlüsselung in Amazon OpenSearch Serverless

Verschlüsselung im Ruhezustand

Jede Amazon OpenSearch Serverless-Sammlung, die Sie erstellen, ist durch Verschlüsselung ruhender Daten geschützt. Diese Sicherheitsfunktion verhindert unbefugten Zugriff auf Ihre Daten. Encryption at Rest verwendet AWS Key Management Service (AWS KMS), um Ihre Verschlüsselungsschlüssel zu speichern und zu verwalten. Es verwendet den Advanced-Encryption-Standard-Algorithmus mit 256-Bit-Schlüsseln (AES-256) zur Durchführung der Verschlüsselung.

Themen

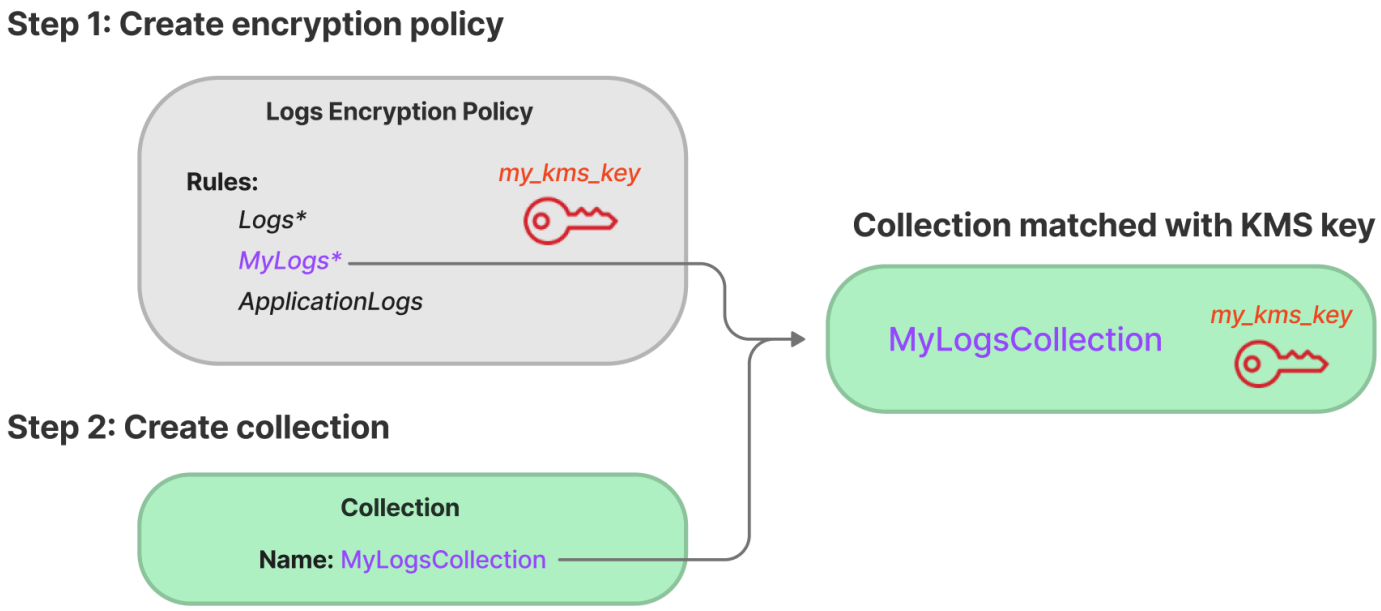
- Verschlüsselungsrichtlinien
- Überlegungen
- Erforderliche Berechtigungen
- Schlüsselrichtlinie für einen kundenverwalteten Schlüssel
- So verwendet Serverless Grants in OpenSearch AWS KMS
- Erstellen von Verschlüsselungsrichtlinien (Konsole)

- Erstellen von Verschlüsselungsrichtlinien (AWS CLI)
- Anzeigen von Verschlüsselungsrichtlinien
- Aktualisieren von Verschlüsselungsrichtlinien
- Aktualisieren von Verschlüsselungsrichtlinien

Verschlüsselungsrichtlinien

Mit Verschlüsselungsrichtlinien können Sie viele Sammlungen in großem Umfang verwalten. Dazu weisen Sie neu erstellten Sammlungen, die einem bestimmten Namen oder Muster entsprechen, automatisch einen Verschlüsselungsschlüssel zu.

Wenn Sie eine Verschlüsselungsrichtlinie erstellen, können Sie entweder ein Präfix angeben, bei dem es sich um eine auf Platzhaltern basierende Abgleichregel wie `MyCollection*` handelt, oder einen einzelnen Sammlungsnamen eingeben. Wenn Sie dann eine Sammlung erstellen, die mit diesem Namen oder Präfixmuster übereinstimmt, werden ihr automatisch die Richtlinie und der entsprechende KMS-Schlüssel zugewiesen.



Verschlüsselungsrichtlinien unterstützen die folgenden Elemente:

- `Rules` – eine oder mehrere Regeln für den Sammlungsabgleich, jeweils mit den folgenden Unterelementen:
  - `ResourceType` – Derzeit ist die einzige Option „Sammlung“. Verschlüsselungsrichtlinien gelten nur für Sammlungsressourcen.

  - `Resource` – Ein oder mehrere Sammlungsnamen oder Muster, auf die die Richtlinie angewendet wird, im Format `collection/<collection name|pattern>`.
- `AWSOwnedKey` – Ob ein AWS-eigener Schlüssel verwendet werden soll.
- `KmsARN` – Wenn Sie `AWSOwnedKey` auf „falsch“ festlegen, geben Sie den Amazon-Ressourcennamen (ARN) des KMS-Schlüssels an, mit dem die zugehörigen Sammlungen verschlüsselt werden sollen. Wenn Sie diesen Parameter angeben, ignoriert OpenSearch Serverless den `AWSOwnedKey` Parameter.

Die folgende Beispielrichtlinie weist jeder zukünftigen Sammlung mit dem Namen `autopartsinventory` sowie Sammlungen, die mit dem Begriff „Vertrieb“ beginnen, einen vom Kunden verwalteten Schlüssel zu:

```
{
   "Rules":[
      {
         "ResourceType":"collection",
         "Resource":[
            "collection/autopartsinventory",
            "collection/sales*"
         ]
      }
   ],
   "AWSOwnedKey":false,
   "KmsARN":"arn:aws:encryption:us-east-1:123456789012:key/93fd6da4-a317-4c17-
bfe9-382b5d988b36"
}
```

Selbst wenn eine Richtlinie mit einem Sammlungsnamen übereinstimmt, können Sie diese automatische Zuweisung während der Sammlungserstellung außer Kraft setzen, wenn das Ressourcenmuster einen Platzhalter (*) enthält. Wenn Sie sich dafür entscheiden, die automatische Schlüsselzuweisung außer Kraft zu setzen, erstellt OpenSearch Serverless für Sie eine Verschlüsselungsrichtlinie mit dem Namen auto-**< *collection-name* >** und hängt sie der Sammlung an. Die Richtlinie gilt zunächst nur für eine einzelne Sammlung, Sie können sie jedoch ändern, um weitere Sammlungen einzubeziehen.

Wenn Sie Richtlinienregeln so ändern, dass sie nicht mehr mit einer Sammlung übereinstimmen, wird die Zuweisung des zugeordneten KMS-Schlüssels zu dieser Sammlung nicht aufgehoben. Die Sammlung bleibt immer mit ihrem ursprünglichen Verschlüsselungsschlüssel verschlüsselt. Wenn Sie

den Verschlüsselungsschlüssel für eine Sammlung ändern möchten, müssen Sie die Sammlung neu erstellen.

Wenn Regeln aus mehreren Richtlinien mit einer Sammlung übereinstimmen, wird die spezifischere Regel verwendet. Wenn beispielsweise eine Richtlinie eine Regel für `collection/log*` und eine andere für `collection/logSpecial` enthält, wird der Verschlüsselungsschlüssel für die zweite Richtlinie verwendet, da dieser spezifischer ist.

Sie können in einer Richtlinie keinen Namen oder ein Präfix verwenden, wenn es bereits in einer anderen Richtlinie vorhanden ist. OpenSearch Serverless zeigt einen Fehler an, wenn Sie versuchen, identische Ressourcenmuster in verschiedenen Verschlüsselungsrichtlinien zu konfigurieren.

Überlegungen

Berücksichtigen Sie Folgendes, wenn Sie die Verschlüsselung für Ihre Sammlungen konfigurieren:

- Die Verschlüsselung im Ruhezustand ist für alle Serverless-Sammlungen erforderlich.
- Sie haben die Möglichkeit, einen vom Kunden verwalteten Schlüssel oder ein AWS-eigener Schlüssel zu verwenden. Wenn Sie sich für einen vom Kunden verwalteten Schlüssel entscheiden, empfehlen wir Ihnen, die automatische Schlüsselrotation zu aktivieren.
- Sie können den Verschlüsselungsschlüssel für eine Sammlung nicht ändern, nachdem die Sammlung erstellt wurde. Wählen Sie sorgfältig aus, welche Sie verwenden AWS KMS möchten, wenn Sie zum ersten Mal eine Sammlung einrichten.
- Eine Sammlung kann nur mit einer einzigen Verschlüsselungsrichtlinie übereinstimmen.
- Sammlungen mit eindeutigen KMS-Schlüsseln können OpenSearch Recheneinheiten (OCUs) nicht mit anderen Sammlungen gemeinsam nutzen. Jede Sammlung mit einem eindeutigen Schlüssel benötigt ihre eigenen OCUs 4.
- Wenn Sie den KMS-Schlüssel in einer Verschlüsselungsrichtlinie aktualisieren, hat die Änderung keine Auswirkungen auf bestehende übereinstimmende Sammlungen mit bereits zugewiesenen KMS-Schlüsseln.
- OpenSearch Serverless überprüft die Benutzerberechtigungen für vom Kunden verwaltete Schlüssel nicht explizit. Wenn ein Benutzer über die Berechtigung verfügt, über eine Datenzugriffsrichtlinie auf eine Sammlung zuzugreifen, kann er die mit dem zugehörigen Schlüssel verschlüsselten Daten aufnehmen und abfragen.

Erforderliche Berechtigungen

Die Verschlüsselung im Ruhezustand für OpenSearch Serverless verwendet die folgenden AWS Identity and Access Management (IAM-) Berechtigungen. Sie können IAM-Bedingungen festlegen, um Benutzer auf bestimmte Sammlungen zu beschränken.

- `aoss:CreateSecurityPolicy` – Erstellt eine Verschlüsselungsrichtlinie.
- `aoss:ListSecurityPolicies` – Listet alle Verschlüsselungsrichtlinien und Sammlungen auf, denen diese angefügt sind.
- `aoss:GetSecurityPolicy` – Zeigt Details zu einer bestimmten Verschlüsselungsrichtlinie an.
- `aoss:UpdateSecurityPolicy` – Erstellt eine Verschlüsselungsrichtlinie.
- `aoss:DeleteSecurityPolicy` – Löscht eine Verschlüsselungsrichtlinie.

Das folgende Beispiel für eine identitätsbasierte Zugriffsrichtlinie stellt die Mindestberechtigungen bereit, die ein Benutzer zum Verwalten von Verschlüsselungsrichtlinien mit dem Ressourcenmuster `collection/application-logs` benötigt.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "aoss:CreateSecurityPolicy",
            "aoss:UpdateSecurityPolicy",
            "aoss:DeleteSecurityPolicy",
            "aoss:GetSecurityPolicy"
         ],
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "aoss:collection":"application-logs"
            }
         }
      },
      {
         "Effect":"Allow",
```

```
            "Action":[
               "aoss:ListSecurityPolicies"
            ],
            "Resource":"*"
         }
      ]
}
```

Schlüsselrichtlinie für einen kundenverwalteten Schlüssel

Wenn Sie einen vom Kunden verwalteten Schlüssel zum Schutz einer Sammlung auswählen, erhält OpenSearch Serverless die Erlaubnis, den KMS-Schlüssel im Namen des Prinzipals zu verwenden, der die Auswahl trifft. Dieser Prinzipal, ein Benutzer oder eine Rolle, muss über die für OpenSearch Serverless erforderlichen Berechtigungen für den KMS-Schlüssel verfügen. Sie können diese Berechtigungen in einer Schlüsselrichtlinie oder einer IAM-Richtlinie bereitstellen.

OpenSearch Serverless benötigt mindestens die folgenden Berechtigungen für einen vom Kunden verwalteten Schlüssel:

- km: DescribeKey
- km: CreateGrant

Zum Beispiel:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:DescribeKey",
        "kms:CreateGrant"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "kms:ViaService": "aoss.us-east-1.amazonaws.com"
        },
```

```
        "Bool": {
          "kms:GrantIsForAWSResource": "true"
        }
      }
    }
  ]
}
```

OpenSearch Serverless erstellt einen Grant mit den Berechtigungen kms: GenerateDataKey und kms:Decrypt.

Weitere Informationen finden Sie unter Verwenden von Schlüsselrichtlinien in AWS KMS im Entwicklerhandbuch für AWS Key Management Service .

So verwendet Serverless Grants in OpenSearch AWS KMS

OpenSearch Für Serverless ist ein Zuschuss erforderlich, um einen vom Kunden verwalteten Schlüssel verwenden zu können.

Wenn Sie in Ihrem Konto eine Verschlüsselungsrichtlinie mit einem neuen Schlüssel erstellen, erstellt OpenSearch Serverless in Ihrem Namen einen Zuschuss, indem es eine CreateGrantAnfrage an sendet. AWS KMS Grants in AWS KMS werden verwendet, um OpenSearch serverlosen Zugriff auf einen KMS-Schlüssel in einem Kundenkonto zu gewähren.

OpenSearch Serverless setzt voraus, dass der Zuschuss Ihren vom Kunden verwalteten Schlüssel für die folgenden internen Operationen verwenden kann:

- Senden Sie DescribeKeyAnfragen an, AWS KMS um zu überprüfen, ob die angegebene symmetrische, vom Kunden verwaltete Schlüssel-ID gültig ist.
- Senden Sie GenerateDataKeyAnfragen an den KMS-Schlüssel, um Datenschlüssel zu erstellen, mit denen Objekte verschlüsselt werden können.
- Senden Sie Entschlüsselungsanforderungen an AWS KMS , um die verschlüsselten Datenschlüssel zu entschlüsseln, sodass sie zum Verschlüsseln Ihrer Daten verwendet werden können.

Sie können den Zugriff auf die Genehmigung jederzeit widerrufen oder den Zugriff des Services auf den vom Kunden verwalteten Schlüssel entfernen. Wenn Sie dies tun, kann OpenSearch Serverless auf keine der mit dem vom Kunden verwalteten Schlüssel verschlüsselten Daten zugreifen. Dies wirkt

sich auf alle Vorgänge aus, die von diesen Daten abhängig sind, was zu `AccessDeniedException` Fehlern und Ausfällen in den asynchronen Workflows führt.

OpenSearch Serverless zieht Zuschüsse in einem asynchronen Workflow zurück, wenn ein bestimmter vom Kunden verwalteter Schlüssel keinen Sicherheitsrichtlinien oder Sammlungen zugeordnet ist.

Erstellen von Verschlüsselungsrichtlinien (Konsole)

In einer Verschlüsselungsrichtlinie geben Sie einen KMS-Schlüssel und eine Reihe von Erfassungsmustern an, auf die die Richtlinie angewendet wird. Allen neuen Sammlungen, die mit einem der in der Richtlinie definierten Muster übereinstimmen, wird beim Erstellen der Sammlung der entsprechende KMS-Schlüssel zugewiesen. Wir empfehlen Ihnen, Verschlüsselungsrichtlinien zu erstellen, bevor Sie mit dem Erstellen von Sammlungen beginnen.

Um eine Richtlinie für serverlose Verschlüsselung zu erstellen OpenSearch

1. Öffnen Sie die Amazon OpenSearch Service-Konsole zu https://console.aws.amazon.com/aos/Hause.
2. Erweitern Sie im linken Navigationsbereich Serverless und wählen Sie Encryption policies (Verschlüsselungsrichtlinien) aus.
3. Wählen Sie Create encryption policy (Verschlüsselungsrichtlinie erstellen).
4. Geben Sie einen Namen und eine Beschreibung für die Richtlinie an.
5. Geben Sie unter Resources (Ressourcen) ein oder mehrere Ressourcenmuster für diese Verschlüsselungsrichtlinie ein. Alle neu erstellten Sammlungen im aktuellen AWS-Konto und in der aktuellen Region, die mit einem der Muster übereinstimmen, werden dieser Richtlinie automatisch zugewiesen. Wenn Sie beispielsweise `ApplicationLogs` (ohne Platzhalter) eingeben und später eine Sammlung mit diesem Namen erstellen, werden die Richtlinie und der entsprechende KMS-Schlüssel dieser Sammlung zugewiesen.

   Sie können auch ein Präfix wie `Logs*` angeben, das die Richtlinie allen neuen Sammlungen zuweist, deren Namen mit `Logs` beginnen. Durch die Verwendung von Platzhaltern können Sie die Verschlüsselungseinstellungen für mehrere Sammlungen in großem Umfang verwalten.
6. Wählen Sie unter Encryption (Verschlüsselung) einen zu verwendenden KMS-Schlüssel aus.
7. Wählen Sie Erstellen aus.

Nächster Schritt: Erstellen von Sammlungen

Nachdem Sie eine oder mehrere Verschlüsselungsrichtlinien konfiguriert haben, können Sie mit der Erstellung von Sammlungen beginnen, die den in diesen Richtlinien definierten Regeln entsprechen. Detaillierte Anweisungen finden Sie unter the section called “Erstellen von Sammlungen”.

Im Schritt Verschlüsselungen bei der Erstellung der Sammlung informiert Sie OpenSearch Serverless darüber, dass der von Ihnen eingegebene Name dem in einer Verschlüsselungsrichtlinie definierten Muster entspricht, und weist der Sammlung automatisch den entsprechenden KMS-Schlüssel zu. Wenn das Ressourcenmuster einen Platzhalter (*) enthält, können Sie die Übereinstimmung überschreiben und Ihren eigenen Schlüssel auswählen.

Erstellen von Verschlüsselungsrichtlinien (AWS CLI)

Um mithilfe der OpenSearch serverlosen API-Operationen eine Verschlüsselungsrichtlinie zu erstellen, geben Sie Ressourcenmuster und einen Verschlüsselungsschlüssel im JSON-Format an. Die CreateSecurityPolicyAnfrage akzeptiert sowohl Inline-Richtlinien als auch JSON-Dateien.

Verschlüsselungsrichtlinien haben folgendes Format. Diese Beispieldatei `my-policy.json` stimmt mit jeder zukünftigen Sammlung mit dem Namen `autopartsinventory` überein, ebenso wie mit allen Sammlungen, deren Namen mit `sales` beginnen.

```
{
   "Rules":[
      {
         "ResourceType":"collection",
         "Resource":[
            "collection/autopartsinventory",
            "collection/sales*"
         ]
      }
   ],
   "AWSOwnedKey":false,
   "KmsARN":"arn:aws:encryption:us-east-1:123456789012:key/93fd6da4-a317-4c17-bfe9-382b5d988b36"
}
```

Um einen Service-eigenen Schlüssel zu verwenden, legen Sie `AWSOwnedKey` auf `true` fest:

```
{
   "Rules":[
      {
```

```
         "ResourceType":"collection",
         "Resource":[
            "collection/autopartsinventory",
            "collection/sales*"
         ]
      }
   ],
   "AWSOwnedKey":true
}
```

Die folgende Anfrage erstellt die Verschlüsselungsrichtlinie:

```
aws opensearchserverless create-security-policy \
    --name sales-inventory \
    --type encryption \
    --policy file://my-policy.json
```

Verwenden Sie dann den CreateCollectionAPI-Vorgang, um eine oder mehrere Sammlungen zu erstellen, die einem der Ressourcenmuster entsprechen.

Anzeigen von Verschlüsselungsrichtlinien

Bevor Sie eine Sammlung erstellen, möchten Sie möglicherweise eine Vorschau der vorhandenen Verschlüsselungsrichtlinien in Ihrem Konto anzeigen, um zu sehen, welche ein Ressourcenmuster hat, das mit dem Namen Ihrer Sammlung übereinstimmt. In der folgenden ListSecurityPoliciesAnfrage werden alle Verschlüsselungsrichtlinien in Ihrem Konto aufgeführt:

```
aws opensearchserverless list-security-policies --type encryption
```

Die Anfrage gibt Informationen über alle konfigurierten Verschlüsselungsrichtlinien zurück. Verwenden Sie den Inhalt des `policy`-Elements, um die Musterregeln anzuzeigen, die in der Richtlinie definiert sind:

```
{
   "securityPolicyDetails": [
      {
         "createdDate": 1663693217826,
         "description": "Sample encryption policy",
         "lastModifiedDate": 1663693217826,
         "name": "my-policy",
         "policy": "{\"Rules\":[{\"ResourceType\":\"collection\",\"Resource\":
[\"collection/autopartsinventory\",\"collection/sales*\"]}],\"AWSOwnedKey\":true}",
```

```
        "policyVersion": "MTY2MzY5MzIxNzgyNl8x",
        "type": "encryption"
      }
   ]
}
```

Verwenden Sie den GetSecurityPolicyBefehl, um detaillierte Informationen zu einer bestimmten Richtlinie, einschließlich des KMS-Schlüssels, anzuzeigen.

Aktualisieren von Verschlüsselungsrichtlinien

Wenn Sie den KMS-Schlüssel in einer Verschlüsselungsrichtlinie aktualisieren, gilt die Änderung nur für neu erstellte Sammlungen, die mit dem konfigurierten Namen oder Muster übereinstimmen. Bestehende Sammlungen, denen bereits KMS-Schlüssel zugewiesen sind, sind davon nicht betroffen.

Dasselbe gilt für Regeln zum Richtlinienabgleich. Wenn Sie eine Regel hinzufügen, ändern oder löschen, gilt die Änderung nur für neu erstellte Sammlungen. Vorhandene Sammlungen verlieren ihren zugewiesenen KMS-Schlüssel nicht, wenn Sie die Regeln einer Richtlinie so ändern, dass sie nicht mehr mit dem Namen einer Sammlung übereinstimmen.

Um eine Verschlüsselungsrichtlinie in der OpenSearch Serverless-Konsole zu aktualisieren, wählen Sie Verschlüsselungsrichtlinien, wählen Sie die zu ändernde Richtlinie aus und klicken Sie auf Bearbeiten. Nehmen Sie Ihre Änderungen vor und wählen Sie Save (Speichern).

Verwenden Sie den Vorgang, um eine Verschlüsselungsrichtlinie mithilfe der OpenSearch Serverless API zu aktualisieren. UpdateSecurityPolicy Die folgende Anfrage aktualisiert eine Verschlüsselungsrichtlinie mit einem neuen Richtlinien-JSON-Dokument:

```
aws opensearchserverless update-security-policy \
    --name sales-inventory \
    --type encryption \
    --policy-version 2 \
    --policy file://my-new-policy.json
```

Aktualisieren von Verschlüsselungsrichtlinien

Wenn Sie eine Verschlüsselungsrichtlinie löschen, sind alle Sammlungen, die derzeit den in der Richtlinie definierten KMS-Schlüssel verwenden, nicht betroffen. Um eine Richtlinie in der OpenSearch Serverless-Konsole zu löschen, wählen Sie die Richtlinie aus und klicken Sie auf Löschen.

Sie können auch den DeleteSecurityPolicyVorgang verwenden:

```
aws opensearchserverless delete-security-policy --name my-policy --type encryption
```

Verschlüsselung während der Übertragung

In OpenSearch Serverless werden alle Pfade in einer Sammlung während der Übertragung mithilfe von Transport Layer Security 1.2 (TLS) mit einer dem Industriestandard entsprechenden AES-256-Verschlüsselung verschlüsselt. Der Zugriff auf alle Dashboards APIs und Dashboards für Opensearch erfolgt ebenfalls über TLS 1.2. TLS ist eine Reihe von branchenüblichen kryptografischen Protokollen, die zur Verschlüsselung von Informationen verwendet werden, die über das Netzwerk ausgetauscht werden.

Netzwerkzugriff für Amazon OpenSearch Serverless

Die Netzwerkeinstellungen für eine Amazon OpenSearch Serverless-Sammlung bestimmen, ob auf die Sammlung über das Internet von öffentlichen Netzwerken aus zugegriffen werden kann oder ob privat darauf zugegriffen werden muss.

Der private Zugriff kann für eine oder beide der folgenden Bedingungen gelten:

- OpenSearch Serverlos verwaltete VPC-Endpunkte
- Unterstützt AWS-Services wie Amazon Bedrock

Sie können den Netzwerkzugriff für den Endpunkt einer Sammlung und den entsprechenden OpenSearchOpenSearch Dashboard-Endpunkt separat konfigurieren.

Der Netzwerkzugriff ist der Isolationsmechanismus, mit dem Sie den Zugriff aus verschiedenen Quellnetzwerken ermöglichen können. Wenn beispielsweise der OpenSearch Dashboard-Endpunkt einer Sammlung öffentlich zugänglich ist, der OpenSearch API-Endpunkt jedoch nicht, kann ein Benutzer nur über Dashboards auf die Sammlungsdaten zugreifen, wenn er von einem öffentlichen Netzwerk aus eine Verbindung herstellt. Wenn sie versuchen, sie OpenSearch APIs direkt von einem öffentlichen Netzwerk aus anzurufen, werden sie blockiert. Die Netzwerkeinstellungen können für solche Permutationen von Quelle zu Ressource-Typ verwendet werden. Amazon OpenSearch Serverless unterstützt sowohl IPv6 Konnektivität als IPv4 auch.

Themen

- Netzwerkrichtlinien

- Überlegungen
- Für die Konfiguration von Netzwerkrichtlinien sind Berechtigungen erforderlich
- Vorrang der Richtlinie
- Erstellen von Netzwerkrichtlinien (Konsole)
- Erstellen von Netzwerkrichtlinien (AWS CLI)
- Anzeigen von Netzwerkrichtlinien
- Aktualisieren von Netzwerkrichtlinien
- Löschen von Netzwerkrichtlinien

Netzwerkrichtlinien

Mit Netzwerkrichtlinien können Sie viele Sammlungen in großem Umfang verwalten, indem Sie Sammlungen, die den in der Richtlinie definierten Regeln entsprechen, automatisch Netzwerkzugriffseinstellungen zuweisen.

In einer Netzwerkrichtlinie legen Sie eine Reihe von Regeln fest. Diese Regeln definieren Zugriffsberechtigungen für Sammelendpunkte und OpenSearch Dashboard-Endpunkte. Jede Regel besteht aus einem Zugriffstyp (öffentlich oder privat) und einem Ressourcentyp (Sammlungs- und/oder OpenSearch Dashboard-Endpunkt). Für jeden Ressourcentyp (`collection` and `dashboard`) legen Sie eine Reihe von Regeln fest, die definieren, für welche Sammlungen die Richtlinie gilt.

In dieser Beispielrichtlinie spezifiziert die erste Regel den VPC-Endpunktzugriff sowohl auf den Sammlungsendpunkt als auch auf den Dashboards-Endpunkt für alle Sammlungen, die mit dem Begriff beginnen. `marketing*` Es spezifiziert auch den Zugriff auf Amazon Bedrock.

> **Note**
>
> Der private Zugriff auf AWS-Services z. B. Amazon Bedrock gilt nur für den Endpunkt der Sammlung, nicht für den OpenSearch Endpunkt der OpenSearch Dashboards. Selbst wenn dies der Fall `ResourceType` ist`dashboard`, AWS-Services kann kein Zugriff auf Dashboards gewährt werden. OpenSearch

Die zweite Regel legt den öffentlichen Zugriff auf die `finance`-Sammlung fest, jedoch nur für den Sammlungsendpunkt (kein Zugriff auf Dashboards).

```
[
```

```
   {
      "Description":"Marketing access",
      "Rules":[
         {
            "ResourceType":"collection",
            "Resource":[
               "collection/marketing*"
            ]
         },
         {
            "ResourceType":"dashboard",
            "Resource":[
               "collection/marketing*"
            ]
         }
      ],
      "AllowFromPublic":false,
      "SourceVPCEs":[
         "vpce-050f79086ee71ac05"
      ],
      "SourceServices":[
         "bedrock.amazonaws.com"
      ],
   },
   {
      "Description":"Sales access",
      "Rules":[
         {
            "ResourceType":"collection",
            "Resource":[
               "collection/finance"
            ]
         }
      ],
      "AllowFromPublic":true
   }
]
```

Diese Richtlinie gewährt der Öffentlichkeit nur Zugriff auf OpenSearch Dashboards für Sammlungen, die mit „Finanzen“ beginnen. Alle Versuche, direkt auf die OpenSearch API zuzugreifen, schlagen fehl.

```
[
```

```
  {
    "Description": "Dashboards access",
    "Rules": [
      {
        "ResourceType": "dashboard",
        "Resource": [
          "collection/finance*"
        ]
      }
    ],
    "AllowFromPublic": true
  }
]
```

Netzwerkrichtlinien können sowohl für bestehende Sammlungen als auch für zukünftige Sammlungen gelten. Sie können beispielsweise eine Sammlung erstellen und dann eine Netzwerkrichtlinie mit einer Regel erstellen, die dem Sammlungsnamen entspricht. Vor dem Erstellen von Sammlungen müssen Sie keine Netzwerkrichtlinien erstellen.

Überlegungen

Berücksichtigen Sie Folgendes, wenn Sie den Netzwerkzugriff für Ihre Sammlungen konfigurieren:

- Wenn Sie den VPC-Endpunktzugriff für eine Sammlung konfigurieren möchten, müssen Sie zunächst mindestens einen OpenSearch serverlos verwalteten VPC-Endpunkt erstellen.
- Der private Zugriff auf gilt AWS-Services nur für den Endpunkt der Sammlung, nicht für den OpenSearch Dashboard-Endpunkt. OpenSearch Selbst wenn dies der Fall `ResourceType` ist`dashboard`, AWS-Services kann kein Zugriff auf OpenSearch Dashboards gewährt werden.
- Wenn auf eine Sammlung von öffentlichen Netzwerken aus zugegriffen werden kann, ist sie auch von allen OpenSearch serverlos verwalteten VPC-Endpunkten und allen zugänglich. AWS-Services
- Für eine einzelne Sammlung können mehrere Netzwerkrichtlinien gelten. Weitere Informationen finden Sie unter the section called “Vorrang der Richtlinie”.

Für die Konfiguration von Netzwerkrichtlinien sind Berechtigungen erforderlich

Der Netzwerkzugriff für OpenSearch Serverless verwendet die folgenden AWS Identity and Access Management (IAM-) Berechtigungen. Sie können IAM-Bedingungen festlegen, um Benutzer auf Netzwerkrichtlinien zu beschränken, die bestimmten Sammlungen zugeordnet sind.

- `aoss:CreateSecurityPolicy` – Erstellt eine Netzwerkzugriffsrichtlinie.
- `aoss:ListSecurityPolicies` – Listet alle Netzwerkrichtlinien im aktuellen Konto auf.
- `aoss:GetSecurityPolicy` – Zeigt die Spezifikation einer Netzwerkzugriffsrichtlinie an.
- `aoss:UpdateSecurityPolicy` – Ändert eine bestimmte Netzwerkzugriffsrichtlinie und ändert die VPC-ID oder die Bezeichnung für den öffentlichen Zugriff.
- `aoss:DeleteSecurityPolicy` – Löscht eine Netzwerkzugriffsrichtlinie (nachdem sie von allen Sammlungen getrennt wurde).

Die folgende identitätsbasierte Zugriffsrichtlinie ermöglicht es einem Benutzer, alle Netzwerkrichtlinien anzuzeigen und Richtlinien mit dem Ressourcenmuster `collection/application-logs` zu aktualisieren:

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "aoss:UpdateSecurityPolicy"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aoss:collection": "application-logs"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "aoss:ListSecurityPolicies",
                "aoss:GetSecurityPolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

> **Note**
>
> Darüber hinaus benötigt OpenSearch Serverless die `aoss:DashboardsAccessAll` Berechtigungen `aoss:APIAccessAll` und für die Erfassung von Ressourcen. Weitere Informationen finden Sie unter the section called “ OpenSearchAPI-Operationen verwenden”.

Vorrang der Richtlinie

Es kann Situationen geben, in denen sich Netzwerkrichtlinienregeln innerhalb oder zwischen Richtlinien überschneiden. In diesem Fall überschreibt eine Regel, die den öffentlichen Zugriff festlegt, eine Regel, die privaten Zugriff für alle Sammlungen festlegt, die beiden Regeln gemeinsam sind.

In der folgenden Richtlinie weisen beispielsweise beide Regeln der `finance`-Sammlung Netzwerkzugriff zu, aber eine Regel legt den VPC-Zugriff fest, während die andere den öffentlichen Zugriff festlegt. In dieser Situation überschreibt der öffentliche Zugriff den VPC-Zugriff nur für die Finanzsammlung (weil er in beiden Regeln vorhanden ist), sodass die Finanzsammlung über öffentliche Netzwerke zugänglich ist. Die Verkaufssammlung verfügt über VPC-Zugriff vom angegebenen Endpunkt aus.

```
[
   {
      "Description":"Rule 1",
      "Rules":[
         {
            "ResourceType":"collection",
            "Resource":[
               "collection/sales",
               "collection/finance"
            ]
         }
      ],
      "AllowFromPublic":false,
      "SourceVPCEs":[
         "vpce-050f79086ee71ac05"
      ]
   },
   {
      "Description":"Rule 2",
      "Rules":[
```

```
         {
            "ResourceType":"collection",
            "Resource":[
               "collection/finance"
            ]
         }
      ],
      "AllowFromPublic":true
   }
]
```

Wenn mehrere VPC-Endpunkte aus unterschiedlichen Regeln auf eine Sammlung zutreffen, sind die Regeln additiv und die Sammlung ist von allen angegebenen Endpunkten aus zugänglich. Wenn Sie `AllowFromPublic` auf oder festlegen, `true` aber auch eines `SourceVPCEs` oder mehrere angeben`SourceServices`, ignoriert OpenSearch Serverless die VPC-Endpunkte und Dienstkennungen, sodass die zugehörigen Sammlungen öffentlich zugänglich sind.

Erstellen von Netzwerkrichtlinien (Konsole)

Netzwerkrichtlinien können sowohl für bestehende Richtlinien als auch für zukünftige Richtlinien gelten. Wir empfehlen, dass Sie Netzwerkrichtlinien erstellen, bevor Sie mit dem Erstellen von Sammlungen beginnen.

Um eine Serverless-Netzwerkrichtlinie zu erstellen OpenSearch

1. Öffnen Sie die Amazon OpenSearch Service-Konsole zu https://console.aws.amazon.com/aos/Hause.
2. Erweitern Sie im linken Navigationsbereich Serverless und wählen Sie Network policies (Netzwerkrichtlinien) aus.
3. Wählen Sie Create network policy (Netzwerkrichtlinie erstellen) aus.
4. Geben Sie einen Namen und eine Beschreibung für die Sammlung an.
5. Geben Sie eine oder mehrere Regeln an. Diese Regeln definieren die Zugriffsberechtigungen für Ihre OpenSearch serverlosen Sammlungen und deren OpenSearch Dashboard-Endpunkte.

   Jede Regel enthält die folgenden Elemente:

Element	Beschreibung
Rule name (Regelname)	Ein Name, der den Inhalt der Regel beschreibt. Beispiel: „VPC-Zugriff für Marketingteam“.
Access type (Art des Zugriffs)	Wählen Sie entweder öffentlichen oder privaten Zugriff. Wählen Sie dann eine oder beide der folgenden Optionen aus: • VPC-Endpunkte für den Zugriff — Geben Sie einen oder OpenSearch mehrere serverlos verwaltete VPC-Endpunkte an — verwaltete VPC-Endpunkte. • AWS-Service privater Zugriff — Wählen Sie eine oder AWS-Services mehrere unterstützte Optionen aus.
Ressourcentyp	Wählen Sie aus, ob Sie Zugriff auf OpenSearch Endpunkte (was Aufrufe an die OpenSearch API ermöglicht), auf OpenSearch Dashboards (die den Zugriff auf Visualisierungen und die Benutzeroberfläche für OpenSearch Plugins ermöglichen) oder auf beides gewähren möchten. **Note** AWS-Service Der private Zugriff gilt nur für den Endpunkt der Sammlung, nicht für den OpenSearch Endpunkt der Dashboards. OpenSearch Auch wenn Sie OpenSearch Dashboards auswählen, AWS-Services kann nur Endpunktzugriff gewährt werden.

Für jeden Ressourcentyp, den Sie auswählen, können Sie vorhandene Sammlungen auswählen, auf die Sie die Richtlinieneinstellungen anwenden möchten, und ein oder mehrere Ressourcenmuster and/or erstellen. Ressourcenmuster bestehen aus einem Präfix und einem Platzhalter (*) und definieren, für welche Sammlungen die Richtlinieneinstellungen gelten.

Wenn Sie beispielsweise ein Muster mit dem Namen `Marketing*` einfügen, werden auf alle neuen oder vorhandenen Sammlungen, deren Namen mit „Marketing“ beginnen, automatisch die Netzwerkeinstellungen in dieser Richtlinie angewendet. Ein einzelner Platzhalter (*) wendet die Richtlinie auf alle aktuellen und zukünftigen Sammlungen an.

Darüber hinaus können Sie den Namen einer future Sammlung ohne Platzhalter angeben, z. B. `Finance` OpenSearch Serverless wendet die Richtlinieneinstellungen auf jede neu erstellte Sammlung mit genau diesem Namen an.

6. Wenn Sie mit der Konfiguration Ihrer Richtlinie zufrieden sind, wählen Sie Create (Erstellen).

Erstellen von Netzwerkrichtlinien (AWS CLI)

Um mithilfe der OpenSearch serverlosen API-Operationen eine Netzwerkrichtlinie zu erstellen, geben Sie Regeln im JSON-Format an. Die CreateSecurityPolicyAnfrage akzeptiert sowohl Inline-Richtlinien als auch JSON-Dateien. Alle Sammlungen und Muster müssen das Format `collection/<collection name|pattern>` aufweisen.

> **Note**
>
> Der Ressourcentyp erlaubt `dashboards` nur Zugriff auf OpenSearch Dashboards. Damit OpenSearch Dashboards funktionieren, müssen Sie jedoch auch den Zugriff auf Sammlungen aus denselben Quellen zulassen. Ein Beispiel finden Sie in der zweiten Richtlinie unten.

Um privaten Zugriff zu spezifizieren, fügen Sie eines oder beide der folgenden Elemente hinzu:

- `SourceVPCEs`— Geben Sie einen oder mehrere OpenSearch serverlos verwaltete VPC-Endpunkte an.
- `SourceServices`— Geben Sie die Kennung eines oder mehrerer unterstützter Geräte an. AWS-Services Derzeit werden die folgenden Dienstkennungen unterstützt:

- `bedrock.amazonaws.com`— Amazonas-Grundgestein

Die folgende Beispielnetzwerkrichtlinie bietet privaten Zugriff auf einen VPC-Endpunkt und Amazon Bedrock auf Sammlungsendpunkte nur für Sammlungen, die mit dem Präfix beginnen. `log*` Authentifizierte Benutzer können sich nicht bei OpenSearch Dashboards anmelden. Sie können nur programmgesteuert auf den Sammlungsendpunkt zugreifen.

```
[
   {
      "Description":"Private access for log collections",
      "Rules":[
         {
            "ResourceType":"collection",
            "Resource":[
               "collection/log*"
            ]
         }
      ],
      "AllowFromPublic":false,
      "SourceVPCEs":[
         "vpce-050f79086ee71ac05"
      ],
      "SourceServices":[
         "bedrock.amazonaws.com"
      ],
   }
]
```

Die folgende Richtlinie gewährt öffentlichen Zugriff auf den OpenSearch Endpunkt und die OpenSearch Dashboards für eine einzelne Sammlung mit dem Namen. `finance` Wenn die Sammlung nicht vorhanden ist, werden die Netzwerkeinstellungen auf die Sammlung angewendet, wenn und sobald sie erstellt wird.

```
[
   {
      "Description":"Public access for finance collection",
      "Rules":[
         {
            "ResourceType":"dashboard",
            "Resource":[
               "collection/finance"
```

```
            ]
         },
         {
            "ResourceType":"collection",
            "Resource":[
               "collection/finance"
            ]
         }
      ],
      "AllowFromPublic":true
   }
]
```

Die folgende Anfrage erstellt die oben genannte Netzwerkrichtlinie:

```
aws opensearchserverless create-security-policy \
    --name sales-inventory \
    --type network \
    --policy "[{\"Description\":\"Public access for finance collection\",\"Rules
\":[{\"ResourceType\":\"dashboard\",\"Resource\":[\"collection\/finance\"]},
{\"ResourceType\":\"collection\",\"Resource\":[\"collection\/finance\"]}],
\"AllowFromPublic\":true}]"
```

Verwenden Sie das Format `--policy file://my-policy.json` die Richtlinie in einer JSON-Datei bereitzustellen

Anzeigen von Netzwerkrichtlinien

Bevor Sie eine Sammlung erstellen, möchten Sie möglicherweise eine Vorschau der vorhandenen Netzwerkrichtlinien in Ihrem Konto anzeigen, um zu sehen, welche ein Ressourcenmuster hat, das mit dem Namen Ihrer Sammlung übereinstimmt. Die folgende ListSecurityPoliciesAnfrage listet alle Netzwerkrichtlinien in Ihrem Konto auf:

```
aws opensearchserverless list-security-policies --type network
```

Die Anfrage gibt Informationen zu allen konfigurierten Netzwerkrichtlinien zurück. Um die in einer bestimmten Richtlinie definierten Musterregeln einzusehen, suchen Sie die Richtlinieninformationen im Inhalt des `securityPolicySummaries` Elements in der Antwort. Notieren Sie sich das `name` Ende `type` dieser Richtlinie und verwenden Sie diese Eigenschaften in einer GetSecurityPolicyAnfrage, um eine Antwort mit den folgenden Richtliniendetails zu erhalten:

```
{
    "securityPolicyDetail": [
        {
            "type": "network",
            "name": "my-policy",
            "policyVersion": "MTY2MzY5MTY1MDA3Ml8x",
            "policy": "[{\"Description\":\"My network policy rule\",\"Rules\":
[{\"ResourceType\":\"dashboard\",\"Resource\":[\"collection/*\"]}],\"AllowFromPublic
\":true}]",
            "createdDate": 1663691650072,
            "lastModifiedDate": 1663691650072
        }
    ]
}
```

Verwenden Sie den GetSecurityPolicyBefehl, um detaillierte Informationen zu einer bestimmten Richtlinie anzuzeigen.

Aktualisieren von Netzwerkrichtlinien

Wenn Sie die VPC-Endpunkte oder die Bezeichnung des öffentlichen Zugriffs für ein Netzwerk ändern, sind alle zugehörigen Sammlungen betroffen. Um eine Netzwerkrichtlinie in der OpenSearch Serverless-Konsole zu aktualisieren, erweitern Sie Netzwerkrichtlinien, wählen Sie die zu ändernde Richtlinie aus und klicken Sie auf Bearbeiten. Nehmen Sie Ihre Änderungen vor und wählen Sie Save (Speichern).

Verwenden Sie den Befehl, um eine Netzwerkrichtlinie mithilfe der OpenSearch Serverless API zu aktualisieren. UpdateSecurityPolicy Sie müssen eine Richtlinienversion in die Anfrage aufnehmen. Sie können die Richtlinienversion mithilfe der `ListSecurityPolicies`- oder `GetSecurityPolicy`-Befehle abrufen. Durch die Angabe der neuesten Richtlinienversion wird sichergestellt, dass Sie nicht versehentlich eine von einem anderen Benutzer vorgenommene Änderung überschreiben.

Die folgende Anfrage aktualisiert eine Netzwerkrichtlinie mit einem neuen JSON-Richtliniendokument:

```
aws opensearchserverless update-security-policy \
    --name sales-inventory \
    --type network \
    --policy-version MTY2MzY5MTY1MDA3Ml8x \
    --policy file://my-new-policy.json
```

Löschen von Netzwerkrichtlinien

Bevor Sie eine Netzwerkrichtlinie löschen können, müssen Sie sie von allen Sammlungen trennen. Um eine Richtlinie in der OpenSearch Serverless-Konsole zu löschen, wählen Sie die Richtlinie aus und klicken Sie auf Löschen.

Sie können auch den DeleteSecurityPolicyfolgenden Befehl verwenden:

```
aws opensearchserverless delete-security-policy --name my-policy --type network
```

Datenzugriffskontrolle für Amazon OpenSearch Serverless

Mit der Datenzugriffskontrolle in Amazon OpenSearch Serverless können Sie Benutzern den Zugriff auf Sammlungen und Indizes ermöglichen, unabhängig von ihrem Zugriffsmechanismus oder ihrer Netzwerkquelle. Sie können IAM-Rollen und SAML-Identitäten Zugriff gewähren.

Sie verwalten Zugriffsberechtigungen über Datenzugriffsrichtlinien, die für Sammlungen und Indexressourcen gelten. Datenzugriffsrichtlinien unterstützen Sie bei der Verwaltung von Sammlungen in großem Umfang, indem sie automatisch Zugriffsberechtigungen für Sammlungen und Indizes zuweisen, die einem bestimmten Muster übereinstimmen. Für eine einzelne Ressource können mehrere Datenzugriffsrichtlinien gelten. Beachten Sie, dass Sie über eine Datenzugriffsrichtlinie für Ihre Sammlung verfügen müssen, um auf Ihre OpenSearch Dashboard-URL zugreifen zu können.

Themen

- Datenzugriffsrichtlinien im Vergleich zu IAM-Richtlinien
- Für die Konfiguration von Datenzugriffsrichtlinien sind IAM-Berechtigungen erforderlich
- Richtliniensyntax
- Unterstützte Richtlinienberechtigungen
- Beispieldatensätze auf Dashboards OpenSearch
- Erstellen von Datenzugriffsrichtlinien (Konsole)
- Erstellen von Datenzugriffsrichtlinien (AWS CLI)
- Ansicht von Datenzugriffsrichtlinien
- Aktualisieren von Datenzugriffsrichtlinien
- Löschen von Datenzugriffsrichtlinien

- Kontoübergreifender Datenzugriff

Datenzugriffsrichtlinien im Vergleich zu IAM-Richtlinien

Datenzugriffsrichtlinien sind logisch von AWS Identity and Access Management (IAM-) Richtlinien getrennt. IAM-Berechtigungen steuern den Zugriff auf die Serverless API-Operationen wie z. B. `CreateCollection` und `ListAccessPolicies`. Datenzugriffsrichtlinien steuern den Zugriff auf die von OpenSearch Serverless unterstützten OpenSearch Operationen wie oder. `PUT <index>` `GET _cat/indices`

Die IAM-Berechtigungen, die den Zugriff auf API-Operationen der Datenzugriffsrichtlinie steuern, wie z. B. `aoss:CreateAccessPolicy` and `aoss:GetAccessPolicy` (im nächsten Abschnitt beschrieben), wirken sich nicht auf die in einer Datenzugriffsrichtlinie angegebene Berechtigung aus.

Angenommen, eine IAM-Richtlinie verweigert einem Benutzer beispielsweise das Erstellen von Datenzugriffsrichtlinien für `collection-a`, erlaubt ihm jedoch, Datenzugriffsrichtlinien für alle Sammlungen (*) zu erstellen:

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "aoss:CreateAccessPolicy"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "aoss:collection": "collection-a"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "aoss:CreateAccessPolicy"
            ],
            "Resource": "*"
```

```
        }
    ]
}
```

Wenn der Benutzer eine Datenzugriffsrichtlinie erstellt, die bestimmte Berechtigungen für alle Sammlungen (`collection/*` oder `index/*/*`) gewährt, gilt die Richtlinie für alle Sammlungen, einschließlich Sammlung A.

> **Important**
>
> Die Erteilung von Berechtigungen im Rahmen einer Datenzugriffsrichtlinie reicht nicht aus, um auf Daten in Ihrer OpenSearch serverlosen Sammlung zuzugreifen. Einem zugehörigen Principal muss außerdem Zugriff auf die IAM-Berechtigungen `aoss:APIAccessAll` und gewährt werden. `aoss:DashboardsAccessAll` Beide Berechtigungen gewähren vollen Zugriff auf Sammlungsressourcen, während die Dashboard-Berechtigung auch Zugriff OpenSearch auf Dashboards gewährt. Wenn ein Principal nicht über diese beiden IAM-Berechtigungen verfügt, erhält er 403-Fehler, wenn er versucht, Anfragen an die Sammlung zu senden. Weitere Informationen finden Sie unter the section called “ OpenSearchAPI-Operationen verwenden”.

Für die Konfiguration von Datenzugriffsrichtlinien sind IAM-Berechtigungen erforderlich

Die Datenzugriffskontrolle für OpenSearch Serverless verwendet die folgenden IAM-Berechtigungen. Sie können IAM-Bedingungen festlegen, um Benutzer auf bestimmte Zugriffsrichtliniennamen zu beschränken.

- `aoss:CreateAccessPolicy` – Erstellt eine Zugriffsrichtlinie.
- `aoss:ListAccessPolicies` – Listet alle Zugriffsrichtlinien auf.
- `aoss:GetAccessPolicy` – Zeigt Details zu einer bestimmten Zugriffsrichtlinie an.
- `aoss:UpdateAccessPolicy` – Ändert eine Zugriffsrichtlinie.
- `aoss:DeleteAccessPolicy` – Löscht eine Zugriffsrichtlinie.

Die folgende identitätsbasierte Zugriffsrichtlinie ermöglicht es einem Benutzer, alle Zugriffsrichtlinien anzuzeigen und Richtlinien zu aktualisieren, die das Ressourcenmuster `collection/logs` enthalten.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "aoss:ListAccessPolicies",
                "aoss:GetAccessPolicy"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "aoss:UpdateAccessPolicy"
            ],
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aoss:collection": [
                        "logs"
                    ]
                }
            }
        }
    ]
}
```

> **Note**
>
> Darüber hinaus benötigt OpenSearch Serverless die `aoss:DashboardsAccessAll` Berechtigungen `aoss:APIAccessAll` und für die Erfassung von Ressourcen. Weitere Informationen finden Sie unter the section called “ OpenSearchAPI-Operationen verwenden”.

Richtliniensyntax

Eine Datenzugriffsrichtlinie enthält eine Reihe von Regeln, die jeweils die folgenden Elemente enthalten:

Element	Beschreibung
`ResourceType`	Der Ressourcentyp (Sammlung oder Index), für den die Berechtigungen gelten. Alias- und Vorlagenberechtigungen befinden sich auf Sammlungsebene, während Berechtigungen zum Erstellen, Ändern und Suchen von Daten auf Indexebene liegen. Weitere Informationen finden Sie unter Unterstützte Richtlinienberechtigungen.
`Resource`	Eine Liste von and/or Mustern für Ressourcennamen. Muster sind Präfixe gefolgt von einem Platzhalter (*), wodurch die zugehörigen Berechtigungen auf mehrere Ressourcen angewendet werden können. • Sammlungen haben das Format `collection/ <name|pattern>` . • Indizes haben das Format `index/<collection-name|pattern> /<index-name|pattern/>` .
`Permission`	Eine Liste der Berechtigungen, die für die angegebenen Ressourcen gewährt werden sollen. Eine vollständige Liste der Berechtigungen und der zulässigen API-Operationen finden Sie unter the section called “Unterstützte OpenSearch API-Operationen und -Berechtigungen”.
`Principal`	Eine Liste mit einem oder mehreren Prinzipalen, denen Zugriff gewährt werden soll. Prinzipale können IAM-Rollen ARNs - oder SAML-Identitäten sein. Diese Prinzipien müssen dem aktuellen AWS-Konto entsprechen. Datenzugriffsrichtlinien unterstützen den kontoübergreifenden Zugriff nicht direkt, Sie können jedoch eine Rolle in Ihre Richtlinie aufnehmen, die ein Benutzer aus einem anderen Land in dem Konto übernehmen AWS-Konto kann, dem die Sammlung gehört. Weitere Informationen finden Sie unter the section called “Kontoübergreifender Datenzugriff”.

Die folgende Beispielrichtlinie gewährt Alias- und Vorlagenberechtigungen für die Sammlung mit dem Namen `autopartsinventory` sowie alle Sammlungen, die mit dem Präfix `sales*`

beginnen. Es gewährt auch Lese- und Schreibberechtigungen für alle Indizes innerhalb der `autopartsinventory`-Sammlung und alle Indizes in der `salesorders`-Sammlung, die mit dem Präfix `orders*` beginnen.

```
[
   {
      "Description": "Rule 1",
      "Rules":[
         {
            "ResourceType":"collection",
            "Resource":[
               "collection/autopartsinventory",
               "collection/sales*"
            ],
            "Permission":[
               "aoss:CreateCollectionItems",
               "aoss:UpdateCollectionItems",
               "aoss:DescribeCollectionItems"
            ]
         },
         {
            "ResourceType":"index",
            "Resource":[
               "index/autopartsinventory/*",
               "index/salesorders/orders*"
            ],
            "Permission":[
               "aoss:*"
            ]
         }
      ],
      "Principal":[
         "arn:aws:iam::123456789012:user/Dale",
         "arn:aws:iam::123456789012:role/RegulatoryCompliance",
         "saml/123456789012/myprovider/user/Annie",
         "saml/123456789012/anotherprovider/group/Accounting"
      ]
   }
]
```

Sie können den Zugriff innerhalb einer Richtlinie nicht explizit verweigern. Daher sind alle Richtlinienberechtigungen additiv. Wenn beispielsweise eine Richtlinie einem Benutzer

`aoss:ReadDocument` und eine andere Richtlinie `aoss:WriteDocument` gewährt, verfügt der Benutzer über beide Berechtigungen. Wenn eine dritte Richtlinie denselben Benutzer `aoss:*` gewährt, kann der Benutzer alle Aktionen für den zugeordneten Index ausführen. Restriktivere Berechtigungen überschreiben weniger restriktive nicht.

Unterstützte Richtlinienberechtigungen

Die folgenden Berechtigungen werden in Datenzugriffsrichtlinien unterstützt. Informationen zu den OpenSearch API-Vorgängen, die die einzelnen Berechtigungen zulassen, finden Sie unter. the section called “Unterstützte OpenSearch API-Operationen und -Berechtigungen”

Sammlungssberechtigungen

- `aoss:CreateCollectionItems`
- `aoss:DeleteCollectionItems`
- `aoss:UpdateCollectionItems`
- `aoss:DescribeCollectionItems`
- `aoss:*`

Indexberechtigungen

- `aoss:ReadDocument`
- `aoss:WriteDocument`
- `aoss:CreateIndex`
- `aoss:DeleteIndex`
- `aoss:UpdateIndex`
- `aoss:DescribeIndex`
- `aoss:*`

Beispieldatensätze auf Dashboards OpenSearch

OpenSearch Dashboards bietet Beispieldatensätze mit Visualisierungen, Dashboards und anderen Tools, die Ihnen helfen, Dashboards zu erkunden, bevor Sie Ihre eigenen Daten hinzufügen.
Um Indizes aus diesen Beispieldaten zu erstellen, benötigen Sie eine Datenzugriffsrichtlinie, die

Berechtigungen für den Datensatz bereitstellt, mit dem Sie arbeiten möchten. Die folgende Richtlinie verwendet einen Platzhalter (*), um Berechtigungen für alle drei Beispieldatensätze zu gewähren.

```
[
  {
    "Rules": [
      {
        "Resource": [
          "index/<collection-name>/opensearch_dashboards_sample_data_*"
        ],
        "Permission": [
          "aoss:CreateIndex",
          "aoss:DescribeIndex",
          "aoss:ReadDocument"
        ],
        "ResourceType": "index"
      }
    ],
    "Principal": [
      "arn:aws:iam::<account-id>:user/<user>"
    ]
  }
]
```

Erstellen von Datenzugriffsrichtlinien (Konsole)

Sie können eine Datenzugriffsrichtlinie mit dem visuellen Editor oder im JSON-Format erstellen. Allen neuen Sammlungen, die mit einem der in der Richtlinie definierten Muster übereinstimmen, werden beim Erstellen der Sammlung die entsprechenden Berechtigungen zugewiesen.

Um eine Richtlinie für den OpenSearch serverlosen Datenzugriff zu erstellen

1. Öffnen Sie die Amazon OpenSearch Service-Konsole zu https://console.aws.amazon.com/aos/Hause.
2. Erweitern Sie im linken Navigationsbereich Serverless und wählen Sie unter Sicherheit die Option Datenzugriffsrichtlinien aus.
3. Wählen Sie Create access policy (Zugriffsrichtlinie erstellen) aus.
4. Geben Sie einen Namen und eine Beschreibung für die Richtlinie an.
5. Geben Sie einen Namen für die erste Regel in Ihrer Richtlinie an. Beispiel: „Zugriff auf die Protokollsammlung“.

6. Wählen Sie Add principals (Prinzipale hinzufügen) und wählen Sie eine oder mehrere IAM-Rollen oder SAML users and groups (SAML-Benutzer und -Gruppen) aus, denen Sie Datenzugriff gewähren möchten.

   > **Note**
   >
   > Um Prinzipale aus den Dropdown-Menüs auswählen zu können, müssen Sie über die `iam:ListUsers`- und `iam:ListRoles`-Berechtigungen (für IAM-Prinzipale) und die `aoss:ListSecurityConfigs`-Berechtigung (für SAML-Identitäten) verfügen.

7. Wählen Sie Grant (Gewähren) und wählen Sie die Alias-, Vorlagen- und Indexberechtigungen aus, um die zugehörigen Prinzipale zu erteilen. Eine vollständige Liste der Berechtigungen und des von ihnen gewährten Zugriffs finden Sie unter the section called “Unterstützte OpenSearch API-Operationen und -Berechtigungen”.
8. (Optional) Konfigurieren Sie zusätzliche Regeln für die Richtlinie.
9. Wählen Sie Erstellen aus. Zwischen der Erstellung der Richtlinie und dem Erzwingen von Berechtigungen kann eine Verzögerung von etwa einer Minute liegen. Wenn es länger als 5 Minuten dauert, wenden Sie sich an Support.

> **Important**
>
> Wenn Ihre Richtlinie nur Indexberechtigungen (und keine Sammlungsberechtigungen) umfasst, wird Ihnen möglicherweise trotzdem eine Meldung mit dem Hinweis `Collection cannot be accessed yet. Configure data access policies so that users can access the data within this collection` für passende Sammlungen angezeigt. Sie können diese Warnung ignorieren. Zulässige Prinzipale können weiterhin ihre zugewiesenen indexbezogenen Operationen für die Sammlung ausführen.

Erstellen von Datenzugriffsrichtlinien (AWS CLI)

Verwenden Sie den Befehl, um eine Datenzugriffsrichtlinie mithilfe der OpenSearch Serverless API zu erstellen. `CreateAccessPolicy` Der Befehl akzeptiert sowohl Inline-Richtlinien als auch .json-Dateien. Inline-Richtlinien müssen als JSON-Zeichenfolge mit Escape-Zeichen codiert werden.

Die folgende Anfrage erstellt eine Datenzugriffsrichtlinie:

```
aws opensearchserverless create-access-policy \
    --name marketing \
    --type data \
    --policy "[{\"Rules\":[{\"ResourceType\":\"collection\",\"Resource\":
[\"collection/autopartsinventory\",\"collection/sales*\"],\"Permission\":
[\"aoss:UpdateCollectionItems\"]},{\"ResourceType\":\"index\",\"Resource\":
[\"index/autopartsinventory/*\",\"index/salesorders/orders*\"],\"Permission
\":[\"aoss:ReadDocument\",\"aoss:DescribeIndex\"]}],\"Principal\":
[\"arn:aws:iam::123456789012:user/Shaheen\"]}]"
```

Verwenden Sie das Format `--policy file://my-policy.json`, um die Richtlinie in einer .json-Datei bereitzustellen.

Die in der Richtlinie enthaltenen Prinzipale können jetzt die OpenSearch Operationen verwenden, für die ihnen Zugriff gewährt wurde.

Ansicht von Datenzugriffsrichtlinien

Bevor Sie eine Sammlung erstellen, möchten Sie möglicherweise eine Vorschau der vorhandenen Datenzugriffsrichtlinien in Ihrem Konto anzeigen, um zu sehen, welche ein Ressourcenmuster hat, das mit dem Namen Ihrer Sammlung übereinstimmt. In der folgenden ListAccessPoliciesAnfrage werden alle Datenzugriffsrichtlinien in Ihrem Konto aufgeführt:

```
aws opensearchserverless list-access-policies --type data
```

Die Anfrage gibt Informationen über alle konfigurierten Datenzugriffsrichtlinien zurück. Die Musterregeln, die in einer bestimmten Richtlinie definiert sind, finden Sie im Inhalt des `accessPolicySummaries` Elements in der Antwort. Notieren Sie sich das `name` Ende `type` dieser Richtlinie und verwenden Sie diese Eigenschaften in einer GetAccessPolicyAnfrage, um eine Antwort mit den folgenden Richtliniendetails zu erhalten:

```
{
    "accessPolicyDetails": [
        {
            "type": "data",
            "name": "my-policy",
            "policyVersion": "MTY2NDA1NDE4MDg1OF8x",
            "description": "My policy",
            "policy": "[{\"Rules\":[{\"ResourceType\":\"collection\",
\"Resource\":[\"collection/autopartsinventory\",\"collection/sales*\"],
\"Permission\":[\"aoss:UpdateCollectionItems\"]},{\"ResourceType\":\"index\",
```

```
\"Resource\":[\"index/autopartsinventory/*\",\"index/salesorders/orders*\"],
\"Permission\":[\"aoss:ReadDocument\",\"aoss:DescribeIndex\"]}],\"Principal\":
[\"arn:aws:iam::123456789012:user/Shaheen\"]}]",
            "createdDate": 1664054180858,
            "lastModifiedDate": 1664054180858
        }
    ]
}
```

Sie können Ressourcenfilter einbeziehen, um die Ergebnisse auf Richtlinien zu beschränken, die bestimmte Sammlungen oder Indizes enthalten:

```
aws opensearchserverless list-access-policies --type data --resource
 "index/autopartsinventory/*"
```

Verwenden Sie den GetAccessPolicyBefehl, um Details zu einer bestimmten Richtlinie anzuzeigen.

Aktualisieren von Datenzugriffsrichtlinien

Wenn Sie eine Datenzugriffsrichtlinie aktualisieren, wirkt sich dies auf alle zugehörigen Sammlungen aus. Um eine Datenzugriffsrichtlinie in der OpenSearch Serverless-Konsole zu aktualisieren, wählen Sie Datenzugriffskontrolle, wählen Sie die zu ändernde Richtlinie aus und klicken Sie auf Bearbeiten. Nehmen Sie Ihre Änderungen vor und wählen Sie Save (Speichern).

Um eine Datenzugriffsrichtlinie mithilfe der OpenSearch Serverless API zu aktualisieren, senden Sie eine `UpdateAccessPolicy` Anfrage. Sie müssen eine Richtlinienversion einbeziehen, die Sie mit den `ListAccessPolicies`- oder `GetAccessPolicy`-Befehlen abrufen können. Durch die Angabe der neuesten Richtlinienversion wird sichergestellt, dass Sie nicht versehentlich eine von einem anderen Benutzer vorgenommene Änderung überschreiben.

Die folgende UpdateAccessPolicyAnfrage aktualisiert eine Datenzugriffsrichtlinie mit einem neuen JSON-Richtliniendokument:

```
aws opensearchserverless update-access-policy \
    --name sales-inventory \
    --type data \
    --policy-version MTY2NDA1NDE4MDg1OF8x \
    --policy file://my-new-policy.json
```

Zwischen dem Aktualisieren der Richtlinie und dem Erzwingen der neuen Berechtigungen kann es einige Minuten Verzögerung geben.

Löschen von Datenzugriffsrichtlinien

Wenn Sie eine Datenzugriffsrichtlinie löschen, verlieren alle zugehörigen Sammlungen den in der Richtlinie definierten Zugriff. Stellen Sie sicher, dass Ihre IAM- und SAML-Benutzer über den entsprechenden Zugriff auf die Sammlung verfügen, bevor Sie eine Richtlinie löschen. Um eine Richtlinie in der OpenSearch Serverless-Konsole zu löschen, wählen Sie die Richtlinie aus und klicken Sie auf Löschen.

Sie können auch den DeleteAccessPolicyfolgenden Befehl verwenden:

```
aws opensearchserverless delete-access-policy --name my-policy --type data
```

Kontoübergreifender Datenzugriff

Sie können zwar keine Datenzugriffsrichtlinie mit kontoübergreifender Identität oder kontoübergreifender Erfassung erstellen, aber Sie können mit der Option „Rolle übernehmen“ dennoch einen kontoübergreifenden Zugriff einrichten. Wenn Sie beispielsweise *account-a* Eigentümer einer Sammlung sind, für die Zugriff *account-b* erforderlich ist, *account-b* kann der Benutzer von aus eine Rolle darin übernehmen. *account-a* Die Rolle muss über die IAM-Berechtigungen verfügen `aoss:APIAccessAll` und `aoss:DashboardsAccessAll` in der Datenzugriffsrichtlinie am *account-a* enthalten sein.

Greifen Sie über einen Schnittstellenendpunkt auf Amazon OpenSearch Serverless zu ()AWS PrivateLink

Sie können AWS PrivateLink damit eine private Verbindung zwischen Ihrer VPC und Amazon OpenSearch Serverless herstellen. Sie können auf OpenSearch Serverless zugreifen, als wäre es in Ihrer VPC, ohne ein Internet-Gateway, ein NAT-Gerät, eine VPN-Verbindung oder AWS Direct Connect eine Verbindung zu verwenden. Instances in Ihrer VPC benötigen keine öffentlichen IP-Adressen, um auf OpenSearch Serverless zuzugreifen. Weitere Informationen zum VPC-Netzwerkzugriff finden Sie unter Netzwerkverbindungsmuster für Amazon OpenSearch Serverless.

Sie stellen diese private Verbindung her, indem Sie einen Schnittstellen-Endpunkt erstellen, der von AWS PrivateLink unterstützt wird. Wir erstellen eine Endpunkt-Netzwerkschnittstelle in jedem Subnetz, das Sie für den Schnittstellen-Endpunkt angeben. Dabei handelt es sich um vom Anforderer verwaltete Netzwerkschnittstellen, die als Einstiegspunkt für den Datenverkehr dienen, der für Serverless bestimmt ist. OpenSearch

Weitere Informationen finden Sie unter Zugriff auf AWS-Services über AWS PrivateLink im AWS PrivateLink -Leitfaden.

Themen

- DNS-Auflösung der Sammlungsendpunkte
- VPCs und Richtlinien für den Netzwerkzugriff
- VPCs und Endpunktrichtlinien
- Überlegungen
- Erforderliche Berechtigungen
- Erstellen Sie einen Schnittstellenendpunkt für Serverless OpenSearch
- Gemeinsames VPC-Setup für Amazon Serverless OpenSearch

DNS-Auflösung der Sammlungsendpunkte

Wenn Sie einen VPC-Endpunkt erstellen, erstellt der Service eine neue Amazon Route 53 private gehostete Zone und fügt sie der VPC hinzu. Diese private gehostete Zone besteht aus einem Datensatz zur Auflösung des DNS-Wildcard-Eintrags für OpenSearch serverlose Sammlungen (`*.aoss.us-east-1.amazonaws.com`) in die für den Endpunkt verwendeten Schnittstellenadressen. Sie benötigen nur einen OpenSearch serverlosen VPC-Endpunkt in einer VPC, um auf alle Sammlungen und Dashboards in jeder VPC zuzugreifen. AWS-Region Jeder VPC mit einem Endpunkt für OpenSearch Serverless ist eine eigene private Hosting-Zone zugeordnet.

OpenSearch Serverless erstellt außerdem einen öffentlichen Route 53-Platzhalter-DNS-Eintrag für alle Sammlungen in der Region. Der DNS-Name wird in die öffentlichen IP-Adressen von OpenSearch Serverless aufgelöst. Clients OpenSearch ohne serverlosen VPC-Endpunkt oder Clients in öffentlichen Netzwerken können den öffentlichen Route 53-Resolver verwenden und mit VPCs diesen IP-Adressen auf die Sammlungen und Dashboards zugreifen. Der IP-Adresstyp (IPv4, IPv6, oder Dualstack) des VPC-Endpunkts wird anhand der Subnetze bestimmt, die beim Erstellen eines Schnittstellenendpunkts für Serverless bereitgestellt werden. OpenSearch

> **Note**
>
> OpenSearch Serverless erstellt eine zusätzliche private gehostete Amazon Route 53-Zone (`<region>.opensearch.amazonaws.com`) für die Auflösung einer OpenSearch Service-Domain. Sie können Ihren vorhandenen IPv4 VPC-Endpunkt auf Dualstack aktualisieren, indem Sie den update-vpc-endpointBefehl in der verwenden. AWS CLI

Die DNS-Resolver-Adresse für eine bestimmte VPC ist die zweite IP-Adresse der VPC CIDR. Jeder Client in der VPC muss diesen Resolver verwenden, um die VPC-Endpunktadresse für jede Sammlung abzurufen. Der Resolver verwendet eine private gehostete Zone, die von Serverless erstellt wurde. OpenSearch Es reicht aus, diesen Resolver für alle Sammlungen in einem beliebigen Konto zu verwenden. Es ist auch möglich, den VPC-Resolver für einige Sammlungsendpunkte und den öffentlichen Resolver für andere zu verwenden, obwohl dies normalerweise nicht erforderlich ist.

VPCs und Richtlinien für den Netzwerkzugriff

Um Netzwerkberechtigungen OpenSearch APIs und Dashboards für Ihre Sammlungen zu gewähren, können Sie Richtlinien für den OpenSearch serverlosen Netzwerkzugriff verwenden. Sie können diesen Netzwerkzugriff entweder von Ihren VPC-Endpunkten oder dem öffentlichen Internet aus steuern. Da Ihre Netzwerkrichtlinie nur die Zugriffsberechtigungen steuert, müssen Sie auch eine Datenzugriffsrichtlinie einrichten, die die Erlaubnis festlegt, mit den Daten in einer Sammlung und ihren Indizes zu arbeiten. Stellen Sie sich einen OpenSearch serverlosen VPC-Endpunkt als Zugriffspunkt für den Service, eine Netzwerkzugriffsrichtlinie als Zugriffspunkt auf Netzwerkebene für Sammlungen und Dashboards und eine Datenzugriffsrichtlinie als Zugriffspunkt für eine detaillierte Zugriffskontrolle für jeden Vorgang mit Daten in der Sammlung vor.

Da Sie IDs in einer Netzwerkrichtlinie mehrere VPC-Endpunkte angeben können, empfehlen wir, für jede VPC, die auf eine Sammlung zugreifen muss, einen VPC-Endpunkt zu erstellen. Diese VPCs können zu anderen AWS Konten gehören als dem Konto, dem die OpenSearch serverlose Sammlung und die Netzwerkrichtlinie gehören. Es wird nicht empfohlen, eine VPC-to-VPC Peering- oder andere Proxylösung zwischen zwei Konten zu erstellen, sodass die VPC eines Kontos den VPC-Endpunkt eines anderen Kontos verwenden kann. Dies ist weniger sicher und kostengünstiger als wenn jede VPC über einen eigenen Endpunkt verfügt. Die erste VPC wird für den Administrator der anderen VPC, der in der Netzwerkrichtlinie den Zugriff auf den Endpunkt dieser VPC eingerichtet hat, nicht ohne weiteres sichtbar sein.

VPCs und Endpunktrichtlinien

Amazon OpenSearch Serverless unterstützt Endpunktrichtlinien für VPCs. Eine Endpunktrichtlinie ist eine ressourcenbasierte IAM-Richtlinie, die Sie an einen VPC-Endpunkt anhängen, um zu steuern, welche AWS Principals den Endpunkt für den Zugriff auf Ihren Service verwenden können. AWS Weitere Informationen finden Sie unter Steuern des Zugriffs auf VPC-Endpoints mithilfe von Endpunktrichtlinien.

Um eine Endpunktrichtlinie zu verwenden, müssen Sie zunächst einen Schnittstellenendpunkt erstellen. Sie können einen Schnittstellenendpunkt entweder mit der OpenSearch Serverless-Konsole

oder der OpenSearch Serverless-API erstellen. Nachdem Sie Ihren Schnittstellenendpunkt erstellt haben, müssen Sie die Endpunktrichtlinie zum Endpunkt hinzufügen. Weitere Informationen finden Sie unter Zugriff auf Amazon OpenSearch Serverless über einen Schnittstellenendpunkt (AWS PrivateLink).

> **Note**
>
> Sie können eine Endpunktrichtlinie nicht direkt in der OpenSearch Service-Konsole definieren.

Eine Endpunktrichtlinie überschreibt oder ersetzt keine anderen identitätsbasierten Richtlinien, ressourcenbasierten Richtlinien, Netzwerkrichtlinien oder Datenzugriffsrichtlinien, die Sie möglicherweise konfiguriert haben. Weitere Informationen zur Aktualisierung von Endpunktrichtlinien finden Sie unter Steuern des Zugriffs auf VPC-Endpunkte mithilfe von Endpunktrichtlinien.

Standardmäßig gewährt eine Endpunktrichtlinie vollen Zugriff auf Ihren VPC-Endpunkt.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "*",
            "Resource": "*"
        }
    ]
}
```

Obwohl die standardmäßige VPC-Endpunktrichtlinie vollen Endpunktzugriff gewährt, können Sie eine VPC-Endpunktrichtlinie konfigurieren, um den Zugriff auf bestimmte Rollen und Benutzer zu ermöglichen. Sehen Sie sich dazu das folgende Beispiel an:

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
```

```
            "Principal": {
                "AWS": [
                    "123456789012",
                    "987654321098"
                ]
            },
            "Action": "*",
            "Resource": "*"
        }
    ]
}
```

Sie können eine OpenSearch serverlose Sammlung angeben, die als bedingtes Element in Ihre VPC-Endpunktrichtlinie aufgenommen werden soll. Sehen Sie sich dazu das folgende Beispiel an:

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aoss:collection": [
                        "coll-abc"
                    ]
                }
            }
        }
    ]
}
```

Support für `aoss:CollectionId` wird unterstützt.

```
Condition": {
         "StringEquals": {
```

```
                "aoss:CollectionId": "collection-id"
            }
}
```

Sie können SAML-Identitäten in Ihrer VPC-Endpunktrichtlinie verwenden, um den VPC-Endpunktzugriff zu bestimmen. Sie müssen (*) im Hauptbereich Ihrer VPC-Endpunktrichtlinie einen Platzhalter verwenden. Sehen Sie sich dazu das folgende Beispiel an:

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:SamlGroups": [
                        "saml/123456789012/idp123/group/football",
                        "saml/123456789012/idp123/group/soccer",
                        "saml/123456789012/idp123/group/cricket"
                    ]
                }
            }
        }
    ]
}
```

Darüber hinaus können Sie Ihre Endpunktrichtlinie so konfigurieren, dass sie eine bestimmte SAML-Prinzipalrichtlinie enthält. Sehen Sie sich dazu Folgendes an:

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Effect": "Allow",
            "Principal": "*",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aoss:SamlPrincipal": [
                        "saml/123456789012/idp123/user/user1234"]
                    }
                }
            }
        ]
    }
```

Weitere Informationen zur Verwendung der SAML-Authentifizierung mit Amazon OpenSearch Serverless finden Sie unter SAML-Authentifizierung für Amazon Serverless. OpenSearch

Sie können auch IAM- und SAML-Benutzer in dieselbe VPC-Endpunktrichtlinie aufnehmen. Sehen Sie sich dazu das folgende Beispiel an:

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aoss:SamlGroups": [
                        "saml/123456789012/idp123/group/football",
                        "saml/123456789012/idp123/group/soccer",
                        "saml/123456789012/idp123/group/cricket"
                    ]
                }
            }
        },
```

```
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "123456789012"
                ]
            },
            "Action": "*",
            "Resource": "*"
        }
    ]
}
```

Sie können auch über VPC-Endpunkte mit Schnittstellen auf eine Amazon OpenSearch Serverless-Sammlung von EC2 Amazon zugreifen. Weitere Informationen finden Sie unter Zugriff auf eine OpenSearch serverlose Sammlung von Amazon EC2 (über Schnittstellen-VPC-Endpunkte).

Überlegungen

Bevor Sie einen Schnittstellenendpunkt für OpenSearch Serverless einrichten, sollten Sie Folgendes beachten:

- OpenSearch Serverless unterstützt Aufrufe aller unterstützten OpenSearch API-Operationen (nicht Konfigurations-API-Operationen) über den Schnittstellenendpunkt.
- Nachdem Sie einen Schnittstellenendpunkt für OpenSearch Serverless erstellt haben, müssen Sie ihn dennoch in die Netzwerkzugriffsrichtlinien aufnehmen, damit er auf serverlose Sammlungen zugreifen kann.
- Standardmäßig ist der vollständige Zugriff auf OpenSearch Serverless über den Schnittstellenendpunkt zulässig. Sie können den Endpunkt-Netzwerkschnittstellen eine Sicherheitsgruppe zuordnen, um den Datenverkehr zu OpenSearch Serverless über den Schnittstellenendpunkt zu steuern.
- Ein einzelner AWS-Konto kann maximal 50 OpenSearch serverlose VPC-Endpunkte haben.
- Wenn Sie in einer Netzwerkrichtlinie den öffentlichen Internetzugriff auf die API oder die Dashboards Ihrer Sammlung aktivieren, ist Ihre Sammlung von jeder VPC und über das öffentliche Internet zugänglich.
- Wenn Sie sich vor Ort und außerhalb der VPC befinden, können Sie einen DNS-Resolver nicht direkt für die OpenSearch serverlose VPC-Endpunktlösung verwenden. Wenn Sie VPN-Zugriff benötigen, benötigt die VPC einen DNS-Proxy-Resolver, den externe Clients verwenden können.

Route 53 bietet eine Option für eingehende Endpunkte, mit der Sie DNS-Abfragen an Ihre VPC von Ihrem lokalen Netzwerk oder einer anderen VPC aus auflösen können.

- Die private gehostete Zone, die OpenSearch Serverless erstellt und an die VPC anhängt, wird vom Service verwaltet, sie wird jedoch in Ihren Amazon Route 53 Ressourcen angezeigt und Ihrem Konto in Rechnung gestellt.
- Weitere Überlegungen finden Sie unter Überlegungen im AWS PrivateLink -Leitfaden.

Erforderliche Berechtigungen

Der VPC-Zugriff für OpenSearch Serverless verwendet die folgenden AWS Identity and Access Management (IAM-) Berechtigungen. Sie können IAM-Bedingungen festlegen, um Benutzer auf bestimmte Sammlungen zu beschränken.

- `aoss:CreateVpcEndpoint` – Erstellt einen VPC-Endpunkt.
- `aoss:ListVpcEndpoints` – Listet alle VPC-Endpunkte auf.
- `aoss:BatchGetVpcEndpoint` – Zeigt Details zu einer Untergruppe von VPC-Endpunkten an.
- `aoss:UpdateVpcEndpoint` – Ändert einen VPC-Endpunkt.
- `aoss:DeleteVpcEndpoint` – Löscht einen VPC-Endpunkt.

Darüber hinaus benötigen Sie die folgenden Amazon EC2 - und Route 53-Berechtigungen, um einen VPC-Endpunkt zu erstellen.

- `ec2:CreateTags`
- `ec2:CreateVpcEndpoint`
- `ec2:DeleteVpcEndPoints`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `ec2:DescribeVpcEndpoints`
- `ec2:DescribeVpcs`
- `ec2:ModifyVpcEndPoint`
- `route53:AssociateVPCWithHostedZone`
- `route53:ChangeResourceRecordSets`

- `route53:CreateHostedZone`
- `route53:DeleteHostedZone`
- `route53:GetChange`
- `route53:GetHostedZone`
- `route53:ListHostedZonesByName`
- `route53:ListHostedZonesByVPC`
- `route53:ListResourceRecordSets`

Erstellen Sie einen Schnittstellenendpunkt für Serverless OpenSearch

Sie können einen Schnittstellenendpunkt für OpenSearch Serverless entweder mit der Konsole oder der OpenSearch Serverless API erstellen.

Um einen Schnittstellenendpunkt für eine serverlose Sammlung zu erstellen OpenSearch

1. Öffnen Sie die Amazon OpenSearch Service-Konsole zu https://console.aws.amazon.com/aos/Hause.
2. Erweitern Sie im linken Navigationsbereich Serverless und wählen Sie VPC endpoints (VPC-Endpunkte) aus.
3. Wählen Sie Create VPC endpoint (VPC-Endpunkt) erstellen.
4. Geben Sie einen Namen für den Endpunkt an.
5. Wählen Sie für VPC die VPC aus, von der aus Sie auf OpenSearch Serverless zugreifen möchten.
6. Wählen Sie für Subnetze ein Subnetz aus, von dem aus Sie auf Serverless zugreifen möchten. OpenSearch
   - Die IP-Adresse und der DNS-Typ des Endpunkts basieren auf dem Subnetztyp
     - Dualstack: Wenn alle Subnetze sowohl als auch Adressbereiche haben IPv4 IPv6
     - IPv6: Wenn alle Subnetze nur Subnetze sind IPv6
     - IPv4: Wenn alle Subnetze Adressbereiche haben IPv4
7. Wählen Sie für Sicherheitsgruppen die Sicherheitsgruppen aus, die den Security groups (Endpunkt-Netzwerkschnittstellen) zugeordnet werden sollen. Dies ist ein entscheidender Schritt, bei dem Sie die Ports, Protokolle und Quellen für eingehenden Datenverkehr einschränken, den Sie für Ihren Endpunkt autorisieren. Stellen Sie sicher, dass die Sicherheitsgruppenregeln

den Ressourcen, die den VPC-Endpunkt für die Kommunikation mit OpenSearch Serverless verwenden, die Kommunikation mit der Endpunkt-Netzwerkschnittstelle ermöglichen.

8. Wählen Sie Endpunkt erstellen aus.

Verwenden Sie den Befehl, um einen VPC-Endpunkt mithilfe der OpenSearch Serverless API zu erstellen. `CreateVpcEndpoint`

> **Note**
>
> Nachdem Sie einen Endpunkt erstellt haben, notieren Sie sich seine ID, z. B. `vpce-abc123def4EXAMPLE`. Um dem Endpunkt Zugriff auf Ihre Sammlungen zu gewähren, müssen Sie diese ID in eine oder mehrere Netzwerkzugriffsrichtlinien aufnehmen.

Nachdem Sie einen Schnittstellen-Endpunkt erstellt haben, müssen Sie ihm über Netzwerkzugriffsrichtlinien Zugriff auf Sammlungen gewähren. Weitere Informationen finden Sie unter the section called “Netzwerkzugriff”.

Gemeinsames VPC-Setup für Amazon Serverless OpenSearch

Sie können Amazon Virtual Private Cloud (VPC) verwenden, um VPC-Subnetze mit anderen AWS-Konten in Ihrer Organisation zu teilen und Netzwerkinfrastruktur wie ein VPN zwischen mehreren Ressourcen gemeinsam zu nutzen. AWS-Konten

Derzeit unterstützt Amazon OpenSearch Serverless das Herstellen einer AWS PrivateLink Verbindung zu einer gemeinsam genutzten VPC nur, wenn Sie Eigentümer dieser VPC sind. AWS PrivateLink unterstützt auch nicht die gemeinsame Nutzung von Verbindungen zwischen. AWS-Konten

Basierend auf der flexiblen und modularen Architektur von OpenSearch Serverless können Sie jedoch weiterhin eine gemeinsam genutzte VPC einrichten. Dies liegt daran, dass die OpenSearch serverlose Netzwerkinfrastruktur von der Infrastruktur für individuelle Datenerfassungen (OpenSearch Dienste) getrennt ist. Sie können daher einen AWS PrivateLink VPCe Endpunkt für ein Konto erstellen, auf dem sich eine VPC befindet, und dann eine VPCe ID in der Netzwerkrichtlinie anderer Konten verwenden, um den Datenverkehr so zu beschränken, dass er nur von dieser gemeinsam genutzten VPC kommt.

Die folgenden Verfahren beziehen sich auf ein Besitzerkonto und ein Verbraucherkonto.

Ein Besitzerkonto fungiert als gemeinsames Netzwerkkonto, mit dem Sie eine VPC einrichten und sie mit anderen Konten teilen. Verbraucherkonten sind Konten, die ihre OpenSearch serverlosen Sammlungen in der VPC erstellen und verwalten, die ihnen vom Eigentümerkonto zur Verfügung gestellt werden.

Voraussetzungen

Stellen Sie sicher, dass die folgenden Anforderungen erfüllt sind, bevor Sie die gemeinsam genutzte VPC einrichten:

- Das Konto des beabsichtigten Besitzers muss bereits eine VPC, Subnetze, eine Routing-Tabelle und andere erforderliche Ressourcen in Amazon Virtual Private Cloud eingerichtet haben. Weitere Informationen finden Sie im Amazon VPC-Benutzerhandbuch.
- Das Konto des beabsichtigten Besitzers und die Benutzerkonten müssen derselben Organisation in gehören. AWS Organizations Weitere Informationen finden Sie im AWS Organizations - Benutzerhandbuch.

Um eine gemeinsam genutzte VPC in einem account/common Besitzer-Netzwerkkonto einzurichten.

1. Melden Sie sich zu https://console.aws.amazon.com/aos/Hause bei der Amazon OpenSearch Service-Konsole an.
2. Führen Sie die Schritte unter the section called “Erstellen eines Schnittstellenendpunkts” aus. Treffen Sie dabei die folgenden Auswahlen:
   - Wählen Sie eine VPC und Subnetze aus, die mit den Verbraucherkonten in Ihrer Organisation gemeinsam genutzt werden.
3. Nachdem Sie den Endpunkt erstellt haben, notieren Sie sich die generierte VPCe ID und geben Sie sie an die Administratoren weiter, die die Einrichtungsaufgabe für Verbraucherkonten ausführen sollen.

   VPCe IDs sind im Format`vpce-abc123def4EXAMPLE`.

So richten Sie eine gemeinsam genutzte VPC in einem Verbraucherkonto ein

1. Melden Sie sich zu https://console.aws.amazon.com/aos/Hause bei der Amazon OpenSearch Service-Konsole an.
2. Verwenden Sie die angegebenen Informationen, the section called “Verwalten von Sammlungen” um eine Sammlung zu erstellen, falls Sie noch keine haben.

3. Verwenden Sie die Informationen unterthe section called “Erstellen von Netzwerkrichtlinien (Konsole)”, um eine Netzwerkrichtlinie zu erstellen. Treffen Sie dabei die folgenden Auswahlen.

   > **Note**
   >
   > Sie können zu diesem Zweck auch eine bestehende Netzwerkrichtlinie aktualisieren.

   a. Wählen Sie als Zugriffstyp VPC (empfohlen) aus.

   b. Wählen Sie für VPC-Endpunkte für den Zugriff die VPCe ID, die Sie vom Besitzerkonto erhalten haben, im folgenden Format aus. `vpce-abc123def4EXAMPLE`

   c. Gehen Sie im Bereich Ressourcentyp wie folgt vor:

      - Wählen Sie das Feld Zugriff auf OpenSearch Endpunkt aktivieren und wählen Sie dann den Sammlungsnamen oder das Sammlungsmuster aus, das verwendet werden soll, um den Zugriff von dieser gemeinsam genutzten VPC aus zu aktivieren.
      - Wählen Sie das Feld Zugriff auf OpenSearch Dashboard aktivieren und wählen Sie dann den Sammlungsnamen oder das Sammlungsmuster aus, das verwendet werden soll, um den Zugriff von dieser gemeinsam genutzten VPC aus zu ermöglichen.

4. Wählen Sie für eine neue Richtlinie Create aus. Wählen Sie für eine bestehende Richtlinie die Option Aktualisieren aus.

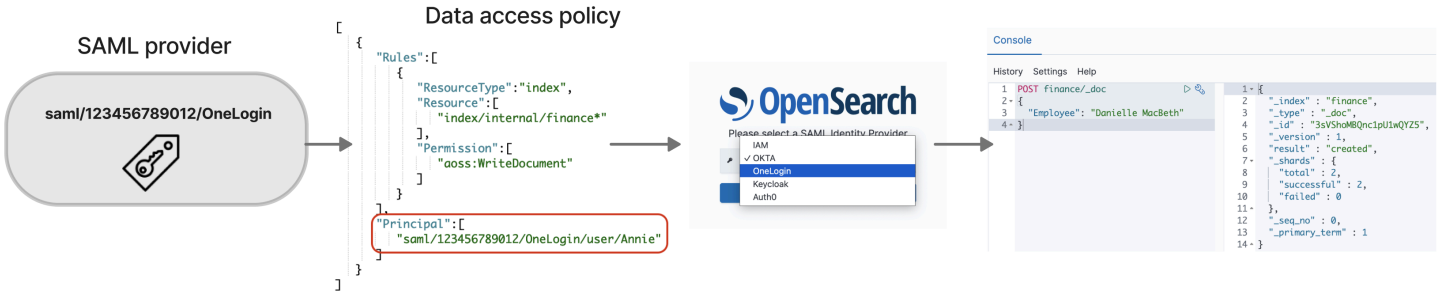
SAML-Authentifizierung für Amazon Serverless OpenSearch

Mit der SAML-Authentifizierung für Amazon OpenSearch Serverless können Sie Ihren bestehenden Identitätsanbieter verwenden, um Single Sign-On (SSO) für die OpenSearch Dashboard-Endpunkte serverloser Sammlungen anzubieten.

Mit der SAML-Authentifizierung können Sie externe Identitätsanbieter verwenden, um sich bei Dashboards anzumelden, um Daten zu indizieren und zu suchen OpenSearch . OpenSearch Serverless unterstützt Anbieter, die den SAML 2.0-Standard verwenden, wie IAM Identity Center, Okta, Keycloak, Active Directory Federation Services (AD FS) und Auth0. Sie können IAM Identity Center so konfigurieren, dass Benutzer und Gruppen aus anderen Identitätsquellen wie Okta und Microsoft OneLogin Entra ID synchronisiert werden. Eine Liste der von IAM Identity Center unterstützten Identitätsquellen und Schritte zu ihrer Konfiguration finden Sie in den Tutorials Erste Schritte im IAM Identity Center-Benutzerhandbuch.

> **Note**
>
> Die SAML-Authentifizierung ist nur für den Zugriff auf OpenSearch Dashboards über einen Webbrowser vorgesehen. Authentifizierte Benutzer können nur über die Entwicklungstools in Dashboards Anfragen an die OpenSearch API-Operationen stellen. OpenSearch Mit Ihren SAML-Anmeldeinformationen können Sie keine direkten HTTP-Anfragen an die OpenSearch API-Operationen stellen.

Zum Einrichten der SAML-Authentifizierung konfigurieren Sie zuerst einen SAML-Identitätsanbieter (IdP). Anschließend nehmen Sie einen oder mehrere Benutzer von diesem IdP in eine Datenzugriffsrichtlinie auf. Diese Richtlinie gewährt ihr bestimmte Berechtigungen für and/or Sammlungsindizes. Ein Benutzer kann sich dann bei OpenSearch Dashboards anmelden und die Aktionen ausführen, die in der Datenzugriffsrichtlinie zulässig sind.



Themen

- Überlegungen
- Erforderliche Berechtigungen
- Erstellen von SAML-Anbietern (Konsole)
- Auf Dashboards zugreifen OpenSearch
- Gewährung von Zugriff für SAML-Identitäten auf Sammlungsdaten
- Erstellen von SAML-Anbietern (AWS CLI)
- Anzeigen von SAML-Anbietern
- Aktualisieren von SAML-Anbietern
- Löschen von SAML-Anbietern

Überlegungen

Berücksichtigen Sie beim Konfigurieren der SAML-Authentifizierung Folgendes:

- Signierte und verschlüsselte Anfragen werden nicht unterstützt.
- Verschlüsselte Aussagen werden nicht unterstützt.
- Vom Identitätsanbieter initiierte Authentifizierung und Abmeldung werden nicht unterstützt.
- Service Control Policies (SCP) werden im Fall von Nicht-IAM-Identitäten (wie SAML in Amazon OpenSearch Serverless und SAML und grundlegende interne Benutzerautorisierung für Amazon Service) nicht angewendet oder bewertet. OpenSearch

Erforderliche Berechtigungen

Die SAML-Authentifizierung für OpenSearch Serverless verwendet die folgenden (IAM-) Berechtigungen: AWS Identity and Access Management

- `aoss:CreateSecurityConfig` – Erstellt einen SAML-Anbieter.
- `aoss:ListSecurityConfig` – Listet alle SAML-Anbieter im aktuellen Konto auf.
- `aoss:GetSecurityConfig` – Zeigt Informationen zum SAML-Anbieter an.
- `aoss:UpdateSecurityConfig` – Ändert eine bestimmte SAML-Anbieterkonfiguration, einschließlich der XML-Metadaten.
- `aoss:DeleteSecurityConfig` – Löscht einen SAML-Anbieter.

Die folgende identitätsbasierte Zugriffsrichtlinie ermöglicht einem Benutzer die Verwaltung aller IdP-Konfigurationen:

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "aoss:CreateSecurityConfig",
                "aoss:DeleteSecurityConfig",
                "aoss:GetSecurityConfig",
```

```
                "aoss:UpdateSecurityConfig",
                "aoss:ListSecurityConfigs"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Beachten Sie, dass das `Resource`-Element ein Platzhalter sein muss.

Erstellen von SAML-Anbietern (Konsole)

In diesen Schritten wird erläutert, wie SAML-Anbieter erstellt werden. Dies ermöglicht die SAML-Authentifizierung mit vom Service Provider (SP) initiierter Authentifizierung für Dashboards. OpenSearch Die vom Identitätsanbieter initiierte Authentifizierung wird nicht unterstützt.

Um die SAML-Authentifizierung für Dashboards zu aktivieren OpenSearch

1. Melden Sie sich zu https://console.aws.amazon.com/aos/Hause bei der Amazon OpenSearch Service-Konsole an.
2. Erweitern Sie im linken Navigationsbereich Serverless und wählen Sie SAML authentication (SAML-Authentifizierung) aus.
3. Wählen Sie Add SAML provider (SAML-Anbieter hinzufügen).
4. Geben Sie einen Namen und eine Beschreibung für die Sammlung an.

   > **Note**
   >
   > Der von Ihnen angegebene Name ist öffentlich zugänglich und wird in einem Drop-down-Menü angezeigt, wenn sich Benutzer bei OpenSearch Dashboards anmelden. Stellen Sie sicher, dass der Name leicht erkennbar ist und keine vertraulichen Informationen über Ihren Identitätsanbieter preisgibt.

5. Kopieren Sie unter Configure your IdP (Konfigurieren Ihres IdP) die URL des Assertion Consumer Service (ACS).
6. Verwenden Sie die ACS-URL, die Sie gerade kopiert haben, um Ihren Identitätsanbieter zu konfigurieren. Terminologie und Schritte variieren je nach Anbieter. Schlagen Sie in der Dokumentation Ihres Anbieters nach.

In Okta erstellen Sie beispielsweise eine „SAML 2.0-Webanwendung“ und geben die ACS-URL als Single Sign On URL (Single-Sign-On-URL), Recipient URL (Empfänger-URL) und Destination URL (Ziel-URL) an. Für Auth0 geben Sie ihn unter Zulässiger Rückruf an. URLs

7. Geben Sie die Zielgruppeneinschränkung an, falls Ihr IdP ein Feld dafür aufweist. Die Zielgruppenbeschränkung ist ein Wert innerhalb der SAML-Aussagen, der angibt, für wen die Aussagen bestimmt ist. Geben Sie für OpenSearch Serverless an. `aws:opensearch:<aws account id>` Beispiel, `aws:opensearch:`*`123456789012`*.

   Der Name des Feldes für die Zielgruppenbeschränkung variiert je nach Anbieter. Für Okta ist es der Audience URI (SP Entity ID) (Zielgruppen-URI (SP-Entitäts-ID)). Für IAM Identity Center ist es die Application SAML audience (SAML-Zielgruppe der Anwendung).

8. Wenn Sie IAM Identity Center verwenden, müssen Sie außerdem die folgende Attributzuordnung angeben: `Subject=${user:name}`, mit einem Format von `unspecified`.

9. Nachdem Sie Ihren Identitätsanbieter konfiguriert haben, wird eine IdP-Metadatendatei generiert. Diese XML-Datei enthält Informationen zum Anbieter, z. B. ein TLS-Zertifikat, Single Sign-On-Endpunkte und die Entitäts-ID des Identitätsanbieters.

   Kopieren Sie den Text aus der IdP-Metadaten-Datei und fügen Sie ihn in das Feld Provide metadata from your IdP (Metadaten von Ihrem IdP bereitstellen) ein. Wählen Sie alternativ Aus XML-Datei importieren und laden Sie die Datei hoch. Die Metadatendatei sollte ungefähr so aussehen:

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor entityID="entity-id"
 xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
  <md:IDPSSODescriptor WantAuthnRequestsSigned="false"
 protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>tls-certificate</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>s
    </md:KeyDescriptor>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</
md:NameIDFormat>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</
md:NameIDFormat>
```

```
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
POST" Location="idp-sso-url"/>
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
Redirect" Location="idp-sso-url"/>
  </md:IDPSSODescriptor>
</md:EntityDescriptor>
```

10. Lassen Sie das Feld Benutzerdefiniertes Benutzer-ID-Attribut leer, um das `NameID` Element der SAML-Assertion für den Benutzernamen zu verwenden. Wenn Ihre Assertion dieses Standardelement nicht verwendet und stattdessen den Benutzernamen als benutzerdefiniertes Attribut enthält, geben Sie dieses Attribut hier an. Bei Attributen wird zwischen Groß- und Kleinschreibung unterschieden. Es wird nur ein einzelnes Benutzerattribut unterstützt.

    Das folgende Beispiel zeigt ein Überschreibungsattribut für `NameID` in der SAML-Aussage:

    ```
    <saml2:Attribute Name="UserId" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
    format:basic">
      <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:type="xs:string">annie</saml2:AttributeValue>
    </saml2:Attribute>
    ```

11. (Optional) Geben Sie im Feld Group attribute (Gruppenattribut) ein benutzerdefiniertes Attribut an, z. B. `role` oder `group`. Es wird nur ein einzelnes Gruppenattribut unterstützt. Es gibt kein Standard-Gruppenattribut. Wenn Sie keine angeben, können Ihre Datenzugriffsrichtlinien nur Benutzerprinzipale enthalten.

    Das folgende Beispiel zeigt ein Gruppenattribut in der SAML-Aussage:

    ```
    <saml2:Attribute Name="department"
     NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
        <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:type="xs:string">finance</saml2:AttributeValue>
    </saml2:Attribute>
    ```

12. Standardmäßig meldet OpenSearch Dashboards Benutzer nach 24 Stunden ab. Sie können diesen Wert auf eine beliebige Zahl zwischen 1 und 12 Stunden (15 und 720 Minuten) konfigurieren, indem Sie das OpenSearch Dashboard-Timeout angeben. Wenn Sie versuchen, das Timeout auf 15 Minuten oder weniger festzulegen, wird Ihre Sitzung auf eine Stunde zurückgesetzt.

13. Wählen Sie Create SAML provider (SAML-Anbieter erstellen).

Auf Dashboards zugreifen OpenSearch

Nachdem Sie einen SAML-Anbieter konfiguriert haben, können alle Benutzer und Gruppen, die diesem Anbieter zugeordnet sind, zum OpenSearch Dashboards-Endpunkt navigieren. Die Dashboard-URL hat das Format *`collection-endpoint`*`/_dashboards/` für alle Sammlungen.

Wenn Sie SAML aktiviert haben, werden Sie durch Auswahl des Links in der AWS Management Console zur IdP-Auswahlseite weitergeleitet, auf der Sie sich mit Ihren SAML-Anmeldeinformationen anmelden können. Verwenden Sie zunächst das Dropdown-Menü, um einen Identitätsanbieter auszuwählen:



Melden Sie sich anschließend mit den Anmeldeinformationen Ihres Identitätsanbieters an.

Wenn Sie SAML nicht aktiviert haben, werden Sie durch Auswahl des Links auf der AWS Management Console weitergeleitet, um sich als IAM-Benutzer oder als IAM-Rolle anzumelden, ohne dass SAML aktiviert ist.

Gewährung von Zugriff für SAML-Identitäten auf Sammlungsdaten

Nachdem Sie einen SAML-Anbieter erstellt haben, müssen Sie den zugrunde liegenden Benutzern und Gruppen immer noch Zugriff auf die Daten in Ihren Sammlungen gewähren. Sie gewähren Zugriff über Datenzugriffsrichtlinien. Solange Sie Benutzern keinen Zugriff gewähren, können diese keine Daten in Ihren Sammlungen lesen, schreiben oder löschen.

Um Zugriff zu gewähren, erstellen Sie eine Datenzugriffsrichtlinie und geben Sie Ihre and/or SAML-Benutzergruppe IDs in der Erklärung an: `Principal`

```
[
   {
      "Rules":[
       ...
      ],
      "Principal":[
         "saml/987654321098/myprovider/user/Shaheen",
         "saml/987654321098/myprovider/group/finance"
      ]
   }
]
```

Sie können Zugriff auf Sammlungen, Indizes oder beides gewähren. Wenn Sie möchten, dass verschiedene Benutzer über unterschiedliche Berechtigungen verfügen, erstellen Sie mehrere Regeln. Eine Liste der verfügbaren Berechtigungen finden Sie unter Unterstützte Richtlinienberechtigungen. Weitere Informationen zum Formatieren einer Zugriffsrichtlinie finden Sie unter Richtliniensyntax.

Erstellen von SAML-Anbietern (AWS CLI)

Um einen SAML-Anbieter mithilfe der OpenSearch Serverless API zu erstellen, senden Sie eine Anfrage: CreateSecurityConfig

```
aws opensearchserverless create-security-config \
    --name myprovider \
    --type saml \
```

```
    --saml-options file://saml-auth0.json
```

Geben Sie `saml-options`, einschließlich der Metadaten-XML, als Schlüsselwert-Zuordnung in einer .json-Datei an. Die Metadaten-XML muss als JSON-Escape-Zeichenfolge codiert werden.

```
{
   "sessionTimeout": 70,
   "groupAttribute": "department",
   "userAttribute": "userid",
   "metadata": "<EntityDescriptor xmlns=\"urn:oasis:names:tc:SAML:2.0:metadata
\" ... ... ... IDPSSODescriptor>\r\n<\/EntityDescriptor>"
}
```

Anzeigen von SAML-Anbietern

In der folgenden ListSecurityConfigsAnfrage sind alle SAML-Anbieter in Ihrem Konto aufgeführt:

```
aws opensearchserverless list-security-configs --type saml
```

Die Anfrage gibt Informationen zu allen vorhandenen SAML-Anbietern zurück, einschließlich der vollständigen IdP-Metadaten, die Ihr Identitätsanbieter generiert:

```
{
   "securityConfigDetails": [
      {
         "configVersion": "MTY2NDA1MjY4NDQ5M18x",
         "createdDate": 1664054180858,
         "description": "Example SAML provider",
         "id": "saml/123456789012/myprovider",
         "lastModifiedDate": 1664054180858,
         "samlOptions": {
            "groupAttribute": "department",
            "metadata": "<EntityDescriptor xmlns=\"urn:oasis:names:tc:SAML:2.0:metadata
\" ... ... ... IDPSSODescriptor>\r\n<\/EntityDescriptor>",
            "sessionTimeout": 120,
            "userAttribute": "userid"
         }
      }
   ]
}
```

Um Details zu einem bestimmten Anbieter anzuzeigen, einschließlich des `configVersion` für zukünftige Updates, senden Sie eine `GetSecurityConfig`-Anfrage.

Aktualisieren von SAML-Anbietern

Um einen SAML-Anbieter mithilfe der OpenSearch Serverless-Konsole zu aktualisieren, wählen Sie SAML-Authentifizierung, wählen Sie Ihren Identitätsanbieter aus und klicken Sie auf Bearbeiten. Sie können alle Felder ändern, einschließlich der Metadaten und derb benutzerdefinierten Attribute.

Um einen Anbieter über die OpenSearch Serverless API zu aktualisieren, senden Sie eine UpdateSecurityConfigAnfrage und geben Sie die ID der zu aktualisierenden Richtlinie an. Sie müssen auch eine Konfigurationsversion angeben, die Sie mithilfe der `ListSecurityConfigs`- oder `GetSecurityConfig`-Befehle abrufen können. Die Angabe der neuesten Version stellt sicher, dass Sie nicht versehentlich eine Änderung überschreiben, die von jemand anderem vorgenommen wurde.

Die folgende Anfrage aktualisiert die SAML-Optionen für einen Anbieter:

```
aws opensearchserverless update-security-config \
    --id saml/123456789012/myprovider \
    --type saml \
    --saml-options file://saml-auth0.json \
    --config-version MTY2NDA1MjY4NDQ5M18x
```

Geben Sie Ihre SAML-Konfigurationsoptionen als Schlüsselwert-Zuordnung in einer .json-Datei an.

> **Important**
>
> Aktualisierungen von SAML-Optionen erfolgen nicht inkrementell. Wenn Sie bei einer Aktualisierung keinen Wert für einen Parameter im `SAMLOptions`-Objekt angeben, werden die vorhandenen Werte mit leeren Werten überschrieben. Wenn die aktuelle Konfiguration beispielsweise einen Wert für `userAttribute` enthält und Sie dann eine Aktualisierung vornehmen und diesen Wert nicht angeben, wird der Wert aus der Konfiguration entfernt. Stellen Sie sicher, dass Sie die vorhandenen Werte kennen, bevor Sie eine Aktualisierung durch Aufrufen der `GetSecurityConfig`-Operation vornehmen.

Löschen von SAML-Anbietern

Wenn Sie einen SAML-Anbieter löschen, sind alle Verweise auf zugeordnete Benutzer und Gruppen in Ihren Datenzugriffsrichtlinien nicht mehr funktionsfähig. Um Verwirrung zu vermeiden, empfehlen

wir Ihnen, alle Verweise auf den Endpunkt in Ihren Zugriffsrichtlinien zu entfernen, bevor Sie den Endpunkt löschen.

Um einen SAML-Anbieter mithilfe der OpenSearch Serverless-Konsole zu löschen, wählen Sie Authentifizierung, wählen Sie den Anbieter aus und klicken Sie auf Löschen.

Um einen Anbieter über die OpenSearch Serverless API zu löschen, senden Sie eine Anfrage: DeleteSecurityConfig

```
aws opensearchserverless delete-security-config --id saml/123456789012/myprovider
```

Compliance-Validierung für Amazon OpenSearch Serverless

Externe Prüfer bewerten im Rahmen verschiedener -Compliance-Programme die Sicherheit und AWS Compliance von Amazon OpenSearch Serverless. Zu diesen Programmen gehören SOC, PCI und HIPAA.

Um zu erfahren, ob AWS-Service ein in den Geltungsbereich bestimmter Compliance-Programme fällt, siehe AWS-Services in Geltungsbereich nach Compliance-Programm AWS-Services und wählen Sie das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter AWS Compliance-Programme AWS .

Die Auditberichte von Drittanbietern lassen sich mit herunterlade AWS Artifact. Weitere Informationen finden Sie unter Herunterladen AWS Artifact .

Ihre Compliance-Verantwortung bei Verwendung AWS-Services hängt von der Vertraulichkeit der Daten, den Compliance-Zielen des Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS stellt die folgenden Ressourcen bereit, um Sie bei der Compliance zu unterstützen:

- Compliance und Governance im Bereich Sicherheit – In diesen Anleitungen für die Lösungsimplementierung werden Überlegungen zur Architektur behandelt. Außerdem werden Schritte für die Bereitstellung von Sicherheits- und Compliance-Features beschrieben.
- Referenz für berechtigte HIPAA-Services – Listet berechtigte HIPAA-Services auf. Nicht alle AWS-Services sind HIPAA-berechtigt.
- AWS -Compliance-Ressourcen AWS — Diese Arbeitsbücher und Leitfäden könnten für Ihre Branche und Ihren Standort relevant sein.
- AWS -Compliance-Leitfäden für Kunden — Verstehen Sie das Modell der geteilten Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten

Methoden zum Schutz von zusammengefasst AWS-Services und die Leitlinien den Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO) zugeordnet.

- Auswertung von Ressourcen mit Regeln im AWS Config -Entwicklerhandbuch — Der AWS Config -Service bewertet, wie gut Ihre Ressourcenkonfigurationen mit internen Praktiken, Branchenrichtlinien und Vorschriften übereinstimmen.
- AWS Security Hub— Auf diese AWS-Service Weise erhalten Sie einen umfassenden Überblick über Ihren internen Sicherheitsstatus. AWS Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Die Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerelementreferenz.
- Amazon GuardDuty — Dieser AWS-Service erkennt potenzielle Bedrohungen für Ihre AWS-Konten, Workloads, Container und Daten, indem er Ihre Umgebung auf verdächtige und böswillige Aktivitäten überwacht. GuardDuty kann Ihnen helfen, verschiedenen Compliance-Anforderungen wie PCI DSS nachzukommen, indem es die Anforderungen zur Erkennung von Eindringlingen erfüllt, die in bestimmten Compliance-Frameworks vorgeschrieben sind.
- AWS Audit Manager— Dieser AWS-Service hilft Ihnen, Ihre AWS -Nutzung kontinuierlich zu überprüfen, um den Umgang mit Risiken und die Compliance von Branchenstandards zu vereinfachen.

Markieren von OpenSearch Amazon--Serverless-Sammlungen

Mit Tags können Sie einer OpenSearch Amazon--Serverless-Sammlung beliebige Informationen zuweisen, damit Sie diese Informationen kategorisieren und filtern können. Ein Tag ist ein Metadaten-Etikett, das von Ihnen oder von einer AWS -Ressource AWS zugewiesen wird.

Jedes Tag besteht aus einem Schlüssel und einem Wert. Für Tags, die Sie zuweisen, definieren Sie einen Schlüssel und einen Wert. So können Sie beispielsweise den Schlüssel als `stage` und den Wert für eine Ressource als `test` definieren.

Mit Tags können Sie Ihre AWS Ressourcen identifizieren und organisieren. Viele AWS -Services unterstützen das Markieren mit Tags (kurz: Tagging). So können Ressourcen aus verschiedenen Services dasselbe Tag zuweisen, um anzugeben, dass die Ressourcen verbunden sind. Beispielsweise könnten Sie einer OpenSearch Serverless-Sammlung dasselbe Tag zuweisen, das Sie einer OpenSearch Amazon-Service-Domain zuweisen.

Die primäre Ressource in OpenSearch Serverless ist eine Sammlung. Sie können die OpenSearch Servicekonsole, die AWS CLI, die OpenSearch serverlosen API-Operationen oder die verwenden, um Stichwörter AWS SDKs zu einer Sammlung hinzuzufügen, zu verwalten und zu entfernen.

Erforderliche Berechtigungen

OpenSearch Serverless verwendet die folgenden AWS Identity and Access Management Access Analyzer (IAM) -Berechtigungen zum Markieren von Sammlungen:

- `aoss:TagResource`
- `aoss:ListTagsForResource`
- `aoss:UntagResource`

Markieren von Sammlungen (Konsole)

Die Konsole ist die einfachste Möglichkeit, eine Sammlung zu markieren.

So erstellen Sie ein Tag (Konsole)

1. Melden Sie sich zu https://console.aws.amazon.com/aos/Hause bei der Amazon OpenSearch Service-Konsole an.
2. Erweitern Sie im linken Navigationsbereich Serverless und wählen Sie Collections (Sammlungen) aus.
3. Wählen Sie die Sammlung aus, der Sie Tags hinzufügen möchten, und gehen Sie zur Registerkarte Tags.
4. Wählen Sie Verwalten und neues Tag hinzufügen.
5. Geben Sie einen Tag-Schlüssel und einen optionalen Wert ein.
6. Wählen Sie Speichern.

Um ein Tag zu löschen, führen Sie die gleichen Schritte aus und wählen Sie Entfernen auf der Seite Tags verwalten.

Weitere Informationen zur Verwendung der Konsole für die Arbeit mit Tags finden Sie unter Tag Editor im AWS Handbuch „Erste Schritte“ der Managementkonsole.

Sammlungen taggen ()AWS CLI

Um eine Sammlung mit dem zu taggen AWS CLI, senden Sie eine TagResourceAnfrage:

```
aws opensearchserverless tag-resource
  --resource-arn arn:aws:aoss:us-east-1:123456789012:collection/my-collection
  --tags Key=service,Value=aoss Key=source,Value=logs
```

Zeigen Sie die vorhandenen Tags für eine Sammlung mit dem ListTagsForResourcefolgenden Befehl an:

```
aws opensearchserverless list-tags-for-resource
  --resource-arn arn:aws:aoss:us-east-1:123456789012:collection/my-collection
```

Entfernen Sie Tags mit dem UntagResourcefolgenden Befehl aus einer Sammlung:

```
aws opensearchserverless untag-resource
  --resource-arn arn:aws:aoss:us-east-1:123456789012:collection/my-collection
  --tag-keys service
```

Unterstützte Vorgänge und Plugins OpenSearch

Amazon OpenSearch Serverless unterstützt eine Vielzahl von OpenSearch Plugins sowie eine Teilmenge der in verfügbaren API-Operationen für Indizierung, Suche und Metadaten. OpenSearch Sie können die Berechtigungen in der linken Spalte der Tabelle in Datenzugriffsrichtlinien aufnehmen, um den Zugriff auf bestimmte Vorgänge zu beschränken.

Themen

- Unterstützte OpenSearch API-Operationen und -Berechtigungen
- Unterstützte OpenSearch Plugins

Unterstützte OpenSearch API-Operationen und -Berechtigungen

Die folgende Tabelle listet die API-Operationen auf, die OpenSearch Serverless unterstützt, zusammen mit ihren entsprechenden Berechtigungen für Datenzugriffsrichtlinien:

Berechtigung der Datenzugriffsrichtlinie	OpenSearch API-Operationen	Beschreibung und Vorbehalte
`aoss:CreateIndex`	PUT <index>	Erstellen Sie Indizes. Weitere Informationen finden Sie unter Index erstellen. **Note** Diese Berechtigung gilt auch für die Erstellung von Indizes mit den Beispieldaten auf OpenSearch Dashboards.
`aoss:DescribeIndex`	• GET <index> • GET <index>/_mapping • GET <index>/_mappings • GET <index>/_setting • GET <index>/_setting/<setting> • GET <index>/_settings • GET <index>/_settings/<setting> • GET _cat/indices • GET _mapping • GET _mappings • GET _resolve/index/<index> • KOPF <index>	Beschreiben Sie Indizes. Weitere Informationen finden Sie in den folgenden Ressourcen: • Get index • Eine Zuordnung abrufen • Einstellungen abrufen • Der Index ist vorhanden • CAT-Indizes (Die Antwort enthält keine `health status` Or-Felder.)
`aoss:WriteDocument`	• LÖSCHEN SIE <index>/_doc/<id> • POST <index>/_bulk	Schreiben und Aktualisieren Sie Dokumente. Weitere Informationen

Berechtigung der Datenzugriffsrichtlinie	OpenSearch API-Operationen	Beschreibung und Vorbehalte
	• POST <index>/_create/<id> (nur für Suchsammlungstypen) • POST <index>/_doc • POST <index>/_update/<id> (nur für Suchsammlungstypen) • POST _bulk • PUT <index>/_create/<id> (nur für Suchsammlungstypen) • PUT <index>/_doc/<id> (nur für Suchsammlungstypen)	finden Sie in den folgenden Ressourcen: • Masse • Datenindex **Note** Einige Operationen sind nur für Sammlungen des Typs SEARCH zulässig. Weitere Informationen finden Sie unter the section called “Auswahl eines Sammlungstyps”.

Berechtigung der Datenzugriffsrichtlinie	OpenSearch API-Operationen	Beschreibung und Vorbehalte
`aoss:ReadDocument`	• Holen Sie sich <index>/_analyz • GET <index>/_doc/<id> • GET <index>/_explain/<id> • GET <index>/_mget • GET <index>/_source/<id> • GET <index>/_count • GET <index>/_field_caps • GET <index>/_msearch • GET <index>/_rank_eval • GET <index>/_search • GET <index>/_validate/<query> • GET _analyze • GET _field_caps • GET _mget • GET _search • GET /_search/point_in_time/_all • HEAD <index>/_doc/<id> • HEAD <index>/_source/<id> • BEITRAG /_plugins/_sql • POST /_plugins/_ppl • BEITRAG /_plugins/_sql/_explain • BEITRAG /_plugins/_ppl/_explain • BEITRAG /_plugins/_ppl/_close • POST <index>/_analyze • BEITRAG /_search/point_in_time • POST <index>/_explain/<id> • POST <index>/_count • POST <index>/_field_caps	Lesen Sie Dokumente . Weitere Informationen finden Sie in den folgenden Ressourcen: • Textanalyse durchführen • Dokument abrufen • Count • DSL abfragen • Auswertung der Evaluierung • API analysieren • Explain • Zeitpunkt • SQL und PPL

Berechtigung der Datenzugriffsrichtlinie	OpenSearch API-Operationen	Beschreibung und Vorbehalte
	• POST <index>/_rank_eval • POST <index>/_search • POST _analyze • POST _field_caps • POST _search • LÖSCHEN SIE /_search/point_in_time/_all • LÖSCHEN SIE /_search/point_in_time	
`aoss:DeleteIndex`	DELETE <target>	Löschen Sie Indizes. Weitere Informationen finden Sie unter Index löschen.
`aoss:UpdateIndex`	• POST _mapping • POST <index>/_mapping/ • POST <index>/_mappings/ • POST <index>/_setting • POST <index>/_settings • POST _setting • POST _settings • PUT _mapping • GET <index>/_mapping • GET <index>/_mappings/ • GET <index>/_setting • GET <index>/_settings • PUT _setting • PUT _settings	Aktualisieren von Index-Einstellungen. Weitere Informationen finden Sie in den folgenden Ressourcen: • Zuweisung • Einstellungen aktualisieren

Berechtigung der Datenzugriffsrichtlinie	OpenSearch API-Operationen	Beschreibung und Vorbehalte
`aoss:CreateCollectionItems`	POST _aliases	Erstellen Sie Index-Aliase. Weitere Informationen finden Sie unter Aliasse erstellen.
`aoss:DescribeCollectionItems`	• GET <index>/_alias/<alias> • GET _alias • GET _alias/<alias> • GET _cat/aliases • GET _cat/templates • GET _cat/templates/<template_name> • GET _component_template • GET _component_template/<component-template> • GET _index_template • GET _index_template/<index-template> • HEAD _alias/<alias> • HEAD _component_template/<component-template> • HEAD _index_template/<name> • HEAD <index>/_alias/<alias>	Beschreiben Sie Aliase und Index-Vorlagen. Weitere Informationen finden Sie in den folgenden Ressourcen: • Verwalten von Aliase • Index-Vorlagen

Berechtigung der Datenzugriffsrichtlinie	OpenSearch API-Operationen	Beschreibung und Vorbehalte
`aoss:UpdateCollectionItems`	• POST <index>/_alias/<alias> • POST <index>/_aliases/<alias> • POST _component_template/<component-template> • POST _index_template/<index-template> • PUT <index>/_alias/<alias> • PUT <index>/_aliases/<alias> • PUT _component_template/<component-template> • PUT _index_template/<index-template>	Aktualisieren Sie Aliase und Index-Vorlagen. Weitere Informationen finden Sie in den folgenden Ressourcen: • Aliase indizieren • Index-Vorlagen
`aoss:DeleteCollectionItems`	• DELETE <index>/_alias/<alias> • DELETE _component_template/<component-template> • DELETE _index_template/<index-template> • DELETE <index>/_aliases/<alias>	Löschen Sie Aliase und Index-Vorlagen. Weitere Informationen finden Sie in den folgenden Ressourcen: • Aliase löschen • Eine Vorlage löschen

Unterstützte OpenSearch Plugins

OpenSearch Serverless OpenSearch Serverless stellt Plugins automatisch bereit und verwaltet sie für Sie.

Analyse-Plugins

- ICU Analysis
- Japanese (kuromoji) Analysis
- Koreanische (Nori)-Analyse
- Phonetic Analysis

- Smart Chinese Analysis
- Stempel Polish Analysis
- Ukrainische Analyse

Mapper-Plugins

- Mapper Size
- Mapper Murmur3
- Mapper-annotierter Text

Skript-Plugins

- Painless
- Expression
- Mustache

Darüber hinaus enthält OpenSearch Serverless alle Plugins, die als Module geliefert werden.

Überwachen von Amazon OpenSearch Serverless

Überwachung ist wichtig, um die Zuverlässigkeit, Verfügbarkeit und Leistung von Amazon OpenSearch Serverless und Ihren anderen AWS -Lösungen aufrechtzuerhalten. AWS stellt die folgenden Überwachungstools zur Verfügung, um OpenSearch Serverless zu überwachen, Sie zu informieren, wenn etwas nicht funktioniert, und gegebenenfalls automatische Maßnahmen zu ergreifen:

- Amazon CloudWatch überwacht Ihre AWS -Ressourcen und die in ausgeführten Anwendungen AWS in Echtzeit. Sie können Kennzahlen erfassen und verfolgen, benutzerdefinierte Dashboards erstellen und Alarme festlegen, die Sie benachrichtigen oder Maßnahmen ergreifen, wenn eine bestimmte Metrik einen von Ihnen festgelegten Schwellenwert erreicht.

  Beispielsweise können Sie mit die CPU-Auslastung oder andere Metriken Ihrer EC2 Amazon-Instances CloudWatch erfassen und bei Bedarf automatisch neue Instances starten. Weitere Informationen finden Sie im CloudWatch Benutzerhandbuch für Amazon.
- AWS CloudTrail erfasst API-Aufrufe und zugehörige Ereignisse, die von oder im Namen Ihrer AWS-Konto. Es stellt die Protokolldateien in einem von Ihnen angegebenen Amazon-S3-Bucket

bereit. Sie können die Benutzer und Konten, die aufgerufen haben AWS, identifizieren, sowie die Quell-IP-Adresse, von der diese Aufrufe stammen, und den Zeitpunkt der Aufrufe ermitteln. Weitere Informationen finden Sie im AWS CloudTrail -Benutzerhandbuch.

- Amazon EventBridge liefert nahezu in Echtzeit einen Strom von Systemereignissen, die Änderungen in Ihren OpenSearch Service-Domänen beschreiben. Sie können Regeln erstellen, die bestimmte Ereignisse überwachen und automatisierte Aktionen in anderen auslösen, AWS-Services wenn diese Ereignisse auftreten. Weitere Informationen finden Sie im EventBridge Benutzerhandbuch für Amazon.

OpenSearch Serverlose Überwachung mit Amazon CloudWatch

Sie können Amazon OpenSearch Serverless mit überwachen CloudWatch, wobei Rohdaten erfasst und in lesbare Metriken nahezu in Echtzeit verarbeitet werden. Diese Statistiken werden 15 Monate gespeichert, damit Sie auf Verlaufsinformationen zugreifen können und einen besseren Überblick darüber erhalten, wie Ihre Webanwendung oder der Service ausgeführt werden.

Sie können auch Alarme einrichten, die auf bestimmte Grenzwerte achten und Benachrichtigungen senden oder Aktivitäten auslösen, wenn diese Grenzwerte erreicht werden. Weitere Informationen finden Sie im CloudWatch Benutzerhandbuch für Amazon.

OpenSearch Serverless meldet die folgenden Metriken im `AWS/AOSS` Namespace.

Metrik	Beschreibung
`ActiveCollection`	Zeigt an, ob eine Sammlung aktiv ist. Ein Wert von 1 bedeutet, dass sich die Sammlung in einem `ACTIVE`-Status befindet. Dieser Wert wird bei erfolgreicher Erstellung einer Sammlung ausgegeben und verbleibt 1, bis Sie die Sammlung löschen. Die Metrik darf keinen Wert von 0 haben. Relevante Statistiken: Maximum Dimensionen: `ClientId`, `CollectionId` , `CollectionName` Frequenz: 60 Sekunden

Metrik	Beschreibung
`DeletedDocuments`	Die Gesamtzahl der gelöschten Dokumente. Relevante Statistiken: Durchschnitt, Summe Dimensionen: `ClientId`, `CollectionId` , `CollectionName` , `IndexId`, `IndexName` Frequenz: 60 Sekunden
`IndexingOCU`	Die Anzahl der OpenSearch Recheneinheiten (OCUs), die zum Erfassen von Sammlungsdaten verwendet werden. Diese Metrik gilt auf Kontoebene. Relevante Statistiken: Summe Dimensionen: `ClientId` Frequenz: 60 Sekunden
`IngestionDataRate`	Die Indexierungsrate in GB pro Sekunde für eine Sammlung oder einen Index. Diese Metrik gilt nur für Anfragen zur Massenindexierung. Relevante Statistiken: Summe Dimensionen: `ClientId`, `CollectionId` , `CollectionName` , `IndexId`, `IndexName` Frequenz: 60 Sekunden

Metrik	Beschreibung
IngestionDocumentErrors	Die Gesamtzahl von Dokumentfehlern während der Erfassung für eine Sammlung oder einen Index. Nach einer erfolgreichen Massenindizierungsanfrage verarbeiten Autoren die Anfrage und geben Fehler für alle fehlgesch lagenen Dokumente innerhalb der Anfrage aus. Relevante Statistiken: Summe Dimensionen: ClientId, CollectionId , CollectionName , IndexId, IndexName Frequenz: 60 Sekunden
IngestionDocumentRate	Die Rate pro Sekunde, mit der Dokumente in eine Sammlung oder einen Index aufgenommen werden. Diese Metrik gilt nur für Anfragen zur Massenindizierung. Relevante Statistiken: Summe Dimensionen: ClientId, CollectionId , CollectionName , IndexId, IndexName Frequenz: 60 Sekunden
IngestionRequestErrors	Die Gesamtzahl der Fehler bei Anfragen zur Massenind izierung für eine Sammlung. OpenSearch Serverless gibt diese Metrik aus, wenn eine Massenindizierungsanfrage aus irgendeinem Grund fehlschlägt, z. B. aufgrund eines Authentifizierungs- oder Verfügbarkeitsproblems. Relevante Statistiken: Summe Dimensionen: ClientId, CollectionId , CollectionName Frequenz: 60 Sekunden

Metrik	Beschreibung
IngestionRequestLatency	Die Latenz in Sekunden für Massenschreibvorgänge in eine Sammlung. Relevante Statistiken: Minimum, Maximum, Durchschnitt Dimensionen: ClientId, CollectionId , CollectionName Frequenz: 60 Sekunden
IngestionRequestRate	Die Gesamtzahl der von einer Sammlung empfangenen Massenschreibvorgänge. Relevante Statistiken: Minimum, Maximum, Durchschnitt Dimensionen: ClientId, CollectionId , CollectionName Frequenz: 60 Sekunden
IngestionRequestSuccess	Die Gesamtzahl der erfolgreichen Indizierungsvorgänge einer Sammlung. Relevante Statistiken: Summe Dimensionen: ClientId, CollectionId , CollectionName Frequenz: 60 Sekunden
SearchableDocuments	Die Gesamtzahl der durchsuchbaren Dokumente in einer Sammlung oder einem Index. Relevante Statistiken: Summe Dimensionen: ClientId, CollectionId , CollectionName , IndexId, IndexName Frequenz: 60 Sekunden

Metrik	Beschreibung
`SearchRequestErrors`	Die Gesamtzahl der Abfragefehler pro Minute für eine Sammlung. Relevante Statistiken: Summe Dimensionen: `ClientId`, `CollectionId` , `CollectionName` Frequenz: 60 Sekunden
`SearchRequestLatency`	Die durchschnittliche Zeit in Millisekunden, die zum Abschließen eines Suchvorgangs für eine Sammlung benötigt wird. Relevante Statistiken: Minimum, Maximum, Durchschnitt Dimensionen: `ClientId`, `CollectionId` , `CollectionName` Frequenz: 60 Sekunden
`SearchOCU`	Die Anzahl der OpenSearch Recheneinheiten (OCUs), die zum Durchsuchen von Sammlungsdaten verwendet werden. Diese Metrik gilt auf Kontoebene. Relevante Statistiken: Summe Dimensionen: `ClientId` Frequenz: 60 Sekunden

Metrik	Beschreibung
SearchRequestRate	Die Gesamtzahl der Suchanfragen pro Minute für eine Sammlung. Relevante Statistiken: Durchschnitt, Maximum, Summe Dimensionen: ClientId, CollectionId , CollectionName Frequenz: 60 Sekunden
StorageUsedInS3	Die Menge des verwendeten Amazon S3 S3-Speichers in Byte. OpenSearch Serverless speichert indizierte Daten in Amazon S3. Sie müssen den Zeitraum auf einer Minute auswählen, um einen genauen Wert zu erhalten. Relevante Statistiken: Summe Dimensionen: ClientId, CollectionId , CollectionName , IndexId, IndexName Frequenz: 60 Sekunden
2xx, 3xx, 4xx, 5xx	Die Anzahl der Anforderungen an die Sammlung, die zu dem angegebenen HTTP-Antwortcode (2xx, 3xx, 4xx, 5xx) geführt haben. Relevante Statistiken: Summe Dimensionen: ClientId, CollectionId , CollectionName Frequenz: 60 Sekunden

Protokollierung von OpenSearch Serverless-API-Aufrufen mit AWS CloudTrail

Amazon OpenSearch Serverless ist mit integriert AWS CloudTrail, einem Service, der Aufzeichnungen von Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem AWS -Service in Serverless ausgeführt werden.

CloudTrail erfasst alle API-Aufrufe für OpenSearch Serverless als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe aus dem Serverless-Bereich der OpenSearch Service-Konsole und Code-Aufrufe an die OpenSearch Serverless-API-Operationen.

Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen Amazon-S3-Bucket, einschließlich Ereignisse für OpenSearch Serverless aktivieren. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse in der CloudTrail -Konsole trotzdem in Event history (Ereignisverlauf) anzeigen.

Anhand der von CloudTrail gesammelten Informationen können Sie die an OpenSearch Serverless gestellte Anfrage, die IP-Adresse, von der die Anfrage gestellt wurde, den Zeitpunkt der Anfrage und zusätzliche Details bestimmen.

Weitere Informationen CloudTrail dazu finden Sie im AWS CloudTrail Benutzerhandbuch.

OpenSearch Serverlose Informationen in CloudTrail

CloudTrail wird AWS-Konto beim Erstellen Ihres für Sie aktiviert. Wenn eine Aktivität in OpenSearch Serverless auftritt, wird diese Aktivität in einem CloudTrail Ereignis zusammen mit anderen AWS -Service-Ereignissen im Event history (Ereignisverlauf) aufgezeichnet. Sie können aktuelle Ereignisse in Ihr (em) anzeigen, suchen und herunterladen AWS-Konto. Weitere Informationen finden Sie unter Anzeigen von Ereignissen mit dem CloudTrail -Ereignisverlauf.

Erstellen Sie einen Trail zur laufenden Aufzeichnung von Ereignissen in Ihrem AWS-Konto, einschließlich Ereignissen für OpenSearch Serverless. Ein Trail ermöglicht es CloudTrail , Protokolldateien in einem Amazon-S3-Bucket bereitzustellen. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen-Regionen.

Der Trail protokolliert Ereignisse aus allen Regionen in der AWS -Partition und stellt die Protokolldateien in dem Amazon-S3-Bucket bereit, den Sie angeben. Darüber hinaus können Sie andere AWS -Services konfigurieren, um die in den CloudTrail -Protokollen erfassten Ereignisdaten weiter zu analysieren und entsprechend zu agieren. Weitere Informationen finden Sie hier:

- Übersicht zum Erstellen eines Trails
- CloudTrail unterstützte Dienste und Integrationen
- Konfigurieren von Amazon SNS SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail -Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail -Protokolldateien aus mehreren Konten

Alle OpenSearch serverlosen Aktionen werden von der OpenSearch Serverless API-Referenz protokolliert CloudTrail und sind in dieser dokumentiert. Beispielsweise generieren Aufrufe der `DeleteCollection` Aktionen `CreateCollectionListCollections`, und Einträge in den CloudTrail Protokolldateien.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen helfen Ihnen beim Bestimmen der Folgenden Elemente:

- Ob die Anfrage mit Stammbenutzer- oder AWS Identity and Access Management (IAM) -Anmeldeinformationen ausgeführt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anfrage von einem anderen AWS -Service gesendet wurde

Weitere Informationen finden Sie unter CloudTrail -Element userIdentity.

Grundlegendes zu OpenSearch Serverless-Protokolldateieinträgen

Ein Trail ist eine Konfiguration, durch die Ereignisse als Protokolldateien an den von Ihnen angegebenen Amazon-S3-Bucket übermittelt werden. CloudTrail Protokolldateien können einen oder mehrere Einträge enthalten.

Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar. Es enthält unter anderem Informationen über die angeforderte Aktion, etwaige Anforderungsparameter und das Datum und die Uhrzeit der Aktion. CloudTrail Protokolldateien sind kein geordnetes Stacktrace der öffentlichen API-Aufrufe und erscheinen daher nicht in einer bestimmten Reihenfolge.

Das folgende Beispiel zeigt einen CloudTrail -Protokolleintrag, der die `CreateCollection` Aktion demonstriert.

```
{
   "eventVersion":"1.08",
```

```
   "userIdentity":{
      "type":"AssumedRole",
      "principalId":"AIDACKCEVSQ6C2EXAMPLE",
      "arn":"arn:aws:iam::123456789012:user/test-user",
      "accountId":"123456789012",
      "accessKeyId":"access-key",
      "sessionContext":{
         "sessionIssuer":{
            "type":"Role",
            "principalId":"AIDACKCEVSQ6C2EXAMPLE",
            "arn":"arn:aws:iam::123456789012:role/Admin",
            "accountId":"123456789012",
            "userName":"Admin"
         },
         "webIdFederationData":{

         },
         "attributes":{
            "creationDate":"2022-04-08T14:11:34Z",
            "mfaAuthenticated":"false"
         }
      }
   },
   "eventTime":"2022-04-08T14:11:49Z",
   "eventSource":"aoss.amazonaws.com",
   "eventName":"CreateCollection",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"AWS Internal",
   "userAgent":"aws-cli/2.1.30 Python/3.8.8 Linux/5.4.176-103.347.amzn2int.x86_64 exe/
x86_64.amzn.2 prompt/off command/aoss.create-collection",
   "errorCode":"HttpFailureException",
   "errorMessage":"An unknown error occurred",
   "requestParameters":{
      "accountId":"123456789012",
      "name":"test-collection",
      "description":"A sample collection",
      "clientToken":"d3a227d2-a2a7-49a6-8fb2-e5c8303c0718"
   },
   "responseElements": null,
   "requestID":"12345678-1234-1234-1234-987654321098",
   "eventID":"12345678-1234-1234-1234-987654321098",
   "readOnly":false,
   "eventType":"AwsApiCall",
   "managementEvent":true,
```

```
    "recipientAccountId":"123456789012",
    "eventCategory":"Management",
    "tlsDetails":{
       "clientProvidedHostHeader":"user.aoss-sample.us-east-1.amazonaws.com"
    }
}
```

Überwachung OpenSearch serverloser Ereignisse mit Amazon EventBridge

Amazon OpenSearch Service ist in Amazon integriert EventBridge , um Sie über bestimmte, Ihre Domains betreffende Ereignisse zu informieren. Ereignisse von AWS -Services werden für EventBridge nahezu in Echtzeit bereitgestellt. Die gleichen Ereignisse werden auch an Amazon CloudWatch Events gesendet, dem Vorgänger von Amazon EventBridge. Sie können Regeln schreiben, um anzugeben, welche Ereignisse für Sie interessant sind und welche automatisierten Aktionen ausgeführt werden sollen, wenn sich für ein Ereignis eine Übereinstimmung mit einer Regel ergibt. Zu den Aktionen, die Sie automatisch aktivieren können, gehören beispielsweise die folgenden:

- Aufrufen einer -Funktion AWS Lambda
- Aufrufen eines Amazon EC2 Run-Befehls
- Weiterleiten des Ereignisses an Amazon Kinesis Data Streams
- Aktivieren eines AWS -Step-Functions-Zustandsautomaten
- Benachrichtigen eines Amazon SNS-Themas oder einer Amazon SQS-Warteschlange

Weitere Informationen finden Sie unter Erste Schritte mit Amazon EventBridge im EventBridge Amazon-Benutzerhandbuch.

Einrichten von Benachrichtigungen

Sie können AWS Benutzerbenachrichtigungen verwenden, um Benachrichtigungen zu erhalten, wenn ein OpenSearch serverloses Ereignis eintritt. Ein Ereignis ist ein Indikator für eine Änderung in der OpenSearch serverlosen Umgebung, z. B. wenn Sie das maximale Limit für Ihre OCU-Nutzung erreicht haben. Amazon EventBridge empfängt das Ereignis und leitet eine Benachrichtigung an das AWS Management Console Benachrichtigungscenter und die von Ihnen ausgewählten Zustellungskanäle weiter. Sie erhalten eine Benachrichtigung, wenn ein Ereignis einer von Ihnen angegebenen Regel entspricht.

OpenSearch Ereignisse in Compute Units (OCU)

OpenSearch Serverless sendet Ereignisse an, EventBridge wenn eines der folgenden OCU-Ereignisse auftritt.

Die OCU-Nutzung nähert sich der Höchstgrenze

OpenSearch Serverless sendet dieses Ereignis, wenn Ihre OCU-Nutzung für die Suche oder den Index 75% Ihres Kapazitätslimits erreicht. Ihre OCU-Nutzung wird auf der Grundlage Ihres konfigurierten Kapazitätslimits und Ihres aktuellen OCU-Verbrauchs berechnet.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp (Suche OCU):

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "OCU Utilization Approaching Max Limit",
  "source": "aws.aoss",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "eventTime" : 1678943345789,
    "description": "Your search OCU usage is at 75% and is approaching the configured
 maximum limit."
  }
}
```

Es folgt ein Beispiel für diesen Ereignistyp (Index OCU):

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "OCU Utilization Approaching Max Limit",
  "source": "aws.aoss",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
```

```
  "detail": {
    "eventTime" : 1678943345789,
    "description": "Your indexing OCU usage is at 75% and is approaching the configured
 maximum limit."
  }
```

Die OCU-Nutzung hat das maximale Limit erreicht

OpenSearch Serverless sendet dieses Ereignis, wenn Ihre OCU-Nutzung für die Suche oder den Index 100% Ihres Kapazitätslimits erreicht. Ihre OCU-Nutzung wird auf der Grundlage Ihres konfigurierten Kapazitätslimits und Ihres aktuellen OCU-Verbrauchs berechnet.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp (Suche OCU):

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "OCU Utilization Reached Max Limit",
  "source": "aws.aoss",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "eventTime" : 1678943345789,
    "description": "Your search OCU usage has reached the configured maximum limit."
  }
}
```

Es folgt ein Beispiel für diesen Ereignistyp (Index OCU):

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "OCU Utilization Reached Max Limit",
  "source": "aws.aoss",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
```

```
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "eventTime" : 1678943345789,
    "description": "Your indexing OCU usage has reached the configured maximum limit."
  }
}
```

Amazon OpenSearch Service-Domains erstellen und verwalten

In diesem Kapitel wird beschrieben, wie Amazon OpenSearch Service-Domains erstellt und verwaltet werden. Eine Domain ist das AWS bereitgestellte Äquivalent eines OpenSearch Open-Source-Clusters. Wenn Sie eine Domain erstellen, geben Sie deren Einstellungen, Instanztypen, Instanzzahlen und Speicherzuweisung an. Weitere Informationen zu Open-Source-Clustern finden Sie in der OpenSearch Dokumentation unter Cluster erstellen.

Im Gegensatz zu den kurzen Anweisungen im Erste Schritte-Tutorial werden in diesem Kapitel alle Optionen beschrieben und relevante Referenzinformationen bereitgestellt. Sie können jedes Verfahren anhand der Anweisungen für die OpenSearch Servicekonsole, die AWS Command Line Interface (AWS CLI) oder die abschließen AWS SDKs.

OpenSearch Dienstdomänen erstellen

In diesem Abschnitt wird beschrieben, wie Sie OpenSearch Dienstdomänen mithilfe der OpenSearch Servicekonsole oder AWS CLI mithilfe des `create-domain` Befehls erstellen.

OpenSearch Dienstdomänen erstellen (Konsole)

Gehen Sie wie folgt vor, um mithilfe der Konsole eine OpenSearch Dienstdomäne zu erstellen.

So erstellen Sie eine OpenSearch Dienstdomäne (Konsole)

1. Gehen Sie zu https://aws.amazon.comund wählen Sie In der Konsole anmelden.
2. Wählen Sie unter Analytics Amazon OpenSearch Service aus.
3. Wählen Sie Domain erstellen aus.
4. Geben Sie für Domain name (Domainname) einen Domainnamen ein. Der Name muss die folgenden Kriterien erfüllen:

   - Einzigartig für Ihr Konto und AWS-Region
   - Beginnt mit einem Kleinbuchstaben
   - Enthält zwischen drei und 28 Zeichen
   - Enthält die nur Kleinbuchstaben a–z, die Nummern 0–9 und den Bindestrich (-)

5. Wählen Sie für die Methode zur Domainerstellung die Option Standard create aus.
6. Wählen Sie für Vorlagen die Option aus, die dem Zweck Ihrer Domain am besten entspricht:

   - Produktionsdomänen für Workloads, die hohe Verfügbarkeit und Leistung erfordern. Diese Domänen verwenden Multi-AZ (mit oder ohne Standby) und dedizierte Masterknoten für eine höhere Verfügbarkeit.
   - Entwicklung/Test für Entwicklung oder Test. Diese Domains können Multi-AZ (mit oder ohne Standby) oder eine einzelne Availability Zone verwenden.

   > **Important**
   >
   > Unterschiedliche Bereitstellungstypen präsentieren verschiedene Optionen auf nachfolgenden Seiten. Diese Schritte beinhalten alle Optionen.

7. Wählen Sie unter Bereitstellungsoption (en) die Option Domäne mit Standby aus, um eine 3-AZ-Domäne zu konfigurieren, wobei Knoten in einer der Zonen als Standby reserviert sind. Diese Option setzt eine Reihe von bewährten Methoden durch, z. B. eine bestimmte Anzahl von Datenknoten, die Anzahl der Master-Knoten, den Instanztyp, die Anzahl der Replikate und die Einstellungen für Softwareupdates.
8. Wählen Sie unter Version die Version OpenSearch oder das Legacy-Elasticsearch-OSS aus, das Sie verwenden möchten. Wir empfehlen Ihnen, die neueste Version von OpenSearch zu wählen. Weitere Informationen finden Sie unter the section called “Unterstützte Versionen von Elasticsearch und OpenSearch”.

   (Optional) Wenn Sie eine OpenSearch Version für Ihre Domain ausgewählt haben, wählen Sie Kompatibilitätsmodus aktivieren, damit die Version als 7.10 OpenSearch gemeldet wird. Dadurch können bestimmte Elasticsearch OSS-Clients und -Plugins, die die Version überprüfen, bevor sie eine Verbindung herstellen, weiterhin mit dem Service arbeiten.
9. Wählen Sie unter Instance type (Instance-Typ) einen Instance-Typ für Ihre Datenknoten aus. Weitere Informationen finden Sie unter the section called “Unterstützte Instance-Typen”.

   > **Note**
   >
   > Nicht alle Availability Zones unterstützen alle Instance-Typen. Wenn Sie Multi-AZ mit oder ohne Standby wählen, empfehlen wir, Instance-Typen der aktuellen Generation wie R5 oder I3 zu wählen.

10. Wählen Sie unter Number of instances (Anzahl der Instances) die Anzahl der Datenknoten aus.

    Höchstwerte finden Sie unter Kontingente für OpenSearch Dienstdomänen und Instanzen. Cluster mit einem Knoten sind für die Entwicklung und das Testen verwendbar, jedoch nicht für Produktions-Workloads. Weitere Anleitungen finden Sie unter the section called “Größenanpassung von Domains” und the section called “Konfigurieren einer Multi-AZ-Domain”.

    > **Note**
    >
    > (Optional) Dedizierte Koordinatorknoten unterstützen alle OpenSearch Versionen und ElasticSearch Versionen 6.8 bis 7.10. Dedizierte Koordinatorknoten sind für die Verwendung mit Domänen verfügbar, für die ein dedizierter Clustermanager aktiviert ist. Um dedizierte Koordinatorknoten zu aktivieren, wählen Sie den Instanztyp und die Anzahl der Instanzen aus. Als bewährte Methode sollten Sie die Instanzfamilie für Ihren dedizierten Koordinatorknoten genauso beibehalten wie Ihre Datenknoten (Intel-basierte Instances oder Graviton-basierte Instances).

11. Wählen Sie als Speichertyp Amazon EBS aus. Die in der Liste verfügbaren Volume-Typen hängen von dem Instance-Typ ab, den Sie ausgewählt haben. Eine Anleitung zum Erstellen besonders großer Domains finden Sie unter the section called “Petabyte-Größe”.
12. Konfigurieren Sie für EBS-Speicher die folgenden zusätzlichen Einstellungen. Einige Einstellungen werden je nach gewähltem Volumentyp möglicherweise nicht angezeigt.

Einstellung	Beschreibung
EBS-Volume-Typ	Wählen Sie zwischen universelle (SSD) – gp3 und universelle (SSD) – gp2, oder bereitgestellte IOPS (SSD) der vorherigen Generation, und Magnetic (Standard).
EBS-Speichergröße pro Knoten	Geben Sie die Größe des EBS-Volumes ein, das Sie jedem Datenknoten zuordnen möchten. EBS volume size (EBS-Volume-Größe) bezieht sich auf einen Knoten. Sie können die Gesamtclustergröße für die OpenSearch Service-Domain berechnen, indem Sie die Anzahl der Datenknoten mit der EBS-Volume-Größe multiplizieren. Die Mindest- und Maximalgröße eines EBS-Volumes hängt sowohl vom angegebenen EBS-Volume-Typ als auch vom Instance-

Einstellung	Beschreibung
	Typ ab, dem es zugeordnet ist. Weitere Informationen finden Sie unter EBS-Volume-Größenbeschränkungen.
Bereitgestellte IOPS	Wenn Sie den Volumetyp Provisioned IOPS SSD ausgewählt haben, geben Sie die Anzahl der I/O Operationen pro Sekunde (IOPS) ein, die das Volume unterstützen kann.

13. (Optional) Wenn Sie einen gp3 Volumetyp ausgewählt haben, erweitern Sie Erweiterte Einstellungen und geben Sie zusätzliche IOPS (bis zu 16.000 für jede pro Datenknoten bereitgestellte Volumengröße von 3 TiB) und Durchsatz (bis zu 1.000 MiB/s für jede bereitgestellte Volumengröße von 3 TiB pro Datenknoten) an, die über das hinausgehen, was im Speicherpreis enthalten ist, und zwar gegen Aufpreis. Weitere Informationen finden Sie in den Amazon OpenSearch Service-Preisen.
14. (Optional) Um den UltraWarm Speicher zu aktivieren, wählen Sie UltraWarm Datenknoten aktivieren. Jeder Instance-Typ verfügt über eine maximale Speichermenge, die er adressieren kann. Multiplizieren Sie diesen Betrag mit der Anzahl der Warm-Datenknoten für den gesamten adressierbaren Warm-Speicher.
15. (Optional) Um Cold Storage zu aktivieren, wählen Sie Cold Storage aktivieren. Sie müssen die Option aktivieren UltraWarm , um Cold Storage zu aktivieren.
16. Wenn Sie Multi-AZ mit Standby verwenden, sind bereits drei dedizierte Master-Knoten aktiviert. Wählen Sie den gewünschten Master-Knotentyp aus. Wenn Sie sich für eine Multi-AZ-Domain ohne Standby-Domain entschieden haben, wählen Sie Dedizierte Masterknoten aktivieren und wählen Sie den Typ und die Anzahl der gewünschten Master-Knoten aus. Dedizierte Hauptknoten erhöhen die Cluster-Stabilität und sind für Domains mit einer höheren Instance-Anzahl als 10 erforderlich. Für Produktions-Domains werden drei dedizierte Hauptknoten empfohlen.

> **Note**
>
> Sie können für Ihre dedizierte Hauptknoten und Ihre Datenknoten verschiedene Instance-Typen wählen. Sie können beispielsweise universelle oder speicheroptimierte Instances für Ihre Datenknoten, aber für die Datenverarbeitung optimierte Instances für Ihre dedizierten Hauptknoten auswählen.

17. (Optional) Für Domains, die OpenSearch oder Elasticsearch 5.3 und höher ausgeführt werden, ist die Snapshot-Konfiguration irrelevant. Weitere Informationen zu automatisierten Snapshots finden Sie unter the section called “Erstellen von Index-Snapshots”.
18. Wenn Sie einen benutzerdefinierten Endpunkt anstelle des standardmäßigen `https://search-mydomain-1a2a3a4a5a6a7a8a9a0a9a8a7a.us-east-1.es.amazonaws.com` verwenden möchten, wählen Sie Benutzerdefinierten Endpunkt aktivieren und geben Sie einen Namen und ein Zertifikat an. Weitere Informationen finden Sie unter the section called “Erstellen eines benutzerdefinierten Endpunkts”.
19. Wählen Sie für Netzwerk entweder VPC-Zugriff oder Öffentlicher Zugriff. Fahren Sie bei Wahl von Public access (Öffentlicher Zugriff) mit dem nächsten Schritt fort. Wenn Sie VPC-Zugriff ausgewählt haben, stellen Sie zunächst sicher, dass die Voraussetzungen erfüllt sind und führen Sie dann die folgenden Schritte aus:

Einstellung	Beschreibung
VPC	Wählen Sie für die Virtual Private Cloud (VPC) die ID, die Sie verwenden möchten. Die VPC und die Domain müssen identisch sein AWS-Region, und Sie müssen eine VPC auswählen, bei der die Tenancy auf Standard gesetzt ist. OpenSearch Der Service unterstützt diese Verwendung eines dedizierten Mandats VPCs noch nicht.
Subnetz	Wählen Sie Add subnet (Subnetz hinzufügen). Wenn Sie Multi-AZ aktiviert haben, müssen Sie zwei oder drei Subnetze auswählen. OpenSearch Der Service platziert einen VPC-Endpunkt und elastische Netzwerkschnittstellen in den Subnetzen. Sie müssen eine ausreichende Anzahl von IP-Adressen in dem oder den Subnetzen für die Netzwerkschnittstellen reservieren. Weitere Informationen finden Sie unter Reservieren von IP-Adressen in einem VPC-Subnetz.
Sicherheitsgruppen	Wählen Sie eine oder mehrere VPC-Sicherheitsgruppen aus, die es Ihrer gewünschten Anwendung ermöglichen, die OpenSearch Service-Domain über die von der Domain bereitgestellten Ports (80 oder 443) und Protokolle (HTTP oder HTTPS) zu erreichen. Weitere Informationen finden Sie unter the section called “VPC-Unterstützung”.

Einstellung	Beschreibung
IAM Role (IAM-Rolle)	Behalten Sie die Standardrolle bei. OpenSearch Der Service verwendet diese vordefinierte Rolle (auch als dienstverknüpfte Rolle bezeichnet), um auf Ihre VPC zuzugreifen und einen VPC-Endpunkt und Netzwerks chnittstellen im Subnetz der VPC zu platzieren. Weitere Informationen finden Sie unter Serviceverknüpfte Rolle für den VPC-Zugriff.
Typ der IP-Adresse	Wählen Sie entweder Dual Stack oder IPv4 als IP-Adresstyp. Dual-Stac k ermöglicht die gemeinsame Nutzung von IPv4 Domänenressourcen für verschiedene IPv6 Adresstypen. Dies ist die empfohlene Option. Wenn Sie Ihren IP-Adresstyp auf Dual-Stack einstellen, können Sie Ihren Adresstyp später nicht mehr ändern.

20. Aktivieren oder deaktivieren Sie die abgestimmte Zugriffskontrolle:

    - Wenn Sie IAM für die Benutzerverwaltung verwenden möchten, wählen Sie IAM-ARN als Haupt-Benutzer festlegen, und geben Sie den ARN für eine IAM-Rolle an.
    - Wenn Sie die interne Benutzerdatenbank verwenden möchten, wählen Sie Masterbenutzer erstellen und geben Sie einen Benutzernamen und ein Passwort an.

    Für welche Option Sie sich auch entscheiden, der Masterbenutzer kann auf alle Indizes im Cluster und auf alle zugreifen. OpenSearch APIs Hinweise zur Auswahl der Option finden Sie unter the section called “Die wichtigsten Konzepte”.

    Wenn Sie die differenzierte Zugriffskontrolle deaktivieren, können Sie den Zugriff auf Ihre Domain weiterhin steuern, indem Sie sie in einer VPC platzieren, eine restriktive Zugriffsrichtlinie anwenden oder beides tun. Sie müssen node-to-node Verschlüsselung und Verschlüsselung im Ruhezustand aktivieren, um eine differenzierte Zugriffskontrolle verwenden zu können.

    > **Note**
    >
    > Wir empfehlen dringend, eine abgestimmte Zugriffskontrolle zu aktivieren, um die Daten in Ihrer Domain zu schützen. Eine abgestimmte Zugriffssteuerung bietet Sicherheit auf Cluster-, Index-, Dokument- und Feldebene.

21. (Optional) Wenn Sie die SAML-Authentifizierung für OpenSearch Dashboards verwenden möchten, wählen Sie SAML-Authentifizierung aktivieren und konfigurieren Sie die SAML-

Optionen für die Domain. Detaillierte Anweisungen finden Sie unter the section called “SAML-Authentifizierung für Dashboards OpenSearch ”.

22. (Optional) Wenn Sie die Amazon Cognito Cognito-Authentifizierung für OpenSearch Dashboards verwenden möchten, wählen Sie Amazon Cognito Cognito-Authentifizierung aktivieren. Wählen Sie dann den Amazon Cognito Cognito-Benutzerpool und den Identitätspool aus, den Sie für die OpenSearch Dashboard-Authentifizierung verwenden möchten. Eine Anleitung zum Erstellen dieser Ressourcen finden Sie unter the section called “Amazon Cognito Cognito-Authentifizierung für Dashboards OpenSearch ”.
23. Wählen Sie für die Zugriffsrichtlinie eine Zugriffsrichtlinie aus oder konfigurieren Sie eine eigene. Wenn Sie eine benutzerdefinierte Richtlinie erstellen möchten, können Sie sie selbst konfigurieren oder aus einer anderen Domain importieren. Weitere Informationen finden Sie unter the section called “Identitäts- und Zugriffsverwaltung”.

    > **Note**
    >
    > Wenn der VPC-Zugriff aktiviert wurde, können Sie keine IP-basierten Richtlinien verwenden. Sie können stattdessen mit Sicherheitsgruppen steuern, welche IP-Adressen auf die Domain zugreifen dürfen. Weitere Informationen finden Sie unter the section called “Zugriffsrichtlinien für VPC-Domänen”.

24. (Optional) Wenn alle Anfragen an die Domain über HTTPS eingehen sollen, wählen Sie HTTPS für allen Datenverkehr zur Domain erfordern. Um die node-to-node Verschlüsselung zu aktivieren, wählen Sie ode-to-nodeN-Verschlüsselung aus. Weitere Informationen finden Sie unter the section called “Node-to-node Verschlüsselung”. Um die Verschlüsselung von Daten im Ruhezustand zu aktivieren, wählen Sie Verschlüsselung von Daten im Ruhezustand aktivieren aus. Diese Optionen sind vorausgewählt, wenn Sie sich für die Bereitstellungsoption Multi-AZ mit Standby entschieden haben.
25. (Optional) Wählen Sie AWS Eigenen Schlüssel verwenden aus, damit der OpenSearch Service in Ihrem Namen einen AWS KMS Verschlüsselungsschlüssel erstellt (oder verwenden Sie den bereits erstellten). Wählen Sie andernfalls Ihren eigenen KMS-Schlüssel aus. Weitere Informationen finden Sie unter the section called “Verschlüsselung im Ruhezustand”.
26. Wählen Sie für das Fenster außerhalb der Spitzenzeiten eine Startzeit aus, um Service-Software-Updates und Auto-Tune-Optimierungen zu planen, für die eine Bereitstellung erforderlich ist. blue/green Updates außerhalb der Spitzenzeiten tragen dazu bei, die Belastung der dedizierten Master-Knoten eines Clusters in Zeiten mit hohem Datenaufkommen zu minimieren.

27. Wählen Sie für Auto-Tune aus, ob der OpenSearch Service speicherbezogene Konfigurationsänderungen an Ihrer Domain vorschlagen darf, um Geschwindigkeit und Stabilität zu verbessern. Weitere Informationen finden Sie unter the section called “Automatische Optimierung”.

    (Optional) Wählen Sie Zeitfenster außerhalb der Spitzenzeiten, um ein wiederkehrendes Zeitfenster zu planen, in dem Auto-Tune die Domain aktualisiert.
28. (Optional) Wählen Sie Automatisches Softwareupdate, um automatische Softwareupdates zu aktivieren.
29. (Optional) Fügen Sie Tags hinzu, um Ihre Domain zu beschreiben, damit Sie diese Informationen kategorisieren und filtern können. Weitere Informationen finden Sie unter the section called “Markieren von Domänen”.
30. (Optional) Erweitern und konfigurieren Sie Erweiterte Clustereinstellungen. Eine Zusammenfassung dieser Optionen finden Sie unter the section called “Erweiterte Clustereinstellungen”.
31. Wählen Sie Erstellen aus.

OpenSearch Dienstdomänen erstellen (AWS CLI)

Anstatt eine OpenSearch Dienstdomäne mithilfe der Konsole zu erstellen, können Sie die verwenden AWS CLI. Informationen zur Syntax finden Sie unter Amazon OpenSearch Service in der AWS CLI-Befehlsreferenz a.

Beispielbefehle

Dieses erste Beispiel zeigt die folgende Konfiguration der OpenSearch Service-Domain:

- Erstellt eine OpenSearch Dienstdomäne namens mylogs mit OpenSearch Version 1.2
- Füllt die Domain mit zwei Instances des Instance-Typs `r6g.large.search`
- Verwendet ein 100 GiB universelle (SSD)-EBS `gp3`-Volume als Speicher für jeden Datenknoten
- Ermöglicht anonymen Zugriff, aber nur von einer einzigen IP-Adresse: 192.0.2.0/32

```
aws opensearch create-domain \
    --domain-name mylogs \
    --engine-version OpenSearch_1.2 \
    --cluster-config  InstanceType=r6g.large.search,InstanceCount=2 \
```

```
    --ebs-options
 EBSEnabled=true,VolumeType=gp3,VolumeSize=100,Iops=3500,Throughput=125 \
    --access-policies '{"Version": "2012-10-17", "Statement": [{"Action": "es:*",
 "Principal":"*","Effect": "Allow", "Condition": {"IpAddress":{"aws:SourceIp":
["192.0.2.0/32"]}}}]}'
```

Das nächste Beispiel zeigt die folgende Konfiguration der OpenSearch Dienstdomäne:

- Erstellt eine OpenSearch Service-Domain namens mylogs mit Elasticsearch Version 7.10
- Füllt die Domain mit sechs Instances des Instance-Typs `r6g.large.search`
- Verwendet ein 100 GiB universelle (SSD)-EBS gp2-Volume als Speicher für jeden Datenknoten
- Beschränkt den Zugriff auf den Service auf einen einzelnen Benutzer, der anhand der Benutzer-ID 5555555555 identifiziert wird AWS-Konto
- Verteilt Instances auf mehrere Availability Zones

```
aws opensearch create-domain \
    --domain-name mylogs \
    --engine-version Elasticsearch_7.10 \
    --cluster-config
 InstanceType=r6g.large.search,InstanceCount=6,ZoneAwarenessEnabled=true,ZoneAwarenessConfig={A
 \
    --ebs-options EBSEnabled=true,VolumeType=gp2,VolumeSize=100 \
    --access-policies '{"Version": "2012-10-17", "Statement": [ { "Effect": "Allow",
 "Principal": {"AWS": "arn:aws:iam::555555555555:root" }, "Action":"es:*", "Resource":
 "arn:aws:es:us-east-1:555555555555:domain/mylogs/*" } ] }'
```

Das nächste Beispiel zeigt die folgende Konfiguration der Dienstdomäne: OpenSearch

- Erstellt eine OpenSearch Dienstdomäne namens mylogs mit OpenSearch Version 1.0
- Füllt die Domain mit zehn Instances des Instance-Typs `r6g.xlarge.search`
- Füllt die Domain mit drei Instances des Instance-Typs `r6g.large.search`, die als dedizierte Hauptknoten dienen
- Verwendet ein 100-GiB-EBS-Volume für bereitgestellte IOPS als Speicher, konfiguriert mit einer Basisleistung von 1000 IOPS für jeden Datenknoten
- Beschränkt den Zugriff auf einen Benutzer und eine Unterressource, die `_search`-API

```
aws opensearch create-domain \
```

```
    --domain-name mylogs \
    --engine-version OpenSearch_1.0 \
    --cluster-config
InstanceType=r6g.xlarge.search,InstanceCount=10,DedicatedMasterEnabled=true,DedicatedMasterTyp
\
    --ebs-options EBSEnabled=true,VolumeType=io1,VolumeSize=100,Iops=1000 \
    --access-policies '{"Version": "2012-10-17", "Statement": [ { "Effect": "Allow",
"Principal": { "AWS": "arn:aws:iam::555555555555:root" }, "Action": "es:*",
"Resource": "arn:aws:es:us-east-1:555555555555:domain/mylogs/_search" } ] }'
```

> **Note**
>
> Wenn Sie versuchen, eine OpenSearch Dienstdomäne zu erstellen und eine Domäne mit demselben Namen bereits vorhanden ist, meldet die CLI keinen Fehler. Stattdessen gibt sie die Details der vorhandenen Domain zurück.

OpenSearch Dienstdomänen erstellen (AWS SDKs)

Die AWS SDKs (außer Android und iOS SDKs) unterstützen alle in der Amazon OpenSearch Service API-Referenz definierten Aktionen, einschließlich`CreateDomain`. Einen Beispiel-Code finden Sie unter the section called “Mit dem AWS SDKs”. Weitere Informationen zur Installation und Verwendung von finden Sie AWS SDKs unter AWS Software Development Kits.

OpenSearch Dienstdomänen erstellen (AWS CloudFormation)

OpenSearch Service ist in einen Service integriert AWS CloudFormation, der Sie bei der Modellierung und Einrichtung Ihrer AWS Ressourcen unterstützt, sodass Sie weniger Zeit mit der Erstellung und Verwaltung Ihrer Ressourcen und Infrastruktur verbringen müssen. Sie erstellen eine Vorlage, die die OpenSearch Domäne beschreibt, die Sie erstellen möchten, und die Domäne für Sie CloudFormation bereitstellt und konfiguriert. Weitere Informationen, einschließlich Beispielen für JSON- und YAML-Vorlagen für OpenSearch Domains, finden Sie in der Amazon OpenSearch Service-Referenz zum Ressourcentyp im AWS CloudFormation Benutzerhandbuch.

Konfigurieren von Zugriffsrichtlinien

Amazon OpenSearch Service bietet verschiedene Möglichkeiten, den Zugriff auf Ihre OpenSearch Service-Domains zu konfigurieren. Weitere Informationen erhalten Sie unter the section called “Identitäts- und Zugriffsverwaltung” und the section called “Differenzierte Zugriffskontrolle”.

Die Konsole stellt vorkonfigurierte Zugriffsrichtlinien bereit, die Sie an die spezifischen Anforderungen der jeweiligen Domain anpassen können. Sie können auch Zugriffsrichtlinien aus anderen OpenSearch Service-Domains importieren. Informationen zur Interaktion dieser Zugriffsrichtlinien mit dem VPC-Zugriff finden Sie unter the section called “Zugriffsrichtlinien für VPC-Domänen”.

So konfigurieren Sie Zugriffsrichtlinien (Konsole)

1. Melden Sie sich bei der https://aws.amazon.com an und wählen Sie dann Sign In to the Console (Bei der Konsole anmelden) aus.
2. Wählen Sie unter Analytics Amazon OpenSearch Service aus.
3. Wählen Sie im Navigationsbereich unter Domains die Domain aus, die Sie aktualisieren möchten.
4. Klicken Sie auf Aktionen und Sicherheitskonfiguration bearbeiten.
5. Bearbeiten Sie die Zugriffsrichtlinien-JSON, um eine vorkonfigurierte Option zu importieren.
6. Wählen Sie Änderungen speichern aus.

Erweiterte Clustereinstellungen

Verwenden Sie erweiterte Optionen, um Folgendes zu konfigurieren:

Indizes in Anforderungstexten

Gibt an, ob explizite Verweise auf Indizes im Text von HTTP-Anforderungen zulässig sind. Wenn für diese Eigenschaft `false` festgelegt wird, wird verhindert, dass Benutzer die Zugriffskontrolle für Unterressourcen umgehen können. Der Standardwert ist `true`. Weitere Informationen finden Sie unter the section called “Erweiterte Optionen und Überlegungen zur API”.

Zuweisung des Felddaten-Cache

Gibt den Prozentsatz des Java-Heap-Space an, der den Felddaten zugewiesen ist. Standardmäßig beträgt diese Einstellung 20 % des JVM-Heaps.

> **Note**
>
> Viele Kunden fragen rotierende tägliche Indizes ab. Wir empfehlen, dass Sie Benchmark-Tests mit `indices.fielddata.cache.size` beginnen, die auf 40 % des JVM-Heap für die meisten dieser Anwendungsfälle konfiguriert sind. Für sehr große Indizes benötigen Sie möglicherweise einen Datencache für große Felder.

Maximale Anzahl der Klauseln

Gibt die maximale erlaubte Anzahl der Klauseln in einer booleschen Lucene-Abfrage an. Der Standardwert ist 1.024. Abfragen mit mehr als der erlaubten Anzahl Klauseln erzeugen den Fehler `TooManyClauses`. Weitere Informationen finden Sie in der Lucene-Dokumentation.

Konfigurationsänderungen in Amazon OpenSearch Service vornehmen

Amazon OpenSearch Service verwendet bei der Aktualisierung von Domains einen blauen/grünen Bereitstellungsprozess. Bei einer blue/green Bereitstellung entsteht eine inaktive Umgebung für Domain-Updates, in der die Produktionsumgebung kopiert wird und Benutzer nach Abschluss dieser Updates an die neue Umgebung weitergeleitet werden. In einer blue/green Bereitstellung ist die blaue Umgebung die aktuelle Produktionsumgebung. Die grüne Umgebung ist die inaktive Umgebung.

Daten werden von der blauen Umgebung in die grüne Umgebung migriert. Wenn die neue Umgebung bereit ist, wechselt der OpenSearch Service die Umgebungen, um die grüne Umgebung zur neuen Produktionsumgebung zu machen. Der Switchover erfolgt ohne Datenverlust. Auf diese Weise werden Ausfallzeiten minimiert und die ursprüngliche Umgebung für den Fall beibehalten, dass die Bereitstellung in der neuen Umgebung nicht erfolgreich ist.

Themen

- Änderungen, die normalerweise zu Bereitstellungen führen blue/green
- Änderungen, die normalerweise nicht zu blue/green Bereitstellungen führen
- Feststellen, ob eine Änderung eine Blau/Grün-Bereitstellung verursacht
- Verfolgen einer Konfigurationsänderung
- Stufen einer Konfigurationsänderung
- Auswirkungen von blauen/grünen Bereitstellungen auf die Leistung
- Gebühren für Konfigurationsänderungen
- Beheben von Validierungsfehlern

Änderungen, die normalerweise zu Bereitstellungen führen blue/green

Die folgenden Vorgänge führen zu blue/green Bereitstellungen:

- Ändern des Instance-Typs
- Aktivieren der differenzierten Zugriffskontrolle
- Ausführen von Service-Softwareupdates
- Aktivieren oder Deaktivieren von dedizierten Master-Knoten
- Multi-AZ ohne Standby aktivieren oder deaktivieren
- Ändern des Speichertyps, des Volumetyps oder der Datenträgergröße
- Auswählen von verschiedenen VPC-Subnetzen
- Hinzufügen oder Entfernen von VPC-Sicherheitsgruppen
- Dedizierte Koordinatorknoten hinzufügen oder entfernen
- Amazon Cognito Cognito-Authentifizierung für Dashboards aktivieren oder deaktivieren OpenSearch
- Auswählen eines anderen Amazon-Cognito-Benutzerpools oder Identitätenpools
- Ändern von erweiterten Einstellungen
- Upgrade auf eine neue OpenSearch Version (OpenSearch Dashboards sind möglicherweise während eines Teils oder des gesamten Upgrades nicht verfügbar)
- Aktivierung der Verschlüsselung von Daten im Ruhezustand oder node-to-node Verschlüsselung
- Aktivierung UltraWarm oder Deaktivierung von Cold Storage
- Deaktivieren der automatischen Abstimmung und Zurücksetzen der Änderungen
- Ein optionales Plugin einer Domain zuordnen und ein optionales Plugin von einer Domain trennen
- Erhöhung der Anzahl der dedizierten Master-Knoten für Multi-AZ-Domains mit zwei dedizierten Master-Knoten
- Verringerung der Größe des EBS-Volumes
- Änderung der EBS-Volume-Größe, der IOPS oder des Durchsatzes, wenn die letzte Änderung, die Sie vorgenommen haben, gerade läuft oder vor weniger als 6 Stunden stattgefunden hat
- Aktivierung der Veröffentlichung von Audit-Logs für. CloudWatch

Bei Multi-AZ mit Standby-Domains können Sie jeweils nur eine Änderungsanforderung stellen. Wenn eine Änderung bereits im Gange ist, wird die neue Anfrage abgelehnt. Sie können den Status der aktuellen Änderung mit der `DescribeDomainChangeProgress` API überprüfen.

Änderungen, die normalerweise nicht zu blue/green Bereitstellungen führen

In den meisten Fällen führen die folgenden Vorgänge nicht zu blue/green Bereitstellungen:

- Änderung der Zugriffsrichtlinie
- Ändern des benutzerdefinierten Endpunkts
- Änderung der TLS-Richtlinie (Transport Layer Security)
- Ändern der automatisierten Snapshot-Stunde
- Aktivieren oder Deaktivieren von Require HTTPS (Erzwingung von HTTPS)
- Aktivieren der automatischen Optimierung oder Deaktivierung, ohne die Änderungen rückgängig zu machen
- Wenn Ihre Domain über dedizierte Master-Knoten verfügt, ändern Sie den Datenknoten oder die Anzahl der UltraWarm Knoten
- Wenn Ihre Domain über dedizierte Master-Knoten verfügt, ändern Sie den Typ oder die Anzahl der dedizierten Master-Instances (außer bei Multi-AZ-Domänen mit zwei dedizierten Masterknoten)
- Aktivierung oder Deaktivierung der Veröffentlichung von Fehlerprotokollen oder langsamen Protokollen für CloudWatch
- Deaktivierung der Veröffentlichung von Audit-Logs auf CloudWatch
- Erhöhung der Volumegröße auf bis zu 3 TiB pro Datenknoten, Änderung des Volumetyps, der IOPS oder des Durchsatzes
- Hinzufügen und Entfernen von Tags

> **Note**
>
> Abhängig von Ihrer Service-Softwareversion gibt es einige Ausnahmen. Wenn Sie sichergehen möchten, dass eine Änderung nicht zu einer blue/green Bereitstellung führt, führen Sie vor der Aktualisierung Ihrer Domain einen Probelauf durch, sofern diese Option verfügbar ist. Einige Änderungen bieten keine Option für einen Probelauf. Wir empfehlen generell, dass Sie außerhalb der Hauptverkehrszeiten Änderungen an Ihrem Cluster vornehmen.

Feststellen, ob eine Änderung eine Blau/Grün-Bereitstellung verursacht

Sie können einige Arten von geplanten Konfigurationsänderungen testen, um festzustellen, ob sie zu einer blue/green Bereitstellung führen, ohne sich auf diese Änderungen festlegen zu müssen. Führen Sie, bevor Sie eine Kofigurationsänderung initiieren, über die Konsole oder ein API eine Validierungsprüfung durch, um sicherzustellen, dass Ihre Domain für ein Update in Frage kommt.

Console

Um eine Konfigurationsänderung zu validieren

1. Navigieren Sie zur Amazon OpenSearch Service-Konsole unterhttps://console.aws.amazon.com/aos/.
2. Wählen Sie im linken Navigationsbereich die Option Domains aus.
3. Wählen Sie die Domain aus, für die Sie eine Konfigurationsänderung vornehmen möchten. Dadurch wird die Detailseite der Domain geöffnet. Wählen Sie das Dropdown-Menü Actions (Aktionen) und dann Edit cluster configuration (Clusterkonfiguration bearbeiten) aus.
4. Nehmen Sie Änderungen an der Domain vor, z. B. den Instance-Typ oder die Anzahl der Knoten.
5. Wählen Sie unter Testlaufanalyse die Option Ausführen aus. Beim Probelauf wird Ihre Konfigurationsänderung auf Fehler überprüft und festgestellt, ob dafür eine blue/green Bereitstellung erforderlich ist.
6. Wenn der Probelauf abgeschlossen ist, werden die Ergebnisse zusammen mit einer Probelauf-ID unten auf der Seite angezeigt. Die Analyse zeigt, ob die Konfigurationsänderung eine blue/green Bereitstellung erfordert oder nicht.

   Jeder Testlauf überschreibt den vorherigen. Um die Details der einzelnen Testläufe beizubehalten, speichern Sie die zugehörige Testlauf-ID. Testläufe sind 90 Tage lang oder bis Sie ein Konfigurationsupdate vornehmen, verfügbar.
7. Um mit Ihrem Konfigurationsupdate fortzufahren, wählen Sie Save changes (Änderungen speichern) aus. Wählen Sie andernfalls Abbrechen. Mit jeder Option gelangen Sie zurück zur Registerkarte Cluster configuration (Cluster-Konfiguration). Auf dieser Registerkarte können Sie Dry run details (Testlaufdetails) auswählen, um die Details Ihres letzten Testlaufs zu sehen. Diese Seite enthält auch einen side-by-side Vergleich zwischen der Konfiguration vor dem Probelauf und der Testlaufkonfiguration.

API

Sie können eine Testlaufvalidierung über die Konfigurations-API durchführen. Um Ihre Änderungen mit der API zu testen, stellen Sie `DryRun` auf `true` und `DryRunMode` auf `Verbose` ein. Im Modus „Verbose“ wird zusätzlich eine Validierungsprüfung durchgeführt, um festzustellen, ob durch die Änderung eine Blau/Grün-Bereitstellung ausgelöst wird. Mit dieser

UpdateDomainConfigAnfrage wird beispielsweise der Bereitstellungstyp getestet, der sich aus der Aktivierung von Folgendem ergibt UltraWarm:

```
POST https://es.us-east-1.amazonaws.com/2021-01-01/opensearch/domain/my-domain/
config
{
   "ClusterConfig": {
    "WarmCount": 3,
    "WarmEnabled": true,
    "WarmType": "ultrawarm1.large.search"
   },
   "DryRun": true,
   "DryRunMode": "Verbose"
}
```

Die Anforderung führt eine Validierungsprüfung durch und gibt die Art der Bereitstellung zurück, die die Änderung verursachen wird, führt das Update jedoch nicht tatsächlich durch:

```
{
   "ClusterConfig": {
     ...
    },
   "DryRunResults": {
      "DeploymentType": "Blue/Green",
      "Message": "This change will require a blue/green deployment."
    }
}
```

Mögliche Bereitstellungstypen sind:

- `Blue/Green` – Die Änderung bewirkt eine Blau/Grün-Bereitstellung.
- `DynamicUpdate` – Die Änderung bewirkt keine Blau/Grün-Bereitstellung.
- `Undetermined` – Die Domain befindet sich noch in einem Verarbeitungsstatus, sodass der Bereitstellungstyp nicht bestimmt werden kann.
- `None` – Keine Konfigurationsänderung.

Schlägt die Überprüfung fehl, wird eine Liste der Validierungsfehler zurückgegeben.

```
{
```

```
   "ClusterConfig":{
      "..."
   },
   "DryRunProgressStatus":{
      "CreationDate":"2023-01-12T01:14:33.847Z",
      "DryRunId":"db00ca39-48b2-4774-bbd3-252cf094d205",
      "DryRunStatus":"failed",
      "UpdateDate":"2023-01-12T01:14:33.847Z",
      "ValidationFailures":[
         {
            "Code":"Cluster.Index.WriteBlock",
            "Message":"Cluster has index write blocks."
         }
      ]
   }
}
```

Wenn der Status immer noch lautet`pending`, können Sie die Testlauf-ID in Ihrer UpdateDomainConfig Antwort bei nachfolgenden DescribeDryRunProgressAufrufen verwenden, um den Status der Validierung zu überprüfen.

```
GET https://es.us-east-1.amazonaws.com/2021-01-01/opensearch/domain/my-domain/
dryRun?dryRunId=my-dry-run-id
{
    "DryRunConfig": null,
    "DryRunProgressStatus": {
        "CreationDate": "2023-01-12T01:14:42.998Z",
        "DryRunId": "db00ca39-48b2-4774-bbd3-252cf094d205",
        "DryRunStatus": "succeeded",
        "UpdateDate": "2023-01-12T01:14:49.334Z",
        "ValidationFailures": null
    },
    "DryRunResults": {
        "DeploymentType": "Blue/Green",
        "Message": "This change will require a blue/green deployment."
    }
}
```

Um eine Testlaufanalyse ohne Validierungsprüfung durchzuführen, stellen Sie `DryRunMode` auf `Basic` ein, wenn Sie die Konfigurations-API verwenden.

Python

Der folgende Python-Code verwendet die UpdateDomainConfigAPI, um eine Testlauf-Validierungsprüfung durchzuführen, und wenn die Prüfung erfolgreich ist, ruft er dieselbe API ohne einen Probelauf auf, um das Update zu starten. Wenn die Prüfung fehlschlägt, druckt das Skript den Fehler aus und stoppt.

```
import time
import boto3

client = boto3.client('opensearch')

response = client.UpdateDomainConfig(
    ClusterConfig={
        'WarmCount': 3,
        'WarmEnabled': True,
        'WarmCount': 123,
    },
    DomainName='test-domain',
    DryRun=True,
    DryRunMode='Verbose'
)

dry_run_id = response.DryRunProgressStatus.DryRunId

retry_count = 0

while True:

    if retry_count == 5:
        print('An error occured')
        break

    dry_run_progress_response = client.DescribeDryRunProgress('test-domain',
 dry_run_id)
    dry_run_status = dry_run_progress_response.DryRunProgressStatus.DryRunStatus

    if dry_run_status == 'succeeded':
        client.UpdateDomainConfig(
            ClusterConfig={
            'WarmCount': 3,
            'WarmEnabled': True,
            'WarmCount': 123,
```

```
        })
        break

    elif dry_run_status == 'failed':
        validation_failures_list =
dry_run_progress_response.DryRunProgressStatus.ValidationFailures
        for item in validation_failures_list:
            print(f"Code: {item['Code']}, Message: {item['Message']}")
        break

    retry_count += 1
    time.sleep(30)
```

Verfolgen einer Konfigurationsänderung

Sie können jeweils eine Konfigurationsänderung anfordern oder mehrere Änderungen in einer einzigen Anfrage zusammenfassen. Verwenden Sie die Felder Domain-Verarbeitungsstatus und Status der Konfigurationsänderung in der Konsole, um Konfigurationsänderungen nachzuverfolgen. Warten Sie, bis der Domainstatus erreicht ist, `Active` bevor Sie weitere Änderungen anfordern.

Eine Domain kann die folgenden Bearbeitungsstatus haben:

- `Active`— Es wird keine Konfigurationsänderung durchgeführt. Sie können eine neue Anfrage zur Konfigurationsänderung einreichen.
- `Creating`— Die Domain wird erstellt.
- `Modifying`— Konfigurationsänderungen, wie das Hinzufügen neuer Datenknoten, EBS-, GP3-, IOPS-Bereitstellung oder Einrichtung von KMS-Schlüsseln, sind im Gange.
- `Upgrading engine version`— Ein Upgrade der Engine-Version ist im Gange.
- `Updating service software`— Ein Service-Software-Update ist in Bearbeitung.
- `Deleting`— Die Domain wird gelöscht.
- `Isolated`— Die Domain ist gesperrt.

Eine Domain kann die folgenden Konfigurationsänderungsstatus haben:

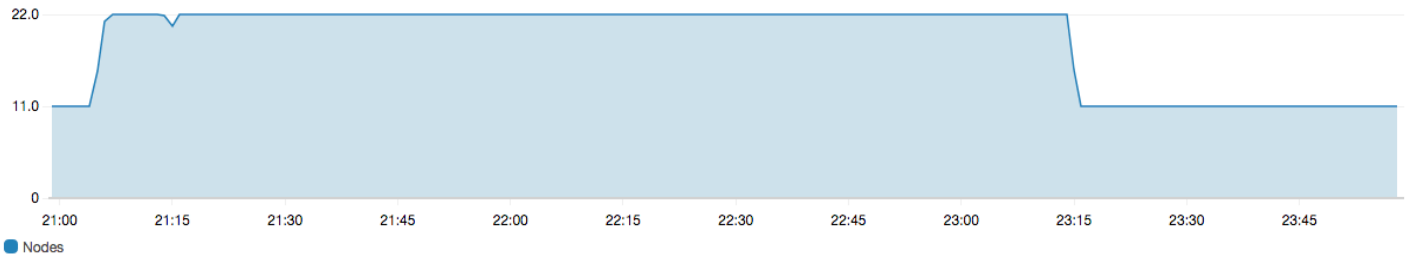
- `Pending`— Eine Anfrage zur Konfigurationsänderung wurde eingereicht.
- `Initializing`— Der Dienst initialisiert eine Konfigurationsänderung.
- `Validating`— Der Dienst validiert die angeforderten Änderungen und die benötigten Ressourcen.

- `Awaiting user inputs`— Der Service geht davon aus, dass Konfigurationsänderungen, wie z. B. eine Änderung des Instanztyps, fortgesetzt werden. Sie können die Konfigurationsänderungen bearbeiten.
- `Applying changes`— Der Service wendet die angeforderten Konfigurationsänderungen an.
- `Cancelled`— Die Konfigurationsänderung wurde storniert. Wählen Sie Abbrechen, um alle Änderungen rückgängig zu machen.
- `Completed`— Die angeforderten Konfigurationsänderungen wurden erfolgreich abgeschlossen.
- `Validation failed`— Die angeforderten Konfigurationsänderungen konnten nicht abgeschlossen werden. Es wurden keine Konfigurationsänderungen vorgenommen.

> **Note**
>
> Fehler bei der Überprüfung können auf rote Indizes in Ihrer Domain, auf die Nichtverfügbarkeit eines ausgewählten Instanztyps oder auf zu wenig Festplattenspeicher zurückzuführen sein. Eine Liste der Validierungsfehler finden Sie unter. the section called “Beheben von Validierungsfehlern” Während eines Fehlers bei der Überprüfung können Sie die Konfigurationsänderungen abbrechen, erneut versuchen oder bearbeiten.

Wenn die Konfigurationsänderungen abgeschlossen sind, ändert sich der Domänenstatus wieder auf`Active`.

Sie können die Cluster-Integrität und die CloudWatch Amazon-Metriken überprüfen und feststellen, dass die Anzahl der Knoten im Cluster während der Domain-Aktualisierung vorübergehend zunimmt — häufig verdoppelt — wird. In der folgenden Abbildung sehen Sie, wie sich die Anzahl der Knoten während einer Konfigurationsänderung verdoppelt und sich wieder auf 11 verringert, wenn die Aktualisierung abgeschlossen ist.



Dieser temporäre Anstieg kann die dedizierten Master-Knoten des Clusters belasten, da sie möglicherweise plötzlich viel mehr Knoten zu verwalten haben. Dies kann auch die Such- und

Indizierungslatenzen erhöhen, da der OpenSearch Service Daten vom alten Cluster auf den neuen kopiert. Es ist wichtig, dass auf dem Cluster genügend Kapazität zur Verfügung steht, um den mit diesen blue/green Bereitstellungen verbundenen Mehraufwand bewältigen zu können.

> **Important**
>
> Es fallen keine zusätzlichen Gebühren bei Konfigurationsänderungen und Service-Wartung an. Sie zahlen nur für die Anzahl der Knoten, die Sie für Ihren Cluster anfordern. Weitere Einzelheiten finden Sie unter the section called “Gebühren für Konfigurationsänderungen”.

Um eine Überlastung der dedizierten Master-Knoten zu verhindern, können Sie die Nutzung anhand der CloudWatch Amazon-Metriken überwachen. Weitere Informationen über empfohlene Maximalwerte finden Sie unter the section called “Empfohlene CloudWatch Alarme”.

Stufen einer Konfigurationsänderung

Nachdem Sie eine Konfigurationsänderung initiiert haben, führt OpenSearch Service eine Reihe von Schritten durch, um Ihre Domain zu aktualisieren. Sie können den Fortschritt der Konfigurationsänderung in der Konsole unter Status der Konfigurationsänderung einsehen. Die genauen Schritte, die eine Aktualisierung durchläuft, hängen von der Art der Änderung ab, die Sie vornehmen. Sie können eine Konfigurationsänderung auch mit der DescribeDomainChangeProgress API-Operation überwachen.

Die folgenden Schritte sind mögliche Stufen, die eine Aktualisierung während einer Konfigurationsänderung durchlaufen kann:

Stufenname	Beschreibung
Validierung	Überprüfen, ob die Domain für ein Update berechtigt ist, und ggf. Erkennen von Validierungsproblemen.

Stufenname	Beschreibung
Erstellen einer neuen Umgebung	Erfüllung der erforderlichen Vorausset zungen und Erstellung der erforderlichen Ressourcen für den Start der blue/green Bereitstellung.
Provisioning neuer Knoten	Erstellen einer neuen Gruppe von Instances in der neuen Umgebung.
Routing des Datenverkehrs auf neue Knoten	Umleiten des Datenverk ehrs auf die neu erstellten Datenknoten.
Routing des Datenverkehrs auf alte Knoten	Deaktivieren des Datenverk ehrs auf den alten Datenknoten.

Stufenname	Beschreibung
Vorbereiten von Knoten auf das Entfernen	Vorbereiten der Entfernung von Knoten. Dieser Schritt wird nur ausgeführt, wenn Sie Ihre Domain herunterskalieren (z. B. von 8 Knoten auf 6 Knoten).
Kopieren von Shards auf neue Knoten	Verschieben von Shards von den alten Knoten auf die neuen Knoten.
Beenden von Knoten	Beenden und Löschen alter Knoten, nachdem die Shards entfernt wurden.
Löschen von älteren Ressourcen	Löschen von Ressourcen, die mit der alten Umgebung verknüpft sind (z. B. Load Balancer).

Stufenname	Beschreibung
Dynamisches Update	Wird angezeigt, wenn für das Update keine blue/green Bereitstellung erforderlich ist und es dynamisch angewendet werden kann.
Anwenden von speziellen Änderungen im Zusammenhang mit dem Master	Wird angezeigt, wenn der Typ oder die Anzahl der dedizierten Master-Instances geändert wird.
Volumenbezogene Änderungen werden übernommen	Wird angezeigt, wenn Volumengröße, Typ, IOPS und Durchsatz geändert werden.

Auswirkungen von blauen/grünen Bereitstellungen auf die Leistung

Während der blue/green Bereitstellung steht Ihr Amazon OpenSearch Service-Cluster für eingehende Such- und Indexierungsanfragen zur Verfügung. Es können jedoch die folgenden Leistungsprobleme auftreten:

- Vorübergehender Anstieg der Auslastung auf Leader-Knoten, da Cluster mehr Knoten verwalten müssen.
- Höhere Latenz bei der Suche und Indizierung, da der OpenSearch Service Daten von alten Knoten auf neue Knoten kopiert.
- Zunehmende Ablehnungen für eingehende Anfragen, da die Clusterlast während blue/green der Bereitstellungen zunimmt.
- Um Latenzprobleme und Ablehnungen von Anfragen zu vermeiden, sollten Sie blue/green Bereitstellungen ausführen, wenn der Cluster intakt ist und wenig Netzwerkverkehr herrscht.

Gebühren für Konfigurationsänderungen

Wenn Sie die Konfiguration für eine Domäne ändern, erstellt OpenSearch Service einen neuen Cluster, wie unter beschrieben. the section called “Konfigurationsänderungen” Bei der Migration von alt auf neu fallen die folgenden Gebühren an:

- Wenn Sie den Instance-Typ ändern, bezahlen Sie für beide Cluster für die erste Stunde. Nach der ersten Stunde bezahlen Sie nur für den neuen Cluster. EBS-Volumes werden nicht zweimal belastet, da sie Teil Ihres Clusters sind. Daher folgt die Abrechnung der Instance-Abrechnung.

  Beispiel: Sie ändern die Konfiguration von drei `m3.xlarge`-Instances zu vier `m4.large`-Instances. In der ersten Stunde bezahlen Sie für beide Cluster (3 * `m3.xlarge` + 4 * `m4.large`). Nach der ersten Stunde bezahlen Sie nur für den neuen Cluster (4 * `m4.large`).
- Wenn Sie den Instance-Typ nicht ändern, bezahlen Sie nur für den größten Cluster für die erste Stunde. Nach der ersten Stunde bezahlen Sie nur für den neuen Cluster.

  Beispiel: Sie ändern die Konfiguration von sechs `m3.xlarge`-Instances zu drei `m3.xlarge`-Instances. In der ersten Stunde bezahlen Sie für den größten Cluster (6 * `m3.xlarge`). Nach der ersten Stunde bezahlen Sie nur für den neuen Cluster (3 * `m3.xlarge`).

Beheben von Validierungsfehlern

Wenn Sie eine Konfigurationsänderung initiieren OpenSearch oder ein Upgrade der Elasticsearch-Version durchführen, führt OpenSearch Service zunächst eine Reihe von Validierungsprüfungen durch, um sicherzustellen, dass Ihre Domain für ein Update in Frage kommt. Wenn eine dieser Prüfungen fehlschlägt, erhalten Sie in der Konsole eine Benachrichtigung mit den spezifischen Problemen, die Sie beheben müssen, bevor Sie Ihre Domain aktualisieren. In der folgenden Tabelle

sind die möglichen Domain-Probleme aufgeführt, die bei OpenSearch Service auftreten könnten, sowie die Schritte zu deren Behebung.

Problem	Fehlercode	Fehlerbehebungsschritte
Sicherheitsgruppe wurde nicht gefunden	`SecurityGroupNotFound`	Die mit Ihrer OpenSearch Dienstdomäne verknüpfte Sicherheitsgruppe ist nicht vorhanden. Um dieses Problem zu lösen, erstellen Sie eine Sicherheitsgruppe mit dem angegebenen Namen.
Subnetz nicht gefunden	`SubnetNotFound`	Das mit Ihrer OpenSearch Service-Domain verknüpfte Subnetz ist nicht vorhanden. Um dieses Problem zu lösen, erstellen Sie ein Subnetz in Ihrer VPC.
Serviceverknüpfte Rolle nicht konfiguriert	`SLRNotConfigured`	Die dienstverknüpfte Rolle für OpenSearch Service ist nicht konfiguriert. Die dienstbezogene Rolle ist von OpenSearch Service vordefiniert und umfasst alle Berechtigungen, die der Dienst benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen. Wenn die Rolle nicht vorhanden ist, müssen Sie sie ggf. manuell erstellen.
Nicht genügend IP-Adressen	`InsufficientFreeIPsForSubnets`	Eines oder mehrere Ihrer VPC-Subnetze verfügen nicht über genügend IP-Adressen, um Ihre Domain zu aktualisieren. Informationen dazu, wie viele IP-Adressen Sie benötigen, finden Sie unter the section called “Reservieren von IP-Adressen in einem VPC-Subnetz”.
Cognito-Benutzerpool ist nicht vorhanden	`CognitoUserPoolNotFound`	OpenSearch Der Service kann den Amazon Cognito Cognito-Benutzerpool nicht finden. Stellen Sie sicher, dass Sie einen Benutzerpool erstellt haben und die korrekte ID verwenden. Die ID können Sie mithilfe der Amazon-Cognito-Konsole oder dem folgenden AWS CLI -Befehl bestimmen: `aws cognito-idp list-user-pools --max-results 60 --region us-east-1`
Cognito-Identitätspool ist	`CognitoIdentityPoo`	OpenSearch Der Dienst kann den Cognito-Identitätspool nicht finden. Stellen Sie sicher, dass Sie einen Benutzerpool erstellt haben und die

Problem	Fehlercode	Fehlerbehebungsschritte
nicht vorhanden	`lNotFound`	korrekte ID verwenden. Die ID können Sie mithilfe der Amazon-Cognito-Konsole oder dem folgenden AWS CLI -Befehl bestimmen: `aws cognito-identity list-identity-pools --max-results 60 --region us-east-1`
Cognito-Domain nicht für Benutzerpool gefunden	`CognitoDomainNotFound`	Der Benutzerpool verfügt nicht über einen Domain-Namen. Sie können eine mit der Amazon Cognito Cognito-Konsole oder mit dem folgenden AWS CLI Befehl konfigurieren: `aws cognito-idp create-user-pool-domain --domain my-domain --user-pool-id id`
Cognito-Rolle nicht konfiguriert	`CognitoRoleNotConfigured`	Die IAM-Rolle, die dem OpenSearch Service die Berechtigung erteilt, die Benutzer- und Identitätspools von Amazon Cognito zu konfigurieren und für die Authentifizierung zu verwenden, ist nicht konfiguriert. Konfigurieren Sie die Rolle mit passenden Berechtigungen und einer entsprechenden Vertrauensstellung. Sie können die Konsole verwenden, die die Standardrolle CognitoAccessForAmazonOpenSearchfür Sie erstellt, oder Sie können eine Rolle mithilfe des AWS CLI oder des AWS SDK manuell konfigurieren.
Benutzerpool kann nicht beschrieben werden	`UserPoolNotDescribable`	Die angegebene Amazon-Cognito-Rolle hat keine Berechtigung, den mit Ihrer Domain verknüpften Benutzerpool zu beschreiben. Vergewissern Sie sich, dass die Richtlinie für Rollenberechtigungen die Aktion `cognito-identity:DescribeUserPool` zulässt. Siehe the section called “Informationen über die CognitoAccessForAmazonOpenSearch-Rolle” für die vollständige Berechtigungsrichtlinie.

Problem	Fehlercode	Fehlerbehebungsschritte
Identitätspool kann nicht beschrieben werden	`IdentityPoolNotDescribable`	Die angegebene Amazon-Cognito-Rolle hat keine Berechtigung, den mit Ihrer Domain verknüpften Identitätspool zu beschreiben. Vergewissern Sie sich, dass die Richtlinie für Rollenberechtigungen die Aktion `cognito-identity:DescribeIdentityPool` zulässt. Siehe the section called “Informationen über die CognitoAccessForAmazonOpenSearch-Rolle” für die vollständige Berechtigungsrichtlinie.
Benutzer und Identitätspool können nicht beschrieben werden	`CognitoPoolsNotDescribable`	Die angegebene Amazon-Cognito-Rolle hat keine Berechtigung, die mit Ihrer Domain verknüpften Benutzer- und Identitätspools zu beschreiben. Vergewissern Sie sich, dass die Richtlinie für Rollenberechtigungen die Aktionen `cognito-identity:DescribeIdentityPool` und `cognito-identity:DescribeUserPool` zulässt. Siehe the section called “Informationen über die CognitoAccessForAmazonOpenSearch-Rolle” für die vollständige Berechtigungsrichtlinie.
KMS-Schlüssel nicht aktiviert	`KMSKeyNotEnabled`	Der zur Verschlüsselung Ihrer Domain verwendete Schlüssel AWS Key Management Service (AWS KMS) ist deaktiviert. Aktivieren Sie den Schlüssel sofort erneut.
Benutzerdefiniertes Zertifikat befindet sich nicht im Status „ISSUED“ (ALLT)	`InvalidCertificate`	Wenn Ihre Domain einen benutzerdefinierten Endpunkt verwendet, sichern Sie ihn, indem Sie entweder ein SSL-Zertifikat in AWS Certificate Manager (ACM) generieren oder eines Ihrer eigenen importieren. Der Zertifikatsstatus muss Issued (Ausgestellt) sein. Wenn dieser Fehler angezeigt wird, überprüfen Sie den Status Ihres Zertifikats in der ACM-Konsole. Wenn der Status „Expired“ (Abgelaufen), „Failed“ (Fehlgeschlagen), „Inactive“ (Inaktiv) oder „Pending“ (Ausstehend) ist, siehe die ACM-Dokumentation zur Fehlerbehebung, um das Problem zu lösen.

Problem	Fehlercode	Fehlerbehebungsschritte
Nicht genügend Kapazität zum Starten des ausgewählten Instance-Typs	`InsufficientInstanceCapacity`	Die angeforderte Kapazität des Instance-Typs ist nicht verfügbar . Möglicherweise haben Sie fünf `i3.16xlarge.search` Knoten angefordert, aber OpenSearch Service hat nicht genügend `i3.16xlarge.search` Hosts verfügbar, sodass die Anfrage nicht erfüllt werden kann. Überprüfen Sie die unterstützten Instanztypen in OpenSearch Service und wählen Sie einen anderen Instanztyp aus.
Rote Indizes im Cluster	`RedCluster`	Ein oder mehrere Indizes in Ihrem Cluster haben einen roten Status, was zu einem allgemeinen roten Cluster-Status führt. Informationen zur Behebung dieses Problems finden Sie unter the section called “Roter Cluster-Status”.
Speicherschutzschalter, zu viele Anfragen	`TooManyRequests`	Es gibt zu viele Such- und Schreibanfragen für Ihre Domain, sodass OpenSearch Service die Konfiguration nicht aktualisieren kann. Sie können die Anzahl der Anforderungen reduzieren, Instances bis zu 64 GiB RAM vertikal skalieren oder eine horizontale Skalierung durchführen, indem Sie Instances hinzufügen.
Neue Konfiguration kann keine Daten aufnehmen (wenig Speicherplatz)	`InsufficientStorageCapacity`	Die konfigurierte Speichergröße kann nicht alle Daten in Ihrer Domain enthalten. Um dieses Problem zu lösen, wählen Sie ein größeres Volume, löschen Sie nicht verwendete Indizes oder erhöhen Sie die Anzahl der Knoten im Cluster, um sofort Speicherplatz freizugeben.

Problem	Fehlercode	Fehlerbehebungsschritte

An bestimmte Knoten angeheftete Shards	`ShardMovementBlocked`	Ein oder mehrere Indizes in Ihrer Domain sind an bestimmte Knoten angehängt und können nicht neu zugewiesen werden. Dies ist höchstwahrscheinlich darauf zurückzuführen, dass Sie die Shard-Zuweisungsfilterung konfiguriert haben, mit der Sie angeben können, welche Knoten die Shards eines bestimmten Indexes hosten dürfen.
		
		Um dieses Problem zu beheben, entfernen Sie Filter für die Shard-Zuweisung aus allen betroffenen Indizes:
		
		`PUT my-index/_settings`
		`{`
		`  "settings": {`
		`  "index.routing.allocation.require._name": null`
		`  }`
		`}`

Neue Konfiguration kann nicht alle Shards enthalten (Shard-Anzahl)	`TooManyShards`	Die Anzahl der Shards in Ihrer Domain ist zu hoch, sodass OpenSearch Service sie nicht in die neue Konfiguration verschieben kann. Um dieses Problem zu beheben, skalieren Sie Ihre Domain horizontal, indem Sie Knoten mit demselben Konfigurationstyp wie Ihre aktuellen Cluster-Knoten hinzufügen. Beachten Sie: Die maximale EBS-Volume-Größe hängt vom Instance-Typ des Knotens ab. Um dieses Problem künftig zu vermeiden, siehe the section called “Auswahl der Anzahl der Shards” und definieren Sie eine Sharding-Strategie, die sich für Ihren Anwendungsfall eignet.

Problem	Fehlercode	Fehlerbehebungsschritte
Das mit Ihrer Domain verknüpfte Subnetz unterstützt keine Adressen IPv4	`ResultCodeIPv4BlockNotExists`	Um dieses Problem zu beheben, erstellen Sie ein Subnetz oder aktualisieren Sie das vorhandene Subnetz in Ihrer VPC entsprechend dem konfigurierten IP-Adresstyp der Domain. Wenn Ihre Domain einen reinen Adresstyp verwendet, verwenden Sie ein IPv4 Subnetz IPv4nur. Wenn Ihre Domain den Dual-Stack-Modus verwendet, verwenden Sie ein Dual-Stack-Subnetz.
Das mit Ihrer Domain verknüpfte Subnetz unterstützt keine Adressen IPv6	`ResultCodeIPv6BlockNotExists`	Um dieses Problem zu beheben, erstellen Sie ein Subnetz oder aktualisieren Sie das vorhandene Subnetz in Ihrer VPC entsprechend dem konfigurierten IP-Adresstyp der Domain. Wenn Ihre Domain einen reinen Adresstyp verwendet, verwenden Sie ein IPv4 Subnetz IPv4nur. Wenn Ihre Domain den Dual-Stack-Modus verwendet, verwenden Sie ein Dual-Stack-Subnetz.

Service-Softwareupdates in Amazon OpenSearch Service

> **Note**
>
> Erläuterungen zu den Änderungen und Ergänzungen, die in jedem größeren Service-Software-Update (ohne Patch) vorgenommen wurden, finden Sie in den Versionshinweisen.

Amazon OpenSearch Service veröffentlicht regelmäßig Service-Software-Updates, die Funktionen hinzufügen oder Ihre Domänen auf andere Weise verbessern. Das Feld Notifications (Benachrichtigungen) in der Konsole ist der einfachste Weg, um festzustellen, ob ein Update verfügbar ist oder um den Status eines Updates zu überprüfen. Jede Benachrichtigung enthält Details zum Service-Software-Update. Alle Service-Softwareupdates verwenden Blau/Grün-Bereitstellungen, um Ausfallzeiten zu minimieren.

Service-Softwareupdates unterscheiden sich von OpenSearch Versions-Upgrades. Weitere Informationen zum Upgraden auf eine neuere Version von OpenSearch finden Sie unterthe section called “Aktualisieren von Domains”.

Optionale und erforderliche Updates

OpenSearch Der Service hat zwei große Kategorien von Service-Softwareupdates:

Optionale Updates

Optionale Service-Softwareupdates beinhalten in der Regel Verbesserungen und Unterstützung für neue Features oder Funktionen. Optionale Updates werden in Ihren Domänen nicht durchgesetzt, und es gibt keine feste Frist für deren Installation. Die Verfügbarkeit des Updates wird per E-Mail und Konsolenbenachrichtigung mitgeteilt. Sie können wählen, ob Sie das Update sofort anwenden oder es für ein geeigneteres Datum und eine geeignetere Uhrzeit verschieben möchten. Sie können es auch außerhalb der Spitzenzeiten der Domain planen. Die meisten Softwareupdates sind optional.

Unabhängig davon, ob Sie ein Update planen oder nicht, aktualisiert Service Ihre OpenSearch Servicesoftware automatisch für Sie, wenn Sie eine Änderung an der Domäne vornehmen, die zu einer blauen/grünen Bereitstellung führt.

Sie können Ihre Domain so konfigurieren, dass optionale Updates außerhalb der Spitzenzeiten automatisch angewendet werden. Wenn diese Option aktiviert ist, wartet der OpenSearch Service mindestens 13 Tage ab dem Zeitpunkt, an dem ein optionales Update verfügbar ist, und plant das Update dann nach 72 Stunden (drei Tagen). Sie erhalten eine Konsolenbenachrichtigung, wenn das Update geplant ist, und Sie können wählen, ob Sie es auf einen späteren Zeitpunkt verschieben möchten.

Um automatische Softwareupdates zu aktivieren, wählen Sie Automatisches Softwareupdate aktivieren, wenn Sie Ihre Domain erstellen oder aktualisieren. Um dieselbe Einstellung mit dem `--software-update-options` zu konfigurieren AWS CLI, legen Sie `true` bei der Erstellung oder Aktualisierung Ihrer Domain fest.

Erforderliche Updates

Zu den erforderlichen Service-Softwareupdates gehören in der Regel wichtige Sicherheitsupdates oder andere obligatorische Updates, um die kontinuierliche Integrität und Funktionalität Ihrer Domain zu gewährleisten. Beispiele für erforderliche Updates sind Log4j Common Vulnerabilities and Exposures (CVEs) und die Durchsetzung von Instance Metadata Service Version 2 (). IMDSv2 Die Anzahl der obligatorischen Updates pro Jahr beträgt in der Regel weniger als drei.

OpenSearch Der Service plant diese Updates automatisch und benachrichtigt Sie 72 Stunden (drei Tage) vor dem geplanten Update per E-Mail und Konsolenbenachrichtigung. Sie können wählen, ob Sie das Update sofort anwenden oder es für ein geeigneteres Datum und eine geeignetere Uhrzeit innerhalb des zulässigen Zeitrahmens verschieben möchten. Sie können es auch während des nächsten Zeitfensters der Domain außerhalb der Spitzenzeiten planen. Wenn Sie bei einem erforderlichen Update keine Maßnahmen ergreifen und keine Domainänderungen vornehmen, die zu einer blauen/grünen Bereitstellung führen, kann der OpenSearch Service das Update jederzeit nach Ablauf der angegebenen Frist (in der Regel 14 Tage ab Verfügbarkeit) innerhalb der Nebenzeiten der Domain einleiten.

Unabhängig davon, für welchen Zeitpunkt das Update geplant ist, aktualisiert der OpenSearch Service Ihre Domain automatisch für Sie, wenn Sie eine Änderung an der Domain vornehmen, die zu einer blauen/grünen Bereitstellung führt.

Patch-Updates

Bei Service-Softwareversionen, die mit „-P“ und einer Zahl enden, wie etwa R20211203-*P4*, handelt es sich um Patch-Versionen. Patches werden vermutlich Leistungsverbesserungen, kleinere Bugfixes und Behebungen von Sicherheitslücken oder Verbesserungen der Sicherheitslage beinhalten. Patch-Versionen beinhalten keine neuen Funktionen oder bahnbrechenden Änderungen und haben im Allgemeinen keine direkten oder merklichen Auswirkungen auf die Benutzer. In der Benachrichtigung zur Service-Software erfahren Sie, ob eine Patch-Version optional oder obligatorisch ist.

Überlegungen

Beachten Sie beim Aktualisieren Ihrer Domain folgende Punkte:

- Durch die manuelle Aktualisierung Ihrer Domain können Sie die Vorteile neuer Funktionen schneller nutzen. Wenn Sie Aktualisieren wählen, stellt der OpenSearch Service die Anfrage in eine Warteschlange und beginnt mit der Aktualisierung, wenn Zeit dafür ist.
- Wenn Sie ein Service-Software-Update initiieren, sendet der OpenSearch Dienst eine Benachrichtigung, wenn das Update startet und wenn es abgeschlossen ist.
- Software-Updates verwenden Blau/Grün-Bereitstellungen, um Ausfallzeiten zu minimieren. Aktualisierungen können die dedizierten Hauptknoten eines Clusters vorübergehend belasten. Stellen Sie daher sicher, dass ausreichende Kapazität für den zugeordneten Overhead beibehalten wird.
- Aktualisierungen werden normalerweise innerhalb von Minuten abgeschlossen, können aber auch mehrere Stunden oder sogar Tage dauern, wenn Ihr System stark ausgelastet ist.

Ziehen Sie in Erwägung, Ihre Domain während des konfigurierten Zeitfensters außerhalb der Hauptverkehrszeiten zu aktualisieren, um lange Aktualisierungszeiten zu vermeiden.

Starten eines Service-Softwareupdates

Sie können ein Service-Software-Update über die OpenSearch Servicekonsole AWS CLI, die oder eine der folgenden anfordern SDKs.

Konsole

So fordern Sie ein Service-Software-Update an

1. Öffnen Sie die Amazon OpenSearch Service-Konsole zu https://console.aws.amazon.com/aos/Hause.
2. Wählen Sie den Domänennamen aus, um seine Konfiguration zu öffnen.
3. Wählen Sie Aktionen, Update und wählen Sie eine der folgenden Optionen:

   - Update jetzt anwenden — Plant sofort, dass die Aktion in der aktuellen Stunde ausgeführt wird, sofern Kapazität verfügbar ist. Wenn keine Kapazität verfügbar ist, stellen wir andere verfügbare Zeitfenster zur Auswahl.
   - Planen Sie es außerhalb der Spitzenzeiten — Nur verfügbar, wenn das Zeitfenster außerhalb der Spitzenzeiten für die Domain aktiviert ist. Plant das Update so, dass es während des für die Domain konfigurierten Zeitfensters außerhalb der Spitzenzeiten stattfindet. Es gibt keine Garantie dafür, dass das Update innerhalb des nächsten unmittelbaren Zeitfensters erfolgt. Je nach Kapazität kann es in den folgenden Tagen passieren. Weitere Informationen finden Sie unter the section called “Zeitfenster außerhalb der Spitzenzeiten”.
   - Zeitplan für ein bestimmtes Datum und eine bestimmte Uhrzeit — Plant das Update so, dass es an einem bestimmten Datum und zu einer bestimmten Uhrzeit stattfindet. Wenn die von Ihnen angegebene Uhrzeit aus Kapazitätsgründen nicht verfügbar ist, können Sie ein anderes Zeitfenster auswählen.

   Wenn Sie das Update für einen späteren Zeitpunkt planen (innerhalb oder außerhalb des Randzeitfensters der Domain), können Sie es jederzeit verschieben. Detaillierte Anweisungen finden Sie unter the section called “So verschieben Sie den Termin”.
4. Wählen Sie Bestätigen aus.

AWS CLI

Senden Sie eine start-service-software-update AWS CLI Anfrage, um ein Service-Software-Update zu initiieren. In diesem Beispiel wird das Update sofort zur Warteschlange hinzugefügt:

```
aws opensearch start-service-software-update \
  --domain-name my-domain \
  --schedule-at "NOW"
```

Antwort:

```
{
    "ServiceSoftwareOptions": {
        "CurrentVersion": "R20220928-P1",
        "NewVersion": "R20220928-P2",
        "UpdateAvailable": true,
        "Cancellable": true,
        "UpdateStatus": "PENDING_UPDATE",
        "Description": "",
        "AutomatedUpdateDate": "1969-12-31T16:00:00-08:00",
        "OptionalDeployment": true
    }
}
```

> **Tip**
>
> Nachdem Sie ein Update angefordert haben, haben Sie ein enges Zeitfenster, in dem Sie es stornieren können. Die Dauer dieses `PENDING_UPDATE` Zustands kann stark variieren und hängt von Ihrer AWS-Region und der Anzahl der gleichzeitigen Updates ab, die der OpenSearch Service durchführt. Verwenden Sie die Konsole oder den `cancel-service-software-update` AWS CLI Befehl, um ein Update abzubrechen.

Wenn die Anfrage mit einem fehlschlägt`BaseException`, bedeutet dies, dass die von Ihnen angegebene Zeit aus Kapazitätsgründen nicht verfügbar ist und Sie eine andere Uhrzeit angeben müssen. OpenSearch Der Service schlägt in der Antwort alternative verfügbare Zeitnischen vor.

AWS SDKs

Dieses Beispiel-Python-Skript verwendet die Methoden describe_domain und start_service_software_update von, AWS SDK für Python (Boto3) um zu prüfen, ob eine Domain für

ein Service-Software-Update berechtigt ist. Wenn ja, startet das Update. Sie müssen einen Wert für `domain_name` angeben.

```
import boto3
from botocore.config import Config
import time

# Build the client using the default credential configuration.
# You can use the CLI and run 'aws configure' to set access key, secret
# key, and default region.

my_config = Config(
    # Optionally lets you specify a Region other than your default.
    region_name='us-east-1'
)

domain_name = ''  # The name of the domain to check and update

client = boto3.client('opensearch', config=my_config)


def getUpdateStatus(client):
    """Determines whether the domain is eligible for an update"""
    response = client.describe_domain(
        DomainName=domain_name
    )
    sso = response['DomainStatus']['ServiceSoftwareOptions']
    if sso['UpdateStatus'] == 'ELIGIBLE':
        print('Domain [' + domain_name + '] is eligible for a service software update
 from version ' +
              sso['CurrentVersion'] + ' to version ' + sso['NewVersion'])
        updateDomain(client)
    else:
        print('Domain is not eligible for an update at this time.')


def updateDomain(client):
    """Starts a service software update for the eligible domain"""
    response = client.start_service_software_update(
        DomainName=domain_name
    )
    print('Updating domain [' + domain_name + '] to version ' +
          response['ServiceSoftwareOptions']['NewVersion'] + '...')
```

```
    waitForUpdate(client)


def waitForUpdate(client):
    """Waits for the domain to finish updating"""
    response = client.describe_domain(
        DomainName=domain_name
    )
    status = response['DomainStatus']['ServiceSoftwareOptions']['UpdateStatus']
    if status == 'PENDING_UPDATE' or status == 'IN_PROGRESS':
        time.sleep(30)
        waitForUpdate(client)
    elif status == 'COMPLETED':
        print('Domain [' + domain_name +
              '] successfully updated to the latest software version')
    else:
        print('Domain is not currently being updated.')

def main():
    getUpdateStatus(client)
```

Planen von Softwareupdates außerhalb der Hauptverkehrszeiten

Jede OpenSearch Service-Domain, die nach dem 16. Februar 2023 erstellt wurde, hat täglich ein 10-Stunden-Fenster zwischen 22:00 Uhr und 8:00 Uhr Ortszeit, das wir als das Zeitfenster außerhalb der Spitzenzeiten betrachten. OpenSearch Der Service verwendet dieses Fenster, um Service-Software-Updates für die Domain zu planen. Updates außerhalb der Spitzenzeiten tragen dazu bei, die Belastung der dedizierten Master-Knoten eines Clusters in Zeiten mit höherem Datenverkehr zu minimieren. OpenSearch Der Service kann ohne Ihre Zustimmung keine Updates außerhalb dieses 10-Stunden-Fensters initiieren.

- Bei optionalen Updates informiert Sie der OpenSearch Service über die Verfügbarkeit des Updates und fordert Sie auf, das Update außerhalb der Hauptverkehrszeiten zu planen.
- Bei erforderlichen Updates plant der OpenSearch Service das Update automatisch während eines bevorstehenden Zeitfensters außerhalb der Spitzenzeiten und benachrichtigt Sie drei Tage im Voraus. Sie können das Update verschieben (innerhalb oder außerhalb der Spitzenzeiten), jedoch nur innerhalb des Zeitrahmens, der für die Fertigstellung des Updates erforderlich ist.

Für jede Domain können Sie festlegen, dass die standardmäßige Startzeit um 22:00 Uhr durch eine benutzerdefinierte Uhrzeit überschrieben wird. Detaillierte Anweisungen finden Sie unter the section called “Konfiguration eines benutzerdefinierten Zeitfensters außerhalb der Spitzenzeiten”.

Konsole

Um ein Update während eines bevorstehenden Zeitfensters außerhalb der Spitzenzeiten zu planen

1. Öffnen Sie die Amazon OpenSearch Service-Konsole zu https://console.aws.amazon.com/aos/Hause.
2. Wählen Sie den Domänennamen aus, um seine Konfiguration zu öffnen.
3. Wählen Sie Aktionen, Aktualisieren.
4. Wählen Sie außerhalb der Spitzenzeiten planen aus.
5. Wählen Sie Bestätigen aus.

Sie können die geplante Aktion auf der Registerkarte „Fenster außerhalb der Spitzenzeiten“ einsehen und sie jederzeit neu planen. Siehe the section called “Geplante Aktionen anzeigen”.

CLI

Um ein Update während eines bevorstehenden Zeitfensters außerhalb der Spitzenzeiten zu planen AWS CLI, senden Sie eine StartServiceSoftwareUpdateAnfrage und geben Sie `OFF_PEAK_WINDOW` für den Parameter Folgendes an: `--schedule-at`

```
aws opensearch start-service-software-update \
  --domain-name my-domain \
  --schedule-at "OFF_PEAK_WINDOW"
```

Überwachung von Service-Softwareupdates

OpenSearch Der Dienst sendet eine Benachrichtigung, wenn ein Service-Software-Update verfügbar, erforderlich, gestartet, abgeschlossen oder fehlgeschlagen ist. Sie können diese Benachrichtigungen auf dem Bedienfeld Benachrichtigungen der OpenSearch Service-Konsole sehen. Der Schweregrad der Benachrichtigung ist`Informational`, wenn das Update optional ist und`High` wenn es erforderlich ist.

OpenSearch Der Service sendet auch Service-Software-Ereignisse an Amazon EventBridge. Sie können verwenden EventBridge , um Regeln zu konfigurieren, die eine E-Mail senden oder eine

bestimmte Aktion ausführen, wenn ein Ereignis empfangen wird. Ein Beispiel-Walkthrough finden Sie unter the section called “Tutorial: Senden von SNS-Warnungen für verfügbare Updates”.

Informationen zum Format der einzelnen Ereignisse der Servicesoftware, die an Amazon gesendet werden EventBridge, finden Sie unterthe section called “Aktualisieren der Software”.

Wenn Domains nicht für ein Update in Frage kommen

Ihre Domain ist für ein Service-Software-Update nicht berechtigt, wenn sie sich in einem der folgenden Zustände befindet:

Status	Beschreibung
Domain in Verarbeitung	Die Domain befindet sich in der Mitte einer Konfigurationsänderung. Überprüfen Sie die Update-Berechtigung, nachdem die Operation abgeschlossen ist.
Roter Cluster-Status	Ein oder mehrere Indizes im Cluster sind rot. Fehlerbehandlungsschritte finden Sie unter the section called “Roter Cluster-Status”.
Hohe Fehlerrate	Der OpenSearch Cluster gibt beim Versuch, Anfragen zu verarbeiten, eine große Anzahl von 5 xx -Fehlern zurück. Dieses Problem ist in der Regel das Ergebnis zu vieler gleichzeitiger Lese- oder Schreibanforderungen. Erwägen Sie, den Datenverkehr zu dem Cluster zu reduzieren oder Ihre Domain zu skalieren.
Split brain	Split brain bedeutet, dass Ihr OpenSearch Cluster über mehr als einen Hauptknoten verfügt und sich in zwei Cluster aufgeteilt hat, die sich nicht von selbst wieder zusammenfügen. Sie können split brain vermeiden, indem Sie die empfohlene Anzahl der dedizierten Hauptknoten verwenden. Für Hilfe zur Wiederherstellung von split brain wenden Sie sich an Support.
Problem mit der Amazon Cognito Integration	Ihre Domain verwendet die Authentifizierung für OpenSearch Dashboards und der OpenSearch Service kann eine oder mehrere Amazon-Cognito-Ressourcen nicht finden. Dieses Problem tritt in der Regel auf, wenn der Amazon-Cognito-Benutzerpool fehlt. Um das Problem zu beheben, erstellen Sie die fehlende Ressource neu und konfigurieren Sie die OpenSearch Service-Domain so, dass sie diese verwenden kann.

Status	Beschreibung
Andere -Service-Probleme	Probleme mit dem OpenSearch Service selbst könnte dazu führen, dass Ihre Domain als nicht Update-berechtigt angezeigt wird. Wenn keine der vorangehenden Bedingungen für Ihre Domain gelten und das Problem mehr als einen Tag bestehen bleibt, wenden Sie sich bitte an Support.

Definition von Zeitfenstern außerhalb der Spitzenzeiten für Amazon Service OpenSearch

Wenn Sie eine Amazon OpenSearch Service-Domain erstellen, definieren Sie ein tägliches 10-Stunden-Fenster, das als Nebenzeiten gilt. OpenSearch Der Service verwendet dieses Fenster, um Service-Software-Updates und Auto-Tune-Optimierungen zu planen, die nach Möglichkeit eine blaue/grüne Bereitstellung während vergleichsweise geringerer Verkehrszeiten erfordern. Blau/Grün bezieht es sich auf das Erstellen einer neuen Umgebung für Domain-Updates und das Weiterleiten von Benutzern auf die neue Umgebung, nachdem die Updates abgeschlossen sind.

Blau/Grün-Bereitstellungen sind zwar unterbrechungsfrei, aber um mögliche Leistungseinbußen zu minimieren, während Ressourcen für eine blaue/grüne Bereitstellung verbraucht werden, empfehlen wir, diese Bereitstellungen während des für die Domäne konfigurierten Zeitfensters außerhalb der Spitzenzeiten zu planen. Updates wie der Austausch von Knoten oder solche, die sofort in der Domain bereitgestellt werden müssen, nutzen das Zeitfenster außerhalb der Spitzenzeiten nicht.

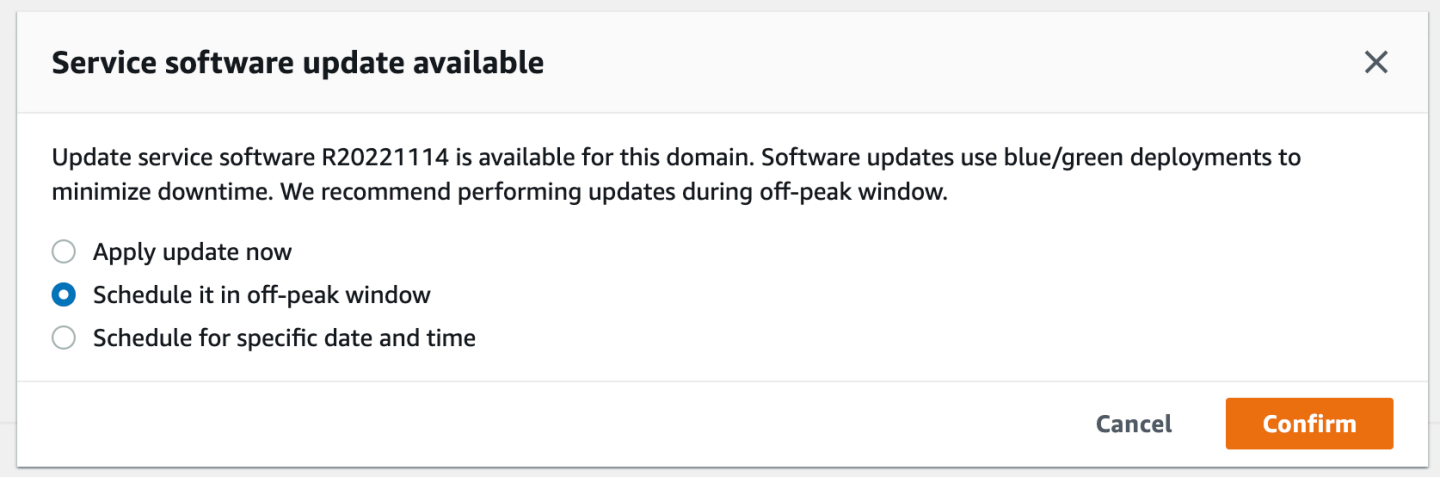
Sie können die Startzeit für das Fenster außerhalb der Spitzenzeiten ändern, aber Sie können die Länge des Fensters nicht ändern.

> **Note**
>
> Fenster außerhalb der Spitzenzeiten wurden am 16. Februar 2023 eingeführt. Bei allen Domains, die vor diesem Datum erstellt wurden, ist das Fenster außerhalb der Spitzenzeiten standardmäßig deaktiviert. Sie müssen das Zeitfenster außerhalb der Spitzenzeiten für diese Domains manuell aktivieren und konfigurieren. Für alle Domains, die nach diesem Datum erstellt werden, ist das Fenster außerhalb der Spitzenzeiten standardmäßig aktiviert. Sie können das Zeitfenster außerhalb der Spitzenzeiten für eine Domain nicht deaktivieren, nachdem es aktiviert wurde.

Softwareupdates für den Service außerhalb der Spitzenzeiten

OpenSearch Der Service umfasst zwei große Kategorien von Servicesoftwareupdates: optional und erforderlich. Beide Typen erfordern blau/grüne Bereitstellungen. Optionale Updates werden auf Ihren Domains nicht durchgesetzt. Erforderliche Updates werden automatisch installiert, wenn Sie vor Ablauf der angegebenen Frist (in der Regel zwei Wochen ab Verfügbarkeit) keine Maßnahmen ergreifen. Weitere Informationen finden Sie unter the section called “Optionale und erforderliche Updates”.

Wenn Sie ein optionales Update initiieren, haben Sie die Wahl, das Update sofort anzuwenden, es für ein späteres Zeitfenster außerhalb der Spitzenzeiten zu planen oder ein benutzerdefiniertes Datum und eine benutzerdefinierte Uhrzeit für die Anwendung anzugeben.



Für erforderliche Updates legt der OpenSearch Service außerhalb der Hauptverkehrszeiten automatisch ein Datum und eine Uhrzeit für die Durchführung des Updates fest. Sie erhalten drei Tage vor dem geplanten Update eine Benachrichtigung, und Sie können das Update auf einen späteren Zeitpunkt innerhalb des erforderlichen Bereitstellungszeitraums verschieben. Detaillierte Anweisungen finden Sie unter the section called “So verschieben Sie den Termin”.

Auto-Tune-Optimierungen außerhalb der Spitzenzeiten

Bisher nutzte Auto-Tune Wartungsfenster, um Änderungen zu planen, die eine blaue/grüne Implementierung erforderten. Domänen, für die Auto-Tune und Wartungsfenster bereits vor der Einführung von Zeitfenstern mit geringer Auslastung aktiviert waren, verwenden weiterhin Wartungsfenster für diese Updates, es sei denn, Sie migrieren sie so, dass sie das Zeitfenster außerhalb der Spitzenzeiten verwenden.

Wir empfehlen Ihnen, Ihre Domains so zu migrieren, dass Sie das Zeitfenster außerhalb der Spitzenzeiten verwenden, da es dazu dient, andere Aktivitäten auf der Domain zu planen, wie z. B. Service-Software-Updates. Detaillierte Anweisungen finden Sie unter the section called “Migration von Auto-Tune-Wartungsfenstern”. Sie können die Wartungsfenster nicht wieder verwenden, nachdem Sie Ihre Domain in das Zeitfenster außerhalb der Spitzenzeiten migriert haben.

Alle Domains, die nach dem 16. Februar 2023 erstellt wurden, verwenden für die Planung von blue/green deployments. You can't disable the off-peak window for a domain. For a list of Auto-Tune optimizations that require blue/green Bereitstellungen das Zeitfenster außerhalb der Spitzenzeiten und nicht die alten Wartungsfenster, siehe. the section called “Änderungsarten”

Aktivierung des Zeitfensters außerhalb der Spitzenzeiten

Bei allen Domains, die vor dem 16. Februar 2023 erstellt wurden (als Zeitfenster außerhalb der Spitzenzeiten eingeführt wurden), ist die Funktion standardmäßig deaktiviert. Sie müssen es für diese Domains manuell aktivieren. Sie können das Zeitfenster außerhalb der Spitzenzeiten nicht mehr deaktivieren, nachdem es aktiviert wurde.

Konsole

Um das Zeitfenster außerhalb der Spitzenzeiten für eine Domain zu aktivieren

1. Öffnen Sie die Amazon OpenSearch Service-Konsole zu https://console.aws.amazon.com/aos/Hause.
2. Wählen Sie den Namen der Domain aus, um die Konfiguration zu öffnen.
3. Navigieren Sie zur Registerkarte Off-Peak-Fenster und wählen Sie Bearbeiten.
4. Geben Sie eine benutzerdefinierte Startzeit in koordinierter Weltzeit (UTC) an. Wenn Sie zum Beispiel in der Region USA West (Oregon) eine Startzeit von 23:30 Uhr konfigurieren möchten, geben Sie 07:30 Uhr an.
5. Wählen Sie Änderungen speichern aus.

CLI

Um das Zeitfenster außerhalb der Spitzenzeiten mit dem zu ändern AWS CLI, senden Sie eine Anfrage: UpdateDomainConfig

```
aws opensearch update-domain-config \
```

```
  --domain-name my-domain \
  --off-peak-window-options 'Enabled=true,
OffPeakWindow={WindowStartTime={Hours=02,Minutes=00}}'
```

Wenn Sie keine benutzerdefinierte Startzeit für das Fenster angeben, wird standardmäßig 00:00 UTC verwendet.

Konfiguration eines benutzerdefinierten Zeitfensters außerhalb der Spitzenzeiten

Sie geben ein benutzerdefiniertes Zeitfenster außerhalb der Spitzenzeiten für Ihre Domain in koordinierter Weltzeit (UTC) an. Wenn Sie beispielsweise möchten, dass das Zeitfenster außerhalb der Spitzenzeiten für eine Domain in der Region USA Ost (Nord-Virginia) um 23:00 Uhr beginnt, geben Sie 04:00 UTC an.

Konsole

Um das Zeitfenster außerhalb der Spitzenzeiten für eine Domain zu ändern

1. Öffnen Sie die Amazon OpenSearch Service-Konsole zu https://console.aws.amazon.com/aos/Hause.
2. Wählen Sie den Namen der Domain aus, um die Konfiguration zu öffnen.
3. Navigieren Sie zur Registerkarte Off-Peak-Fenster. Sie können das konfigurierte Zeitfenster außerhalb der Spitzenzeiten und eine Liste der bevorstehenden geplanten Aktionen für die Domain einsehen.
4. Wählen Sie Bearbeiten und geben Sie eine neue Startzeit in UTC an. Wenn Sie zum Beispiel in der Region USA Ost (Nord-Virginia) als Startzeit festlegen möchten, geben Sie 02:00 Uhr UCT an.
5. Wählen Sie Änderungen speichern aus.

CLI

Um mit dem ein benutzerdefiniertes Zeitfenster außerhalb der Spitzenzeiten zu konfigurieren AWS CLI, senden Sie eine UpdateDomainConfigAnfrage und geben Sie Stunde und Minute im 24-Stunden-Format an.

Die folgende Anforderung ändert beispielsweise die Startzeit des Fensters auf 2:00 Uhr UTC:

```
aws opensearch update-domain-config \
  --domain-name my-domain \
  --off-peak-window-options 'OffPeakWindow={WindowStartTime={Hours=02,Minutes=00}}'
```

Wenn Sie keine Fensterstartzeit angeben, wird standardmäßig 22:00 Uhr Ortszeit für die Domäne verwendet, in der AWS-Region die Domain erstellt wurde.

Geplante Aktionen anzeigen

Sie können für jede Ihrer Domains alle aktuell geplanten, laufenden oder ausstehenden Aktionen einsehen. Aktionen können den Schweregrad `HIGH`, `MEDIUM`, und haben`LOW`.

Aktionen können folgende Status haben:

- `Pending update`— Die Aktion befindet sich in der Warteschlange und muss bearbeitet werden.
- `In progress`— Die Aktion ist derzeit in Bearbeitung.
- `Failed`— Die Aktion konnte nicht abgeschlossen werden.
- `Completed`— Die Aktion wurde erfolgreich abgeschlossen.
- `Not eligible`— Nur für Service-Software-Updates. Das Update kann nicht fortgesetzt werden, da sich der Cluster in einem fehlerhaften Status befindet.
- `Eligible`— Nur für Service-Softwareupdates. Die Domain ist für ein Update berechtigt.

Konsole

In der OpenSearch Servicekonsole werden alle geplanten Aktionen innerhalb der Domänenkonfiguration zusammen mit dem Schweregrad und dem aktuellen Status jeder Aktion angezeigt.

So zeigen Sie geplante Aktionen für eine Domain an

1. Öffnen Sie die Amazon OpenSearch Service-Konsole zu https://console.aws.amazon.com/aos/Hause.
2. Wählen Sie den Namen der Domain aus, um die Konfiguration zu öffnen.
3. Navigieren Sie zur Registerkarte Off-Peak-Fenster.
4. Sehen Sie sich unter Geplante Aktionen alle Aktionen an, die derzeit für die Domain geplant, in Bearbeitung sind oder ausstehen.

CLI

Um geplante Aktionen mit dem anzuzeigen AWS CLI, senden Sie eine ListScheduledActionsAnfrage:

```
aws opensearch list-scheduled-actions \
  --domain-name my-domain
```

Antwort:

```
{
    "ScheduledActions": [
        {
            "Cancellable": true,
            "Description": "The Deployment type is : BLUE_GREEN.",
            "ID": "R20220721-P13",
            "Mandatory": false,
            "Severity": "HIGH",
            "ScheduledBy": "CUSTOMER",
            "ScheduledTime": 1.673871601E9,
            "Status": "PENDING_UPDATE",
            "Type": "SERVICE_SOFTWARE_UPDATE",
        },
        {
            "Cancellable": true,
            "Description": "Amazon Opensearch will adjust the young generation JVM
 arguments on your domain to improve performance",
            "ID": "Auto-Tune",
            "Mandatory": true,
            "Severity": "MEDIUM",
            "ScheduledBy": "SYSTEM",
            "ScheduledTime": 1.673871601E9,
            "Status": "PENDING_UPDATE",
            "Type": "JVM_HEAP_SIZE_TUNING",
        }
    ]
}
```

So verschieben Sie den Termin

OpenSearch Der Service informiert Sie über geplante Service-Softwareupdates und Auto-Tune-Optimierungen. Sie können die Änderung sofort anwenden oder sie auf ein späteres Datum und eine spätere Uhrzeit verschieben.

> **Note**
>
> OpenSearch Der Service kann die Aktion innerhalb einer Stunde nach dem von Ihnen ausgewählten Zeitpunkt planen. Wenn Sie sich beispielsweise dafür entscheiden, ein Update um 17 Uhr anzuwenden, kann es zwischen 17 und 18 Uhr installiert werden.

Konsole

So planen Sie eine Aktion zu verschieben Sie den Termin

1. Öffnen Sie die Amazon OpenSearch Service-Konsole zu https://console.aws.amazon.com/aos/Hause.
2. Wählen Sie den Namen der Domain aus, um die Konfiguration zu öffnen.
3. Navigieren Sie zur Registerkarte Off-Peak-Fenster.
4. Wählen Sie unter Geplante Aktionen die Aktion aus und klicken Sie auf Erneut planen.
5. Wählen Sie eine der folgenden Optionen:
   - Update jetzt anwenden — Plant sofort, dass die Aktion in der aktuellen Stunde ausgeführt wird, sofern Kapazität verfügbar ist. Wenn keine Kapazität verfügbar ist, bieten wir andere verfügbare Zeitfenster zur Auswahl.
   - Außerhalb der Hauptverkehrszeiten einplanen — Markiert die Aktion, die während eines bevorstehenden Zeitfensters außerhalb der Hauptverkehrszeiten aufgenommen werden soll. Es gibt keine Garantie dafür, dass die Änderung innerhalb des nächsten Zeitfensters umgesetzt wird. Je nach Kapazität kann dies in den folgenden Tagen geschehen.
   - Dieses Update neu planen — Hier können Sie ein benutzerdefiniertes Datum und eine Uhrzeit angeben, zu der die Änderung übernommen werden soll. Wenn die von Ihnen angegebene Uhrzeit aus Kapazitätsgründen nicht verfügbar ist, können Sie ein anderes Zeitfenster auswählen.
   - Geplantes Update abbrechen — Bricht das Update ab. Diese Option ist nur für optionale Service-Softwareupdates verfügbar. Sie ist nicht für Auto-Tune-Aktionen oder obligatorische Softwareupdates verfügbar.
6. Wählen Sie Änderungen speichern aus.

CLI

Um eine Aktion mit dem neu zu planen AWS CLI, senden Sie eine UpdateScheduledActionAnfrage. Um die Aktions-ID abzurufen, senden Sie eine `ListScheduledActions` Anfrage.

Mit der folgenden Anfrage verschieben Sie den Termin eines Service-Softwareupdates auf ein bestimmtes Datum und eine bestimmte Uhrzeit:

```
aws opensearch update-scheduled-action \
  --domain-name my-domain \
  --action-id R20220721-P13 \
  --action-type "SERVICE_SOFTWARE_UPDATE" \
  --desired-start-time 1677348395000 \
  --schedule-at TIMESTAMP
```

Antwort:

```
{
   "ScheduledAction": {
      "Cancellable": true,
      "Description": "Cluster status is updated.",
      "Id": "R20220721-P13",
      "Mandatory": false,
      "ScheduledBy": "CUSTOMER",
      "ScheduledTime": 1677348395000,
      "Severity": "HIGH",
      "Status": "PENDING_UPDATE",
      "Type": "SERVICE_SOFTWARE_UPDATE"
   }
}
```

Wenn die Anforderung mit einem fehlschlägt`SlotNotAvailableException`, bedeutet dies, dass die von Ihnen angegebene Uhrzeit aus Kapazitätsgründen nicht verfügbar ist und Sie eine andere Uhrzeit angeben müssen. OpenSearch Der Service schlägt in der Antwort alternative verfügbare Zeitnischen vor.

Migration von Auto-Tune-Wartungsfenstern

Wenn eine Domain vor dem 16. Februar 2023 erstellt wurde, könnte sie Wartungsfenster verwenden, um Auto-Tune-Optimierungen zu planen, die eine blaue/grüne Bereitstellung erfordern. Sie können

Ihre vorhandenen Auto-Tune-Domains migrieren, um stattdessen das Zeitfenster außerhalb der Spitzenzeiten zu nutzen.

> **Note**
>
> Sie können nach der Migration Ihrer Domain nicht wieder zur Verwendung von Wartungsfenstern zurückkehren, um Zeitfenster außerhalb der Spitzenzeiten zu verwenden.

Konsole

So migrieren Sie eine Domain zur Nutzung des Zeitfensters außerhalb der Spitzenzeiten

1. Wählen Sie in der Amazon OpenSearch Service-Konsole den Namen der Domain aus, um die Konfiguration zu öffnen.
2. Gehen Sie zur Registerkarte Auto-Tune und wählen Sie Bearbeiten.
3. Wählen Sie Zu einem Sperrzeitfenster migrieren aus.
4. Geben Sie unter Startzeit (UTC) eine tägliche Startzeit für das Zeitfenster außerhalb der Spitzenzeiten in koordinierter Weltzeit (UTC) an.
5. Wählen Sie Änderungen speichern aus.

CLI

Um von einem Auto-Tune-Wartungsfenster zu einem Wartungsfenster außerhalb der Spitzenzeiten zu migrieren AWS CLI, senden Sie eine Anfrage: UpdateDomainConfig

```
aws opensearch update-domain-config \
  --domain-name my-domain \
  --auto-tune-options
 DesiredState=ENABLED,UseOffPeakWindow=true,MaintenanceSchedules=[]
```

Das Zeitfenster außerhalb der Spitzenzeiten muss aktiviert sein, damit Sie eine Domain vom Auto-Tune-Wartungsfenster in das Wartungsfenster außerhalb der Spitzenzeiten migrieren können. Sie können das Zeitfenster außerhalb der Spitzenzeiten in einer separaten Anfrage oder in derselben Anfrage aktivieren. Detaillierte Anweisungen finden Sie unter the section called “Aktivierung des Zeitfensters außerhalb der Spitzenzeiten”.

Benachrichtigungen in Amazon OpenSearch Service

Benachrichtigungen in Amazon OpenSearch Service enthalten wichtige Informationen über die Leistung und den Zustand Ihrer Domains. OpenSearch Der Service informiert Sie über Service-Software-Updates, Auto-Tune-Verbesserungen, Cluster-Integritätsereignisse und Domainfehler. Benachrichtigungen sind für alle Versionen von OpenSearch und Elasticsearch OSS verfügbar.

Sie können Benachrichtigungen im Bereich Benachrichtigungen der OpenSearch Servicekonsole einsehen. Alle Benachrichtigungen für OpenSearch Service werden auch in Amazon EventBridge angezeigt. Eine vollständige Liste der Benachrichtigungen und Beispielereignisse finden Sie unter the section called “Überwachung von Ereignissen”.

Einstieg in die Verwendung von Benachrichtigungen

Benachrichtigungen werden automatisch aktiviert, wenn Sie eine Domain erstellen. Rufen Sie das Benachrichtigungsfeld der OpenSearch Servicekonsole auf, um Benachrichtigungen zu überwachen und zu bestätigen. Jede Benachrichtigung enthält Informationen wie die Uhrzeit, zu der sie veröffentlicht wurde, die Domain, auf die sie sich bezieht, einen Schweregrad und Statuslevel sowie eine kurze Erklärung. Sie können frühere Benachrichtigungen für bis zu 90 Tage in der Konsole anzeigen.

Nachdem Sie auf das Benachrichtigungsfeld zugegriffen oder eine Benachrichtigung bestätigt haben, erhalten Sie möglicherweise eine Fehlermeldung, dass Sie keine Berechtigungen zum Ausführen von `es:ListNotificationsV2` oder `es:UpdateNotificationStatus` haben. Um dieses Problem zu beheben, erteilen Sie Ihrem Benutzer oder Ihrer Rolle die folgenden Berechtigungen in IAM:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "es:UpdateNotificationStatus",
      "es:ListNotifications"
    ],
    "Resource": "arn:aws:es:*:123456789012:domain/*"
  }]
}
```

Die IAM-Konsole löst einen Fehler aus („IAM erkennt eine oder mehrere Aktionen nicht“), den Sie sicher ignorieren können. Sie können die `es:UpdateNotificationStatus`-Aktion auch auf bestimmte Domains beschränken. Weitere Informationen hierzu finden Sie unter the section called “Richtlinienelementreferenz”.

Schweregrad

Benachrichtigungen im OpenSearch Service können informativ sein und sich auf Maßnahmen beziehen, die Sie bereits ergriffen haben, oder auf den Betrieb Ihrer Domain, oder umsetzbare Benachrichtigungen, bei denen Sie bestimmte Maßnahmen ergreifen müssen, z. B. die Installation eines obligatorischen Sicherheitspatches. Jeder Benachrichtigung ist ein Schweregrad zugeordnet, der `Informational`, `Low`, `Medium`, `High`, oder `Critical` sein kann. In der folgenden Tabelle werden alle Schweregrade zusammengefasst:

Schweregrad	Beschreibung	Beispiele
`Informational`	Informationen zum Betrieb Ihrer Domain.	• Service-Softwareaktualisierung verfügbar • Automatische Optimierung gestartet
`Low`	Eine empfohlene Maßnahme, hat jedoch keine negativen Auswirkungen auf die Domain-Verfügbarkeit oder -leistung, wenn keine Maßnahmen ergriffen werden.	• Automatische Optimierung abgebrochen • Warnung mit hoher Shard-Anzahl
`Medium`	Es kann Auswirkungen haben, wenn die empfohlene Aktion nicht ausgeführt wird, aber es gibt ein erweitertes Zeitfenster für die auszuführende Aktion.	• Service-Softwareaktualisierung fehlgeschlagen • Limit für Shard-Anzahl überschritten
`High`	Dringende Maßnahmen sind erforderlich, um	• Aktualisierung der Servicesoftware erforderlich • KMS-Schlüssel unzugänglich

Schweregrad	Beschreibung	Beispiele
	nachteilige Auswirkungen zu vermeiden.	
`Critical`	Sofortiges Handeln ist erforderlich, um nachteilige Auswirkungen zu vermeiden oder zu reparieren.	Aktuell keine verfügbar

Beispiel für ein Ereignis EventBridge

Das folgende Beispiel zeigt ein OpenSearch Service-Benachrichtigungsereignis, das an Amazon gesendet wurde EventBridge. Die Benachrichtigung hat den Schweregrad von `Informational`, da das Update optional ist:

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Available",
    "severity": "Informational",
    "description": "Service software update [R20200330-p1] available."
  }
}
```

Konfiguration einer Multi-AZ-Domain in Amazon Service OpenSearch

Um Datenverlust zu verhindern und die Ausfallzeiten des Amazon OpenSearch Service-Clusters im Falle einer Serviceunterbrechung zu minimieren, können Sie Knoten auf zwei oder drei Availability Zones in derselben Region verteilen, eine Konfiguration, die als Multi-AZ bezeichnet wird. Availability Zones sind isolierte Standorte innerhalb jeder AWS Region.

Für Domains, auf denen Produktionsworkloads ausgeführt werden, empfehlen wir die Bereitstellungsoption Multi-AZ mit Standby, mit der die folgende Konfiguration erstellt wird:

- Die Domain wurde in drei Zonen bereitgestellt.
- Instance-Typen der aktuellen Generation für dedizierte Master- und Datenknoten.
- Drei dedizierte Masterknoten und drei (oder ein Vielfaches von drei) Datenknoten.
- Mindestens zwei Replikate für jeden Index in Ihrer Domain oder ein Vielfaches von drei Kopien von Daten (einschließlich Primärknoten und Replikaten).

Der Rest dieses Abschnitts enthält Erläuterungen und Kontext zu diesen Konfigurationen.

Multi-AZ mit Standby

Multi-AZ mit Standby ist eine Bereitstellungsoption für Amazon OpenSearch Service-Domains, die eine Verfügbarkeit von 99,99%, konsistente Leistung für Produktionsworkloads und eine vereinfachte Domainkonfiguration und -verwaltung bietet. Wenn Sie Multi-AZ mit Standby verwenden, sind Domains widerstandsfähig gegen Infrastrukturausfälle, ohne dass sich dies auf Leistung oder Verfügbarkeit auswirkt. Diese Bereitstellungsoption erfüllt diesen Standard, indem sie eine Reihe von bewährten Methoden vorschreibt, z. B. eine bestimmte Anzahl von Datenknoten, die Anzahl der Master-Knoten, den Instanztyp, die Anzahl der Replikate, die Einstellungen für Softwareupdates und die Aktivierung von Auto-Tune.

> **Note**
>
> Multi-AZ mit Standby ist für OpenSearch Version 1.3 und höher verfügbar und erfordert Regionen mit mindestens drei Availability Zones.

Wenn Sie Multi-AZ mit Standby verwenden, erstellt OpenSearch Service eine Domain über drei Availability Zones, wobei jede Zone eine vollständige Kopie der Daten enthält und die Daten gleichmäßig auf jede der Zonen verteilt sind. Ihre Domain reserviert Knoten in einer dieser Zonen als Standby-Knoten, was bedeutet, dass sie keine Suchanfragen bearbeiten. Wenn OpenSearch Service einen Fehler in der zugrunde liegenden Infrastruktur feststellt, aktiviert er die Standby-Knoten automatisch in weniger als einer Minute. Die Domain bedient weiterhin Indizierungs- und Suchanfragen, und jede Auswirkung beschränkt sich auf die Zeit, die für die Durchführung des Failovers benötigt wird. Es findet keine Umverteilung von Daten oder Ressourcen statt, sodass die Clusterleistung nicht beeinträchtigt wird und das Risiko einer verminderten Verfügbarkeit entfällt. Multi-AZ mit Standby ist ohne zusätzliche Kosten erhältlich.

Sie haben zwei Möglichkeiten, eine Domain mit Standby auf dem AWS Management Console zu erstellen. Zunächst können Sie eine Domäne mit der Erstellungsmethode Easy Create erstellen. Der OpenSearch Service verwendet dann automatisch eine vordefinierte Konfiguration, die Folgendes umfasst:

- Drei Availability Zones, von denen eine als Standby fungiert
- Drei dedizierte Master-Knoten und Datenknoten
- Auto-Tune ist auf der Domain aktiviert
- GP3 Speicher für die Datenknoten

Sie können auch die Erstellungsmethode „Standard“ wählen und als Bereitstellungsoption „Domäne mit Standby“ auswählen. Auf diese Weise können Sie Ihre Domain individuell anpassen und gleichzeitig wichtige Standby-Funktionen wie drei Zonen und drei Masterknoten vorschreiben. Wir empfehlen, eine Anzahl von Datenknoten zu wählen, die einem Vielfachen von drei (der Anzahl der Availability Zones) entspricht.

Sobald Sie Ihre Domain erstellt haben, können Sie zu den Seiten mit den Domain-Details navigieren und auf der Registerkarte Cluster-Konfiguration überprüfen, ob 3-AZ mit Standby unter Availability Zone (n) angezeigt wird.

Wenn Sie Probleme bei der Migration einer vorhandenen Domain zu Multi-AZ mit Standby haben, finden Sie im Leitfaden zur Fehlerbehebung weitere Informationen unter Fehler bei der Migration zu Multi-AZ mit Standby.

Einschränkungen

Beachten Sie bei der Einrichtung einer Domain mit Multi-AZ mit Standby die folgenden Einschränkungen:

- Die Gesamtzahl der Shards auf einem Knoten darf 1000 nicht überschreiten, die Gesamtzahl der Shards in einem Cluster darf 75000 nicht überschreiten und die Größe eines einzelnen Shards darf 65 GB nicht überschreiten.
- Multi-AZ mit Standby funktioniert nur mit den `m5` Instance-Typen`c5`,,`r5`,`r6g`, `r7gc6g`, `m6g` und. `r6gd` `i3` Weitere Informationen zu unterstützten Instances finden Sie unter Unterstützte Instance-Typen.
- Sie können nur bereitgestellte IOPs SSDs, Allzweck-SSDs (GP3) oder instanzgestützten Speicher im Standby-Modus verwenden.
- Wenn Sie die Aktivierung UltraWarmauf einer Multi-AZ mit Standby-Domain durchführen, muss die Anzahl der warmen Knoten ein Vielfaches der Anzahl der verwendeten Availability Zones sein.

Multi-AZ ohne Standby

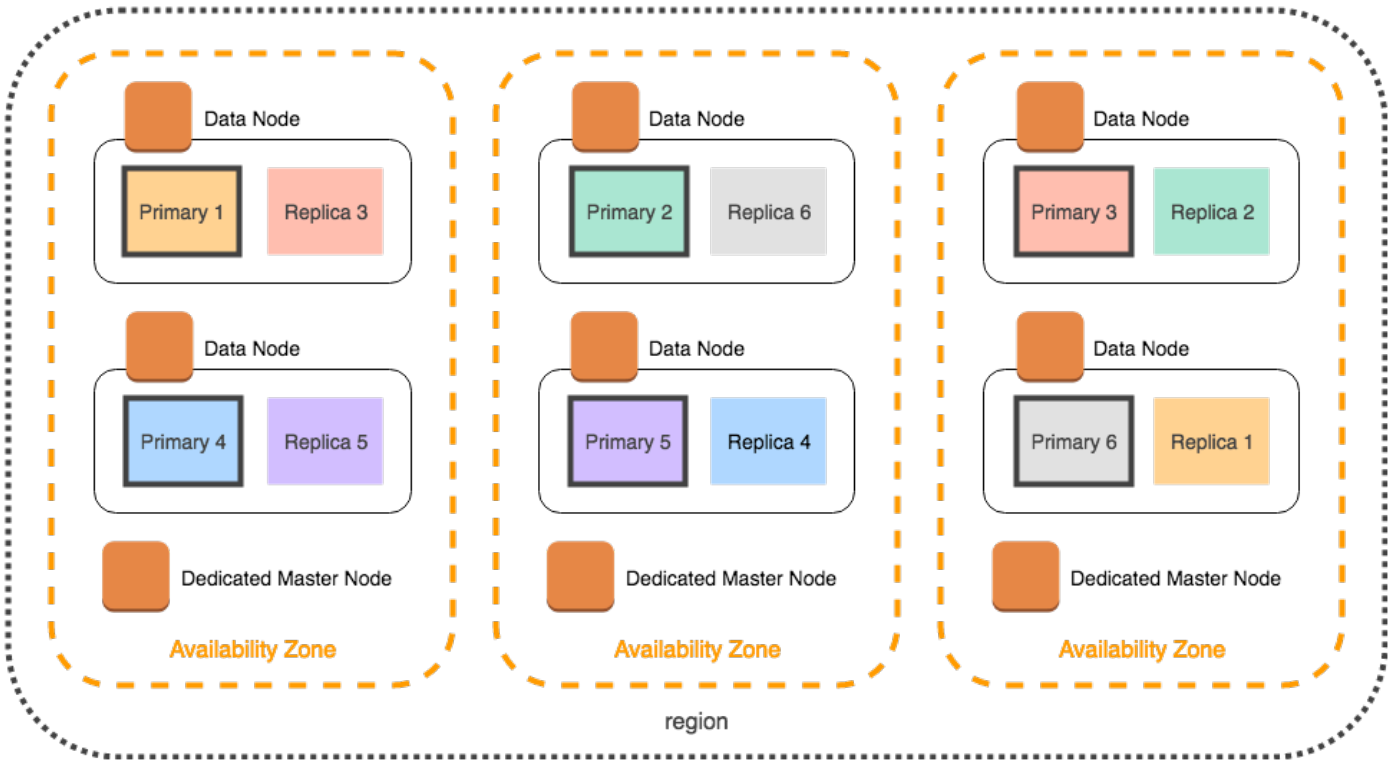
OpenSearch Der Service unterstützt weiterhin Multi-AZ ohne Standby, was eine Verfügbarkeit von 99,9% bietet. Die Knoten sind über die Availability Zone (n) verteilt, und die Verfügbarkeit hängt von der Anzahl der Availability Zones und Datenkopien ab. Während Sie bei Standby Ihre Domain nach bewährten Methoden konfigurieren müssen, können Sie ohne Standby Ihre eigene Anzahl von Availability Zones, Nodes und Replicas wählen. Wir empfehlen diese Option nur, wenn Sie über bestehende Workflows verfügen, die durch die Erstellung von Domains mit Standby gestört würden.

Wenn Sie sich für diese Option entscheiden, empfehlen wir dennoch, drei Availability Zones auszuwählen, um auch bei Knoten-, Festplatten- und Single-AZ-Ausfällen widerstandsfähig zu bleiben. Wenn ein Fehler auftritt, verteilt der Cluster die Daten auf die verbleibenden Ressourcen neu, um Verfügbarkeit und Redundanz aufrechtzuerhalten. Diese Datenverschiebung erhöht die Ressourcennutzung im Cluster und kann sich auf die Leistung auswirken. Wenn der Cluster nicht richtig dimensioniert ist, kann es zu einer verminderten Verfügbarkeit kommen, was den Zweck von Multi-AZ weitgehend zunichte macht.

Die einzige Möglichkeit, eine Domain ohne Standby auf dem zu konfigurieren, AWS Management Console besteht darin, die Erstellungsmethode Standard zu wählen und Domäne ohne Standby als Bereitstellungsoption auszuwählen.

Shard-Verteilung

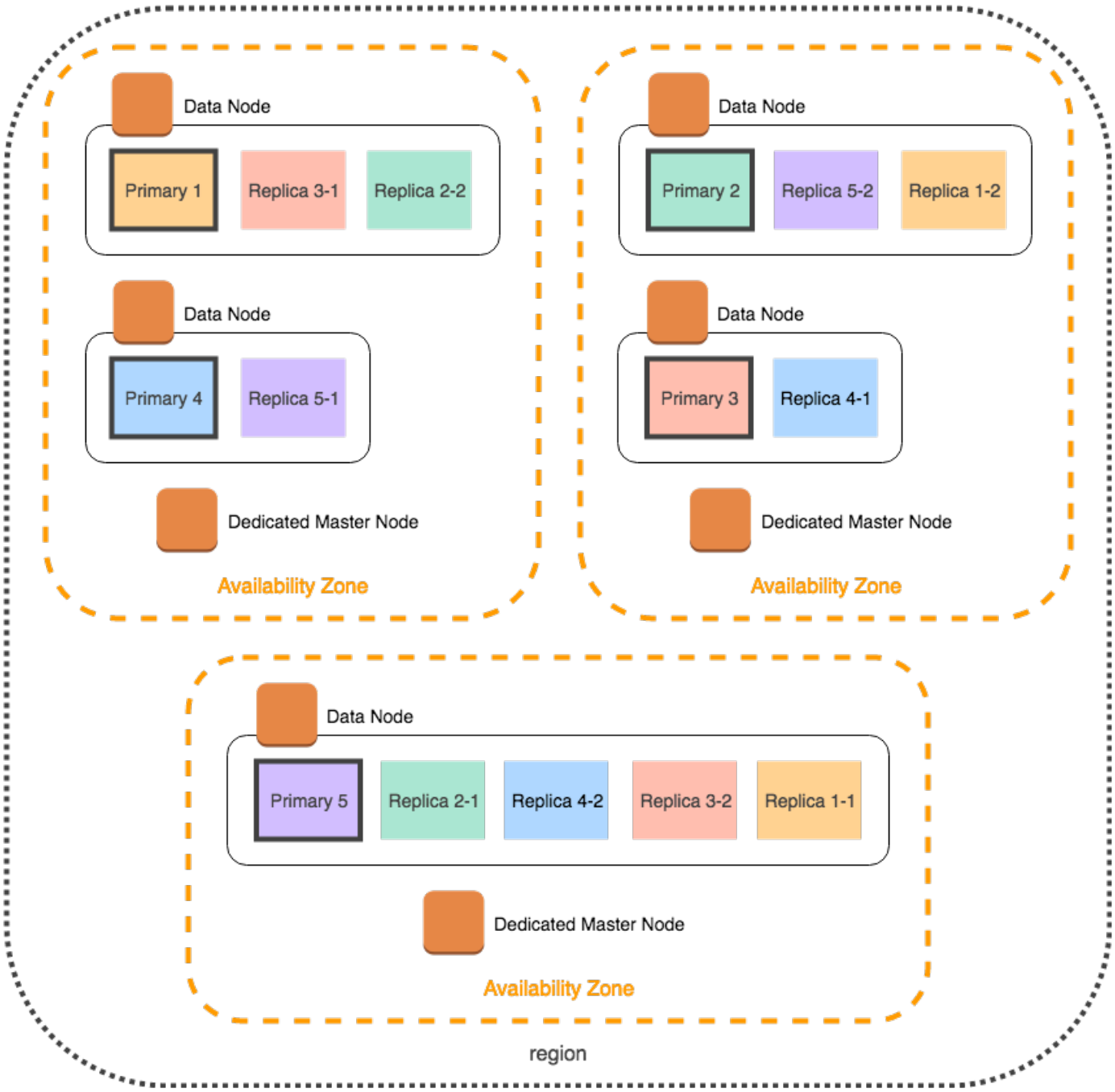
Wenn Sie Multi-AZ ohne Standby aktivieren, sollten Sie mindestens ein Replikat für jeden Index in Ihrem Cluster erstellen. Ohne Replikate kann OpenSearch Service keine Kopien Ihrer Daten an andere Availability Zones verteilen. Die Standardkonfiguration für jeden Index ist eine Replikat-Anzahl von 1. Wie das folgende Diagramm zeigt, bemüht sich OpenSearch Service nach besten Kräften, primäre Shards und die entsprechenden Replikat-Shards auf verschiedene Zonen zu verteilen.



Der OpenSearch Service verteilt die Shards nicht nur nach Availability Zone, sondern auch nach Knoten. Dennoch können bestimmte Domain-Konfigurationen zu einer unausgewogenen Anzahl von Shards führen. Betrachten Sie sich die folgende Domain:

- 5 Datenknoten
- 5 Primär-Shards
- 2 Replikate
- 3 Availability Zones

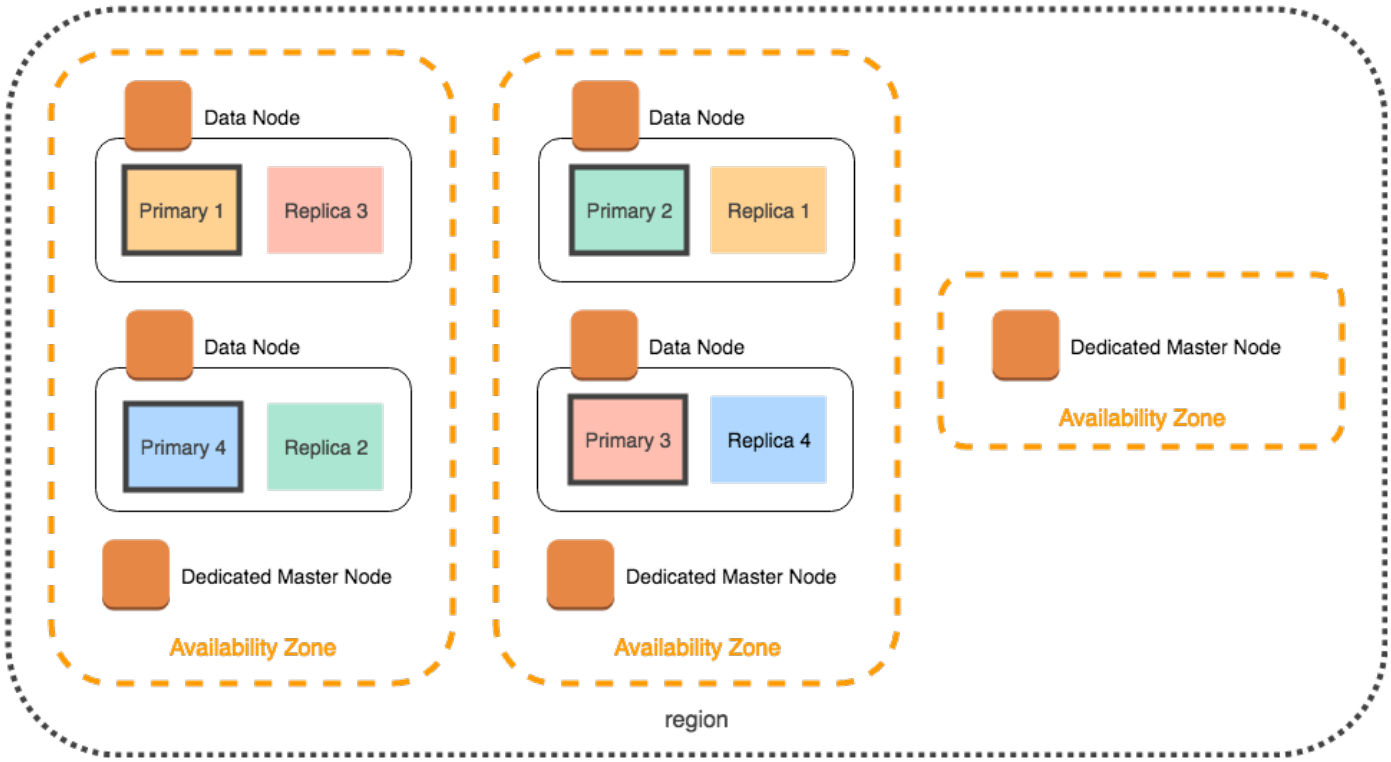
In diesem Fall muss OpenSearch Service einen Knoten überlasten, um die Primär- und Replikat-Shards auf die Zonen zu verteilen, wie in der folgenden Abbildung dargestellt.



Um solche Situationen zu vermeiden, die einzelne Knoten belasten und die Leistung beeinträchtigen können, empfehlen wir, Multi-AZ mit Standby zu wählen oder eine Instanzzahl zu wählen, die ein Vielfaches von drei ist, wenn Sie zwei oder mehr Replikate pro Index haben möchten.

Verteilung dedizierter Hauptknoten

Selbst wenn Sie bei der Konfiguration Ihrer Domain zwei Availability Zones auswählen, verteilt OpenSearch Service die dedizierten Master-Knoten automatisch auf drei Availability Zones. Diese Verteilung wirkt Cluster-Ausfallzeiten entgegen, falls in einer Zone eine Service-Unterbrechung auftritt. Wenn Sie die empfohlenen drei dedizierten Master-Knoten verwenden und eine Availability Zone ausfällt, verfügt Ihr Cluster weiterhin über ein Quorum (2) dedizierter Master-Knoten und kann einen neuen Master auswählen. Diese Konfiguration wird in der folgenden Abbildung veranschaulicht.



Wenn Sie den Instance-Typ einer älteren Generation auswählen, der nicht in drei Availability Zones verfügbar ist, treffen die folgenden Szenarien zu:

- Wenn Sie drei Availability Zones für die Domain ausgewählt haben, gibt OpenSearch Service einen Fehler aus. Wählen Sie einen anderen Instance-Typ aus und versuchen Sie es erneut.
- Wenn Sie zwei Availability Zones für die Domain ausgewählt haben, verteilt OpenSearch Service die dedizierten Master-Knoten auf zwei Zonen.

Unterbrechungen bei Availability Zones

Unterbrechungen bei Availability Zones sind selten, können aber auftreten. In der folgenden Tabelle sind die verschiedenen Multi-AZ-Konfigurationen und Verhaltensweisen während einer Unterbrechung aufgeführt. Die letzte Zeile in der Tabelle bezieht sich auf Multi-AZ mit Standby, während alle anderen Zeilen Konfigurationen haben, die nur für Multi-AZ ohne Standby gelten.

Anzahl der Availability Zones in einer Region	Anzahl der von Ihnen ausgewählten Availability Zones	Anzahl der dedizierten Hauptknoten	Verhalten bei einer Unterbrechung bei einer Availability Zone
2 oder mehr	2	0	Ausfallzeit. Ihr Cluster verliert die Hälfte seiner Datenknoten und muss mindestens einen in der verbleibenden Availability Zone ersetzen, bevor er einen Master auswählen kann.
2	2	3	50/50-Wahrscheinlichkeit von Ausfallzeiten. OpenSearch Der Service verteilt zwei dedizierte Master-Knoten in eine Availability Zone und einen in die andere: • Wenn bei der Availability Zone mit einem dedizierten Master-Knoten eine Unterbrechung auftritt, können die zwei dedizierten Master-Knoten in der verbleibenden Availability Zone einen Master auswählen. • Wenn die Availability Zone mit zwei dedizierten Hauptknoten unterbrochen wird, ist der Cluster nicht verfügbar, bis die verbleibende Availability Zone wiederhergestellt ist.
3 oder mehr	2	3	Keine Ausfallzeiten. OpenSearch Der Service verteilt die dedizierten Masterknoten automatisch auf drei Availability Zones, sodass die

Anzahl der Availability Zones in einer Region	Anzahl der von Ihnen ausgewählten Availability Zones	Anzahl der dedizierten Hauptknoten	Verhalten bei einer Unterbrechung bei einer Availability Zone
			verbleibenden zwei dedizierten Masterknoten einen Master auswählen können.
3 oder mehr	3	0	Keine Ausfallzeit Etwa zwei Drittel Ihrer Datenknoten sind weiterhin zur Wahl eines Masters verfügbar.
3 oder mehr	3	3	Keine Ausfallzeit Die verbleibenden zwei dedizierten Master-Knoten können einen Master auswählen.

In allen Konfigurationen, unabhängig von der Ursache, können Knotenausfälle dazu führen, dass die verbleibenden Datenknoten des Clusters einer Phase erhöhter Belastung ausgesetzt sind, während der OpenSearch Service automatisch neue Knoten konfiguriert, um die jetzt fehlenden zu ersetzen.

Beispiel: Tritt bei einer Availability Zone in einer Konfiguration mit drei Zonen ein Unterbrechung auf, müssen zwei Drittel der Datenknoten genauso so viele Anforderungen an den Cluster wie zuvor verarbeiten. Während sie diese Anforderungen verarbeiten, replizieren die verbleibenden Knoten außerdem Shards auf neuen Knoten, während diese online gehen. Die Leistung kann dadurch noch weiter beeinträchtigt werden. Wenn Verfügbarkeit für Ihre Workload unerlässlich ist, erwägen Sie, dieses Problem durch Hinzufügen von Ressourcen zu Ihrem Cluster zu mildern.

> **Note**
>
> OpenSearch Der Service verwaltet Multi-AZ-Domänen transparent, sodass Sie Störungen in der Availability Zone nicht manuell simulieren können.

Starten Ihrer Amazon OpenSearch Service-Domains innerhalb einer VPC

Sie können AWS Ressourcen wie Amazon OpenSearch Service-Domains in einer Virtual Private Cloud (VPC) starten. Eine VPC ist ein virtuelles Netzwerk, das Ihrem AWS-Konto gewidmet ist. Es ist logisch von anderen virtuellen Netzwerken in der AWS Cloud isoliert. Die Platzierung einer OpenSearch Dienstdomäne innerhalb einer VPC ermöglicht eine sichere Kommunikation zwischen dem OpenSearch Service und anderen Diensten innerhalb der VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud.

> **Note**
>
> Wenn Sie Ihre OpenSearch Service-Domain innerhalb einer VPC platzieren, muss Ihr Computer in der Lage sein, eine Verbindung zur VPC herzustellen. Diese Verbindung besteht oft in Form eines VPN, eines Transit Gateways, eines verwalteten Netzwerks oder eines Proxy-Servers. Sie können nicht direkt von außerhalb der VPC auf Ihre Domänen zugreifen.

VPC im Vergleich zu öffentlichen Domänen

Im Folgenden sind einige der Möglichkeiten aufgeführt, wie sich VPC-Domänen von öffentlichen Domänen unterscheiden. Jeder Unterschied wird weiter unten detailliert beschrieben.

- Domänen, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domänen, die öffentliche Endpunkte nutzen, über eine zusätzliche Sicherheitsebene.
- Während auf öffentliche Domänen von jedem mit dem Internet verbundenen Gerät aus zugegriffen werden kann, benötigen VPC-Domänen eine Form von VPN oder Proxy.
- Im Vergleich zu öffentlichen Domänen werden für VPC-Domänen in der -Konsole weniger Informationen angezeigt. Insbesondere werden auf der Registerkarte Clusterzustand keine Shard-Informationen aufgeführt. Zudem fehlt die Registerkarte Indizes ganz.
- Die Domänenendpunkte haben unterschiedliche Formen (`https://search-domain-name` im Vergleich mit `https://vpc-domain-name`).
- Sie können keine IP-basierten Zugriffsrichtlinien auf Domänen anwenden, die sich in einer VPC befinden, da Sicherheitsgruppen bereits IP-basierte Zugriffsrichtlinien erzwingen.

Einschränkungen

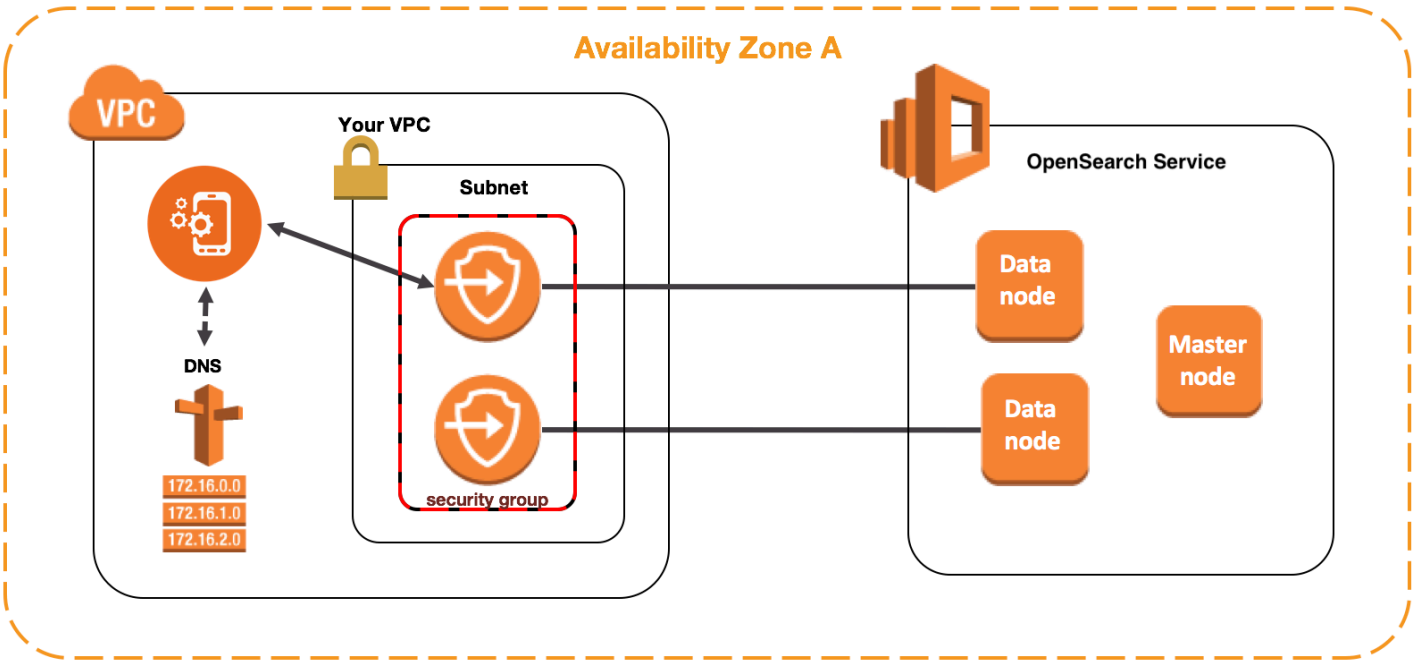
Der Betrieb einer OpenSearch Service-Domain innerhalb einer VPC hat die folgenden Einschränkungen:

- Wenn Sie eine neue Domäne in einer VPC verwenden, können Sie später nicht zu einem öffentlichen Endpunkt wechseln. Dasselbe gilt auch umgekehrt: Wenn Sie eine Domäne mit einem öffentlichen Endpunkt erstellen, können Sie diese später nicht in eine VPC aufnehmen. Sie müssen stattdessen eine neue Domäne erstellen und die Daten übernehmen.
- Sie können entweder die Domäne in eine VPC aufnehmen oder einen öffentlichen Endpunkt verwenden, beides zugleich ist aber nicht möglich. Sie müssen eine der beiden Möglichkeiten beim Erstellen der Domäne auswählen.
- Sie können Ihre Domäne nicht in einer VPC starten, die Dedicated Tenancy verwendet. Sie müssen eine VPC verwenden, deren Tenancy auf Standard gesetzt ist.
- Nachdem Sie eine Domäne in eine VPC aufgenommen haben, kann sie nicht in eine andere VPC verlagert werden, aber Sie können die Subnetze und Sicherheitsgruppeneinstellungen ändern.
- Um auf die Standardinstallation von OpenSearch Dashboards für eine Domain zuzugreifen, die sich in einer VPC befindet, müssen Benutzer Zugriff auf die VPC haben. Der Zugriff auf eine VPC unterscheidet sich je nach Netzwerkkonfiguration, aber wahrscheinlich muss dazu eine Verbindung mit einem VPN bzw. verwalteten Netzwerk hergestellt oder ein Proxyserver oder Transit Gateway verwendet werden. Weitere Informationen finden Sie unter the section called “Zugriffsrichtlinien für VPC-Domänen”, im Amazon VPC User Guide und unter the section called “Steuern des Zugriffs auf Dashboards ”.

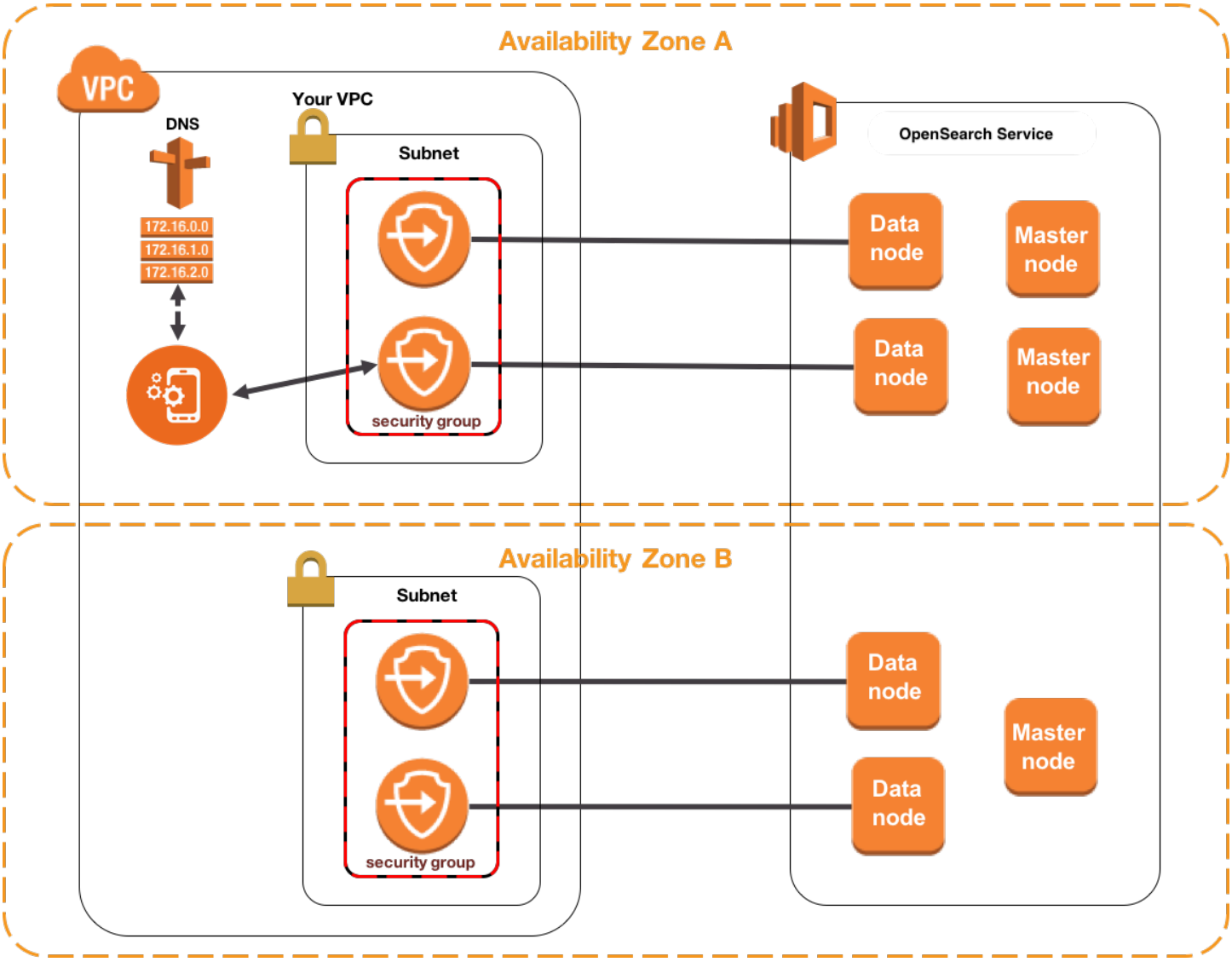
Architektur

Zur Unterstützung VPCs platziert OpenSearch Service einen Endpunkt in einem, zwei oder drei Subnetzen Ihrer VPC. Wenn Sie mehrere Availability Zones für Ihre Domäne aktivieren, muss sich jedes Subnetz in einer anderen Availability Zone in derselben Region befinden. Wenn Sie nur eine Availability Zone verwenden, platziert OpenSearch Service einen Endpunkt in nur einem Subnetz.

Die folgende Abbildung zeigt die VPC-Architektur für eine Availability Zone:



Die folgende Abbildung zeigt die VPC-Architektur für zwei Availability Zones:



OpenSearch Der Service platziert außerdem ein elastic network interface (ENI) in der VPC für jeden Ihrer Datenknoten. OpenSearch Der Service weist jedem ENI eine private IP-Adresse aus dem IPv4 Adressbereich Ihres Subnetzes zu. Der Service weist den IP-Adressen außerdem einen öffentlichen DNS-Hostnamen (Domänenendpunkt) zu. Sie müssen einen öffentlichen DNS-Service zum Auflösen des Endpunkts (DNS-Hostname) in die IP-Adressen der Datenknoten verwenden:

- Wenn Ihre VPC den von Amazon bereitgestellten DNS-Server verwendet und die `enableDnsSupport` Option auf `true` (den Standardwert) setzt, ist die Auflösung für den OpenSearch Service-Endpunkt erfolgreich.
- Wenn Ihre VPC einen privaten DNS-Server verwendet und der Server die öffentlichen autoritativen DNS-Server erreichen kann, um DNS-Hostnamen aufzulösen, ist die Auflösung auch für den OpenSearch Service-Endpunkt erfolgreich.

Da sich die IP-Adressen ändern können, sollten Sie den Domänenendpunkt regelmäßig auflösen, damit stets der Zugriff auf die richtigen Datenknoten gewährleistet ist. Wir empfehlen, das DNS-Auflösungsintervall auf eine Minute einzustellen. Wenn Sie einen Client verwenden, sollten Sie zudem sicherstellen, dass dessen DNS-Cache gelöscht wird.

Migrieren vom öffentlichen Zugriff zum VPC-Zugriff

Beim Erstellen einer Domäne legen Sie fest, ob für den Zugriff ein öffentlicher Endpunkt oder eine VPC verwendet wird. Nach der Erstellung können Sie nicht mehr zwischen den beiden Möglichkeiten wechseln. Sie müssen stattdessen eine neue Domäne erstellen und dann entweder eine manuelle Neuindizierung oder Datenmigration durchführen. Snapshots bieten eine bequeme Möglichkeit für das Migrieren von Daten. Informationen zum Erstellen und Wiederherstellen von Snapshots finden Sie unter the section called “Erstellen von Index-Snapshots”.

Zugriffsrichtlinien für VPC-Domänen

Die Platzierung Ihrer OpenSearch Service-Domain in einer VPC bietet eine inhärente, starke Sicherheitsebene. Wenn Sie eine Domäne mit öffentlichem Zugriff erstellen, hat der Endpunkt das folgende Format:

```
https://search-domain-name-identifier.region.es.amazonaws.com
```

Wie aus der Bezeichnung "öffentlich" zu schließen ist, kann auf diesen Endpunkt von jedem mit dem Internet verbundenen Gerät zugegriffen werden. Sie können jedoch (und sollten) den Zugriff darauf kontrollieren. Wenn Sie in einem Webbrowser auf den Endpunkt zugreifen, erhalten Sie unter Umständen die Nachricht `Not Authorized`. Die Anforderung erreicht jedoch die Domäne.

Wenn Sie eine Domäne mit VPC-Zugriff erstellen, gleicht der Endpunkt einem öffentlichen Endpunkt:

```
https://vpc-domain-name-identifier.region.es.amazonaws.com
```

Wenn Sie versuchen, auf den Endpunkt in einem Webbrowser zuzugreifen, tritt möglicherweise jedoch eine Zeitüberschreitung der Anforderung auf. Selbst zum Ausführen grundlegender `GET`-Anforderungen muss Ihr Computer eine Verbindung mit dem VPC herstellen können. Diese Verbindung besteht oft in Form eines VPN, eines Transit Gateways, eines verwalteten Netzwerks oder eines Proxy-Servers. Details zu den verschiedenen möglichen Verbindungsformen finden Sie unter Beispiele für VPC im Amazon-VPC-Benutzerhandbuch. Ein auf die Entwicklung ausgerichtetes Beispiel finden Sie unter the section called “Testen von VPC-Domänen”.

Zusätzlich zu dieser Konnektivitätsanforderung können VPCs Sie den Zugriff auf die Domain über Sicherheitsgruppen verwalten. Diese Kombination von Sicherheitsfunktionen reicht für viele Anwendungsfälle aus, und die Verwendung einer offenen Zugriffsrichtlinie für die Domäne mag ausreichend erscheinen.

Der Betrieb mit einer Open-Access-Richtlinie bedeutet nicht, dass jeder im Internet auf die OpenSearch Service-Domain zugreifen kann. Es bedeutet vielmehr, dass, wenn eine Anfrage die OpenSearch Service-Domain erreicht und die zugehörigen Sicherheitsgruppen dies zulassen, die Domain die Anfrage akzeptiert. Die einzige Ausnahme gibt es bei der Verwendung einer differenzierten Zugriffskontrolle oder einer Zugriffsrichtlinie, die IAM-Rollen angibt. Damit die Domäne eine Anforderung in diesen Situationen annehmen kann, müssen die Sicherheitsgruppen dies zulassen und sie muss mit gültigen Anmeldeinformationen signiert sein.

> **Note**
>
> Da Sicherheitsgruppen bereits IP-basierte Zugriffsrichtlinien durchsetzen, können Sie IP-basierte Zugriffsrichtlinien nicht auf OpenSearch Dienstdomänen anwenden, die sich in einer VPC befinden. Wenn Sie öffentlichen Zugriff verwenden, sind IP-basierte Richtlinien weiterhin verfügbar.

Bevor Sie beginnen: Voraussetzungen für den VPC-Zugriff

Bevor Sie eine Verbindung zwischen einer VPC und Ihrer neuen OpenSearch Service-Domain aktivieren können, müssen Sie Folgendes tun:

- Erstellen einer VPC

  Um Ihre VPC zu erstellen, können Sie die Amazon VPC-Konsole, die AWS CLI oder eine der folgenden verwenden. AWS SDKs Weitere Informationen finden Sie unter Arbeiten mit VPCs im Amazon VPC-Benutzerhandbuch. Wenn bereits eine VPC vorhanden ist, können Sie diesen Schritt überspringen.
- Reservieren von IP-Adressen

  OpenSearch Der Service ermöglicht die Verbindung einer VPC mit einer Domain, indem Netzwerkschnittstellen in einem Subnetz der VPC platziert werden. Jeder Netzwerkschnittstelle ist eine IP-Adresse zugewiesen. Sie müssen im Subnetz eine ausreichende Anzahl von IP-Adressen für die Netzwerkschnittstellen reservieren. Weitere Informationen finden Sie unter Reservieren von IP-Adressen in einem VPC-Subnetz.

Testen von VPC-Domänen

Die erweiterte Sicherheit einer VPC kann die Herstellung einer Verbindung zu Ihrer Domäne und die Durchführung von Tests zu einer Herausforderung machen. Wenn Sie bereits eine OpenSearch Service-VPC-Domain haben und lieber keinen VPN-Server erstellen möchten, versuchen Sie es mit dem folgenden Prozess:

1. Wählen Sie für die Zugriffsrichtlinie Ihrer Domäne die Option Nur differenzierte Zugriffssteuerung verwenden aus. Sie können diese Einstellung jederzeit aktualisieren, nachdem Sie den Test abgeschlossen haben.
2. Erstellen Sie eine Amazon EC2 Linux-Amazon-Instance in derselben VPC, demselben Subnetz und derselben Sicherheitsgruppe wie Ihre OpenSearch Service-Domain.

   Da diese Instance für Testzwecke vorgesehen ist und nur sehr wenig Arbeit leisten muss, wählen Sie einen kostengünstigen Instance-Typ, beispielsweise `t2.micro`. Weisen Sie der Instance eine öffentliche IP-Adresse zu und erstellen Sie entweder ein neues Schlüsselpaar oder wählen Sie ein vorhandenes aus. Wenn Sie einen neuen Schlüssel erstellen, laden Sie sie in Ihr `~/.ssh`-Verzeichnis herunter.

   Weitere Informationen zum Erstellen von Instances finden Sie unter Erste Schritte mit Amazon EC2 Linux-Instances.
3. Fügen Sie Ihrer VPC ein Internet-Gateway hinzu.
4. Fügen Sie in der Routing-Tabelle für Ihre VPC eine neue Route hinzu. Geben Sie für Destination (Ziel) einen CIDR-Block an, der die öffentliche IP-Adresse Ihres Computers enthält. Geben Sie für Target (Ziel) das Internet-Gateway an, das Sie gerade erstellt haben.

   Sie können beispielsweise `123.123.123.123/32` nur für Ihren Computer oder `123.123.123.0/24` für mehrere Computer angeben.
5. Für die Sicherheitsgruppe geben Sie zwei Regeln für eingehenden Datenverkehr an:

Typ	Protocol (Protokoll)	Port-Bereich	Quelle
SSH (22)	TCP (6)	22	*your-cidr-block*
HTTPS (443)	TCP (6)	443	*your-security-group-id*

Mit der ersten Regel können Sie per SSH auf Ihre EC2 Instance zugreifen. Die zweite ermöglicht es der EC2 Instanz, über HTTPS mit der OpenSearch Service-Domain zu kommunizieren.

6. Führen Sie vom Terminal folgenden Befehl aus:

```
ssh -i ~/.ssh/your-key.pem ec2-user@your-ec2-instance-public-ip -N -L
 9200:vpc-domain-name-identifier.region.es.amazonaws.com:443
```

   Dieser Befehl erstellt einen SSH-Tunnel, der Anfragen an https://localhost:9200 über die Instanz an Ihre OpenSearch Service-Domain weiterleitet. EC2 Die Angabe von Port 9200 im Befehl simuliert eine lokale OpenSearch Installation, verwenden Sie jedoch den gewünschten Port. OpenSearch Der Dienst akzeptiert nur Verbindungen über Port 80 (HTTP) oder 443 (HTTPS).

   Der Befehl stellt kein Feedback bereit und wird unbegrenzt ausgeführt. Um ihn anzuhalten, drücken Sie `Ctrl + C`.

7. Navigieren Sie in Ihrem Webbrowser zu https://localhost:9200/_dashboards/. Möglicherweise müssen Sie eine Sicherheitsausnahme bestätigen.

   Alternativ können Sie Anfragen an https://localhost:9200 unter Verwendung von curl, Postman oder Ihrer bevorzugten Programmiersprache senden.

> **Tip**
>
> Wenn curl-Fehler auftreten, weil ein Zertifikat nicht übereinstimmt, versuchen Sie das `--insecure`-Flag.

Reservieren von IP-Adressen in einem VPC-Subnetz

OpenSearch Der Service verbindet eine Domain mit einer VPC, indem er Netzwerkschnittstellen in einem Subnetz der VPC platziert (oder in mehreren Subnetzen der VPC, wenn Sie mehrere Availability Zones aktivieren). Jeder Netzwerkschnittstelle ist eine IP-Adresse zugewiesen. Bevor Sie Ihre OpenSearch Dienstdomäne erstellen, müssen Sie in jedem Subnetz über eine ausreichende Anzahl von IP-Adressen verfügen, um die Netzwerkschnittstellen aufnehmen zu können.

Die Grundformel lautet wie folgt: Die Anzahl der IP-Adressen, die der OpenSearch Service in jedem Subnetz reserviert, entspricht dem Dreifachen der Anzahl der Datenknoten, geteilt durch die Anzahl der Availability Zones.

Beispiele

- Wenn eine Domäne über neun Datenknoten in drei Availability Zones verfügt, beträgt die IP-Anzahl pro Subnetz 9 * 3 / 3 = 9.
- Wenn eine Domäne über acht Datenknoten in zwei Availability Zones verfügt, beträgt die IP-Anzahl pro Subnetz 8 * 3 / 2 = 12.
- Wenn eine Domäne sechs Datenknoten in einer Availability Zone hat, beträgt die IP-Anzahl pro Subnetz 6 * 3 / 1 = 18.

Wenn Sie die Domäne erstellen, reserviert der OpenSearch Service die IP-Adressen, verwendet einige für die Domäne und reserviert den Rest für blaue/grüne Bereitstellungen. Sie können die Netzwerkschnittstellen und die zugehörigen IP-Adressen im Bereich Netzwerkschnittstellen der EC2 Amazon-Konsole sehen. In der Spalte Beschreibung wird angezeigt, mit welcher OpenSearch Service-Domain die Netzwerkschnittstelle verknüpft ist.

> **Tip**
>
> Wir empfehlen, dass Sie dedizierte Subnetze für die vom OpenSearch Dienst reservierten IP-Adressen erstellen. Dadurch werden Überschneidungen mit anderen Anwendungen und Services vermieden und es ist gewährleistet, dass bei einer künftigen Skalierung des Clusters zusätzliche IP-Adressen reserviert werden können. Weitere Informationen erhalten Sie unter Erstellen eines Subnetzes in Ihrer VPC.

Sie können auch erwägen, dedizierte Koordinatorknoten bereitzustellen, um die Anzahl der für Ihre VPC-Domäne erforderlichen privaten IP-Adressreservierungen zu reduzieren. OpenSearchfügt Ihren dedizierten Koordinatorknoten statt Ihren Datenknoten ein elastic network interface (ENI) hinzu. Dedizierte Koordinatorknoten machen in der Regel etwa 10% der gesamten Datenknoten aus. Infolgedessen wird eine geringere Anzahl von privaten IP-Adressen für VPC-Domänen reserviert.

Service-verknüpfte Rolle für den VPC-Zugriff

Eine Service-verknüpfte Rolle ist ein spezieller Typ der IAM-Rolle zum Übertragen von Berechtigungen an einen Service, damit dieser Ressourcen für Sie erstellen und verwalten kann. OpenSearch Für den Service ist eine dienstverknüpfte Rolle erforderlich, um auf Ihre VPC zuzugreifen, den Domänenendpunkt zu erstellen und Netzwerkschnittstellen in einem Subnetz Ihrer VPC zu platzieren.

OpenSearch Der Service erstellt die Rolle automatisch, wenn Sie die OpenSearch Servicekonsole verwenden, um eine Domäne innerhalb einer VPC zu erstellen. Damit diese automatische Erstellung möglich ist, müssen Sie über Berechtigungen für die Aktion `iam:CreateServiceLinkedRole` verfügen. Weitere Informationen finden Sie unter Berechtigungen von Service-verknüpften Rollen im IAM-Benutzerhandbuch.

Nachdem OpenSearch Service die Rolle erstellt hat, können Sie sie mit der IAM-Konsole anzeigen (`AWSServiceRoleForAmazonOpenSearchService`).

Ausführliche Informationen zu den Berechtigungen dieser Rolle, und wie Sie sie löschen, finden Sie unter the section called “Verwenden von serviceverknüpften Rollen”.

Index-Snapshots in Amazon OpenSearch Service erstellen

Snapshots in Amazon OpenSearch Service sind Backups der Indizes und des Status eines Clusters. Der Status beinhaltet Cluster-Einstellungen, Knoteninformationen, Index-Einstellungen und die Shard-Zuweisung.

OpenSearch Service-Snapshots gibt es in den folgenden Formen:

- Automatisierte Snapshots dienen nur zur Cluster-Wiederherstellung. Sie können sie verwenden, um Ihre Domain im Falle eines roten Cluster-Status oder Datenverlusts wiederherzustellen. Weitere Informationen finden Sie weiter unten unter Snapshots wiederherstellen. OpenSearch Der Service speichert automatische Snapshots ohne zusätzliche Kosten in einem vorkonfigurierten Amazon S3 S3-Bucket.
- Manuelle Snapshots dienen zur Cluster-Wiederherstellung oder zum Verschieben von Daten von einem Cluster zu einem anderen. Sie müssen manuelle Snapshots initiieren. Diese Snapshots werden in Ihrem eigenen Amazon-S3-Bucket gespeichert und es fallen die S3-Standardgebühren an. Wenn Sie über einen Snapshot aus einem selbstverwalteten OpenSearch Cluster verfügen, können Sie diesen Snapshot verwenden, um zu einer OpenSearch Service-Domain zu migrieren. Weitere Informationen finden Sie unter Migration zu Amazon OpenSearch Service.

Alle OpenSearch Service-Domains erstellen automatische Snapshots, aber die Häufigkeit unterscheidet sich in folgenden Punkten:

- Für Domains, die OpenSearch oder Elasticsearch 5.3 und höher laufen, OpenSearch erstellt Service stündlich automatisierte Snapshots und speichert bis zu 336 davon 14 Tage lang.

Stündliche Snapshots sind aufgrund ihrer inkrementellen Natur weniger störend. Sie bieten auch einen neueren Wiederherstellungspunkt für den Fall von Problemen mit Domains.

- Bei Domains, auf denen Elasticsearch 5.1 und früher ausgeführt wird, erstellt OpenSearch Service täglich automatische Snapshots zu der von Ihnen angegebenen Stunde, speichert bis zu 14 davon und speichert keine Snapshot-Daten länger als 30 Tage.

Wenn Ihr Cluster in den roten Status wechselt, schlagen alle automatisierten Snapshots fehl, während der Cluster-Status bestehen bleibt. Wenn Sie das Problem nicht innerhalb von zwei Wochen beheben, können die Daten in Ihrem Cluster dauerhaft verloren gehen. Fehlerbehandlungsschritte finden Sie unter the section called “Roter Cluster-Status”.

Voraussetzungen

Um Snapshots manuell zu erstellen, müssen Sie mit IAM und Amazon S3 arbeiten. Stellen Sie sicher, dass Sie die folgenden Voraussetzungen erfüllen, bevor Sie versuchen, einen Snapshot zu erstellen:

Voraussetzung	Beschreibung
S3-Bucket	Erstellen Sie einen S3-Bucket, um manuelle Snapshots für Ihre OpenSearch Service-Domain zu speichern. Anweisungen finden Sie unter Erstellen eines Allzweck-Buckets im Amazon Simple Storage Service-Benutzerhandbuch. Merken Sie sich den Namen des Buckets, um ihn an den folgenden Stellen zu verwenden: • Die `Resource`-Anweisung der IAM-Richtlinie, die Ihrer IAM-Rolle beigefügt ist • Der Python-Client, der zum Registrieren eines Snapshot-Repositorys verwendet wurde (wenn Sie diese Methode verwenden) **Important** Wenden Sie keine S3 Glacier-Lebenszyklusregel auf diesen Bucket an. Manuelle Snapshots bieten keine Unterstützung für die Speicherklasse S3 Glacier.

Voraussetzung	Beschreibung
IAM-Rolle	Erstellen Sie eine IAM-Rolle, um Berechtigungen an den Service zu OpenSearch delegieren. Detaillierte Anleitungen finden Sie unter Erstellen einer IAM-Rolle (Konsole) im IAM-Benutzerhandbuch. Das restliche Kapitel bezieht sich auf diese Rolle als `TheSnapshotRole` . Anfügen einer IAM-Richtlinie Hängen Sie die folgende Richtlinie an `TheSnapshotRole` an, um den Zugriff auf den S3-Bucket zuzulassen: JSON `{ "Version": "2012-10-17", "Statement": [{ "Action": [ "s3:ListBucket" ], "Effect": "Allow", "Resource": [ "arn:aws:s3::: amzn-s3-demo-bucket " ] }, { "Action": [ "s3:GetObject", "s3:PutObject", "s3:DeleteObject" ], "Effect": "Allow", "Resource": [ "arn:aws:s3::: amzn-s3-demo-bucket /*" ] } ] }`

Voraussetzung	Beschreibung
	Anweisungen zum Anhängen einer Richtlinie an eine Rolle finden Sie unter Hinzufügen von IAM-Identitätsberechtigungen (Konsole) im IAM-Benutzerhandbuch. Bearbeiten der Vertrauensstellung Bearbeiten Sie die Vertrauensstellung von `TheSnapshotRole` , um OpenSearch Service in der `Principal` Anweisung anzugeben, wie im folgenden Beispiel gezeigt: JSON `{ "Version": "2012-10-17", "Statement": [{ "Sid": "", "Effect": "Allow", "Principal": { "Service": "es.amazonaws.com" }, "Action": "sts:AssumeRole" }] }` Anweisungen zum Bearbeiten der Vertrauensbeziehung finden Sie unter Aktualisieren einer Rollenvertrauensrichtlinie im IAM-Benutzerhandbuch.

Voraussetzung	Beschreibung

Berechtigungen	Um das Snapshot-Repository zu registrieren, müssen Sie in der Lage sein, zum OpenSearch Service `TheSnapshotRole` zu wechseln. Sie benötigen außerdem Zugriff auf die Aktion `es:ESHttpPut`. Um diese beiden Berechtigungen zu erteilen, fügen Sie die folgende Richtlinie an die IAM-Rolle an, deren Anmeldeinformationen zum Signieren der Anforderung verwendet werden:
	
	JSON
	
	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": "iam:PassRole", "Resource": "arn:aws:iam:: 123456789012 :role/TheSnapshotRole " }, { "Effect": "Allow", "Action": "es:ESHttpPut", "Resource": "arn:aws:es: region:123456789012 :domain/domain-name /*" } ] }`
	
	Wenn Ihr Benutzer oder Ihre Rolle nicht über die `iam:PassRole` erforderlichen Berechtigungen verfügt`TheSnapshotRole`, tritt möglicherweise der folgende Fehler auf, wenn Sie im nächsten Schritt versuchen, ein Repository zu registrieren:
	
	`$ python register-repo.py {"Message":"User: arn:aws:iam:: 123456789012 :user/MyUserAccount is not authorized to perform: iam:PassRole on resource: arn:aws:iam:: 123456789012 :role/TheSnapshotRole "}`

Registrieren eines manuellen Snapshot-Repositorys

Sie müssen ein Snapshot-Repository bei OpenSearch Service registrieren, bevor Sie manuelle Index-Snapshots erstellen können. Dieser einmalige Vorgang erfordert, dass Sie Ihre AWS Anfrage mit Zugangsdaten signieren, die für den Zugriff berechtigt sind`TheSnapshotRole`, wie unter beschriebenthe section called “Voraussetzungen”.

Schritt 1: Ordnen Sie die Snapshot-Rolle in OpenSearch Dashboards zu (wenn Sie eine differenzierte Zugriffskontrolle verwenden)

Eine differenzierte Zugriffskontrolle führt einen zusätzlichen Schritt bei der Registrierung eines Repositorys ein. Auch wenn Sie die HTTP-Basisauthentifizierung für alle anderen Zwecke verwenden, müssen Sie die `manage_snapshots`-Rolle Ihrer IAM-Rolle mit `iam:PassRole`-Berechtigungen zuordnen, um `TheSnapshotRole` zu übergeben.

1. Navigieren Sie zum OpenSearch Dashboards-Plugin für Ihre Service-Domain. OpenSearch Sie finden den Dashboards-Endpunkt in Ihrem Domain-Dashboard in der OpenSearch Service-Konsole.
2. Wählen Sie im Hauptmenü Sicherheit, Rollen, und wählen Sie die Rolle manage_snapshots.
3. Wählen Sie Zugeordnete Benutzer, Mapping verwalten.
4. Fügen Sie den ARN der Rolle hinzu, die über Berechtigungen zum Weitergeben von `TheSnapshotRole` verfügt. Platzieren Sie die Rolle ARNs unter Backend-Rollen.

   ```
   arn:aws:iam::123456789123:role/role-name
   ```

5. Wählen Sie Zuordnen und bestätigen Sie, dass der Benutzer oder die Rolle unter Zugeordnete Benutzer angezeigt wird.

Schritt 2: Registrieren eines Repositorys

Auf der folgenden Registerkarte „Snapshots“ wird gezeigt, wie ein Snapshot-Verzeichnis registriert wird. Spezifische Optionen für die Verschlüsselung eines manuellen Snapshots und die Registrierung eines Snapshots nach der Migration zu einer neuen Domain finden Sie auf den entsprechenden Registerkarten.

Snapshots

Um ein Snapshot-Repository zu registrieren, senden Sie eine PUT-Anfrage an den Endpunkt der OpenSearch Service-Domäne. Sie können curl, den Python-Beispielclient, Postman oder eine andere Methode verwenden, um eine signierte Anfrage zur Registrierung des Snapshot-Repositorys zu senden. Beachten Sie, dass Sie in der OpenSearch Dashboards-Konsole keine PUT-Anfrage verwenden können, um das Repository zu registrieren.

Die Anfrage hat das folgende Format:

```
PUT domain-endpoint/_snapshot/my-snapshot-repo-name
{
  "type": "s3",
  "settings": {
    "bucket": "amzn-s3-demo-bucket",
    "base_path": "my/snapshot/directory",
    "region": "region",
    "role_arn": "arn:aws:iam::123456789012:role/TheSnapshotRole"
  }
}
```

> **Note**
>
> Repository-Namen dürfen nicht mit „cs-“ beginnen. Darüber hinaus sollten Sie nicht von mehreren Domains in dasselbe Repository schreiben. Nur eine Domain sollte Schreibzugriff auf das Repository haben.

Wenn sich Ihre Domain in einer Virtual Private Cloud (VPC) befindet, muss Ihr Computer mit der VPC verbunden sein, damit die Anforderung zur erfolgreichen Registrierung des Snapshot-Repositorys erfolgt. Der Zugriff auf eine VPC unterscheidet sich je nach Netzwerkkonfiguration, wahrscheinlich muss eine Verbindung mit einem VPN oder Unternehmensnetzwerk hergestellt werden. Um zu überprüfen, ob Sie die OpenSearch Service-Domain erreichen können, navigieren Sie `https://your-vpc-domain.region.es.amazonaws.com` in einem Webbrowser zu und stellen Sie sicher, dass Sie die Standard-JSON-Antwort erhalten.

Wenn sich Ihr Amazon S3 S3-Bucket in einer anderen AWS-Region als Ihrer OpenSearch Domain befindet, fügen Sie den Parameter `"endpoint": "s3.amazonaws.com"` zur Anfrage hinzu.

Encrypted snapshots

Sie können derzeit keine AWS Key Management Service (KMS-) Schlüssel zum Verschlüsseln manueller Snapshots verwenden, aber Sie können sie mit serverseitiger Verschlüsselung (SSE) schützen.

Um SSE mit S3-verwalteten Schlüsseln für den Bucket zu aktivieren, den Sie als Snapshot-Repository verwenden, fügen Sie dem `"settings"` Block der `"server_side_encryption": true` PUT-Anforderung etwas hinzu. Weitere Informationen finden Sie unter Verwenden serverseitiger Verschlüsselung mit von Amazon S3 verwalteten Schlüsseln (SSE-S3) im Benutzerhandbuch zu Amazon Simple Storage Service.

Alternativ können Sie AWS KMS Schlüssel für die serverseitige Verschlüsselung für den S3-Bucket verwenden, den Sie als Snapshot-Repository verwenden. Wenn Sie diesen Ansatz verwenden, stellen Sie sicher, dass Sie dem AWS KMS Schlüssel, der zur Verschlüsselung des S3-Buckets verwendet wird, die `TheSnapshotRole` Erlaubnis erteilen. Weitere Informationen finden Sie unter Schlüsselrichtlinien in AWS KMS.

Domain migration

Das Registrieren eines Snapshot-Repositorys ist ein einmaliger Vorgang. Um jedoch von einer Domain zu einer anderen zu migrieren, müssen Sie dasselbe Snapshot-Repository auf der alten und der neuen Domain registrieren. Der Repository-Name ist beliebig.

Berücksichtigen Sie die folgenden Richtlinien, wenn Sie zu einer neuen Domain migrieren oder dasselbe Repository bei mehreren Domains registrieren:

- Fügen Sie beim Registrieren des Repositorys in der neuen Domain `"readonly": true` zum `"settings"`-Block der PUT-Anforderung hinzu. Diese Einstellung verhindert, dass Sie versehentlich Daten aus der alten Domain überschreiben. Nur eine Domain sollte Schreibzugriff auf das Repository haben.
- Wenn Sie Daten zu einer Domain in einer anderen AWS-Region migrieren (z. B. von einer alten Domain und einem Bucket in us-east-2 zu einer neuen Domain in us-west-2), `"region": "region"` ersetzen Sie sie `"endpoint": "s3.amazonaws.com"` in der PUT-Anweisung durch und versuchen Sie die Anfrage erneut.

Verwenden des Python-Beispielclients

Der Python-Client ist einfacher zu automatisieren als eine einfache HTTP-Anfrage und bietet eine bessere Wiederverwendbarkeit. Wenn Sie diese Methode zum Registrieren eines Snapshot-

Repositorys verwenden, speichern Sie den folgenden Python-Beispielcode als Python-Datei, z. B. `register-repo.py`. Der Client benötigt die Pakete AWS SDK für Python (Boto3), Anforderungen und requests-aws4auth. Der Client enthält auskommentierte Beispiele für andere Snapshot-Vorgänge.

Aktualisieren Sie die folgenden Variablen im Beispiel-Code: `host`, `region`, `path`, und`payload`.

```
import boto3
import requests
from requests_aws4auth import AWS4Auth

host = '' # domain endpoint
region = '' # e.g. us-west-1
service = 'es'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
 session_token=credentials.token)

# Register repository

path = '/_snapshot/my-snapshot-repo-name' # the OpenSearch API endpoint
url = host + path

payload = {
  "type": "s3",
  "settings": {
    "bucket": "amzn-s3-demo-bucket",
    "base_path": "my/snapshot/directory",
    "region": "us-west-1",
    "role_arn": "arn:aws:iam::123456789012:role/snapshot-role"
  }
}

headers = {"Content-Type": "application/json"}

r = requests.put(url, auth=awsauth, json=payload, headers=headers)

print(r.status_code)
print(r.text)

# # Take snapshot
#
# path = '/_snapshot/my-snapshot-repo-name/my-snapshot'
```

```
# url = host + path
#
# r = requests.put(url, auth=awsauth)
#
# print(r.text)
#
# # Delete index
#
# path = 'my-index'
# url = host + path
#
# r = requests.delete(url, auth=awsauth)
#
# print(r.text)
#
# # Restore snapshot (all indexes except Dashboards and fine-grained access control)
#
# path = '/_snapshot/my-snapshot-repo-name/my-snapshot/_restore'
# url = host + path
#
# payload = {
#   "indices": "-.kibana*,-.opendistro_security,-.opendistro-*",
#   "include_global_state": False
# }
#
# headers = {"Content-Type": "application/json"}
#
# r = requests.post(url, auth=awsauth, json=payload, headers=headers)
#
# print(r.text)
#
# # Restore snapshot (one index)
#
# path = '/_snapshot/my-snapshot-repo-name/my-snapshot/_restore'
# url = host + path
#
# payload = {"indices": "my-index"}
#
# headers = {"Content-Type": "application/json"}
#
# r = requests.post(url, auth=awsauth, json=payload, headers=headers)
#
# print(r.text)
```

Manuelle Snapshots erstellen

Snapshots erfolgen nicht augenblicklich. Sie sind zeitaufwändig und bieten keine perfekte point-in-time Ansicht des Clusters. Während ein Snapshot erstellt wird, können Sie weiterhin Dokumente indizieren und andere Anfragen an den Cluster stellen, aber neue Dokumente und Aktualisierungen bestehender Dokumente werden nicht im Allgemeinen in den Snapshot aufgenommen. Der Snapshot enthält primäre Shards, wie sie bei der OpenSearch Initiierung des Snapshots vorhanden waren. Je nach der Größe Ihres Snapshot-Thread-Pools umfassen die Snapshots ggf. verschiedene Shards zu geringfügig unterschiedlichen Zeitpunkten. Bewährte Methoden für Snapshots finden Sie unterthe section called “Verbessern Sie die Snapshot-”.

Snapshot-Speicher und -Leistung

OpenSearch Snapshots sind inkrementell, d. h. sie speichern nur Daten, die sich seit dem letzten erfolgreichen Snapshot geändert haben. Diese inkrementelle Beschaffenheit bedeutet, dass der Unterschied in der Festplattennutzung zwischen häufigen und seltenen Snapshots oft minimal ist. Mit anderen Worten, die Erstellung stündlicher Snapshots für eine Woche (mit insgesamt 168 Snapshots) verbraucht möglicherweise nicht viel mehr Speicherplatz als ein einzelner Snapshot am Ende der Woche. Und je häufiger Sie Snapshots erstellen, desto weniger Zeit nimmt ihre Fertigstellung in Anspruch. Tägliche Snapshots können beispielsweise 20–30 Minuten dauern, während stündliche Snapshots innerhalb weniger Minuten abgeschlossen sein können. Manche OpenSearch Benutzer machen Schnappschüsse bis zu jeder halben Stunde.

Aufnehmen eines Snapshots

Beim Erstellen eines Snapshots geben Sie die folgenden Informationen an:

- Den Namen Ihres Snapshot-Repositorys
- Einen Namen für den Snapshot

In den Beispielen dieses Kapitels wird aufgrund der Einfachheit und Übersichtlichkeit der gängige HTTP-Client curl verwendet. Informationen zum Übergeben eines Benutzernamens und eines Passworts für Ihre Curl-Anfrage finden Sie im Tutorial Erste Schritte.

Wenn Ihre Zugriffsrichtlinien Benutzer oder Rollen angeben, müssen Sie Ihre Snapshot-Anfragen signieren. Für curl können Sie die `--aws-sigv4`Option mit Version 7.75.0 oder höher verwenden. Sie können auch die auskommentierten Beispiele im Python-Beispielclient verwenden, um signierte HTTP-Anfragen an dieselben Endpunkte zu stellen, die die curl-Befehle verwenden.

Führen Sie die folgenden Schritte aus, um einen manuellen Snapshot zu erstellen:

1. Sie können keinen Snapshot erstellen, wenn gerade ein Snapshot ausgeführt wird. Um dies zu überprüfen, führen Sie den folgenden Befehl aus:

   ```
   curl -XGET 'domain-endpoint/_snapshot/_status'
   ```

2. Führen Sie den folgenden Befehl aus, um einen manuellen Snapshot zu erstellen:

   ```
   curl -XPUT 'domain-endpoint/_snapshot/repository-name/snapshot-name'
   ```

   Um bestimmte Indizes ein- oder auszuschließen und andere Einstellungen festzulegen, fügen Sie einen Anforderungstext hinzu. Informationen zur Anforderungsstruktur finden Sie in der Dokumentation unter Schnappschüsse erstellen. OpenSearch

> **Note**
>
> Die für die Erstellung eines Snapshots benötigte Zeit nimmt mit der Größe der OpenSearch Dienstdomäne zu. Bei lange laufenden Snapshot-Operationen tritt gelegentlich der folgende Fehler auf: `504 GATEWAY_TIMEOUT`. In der Regel können Sie diese Fehler ignorieren und warten, bis der Vorgang erfolgreich abgeschlossen werden kann. Führen Sie den folgenden Befehl aus, um den Status aller Snapshots in Ihrer Domain zu überprüfen:
>
> ```
> curl -XGET 'domain-endpoint/_snapshot/repository-name/_all?pretty'
> ```

Wiederherstellen von Snapshots

Bevor Sie einen Snapshot wiederherstellen, stellen Sie sicher, dass die Zieldomäne kein Multi-AZ mit Standby verwendet. Wenn Standby aktiviert ist, schlägt der Wiederherstellungsvorgang fehl.

> **Warning**
>
> Wenn Sie Indexaliase verwenden, sollten Sie entweder die Schreibanforderungen an einen Alias beenden oder den Alias auf einen anderen Index umstellen, bevor Sie seinen Index löschen. Hierdurch lässt sich folgendes Szenario vermeiden:
>
> 1. Sie löschen einen Index und dadurch auch dessen Alias.

2. Eine fehlerhafte Schreibanforderung an einen jetzt gelöschten Alias erstellt einen neuen Index mit demselben Namen wie der Alias.
3. Sie können den Alias aufgrund eines Namenskonflikts mit dem neuen Index nicht mehr verwenden. Wenn Sie den Alias zu einem anderen Index wechseln, geben Sie bei der Wiederherstellung von einem Snapshot `"include_aliases": false` an.

So stellen Sie einen Snapshot wieder her

1. Ermitteln Sie den Snapshot, den Sie wiederherstellen möchten. Stellen Sie sicher, dass alle Einstellungen für diesen Index, z. B. benutzerdefinierte Analyzer-Pakete oder Einstellungen für Zuweisungsanforderungen, mit der Domäne kompatibel sind. Verwenden Sie den folgenden Befehl, um alle Snapshot-Repositorys anzuzeigen:

   ```
   curl -XGET 'domain-endpoint/_snapshot?pretty'
   ```

   Nachdem Sie das Repository ermittelt haben, können Sie mit dem folgenden Befehl alle gespeicherten Snapshots anzeigen:

   ```
   curl -XGET 'domain-endpoint/_snapshot/repository-name/_all?pretty'
   ```

   > **Note**
   >
   > Die meisten automatischen Snapshots werden im `cs-automated`-Repository gespeichert. Wenn Ihre Domain Daten im Ruhezustand verschlüsselt, werden sie im `cs-automated-enc` Repository abgelegt. Wenn das gewünschte Repository für manuelle Snapshots nicht angezeigt wird, registrieren Sie es in der Domain.

2. (Optional) Löschen Sie einen oder mehrere Indizes in der OpenSearch Service-Domäne oder benennen Sie ihn um, wenn Namenskonflikte zwischen den Indizes im Cluster und den Indizes im Snapshot auftreten. Sie können keinen Snapshot Ihrer Indizes in einem OpenSearch Cluster wiederherstellen, der bereits Indizes mit denselben Namen enthält.

   Sie haben die folgenden Optionen, wenn Sie Konflikte bei der Indexbenennung haben:

   - Löschen Sie die Indizes in der vorhandenen OpenSearch Service-Domain und stellen Sie dann den Snapshot wieder her.

- Benennen Sie die Indizes um, wenn Sie sie aus dem Snapshot wiederherstellen, und indizieren Sie sie später neu. Informationen zum Umbenennen von Indizes finden Sie in dieser Beispielanforderung in der OpenSearch Dokumentation.
- Stellen Sie den Snapshot in einer anderen OpenSearch Dienstdomäne wieder her (nur mit manuellen Snapshots möglich).

Der folgende Befehl löscht alle vorhandenen Indizes in einer Domain:

```
curl -XDELETE 'domain-endpoint/_all'
```

Wenn Sie jedoch nicht alle Indizes wiederherstellen möchten, können Sie einfach einen löschen:

```
curl -XDELETE 'domain-endpoint/index-name'
```

3. Um einen Snapshot wiederherzustellen, führen Sie den folgenden Befehl aus:

```
curl -XPOST 'domain-endpoint/_snapshot/repository-name/snapshot-name/_restore'
```

Aufgrund spezieller Berechtigungen für die OpenSearch Dashboards und detaillierter Zugriffskontrollindizes schlagen Versuche, alle Indizes wiederherzustellen, möglicherweise fehl, insbesondere wenn Sie versuchen, die Wiederherstellung anhand eines automatisierten Snapshots durchzuführen. Im folgenden Beispiel wird nur der Index `my-index` aus `2020-snapshot` im Snapshot-Repository `cs-automated` wiederhergestellt:

```
curl -XPOST 'domain-endpoint/_snapshot/cs-automated/2020-snapshot/_restore' \
-d '{"indices": "my-index"}' \
-H 'Content-Type: application/json'
```

Alternativ können Sie alle Indizes außer den Dashboards-Indizes und den Indizes der differenzierten Zugriffskontrolle wiederherstellen:

```
curl -XPOST 'domain-endpoint/_snapshot/cs-automated/2020-snapshot/_restore' \
-d '{"indices": "-.kibana*,-.opendistro*"}' \
-H 'Content-Type: application/json'
```

Mithilfe der Parameter und können Sie einen Snapshot wiederherstellen, ohne die zugehörigen Daten zu löschen. `rename_pattern` `rename_replacement` Weitere Informationen zu

diesen Parametern finden Sie in den Anforderungsfeldern der Restore Snapshot API und in der OpenSearch Dokumentation als Beispielanforderung.

> **Note**
>
> Wenn nicht alle primären Shards für die entsprechenden Indizes zur Verfügung stehen, könnte ein Snapshot den `state` von `PARTIAL` aufweisen. Dieser Wert gibt an, dass Daten aus mindestens einem Shard nicht erfolgreich gespeichert wurden. Sie können aus einem Teil-Snapshot wiederherstellen, aber Sie müssen möglicherweise fehlende Indizes aus älteren Snapshots wiederherstellen.

Löschen von manuellen Snapshots

Führen Sie den folgenden Befehl aus, um einen manuellen Snapshot zu löschen:

```
DELETE _snapshot/repository-name/snapshot-name
```

Automatisieren von Snapshots mit Snapshot Management

Sie können in OpenSearch Dashboards eine Snapshot Management (SM) -Richtlinie einrichten, um das regelmäßige Erstellen und Löschen von Snapshots zu automatisieren. SM kann Snapshots von einer Gruppe von Indizes erstellen, wohingegen Index State Management nur einen Snapshot pro Index erstellen kann. Um SM in OpenSearch Service verwenden zu können, müssen Sie Ihr eigenes Amazon S3 S3-Repository registrieren. Anweisungen zur Registrierung Ihres Repositorys finden Sie unter Manuelles Snapshot-Repository registrieren.

Vor SM bot OpenSearch Service eine kostenlose, automatisierte Snapshot-Funktion an, die immer noch standardmäßig aktiviert ist. Diese Funktion sendet Snapshots an das vom Service verwaltete Repository`cs-*`. Um die Funktion zu deaktivieren, wenden Sie sich an. Support

Weitere Informationen zur SM-Funktion finden Sie in der OpenSearch Dokumentation unter Snapshot-Verwaltung.

SM unterstützt derzeit keine Snapshot-Erstellung für mehrere Indextypen. Wenn Sie beispielsweise versuchen, einen Snapshot für mehrere Indizes zu erstellen, wobei * sich einige Indizes in der Warm-Tier befinden, schlägt die Snapshot-Erstellung fehl. Wenn Ihr Snapshot mehrere Indextypen enthalten soll, verwenden Sie die ISM-Snapshot-Aktion, bis SM diese Option unterstützt.

Konfigurieren von Berechtigungen

Wenn Sie von einer früheren Version der OpenSearch Service-Domain auf 2.5 aktualisieren, sind die Sicherheitsberechtigungen für die Snapshot-Verwaltung möglicherweise nicht für die Domain definiert. Benutzer ohne Administratorrechte müssen dieser Rolle zugeordnet werden, um die Snapshot-Verwaltung in Domänen mit detaillierter Zugriffskontrolle verwenden zu können. Gehen Sie wie folgt vor, um die Snapshot-Verwaltungsrolle manuell zu erstellen:

1. Gehen Sie in OpenSearch Dashboards zu Sicherheit und wählen Sie Berechtigungen aus.
2. Wählen Sie Aktionsgruppe erstellen und konfigurieren Sie die folgenden Gruppen:

Group name (Gruppenname)	Berechtigungen
`snapshot_management_full_access`	• `cluster:admin/opensearch/snapshot_management/*` • `cluster:admin/opensearch/notifications/feature/publish` • `cluster:admin/repository/*` • `cluster:admin/snapshot/*`
`snapshot_management_read_access`	• `cluster:admin/opensearch/snapshot_management/policy/get` • `cluster:admin/opensearch/snapshot_management/policy/search` • `cluster:admin/opensearch/snapshot_management/policy/explain` • `cluster:admin/repository/get` • `cluster:admin/snapshot/get`

3. Wählen Sie Rollen und Rolle erstellen.
4. Nennen Sie die Rolle snapshot_management_role.
5. Wählen Sie für Clusterberechtigungen oder aus. `snapshot_management_full_access` `snapshot_management_read_access`
6. Wählen Sie Erstellen aus.

7. Nachdem Sie die Rolle erstellt haben, ordnen Sie sie einer beliebigen Benutzer- oder Backend-Rolle zu, die Snapshots verwaltet.

Überlegungen

Beachten Sie bei der Konfiguration der Snapshot-Verwaltung Folgendes:

- Pro Repository ist eine Richtlinie zulässig.
- Für eine Richtlinie sind bis zu 400 Snapshots zulässig.
- Diese Funktion kann nicht ausgeführt werden, wenn Ihre Domain den Status Rot hat, unter hohem JVM-Druck steht (85% oder mehr) oder wenn die Snapshot-Funktion nicht mehr funktioniert. Wenn die allgemeine Indexierungs- und Suchleistung Ihres Clusters beeinträchtigt wird, kann dies auch für SM gelten.
- Ein Snapshot-Vorgang beginnt erst, nachdem der vorherige Vorgang abgeschlossen ist, sodass keine gleichzeitigen Snapshot-Vorgänge durch eine Richtlinie aktiviert werden.
- Mehrere Richtlinien mit demselben Zeitplan können zu einem Anstieg der Ressourcen führen. Wenn sich die Snapshot-Indizes der Richtlinien überschneiden, können die Snapshot-Operationen auf Festplattenebene nur sequentiell ausgeführt werden, was zu einem kaskadierten Leistungsproblem führen kann. Wenn sich die Richtlinien ein Repository teilen, kommt es zu einer Zunahme von Schreibvorgängen in dieses Repository.
- Wir empfehlen Ihnen, die Automatisierung von Snapshot-Vorgängen nicht öfter als einmal pro Stunde einzuplanen, es sei denn, Sie haben einen speziellen Anwendungsfall.

Automatisieren von Snapshots mit Index-Statusmanagement

Sie können den Snapshot-Vorgang (Index State Management, ISM) verwenden, um automatisch Snapshots von Indizes auszulösen, die auf Änderungen des Alters, der Größe oder der Anzahl der Dokumente basieren. ISM eignet sich am besten, wenn Sie einen Snapshot pro Index benötigen. Informationen zum Erstellen eines Snapshots einer Gruppe von Indizes finden Sie unterAutomatisieren von Snapshots mit Snapshot Management.

Um SM in OpenSearch Service verwenden zu können, müssen Sie Ihr eigenes Amazon S3 S3-Repository registrieren. Ein Beispiel für eine Richtlinie, die den Vorgang `snapshot` verwendet, finden Sie unter Beispielrichtlinien.

Verwenden von Curator für Snapshots

Wenn ISM für die Index- und Snapshot-Verwaltung nicht funktioniert, können Sie stattdessen Curator verwenden. Es bietet eine erweiterte Filterfunktionalität zur Vereinfachung der Verwaltungsaufgaben auf komplexen Clustern. Verwenden Sie pip zum Installieren von Curator:

```
pip install elasticsearch-curator
```

Sie können Curator als Befehlszeilenschnittstelle (Command Line Interface, CLI) oder Python-API verwenden. Wenn Sie die Python-API verwenden, müssen Sie Version 7.13.4 oder früher des Legacy-elasticsearch-py-Clients verwenden. Sie unterstützt den opensearch-py-Client nicht.

Wenn Sie die CLI verwenden, exportieren Sie Ihre Anmeldeinformationen über die Befehlszeile und konfigurieren Sie `curator.yml` wie folgt:

```
client:
  hosts: search-my-domain.us-west-1.es.amazonaws.com
  port: 443
  use_ssl: True
  aws_region: us-west-1
  aws_sign_request: True
  ssl_no_validate: False
  timeout: 60

logging:
  loglevel: INFO
```

Aktualisierung von OpenSearch Amaz-Service-Domänen

> **Note**
>
> OpenSearch und Elasticsearch-Versions-Upgrades unterscheiden sich von Service-Software-Updates. Weitere Informationen zum Aktualisieren der Service-Software für Ihre OpenSearch Service-Domain finden Sie unterthe section called “Service-Software-Updates”.

Amazon OpenSearch Service bietet direkte Upgrades für Domänen mit OpenSearch 1.0 oder neuer. Wenn Sie Daten mit Diensten wie Amazon Data Firehose oder Amazon CloudWatch Logs an

OpenSearch Service streamen, überprüfen Sie OpenSearch vor der Migration, ob diese Dienste die neueren Versionen von unterstützen.

Unterstützte Upgrade-Pfade

Derzeit unterstützt OpenSearch Service die folgenden Upgrade-Pfade:

Von Version	Auf Version
OpenSearch 1.3 oder 2. x	OpenSearch 2. x OpenSearch 2.17 aktiviert standardmäßig die gleichzeitige Segmentsuche im auto Modus, wenn die Domain die folgenden Bedingungen erfüllt: • Es wurden keine vorherigen Einstellungen für die gleichzeitige Suche explizit festgelegt. • Alle Dateninstanzen (heiß und warm) haben den Instanztyp 2.xl oder höher. • Die durchschnittliche p90-CPU-Auslastung auf Dateninstanzen (heiß und warm) für mehr als eine Woche liegt unter 45%. Weitere Informationen zu den Einstellungen für die gleichzeitige Segmentsuche finden Sie hier unter Gleichzeitige Segmentsuche. Version 2.3 enthält die folgenden grundlegenden Änderungen: • Der `type` Parameter wurde in Version 2.0 von allen OpenSearch API-Endpunkten entfernt. Weitere Informationen finden Sie unter grundlegende Änderungen. • Wenn Ihre Domain Indizes (Hot oder Cold) enthält UltraWarm, die ursprünglich in Elasticsearch 6.8 erstellt wurden, sind diese Indizes nicht mit 2.3 kompatibel. OpenSearch Bevor Sie auf Version 2.3 aktualisieren, müssen Sie die nicht kompatiblen Indizes neu indizieren. Bei nicht kompatiblen UltraWarm oder kalten Indizes migrieren Sie diese in den Hot-Speicher, reindizieren Sie die Daten und migrieren Sie sie dann zurück in den Warm- oder Cold-Speicher. Alternativ können Sie die Indizes auch löschen, wenn Sie sie nicht mehr benötigen.

Von Version	Auf Version
	Wenn Sie Ihre Domain versehentlich auf Version 2.3 aktualisieren, ohne diese Schritte vorher auszuführen, können Sie die nicht kompatiblen Indizes nicht aus ihrer aktuellen Speicherebene migrieren. Ihre einzige Möglichkeit besteht darin, sie zu löschen.
OpenSearch 1. x	OpenSearch 1. x
Elasticsearch 7.x	Elasticsearch 7. x oder OpenSearch 1. x **Important** OpenSearch 1. x führt zahlreiche bahnbrechende Änderungen ein. Details hierzu finden Sie unter Umbenennung von Amazon OpenSearch Service.
Elasticsearch 6.8	Elasticsearch 7. x oder OpenSearch 1. x **Important** Elasticsearch 7.0 und OpenSearch 1.0 umfassen zahlreiche Änderungen. Bevor Sie ein direktes Upgrade starten, empfehlen wir, einen manuellen Snapshot der Version 6 zu erstellen. x-Domain, Wiederherstellung auf einem Test 7. x oder OpenSearch 1. x-Domäne und Verwendung dieser Testdomäne, um potenzielle Upgrade-Probleme zu identifizieren. Informationen Umbenennung von Amazon OpenSearch Service zu den bahnbrechenden Änderungen in OpenSearch 1.0 Wie in Elasticsearch 6.x können Indizes nur einen Mapping-Typ enthalten , aber dieser Typ muss jetzt den Namen `_doc` haben. Daher benötigen bestimmte APIs keinen Mapping-Typ mehr im Anforderungstext (z. B. die `_bulk` API). Elasticsearch 7 wurde für neue Indizes selbst gehostet. x und 1. OpenSearch x haben eine Standardanzahl von Shards von eins. OpenSearch Service-Domains auf Elasticsearch 7. x und neuer behalten den vorherigen Standardwert von fünf bei.

Von Version	Auf Version
Elasticsearch 6.x	Elasticsearch 6.x
Elasticsearch 5.6	Elasticsearch 6.x **Important** Indizes, die in Version 6.x erstellt wurden, unterstützen keine mehrfache n Mapping-Typen mehr. Indizes, die in Version 5.x erstellt wurden, unterstützen noch mehrfache Mapping-Typen, wenn sie in einem 6.x Cluster wiederhergestellt werden. Sehen Sie nach, ob Ihr Code nur einen einzigen Mapping-Typ pro Index erstellt. Um die Ausfallzeiten während des Upgrades von Elasticsearch 5.6 auf 6 zu minimieren. x, OpenSearch Service indexiert den `.kibana` Index neu, löscht ihn `.kibana-6` `.kibana`, erstellt einen Alias mit dem Namen `.kibana` und ordnet den neuen Index dem neuen Alias zu.
Elasticsearch 5.x	Elasticsearch 5.x

Der Upgrade-Prozess besteht aus drei Schritten:

1. Pre-Upgrade-Prüfungen — OpenSearch Der Service führt Prüfungen für Probleme durch, die ein Upgrade blockieren können, und fährt nicht mit dem nächsten Schritt fort, es sei denn, diese Prüfungen sind erfolgreich.
2. Snapshot — Der OpenSearch Service erstellt einen Snapshot des OpenSearch Elasticsearch-Clusters und fährt nicht mit dem nächsten Schritt fort, es sei denn, der Snapshot ist erfolgreich. Wenn das Upgrade fehlschlägt, verwendet OpenSearch Service diesen Snapshot zum Wiederherstellen des Clusters in seinen ursprünglichen Zustand. Weitere Informationen finden Sie unter the section called “Nach einem Upgrade ist kein Downgrade möglich”.
3. Upgrade — Der OpenSearch Service startet das Upgrade. Dies kann 15 Minuten bis mehrere Stunden dauern. OpenSearch Dashboards sind möglicherweise während eines Teils oder dem gesamten Upgrade nicht verfügbar.

Aktualisierung einer Domain (Konsole)

Der Upgrade-Vorgang kann nicht rückgängig gemacht und weder angehalten noch abgebrochen werden. Während eines Upgrades können Sie keine Änderungen an der Konfiguration der Domain vornehmen. Bevor Sie das Upgrade starten, müssen Sie überprüfen, ob Sie fortfahren möchten. Sie können diese Schritte auch zum Ausführen der Pre-Upgrade-Prüfung verwenden ohne tatsächlich das Upgrade zu starten.

Wenn der Cluster über dedizierte Master-Knoten verfügt, werden OpenSearch Upgrades ohne Ausfallzeiten abgeschlossen. Andernfalls reagiert der Cluster nach dem Upgrade möglicherweise mehrere Sekunden lang nicht mehr, während er einen Master-Knoten wählt.

So aktualisieren Sie eine Domäne auf eine neuere Version von OpenSearch Elasticsearch

1. Erstellen Sie einen manuellen Snapshot Ihrer Domain. Dieser Snapshot dient als Backup, das Sie auf einer neuen Domain wiederherstellen können, wenn Sie die vorherige OpenSearch Version verwenden möchten.
2. Gehen Sie zu https://aws.amazon.comund wählen Sie In der Konsole anmelden aus.
3. Wählen Sie unter Analytics Amazon OpenSearch Service aus.
4. Wählen Sie im Navigationsbereich unter My domains (Meine Domains) die Domain aus, die Sie upgraden möchten.
5. Wählen Sie Aktionen und Aktualisieren aus.
6. Wählen Sie die Version aus, auf die aktualisiert werden soll. Wenn Sie auf eine OpenSearch Version upgraden, wird die Option Kompatibilitätsmodus aktivieren angezeigt. Wenn Sie diese Einstellung aktivieren, OpenSearch meldet seine Version als 7.10, damit Elasticsearch OSS-Clients und Plug-Ins wie Logstash weiterhin mit Amazon Service arbeiten können. OpenSearch Sie können diese Einstellung später deaktivieren.
7. Wählen Sie Upgrade.
8. Überprüfen Sie den Status im Domain-Dashboard, um den Status des Upgrades zu überwachen.

Aktualisierung einer Domain (CLI)

Sie können die folgenden Operationen verwenden, um die richtige Elasticsearch-Version für Ihre Domäne zu identifizieren, ein direktes Upgrade zu starten, die Pre-Upgrade-Prüfung durchzuführen und den Fortschritt anzuzeigen: OpenSearch

- `get-compatible-versions` (`GetCompatibleVersions`)
- `upgrade-domain` (`UpgradeDomain`)
- `get-upgrade-status` (`GetUpgradeStatus`)
- `get-upgrade-history` (`GetUpgradeHistory`)

Weitere Informationen finden Sie in der AWS CLI-Befehlsreferenz und in der Amazon OpenSearch Service API-Referenz.

Aktualisierung einer Domain (SDK)

In diesem Beispiel wird der OpenSearchService-Low-Level-Python-Client aus dem verwendet, AWS SDK for Python (Boto) um zu überprüfen, ob eine Domäne für ein Upgrade auf eine bestimmte Version berechtigt ist, sie zu aktualisieren und den Upgrade-Status laufend zu überprüfen.

```
import boto3
from botocore.config import Config
import time

# Build the client using the default credential configuration.
# You can use the CLI and run 'aws configure' to set access key, secret
# key, and default Region.

DOMAIN_NAME = ''  # The name of the domain to upgrade
TARGET_VERSION = ''  # The version you want to upgrade the domain to. For example,
 OpenSearch_1.1

my_config = Config(
    # Optionally lets you specify a Region other than your default.
    region_name='us-east-1'
)
client = boto3.client('opensearch', config=my_config)


def check_versions():
    """Determine whether domain is eligible for upgrade"""
    response = client.get_compatible_versions(
        DomainName=DOMAIN_NAME
    )
    compatible_versions = response['CompatibleVersions']
    for i in range(len(compatible_versions)):
        if TARGET_VERSION in compatible_versions[i]["TargetVersions"]:
```

```
            print('Domain is eligible for upgrade to ' + TARGET_VERSION)
            upgrade_domain()
            print(response)
        else:
            print('Domain not eligible for upgrade to ' + TARGET_VERSION)


def upgrade_domain():
    """Upgrades the domain"""
    response = client.upgrade_domain(
        DomainName=DOMAIN_NAME,
        TargetVersion=TARGET_VERSION
    )
    print('Upgrading domain to ' + TARGET_VERSION + '...' + response)
    time.sleep(5)
    wait_for_upgrade()


def wait_for_upgrade():
    """Get the status of the upgrade"""
    response = client.get_upgrade_status(
        DomainName=DOMAIN_NAME
    )
    if (response['UpgradeStep']) == 'UPGRADE' and (response['StepStatus']) ==
 'SUCCEEDED':
        print('Domain successfully upgraded to ' + TARGET_VERSION)
    elif (response['StepStatus']) == 'FAILED':
        print('Upgrade failed. Please try again.')
    elif (response['StepStatus']) == 'SUCCEEDED_WITH_ISSUES':
        print('Upgrade succeeded with issues')
    elif (response['StepStatus']) == 'IN_PROGRESS':
        time.sleep(30)
        wait_for_upgrade()


def main():
    check_versions()


if __name__ == "__main__":
    main()
```

Beheben von Validierungsfehlern

Wenn Sie ein OpenSearch Versionsupgrade für Elasticsearch durchführen, führt OpenSearch Service zunächst eine Reihe von Validierungsprüfungen durch, um sicherzustellen, dass Ihre Domain für ein Update in Frage kommt. Wenn eine dieser Prüfungen fehlschlägt, erhalten Sie eine Benachrichtigung mit den spezifischen Problemen, die Sie beheben müssen, bevor Sie Ihre Domain aktualisieren. Eine Liste potenzieller Probleme und Schritte zu deren Behebung finden Sie unter the section called “Beheben von Validierungsfehlern”.

Fehlerbehebung bei einem Upgrade

Direkte -Upgrades erfordern gesunde Domains. Ihre Domain ist womöglich nicht für ein Upgrade berechtigt oder kann aus einer Vielzahl von Gründen nicht upgegradet werden. Die folgende Tabelle zeigt die gängigsten Probleme.

Problem	Beschreibung
Optionales Plugin wird nicht unterstützt	Wenn Sie eine Domain mit optionalen Plug-ins aktualisieren, aktualisiert OpenSearch Service automatisch auch die Plug-ins. Daher muss die Zielversion für Ihre Domain auch diese optionalen Plugins unterstützen. Wenn auf der Domain ein optionales Plugin installiert ist, das für die Zielversion nicht verfügbar ist, schlägt die Upgrade-Anfrage fehl.
Zu viele Shards pro Knoten	OpenSearch, sowie 7. x -Versionen von Elasticsearch haben eine Standardeinstellung von nicht mehr als 1.000 Shards pro Knoten. Wenn ein Knoten in Ihrem aktuellen Cluster diese Einstellung überschreitet, lässt OpenSearch Service das Upgrade nicht zu. Informationen zu den Optionen für die Fehlerbehebung finden Sie unter the section called “Maximales Shard-Limit überschritten”.
Domain in Verarbeitung	Die Domain befindet sich in der Mitte einer Konfigurationsänderung. Überprüfen Sie die Upgrade-Berechtigung, nachdem die Operation abgeschlossen ist.
Roter Cluster-Status	Ein oder mehrere Indizes im Cluster sind rot. Fehlerbehandlungsschritte finden Sie unter the section called “Roter Cluster-Status”.
Hohe Fehlerrate	Der Cluster gibt beim Versuch, Anfragen zu verarbeiten, eine große Anzahl von 5xx-Fehlern zurück. Dieses Problem ist in der Regel das

Problem	Beschreibung
	Ergebnis zu vieler gleichzeitiger Lese- oder Schreibanforderungen. Erwägen Sie, den Datenverkehr zu dem Cluster zu reduzieren oder Ihre Domain zu skalieren.
Split brain	Split brain bedeutet, dass Ihr Cluster über mehr als einen Master-Kn oten verfügt und sich in zwei Cluster aufgeteilt hat, die sich nicht von selbst wieder hinzufügen. Sie können split brain vermeiden, indem Sie die empfohlene Anzahl der dedizierten Hauptknoten verwenden. Für Hilfe zur Wiederherstellung von split brain wenden Sie sich an Support.
Master-Knoten wurde nicht gefunden.	OpenSearch Der Service kann den Master-Knoten des Clusters nicht finden. Wenn Ihre Domain Multi-AZ verwendet, kann ein Ausfall einer Availability Zone dazu geführt haben, dass der Cluster das Quorum verliert und keinen neuen Hauptknoten wählen kann. Wenn sich das Problem nicht von selbst löst, wenden Sie sich bitte an Support.
Zu viele ausstehende Aufgaben	Der Master-Knoten ist stark ausgelastet und hat viele ausstehende Aufgaben. Erwägen Sie, den Datenverkehr zu dem Cluster zu reduzieren oder Ihre Domain zu skalieren.
Beeinträchtigtes Speicher-Volume	Das Datenträger-Volume eines oder mehrerer Knoten funktioniert nicht ordnungsgemäß. Dieses Problem tritt oft zusammen mit anderen Problemen, wie z. B. eine hohe Fehlerrate oder zu viele ausstehende Aufgaben, auf. Wenn es isoliert auftritt und sich nicht von selbst löst, wenden Sie sich bitte an Support.
Problem mit KMS-Schlüssel	Der KMS-Schlüssel für die Verschlüsselung der Domain ist entweder nicht zugänglich oder fehlt. Weitere Informationen finden Sie unter the section called “Überwachen von Domains, die Daten im Ruhezustand verschlüsseln”.

Problem	Beschreibung
Snapshot in Arbeit	Die Domain erstellt derzeit einen Snapshot. Überprüfen Sie die Upgrade-Berechtigung, nachdem der Snapshot abgeschlossen ist. Überprüfen Sie auch, ob Sie manuelle Snapshot-Repositorys auflisten, Snapshots innerhalb dieser Repositorys auflisten und manuelle Snapshots erstellen können. Wenn der OpenSearch Service nicht in der Lage ist, zu überprüfen, ob ein Snapshot generiert wird, können Upgrades fehlschlagen.
Snapshot-Timeout oder -Fehler	Der Pre-Upgrade-Snapshot hat zu lange gedauert oder ist fehlgeschlagen. Überprüfen Sie die Cluster-Gesundheit und versuchen Sie es erneut. Wenn das Problem weiterhin besteht, wenden Sie sich bitte an Support.
Inkompatible Indizes	Ein oder mehrere Indizes sind nicht kompatibel mit der Zielversion. Dieses Problem kann auftreten, wenn Sie die Indizes von einer älteren Version von OpenSearch Elasticsearch migriert haben. Indizieren Sie die Indizes neu und versuchen Sie es erneut.
Hohe Festplattennutzung	Die Festplattennutzung für den Cluster übersteigt 90 %. Löschen Sie Daten oder skalieren Sie die Domain und versuchen Sie es erneut.
Hohe JVM-Nutzung	Die JVM-Speicherbelastung übersteigt 75 %. Reduzieren Sie den Datenverkehr an den Cluster oder skalieren Sie die Domain und versuchen Sie es erneut.
OpenSearch Dashboards-Aliasproblem	`.dashboards` ist bereits als Alias konfiguriert und entspricht einem inkompatiblen Index, wahrscheinlich einem von einer früheren Version von OpenSearch Dashboards. Indizieren Sie neu und versuchen Sie es erneut.
Roter Dashboard-Status	OpenSearch Der Dashboard-Status ist rot. Verwenden Sie Dashboards, wenn das Upgrade abgeschlossen ist. Wenn der rote Status weiterhin besteht, beheben Sie den Fehler manuell und versuchen Sie es erneut.

Problem	Beschreibung
Cluster-übergreifende Kompatibilität	Sie können ein Upgrade nur dann durchführen, wenn die Cluster-ü bergreifende Kompatibilität zwischen der Quell- und Ziel-Domain nach dem Upgrade aufrechterhalten wird. Während des Upgrade-Vorgangs werden alle inkompatiblen Verbindungen identifiziert. Um fortzufahren, aktualisieren Sie entweder die Remote-Domain oder löschen Sie die inkompatiblen Verbindungen. Beachten Sie, dass Sie, wenn die Replikati on für die Domain aktiv ist, nicht fortsetzen können, nachdem Sie die Verbindung gelöscht haben.
Anderes OpenSearc h Service-Problem mit dem Service	Probleme mit dem OpenSearch Service selbst könnte dazu führen, dass Ihre Domain als nicht Upgrade-berechtigt angezeigt wird. Wenn keine der vorangehenden Bedingungen für Ihre Domain gelten und das Problem mehr als einen Tag bestehen bleibt, wenden Sie sich bitte an Support.

Verwenden eines Snapshots zum Migrieren von Daten

Direkte Upgrades sind die einfachere, schnellere und zuverlässigere Möglichkeit, um eine Domain auf eine neuere OpenSearch oder Elasticsearch-Version upzugraden. Snapshots sind eine gute Option, wenn Sie aus einer Version von Elasticsearch vor 5.1 migrieren oder einen völlig neuen Cluster migrieren möchten.

Die folgende Tabelle zeigt, wie Sie mithilfe von Snapshots die Daten in eine Domain migrieren, die eine andere OpenSearch Elasticsearch-Version verwendet. Informationen zum Erstellen und Wiederherstellen von Snapshots finden Sie unter the section called “Erstellen von Index-Snapshots”.

Von Version	Auf Version	Migrationsprozess
OpenSearch 1.3 oder 2. x	OpenSearch 2. x	1. Lesen Sie funktionsgefährdende Änderungen in OpenSearch 2.3 nach, um zu prüfen, ob Sie Ihre Indizes oder Anwendungen anpassen müssen. 2. Erstellen Sie einen manuellen Snapshot von 1.3 oder 2. X-Domäne.

Von Version	Auf Version	Migrationsprozess

		3. Erstellen Sie eine 2. x-Domain, die eine höhere Version als Ihre ursprüngliche Version 1.3 oder 2 ist. x-Domäne.
		4. Stellen Sie den Snapshot von der ursprünglichen Domain in der 2. x-Domäne. Während der Operation müssen Sie möglicherweise Ihren `.opensearch` Index unter einem neuen Namen wiederherstellen:
		`POST _snapshot/ <repository-name> /<snapshot-name>/_restore`
		`{`
		`  "indices": "*",`
		`  "ignore_unavailable": true,`
		`  "rename_pattern": ".opensearch",`
		`  "rename_replacement": ".backup-opensearch"`
		`}`
		Anschließend können Sie `.backup-opensearch` in der neuen Domain neu indizieren und als Alias für `.opensearch` verwenden. Beachten Sie, dass der `_restore` REST-Aufruf nicht einschließt`include_global_state`, da der Standardwert in false `_restore` ist. Infolgedessen enthält die Testdomäne keine Indexvorlagen und weist nicht den vollständigen Status aus dem Backup auf.
		5. Wenn Sie Ihre ursprüngliche Domain nicht mehr benötigen, löschen Sie sie. Andernfalls fallen weitere Kosten für die Domain an.

Von Version	Auf Version	Migrationsprozess

OpenSearch 1. x	OpenSearch 1. x	1. Erstellen Sie einen manuellen Snapshot der 1. x-Domäne.
		2. Erstellen Sie eine 1. x-Domain, die eine höhere Version als Ihre ursprüngliche 1 ist. x-Domäne.
		3. Stellen Sie den Snapshot von der ursprünglichen Domain in der neuen 1. x-Domäne. Während der Operation müssen Sie möglicherweise Ihren `.opensearch` Index unter einem neuen Namen wiederherstellen:
		`POST _snapshot/ <repository-name> /<snapshot-name>/_restore`
		`{`
		`"indices": "*",`
		`"ignore_unavailable": true,`
		`"rename_pattern": ".opensearch",`
		`"rename_replacement": ".backup-opensearch"`
		`}`
		Anschließend können Sie `.backup-opensearch` in der neuen Domain neu indizieren und als Alias für `.opensearch` verwenden. Beachten Sie, dass der `_restore` REST-Aufruf nicht einschließt`include_global_state` , da der Standardwert in false `_restore` ist. Infolgedessen enthält die Testdomäne keine Indexvorlagen und weist nicht den vollständigen Status aus dem Backup auf.
		4. Wenn Sie Ihre ursprüngliche Domain nicht mehr benötigen, löschen Sie sie. Andernfalls fallen weitere Kosten für die Domain an.

Von Version	Auf Version	Migrationsprozess

Elasticsearch 6.x oder 7.x	OpenSearch 1. x	1. Lesen Sie funktionsgefährdende Änderungen in OpenSearch 1.0 nach, um zu prüfen, ob Sie Ihre Indizes oder Anwendungen anpassen müssen.
		2. Erstellen Sie einen manuellen Snapshot der Elasticse arch 7.x or 6.x-Domain.
		3. Erstellen Sie eine OpenSearch 1. x-Domäne.
		4. Stellen Sie den Snapshot von der Elasticsearch-Doma in in der OpenSearch Domain wieder her. Während der Operation müssen Sie möglicherweise Ihren `.elasticsearch` Index unter einem neuen Namen wiederherstellen:
		`POST _snapshot/ <repository-name> /<snapshot-name>/_restore`
		`{`
		`"indices": "*",`
		`"ignore_unavailable": true,`
		`"rename_pattern": ".elasticsearch",`
		`"rename_replacement": ".backup-opensearc h"`
		`}`
		Anschließend können Sie `.backup-opensearch` in der neuen Domain neu indizieren und als Alias für `.elasticsearch` verwenden. Beachten Sie, dass der `_restore` REST-Aufruf nicht einschlie ßt`include_global_state` , da der Standardw ert in false `_restore` ist. Infolgedessen enthält die Testdomäne keine Indexvorlagen und weist nicht den vollständigen Status aus dem Backup auf.
		5. Wenn Sie Ihre ursprüngliche Domain nicht mehr benötigen, löschen Sie sie. Andernfalls fallen weitere Kosten für die Domain an.

Von Version	Auf Version	Migrationsprozess

Elasticsearch 6.x	Elasticsearch 7.x	1. Lesen Sie funktionsgefährdende Änderungen in 7.0 nach, um zu prüfen, ob Sie Ihre Indizes oder Anwendungen anpassen müssen.
		2. Erstellen Sie einen manuellen Snapshot der 6.x-Domain.
		3. Erstellen Sie eine 7.x-Domain.
		4. Stellen Sie den Snapshot von der ursprünglichen Domain in der 7.x-Domain wieder her. Während der Operation müssen Sie wahrscheinlich den `.opensearch` -Index unter einem neuen Namen wiederherstellen:
		`POST _snapshot/ <repository-name> /<snapshot-name>/_restore`
		`{`
		`  "indices": "*",`
		`  "ignore_unavailable": true,`
		`  "rename_pattern": ".elasticsearch",`
		`  "rename_replacement": ".backup-elasticsearch"`
		`}`
		Anschließend können Sie `.backup-elasticsearch` in der neuen Domain neu indizieren und als Alias für `.elasticsearch` verwenden. Beachten Sie, dass der `_restore` REST-Aufruf keine Daten enthält`include_global_state` , da die Standardeinstellung „false“ `_restore` ist. Infolgedessen enthält die Testdomäne keine Indexvorlagen und weist nicht den vollständigen Status aus dem Backup auf.
		5. Wenn Sie Ihre ursprüngliche Domain nicht mehr benötigen, löschen Sie sie. Andernfalls fallen weitere Kosten für die Domain an.

Von Version	Auf Version	Migrationsprozess
Elasticsearch 6.x	Elasticsearch 6.8	1. Erstellen Sie einen manuellen Snapshot der 6.x-Domain. 2. Erstellen Sie eine 6.8-Domain. 3. Stellen Sie den Snapshot von der ursprünglichen Domain in der 6.8-Domain wieder her. 4. Wenn Sie Ihre ursprüngliche Domain nicht mehr benötigen, löschen Sie sie. Andernfalls fallen weitere Kosten für die Domain an.
Elasticsearch 5.x	Elasticsearch 6.x	1. Lesen Sie funktionsgefährdende Änderungen in 6.0 nach, um zu prüfen, ob Sie Ihre Indizes oder Anwendungen anpassen müssen. 2. Erstellen Sie einen manuellen Snapshot der 5.x-Domain. 3. Erstellen Sie eine 6.x-Domain. 4. Stellen Sie den Snapshot von der ursprünglichen Domain in der 6.x-Domain wieder her. 5. Falls Sie Ihre 5.x-Domain nicht mehr benötigen, löschen Sie diese. Andernfalls fallen weitere Kosten für die Domain an.
Elasticsearch 5.x	Elasticsearch 5.6	1. Erstellen Sie einen manuellen Snapshot der 5.x-Domain. 2. Erstellen Sie eine 5.6-Domain. 3. Stellen Sie den Snapshot von der ursprünglichen Domain in der 5.6-Domain wieder her. 4. Wenn Sie Ihre ursprüngliche Domain nicht mehr benötigen, löschen Sie sie. Andernfalls fallen weitere Kosten für die Domain an.

Von Version	Auf Version	Migrationsprozess
Elasticsearch 2.3	Elasticsearch 6.x	Elasticsearch 2.3-Snapshots sind nicht kompatibel mit 6.x. Zur direkten Migration Ihrer Daten von 2.3 auf 6.x müssen Sie Ihre Indizes in der neuen Domain manuell wiederherstellen. Alternativ können Sie die Schritte 2.3 bis 5.x in dieser Tabelle befolgen, `_reindex`-Operationen in der neuen 5.x-Domain ausführen, um Ihre 2.3-Indizes in 5.x-Indizes zu konvertieren, und folgen dann den Schritten 5.x bis 6.x.
Elasticsearch 2.3	Elasticsearch 5.x	1. Lesen Sie funktionsgefährdende Änderungen in 5.0 nach, um zu prüfen, ob Sie Ihre Indizes oder Anwendungen anpassen müssen. 2. Erstellen Sie einen manuellen Snapshot der 2.3-Domain. 3. Erstellen Sie eine 5.x-Domain. 4. Stellen Sie den Snapshot der 2.3-Domain auf der 5.x-Domain wieder her. 5. Wenn Sie Ihre 2.3-Domain nicht mehr benötigen, löschen Sie sie. Andernfalls fallen weitere Kosten für die Domain an.

Von Version	Auf Version	Migrationsprozess
Elasticsearch 1.5	Elasticsearch 5.x	Elasticsearch 1.5-Snapshots sind nicht kompatibel mit 5.x. Zur Migration Ihrer Daten von 1.5 auf 5.x müssen Sie Ihre Indizes in der neuen Domain manuell wiederher stellen. **Important** 1.5-Snapshots sind kompatibel mit 2.3, aber OpenSearch Service 2.3-Domänen unterstützen den `_reindex` Vorgang nicht. Da Sie diese nicht neu indizieren können, können Indizes aus einer 1.5-Domain von 2.3-Snapshots dennoch nicht in 5.x-Domains wiederhergestellt werden.

Von Version	Auf Version	Migrationsprozess
Elasticsearch 1.5	Elasticsearch 2.3	1. Verwenden Sie das Migrations-Plugin, um herauszufinden, ob Sie direkt auf Version 2.3 upgraden können. Möglicherweise müssen Sie Ihre Daten vor der Migration ändern. a. Öffnen Sie in einem Webbrowser `http://domain-endpoint /_plugin/migration/` . b. Wählen Sie Run checks now (Prüfungen jetzt ausführen) aus. c. Überprüfen Sie die Ergebnisse und, falls erforderlich, befolgen Sie die Anweisungen, um Änderungen an Ihren Daten vorzunehmen. 2. Erstellen Sie einen manuellen Snapshot der 1.5-Domain. 3. Erstellen Sie eine 2.3-Domain. 4. Stellen Sie den Snapshot der 1.5-Domain auf der 2.3-Domain wieder her. 5. Wenn Sie Ihre 1.5-Domain nicht mehr benötigen, löschen Sie sie. Andernfalls fallen weitere Kosten für die Domain an.

Erstellen eines benutzerdefinierten Endpunkts für Amazon OpenSearch Service

Das Erstellen eines benutzerdefinierten Endpunkts für Ihre OpenSearch Amazon-Domäne erleichtert es Ihnen, auf Ihre OpenSearch und Ihre OpenSearch Dashboards URLs zu verweisen. Sie können das Branding Ihres Unternehmens einbinden oder einfach nur einen kürzeren easier-to-remember Endpunkt verwenden als den Standardendpunkt.

Wenn Sie jemals zu einer neuen Domäne wechseln müssen, aktualisieren Sie einfach Ihren DNS, um auf die neue URL zu verweisen und verwenden Sie den gleichen Endpunkt wie zuvor.

Sie sichern benutzerdefinierte Endpunkte, indem Sie entweder ein Zertifikat in AWS Certificate Manager (ACM) oder ein eigenes importieren.

Benutzerdefinierte Endpunkte für neue Domänen

Sie können einen benutzerdefinierten Endpunkt für eine neue OpenSearch Service-Domäne über die OpenSearch Servicekonsole oder Konfigurations-API aktivieren. AWS CLI

So passen Sie Ihren Endpunkt an (Konsole)

1. Wählen Sie in der OpenSearch Servicekonsole Domäne erstellen aus und geben Sie den Namen für die Domäne ein.
2. Wählen Sie unter Benutzerdefinierter Endpunkt die Option Benutzerdefinierten Endpunkt aktivieren aus.
3. Geben Sie für Benutzerdefinierter Hostname Ihren bevorzugten benutzerdefinierten Endpunkt-Hostnamen ein. Der Hostname sollte ein vollständig qualifizierter Domänenname (Fully Qualified Domäne Name, FQDN) sein, z. B. www.yourDomäne.com oder example.yourDomäne.com.

   > **Note**
   >
   > Wenn Sie kein Platzhalterzertifikat haben, müssen Sie ein neues Zertifikat für die Unterdomänen Ihres benutzerdefinierten Endpunkts anfordern.

4. Wählen Sie als AWS -Zertifikat das SSL-Zertifikat aus, das Sie für die Domäne verwenden möchten. Wenn keine Zertifikate verfügbar sind, können Sie eines in ACM importieren oder ACM für die Bereitstellung eines Zertifikats verwenden. Weitere Informationen finden Sie unter Ausstellen und Verwalten von Zertifikaten im AWS -Certificate-Manager-Benutzerhandbuch.

   > **Note**
   >
   > Das Zertifikat muss den benutzerdefinierten Endpunktnamen haben und sich im gleichen Konto wie Ihre OpenSearch Service-Domäne befinden. Der Zertifikatsstatus sollte AUSGESTELLT sein.

   - Befolgen Sie die restlichen Schritte, um Ihre Domäne zu erstellen und wählen Sie Erstellen aus.

- Wählen Sie die Domäne aus, wenn die Verarbeitung abgeschlossen ist, um Ihren benutzerdefinierten Endpunkt anzuzeigen.

Um die CLI oder die Konfigurations-API zu verwenden, nutzen Sie die `CreateDomain`- und `UpdateDomainConfig`-Operationen. Weitere Informationen finden Sie in der AWS CLI Befehlsreferenz und der Amazon OpenSearch Service API-Referenz.

Benutzerdefinierte Endpunkte für vorhandene Domänen

Um einen benutzerdefinierten Endpunkt zu einer vorhandenen OpenSearch Service-Domäne hinzuzufügen, wählen Sie Bearbeiten und führen Sie die Schritte 2 bis 4 aus.

CNAME-Zuordnung

Nachdem Sie einen benutzerdefinierten Endpunkt für Ihre OpenSearch Service-Domäne aktiviert haben, können Sie eine CNAME-Zuordnung in Amazon Route 53 (oder Ihrem bevorzugten DNS-Serviceanbieter) erstellen. Durch die Erstellung einer CNAME-Zuordnung können Sie den Datenverkehr an Ihren benutzerdefinierten Endpunkt und dessen Subdomänen weiterleiten. Ohne diese Zuordnung können Sie Datenverkehr nicht an Ihren benutzerdefinierten Endpunkt weiterleiten. Schritte zum Erstellen dieser Zuordnung in Route 53 finden Sie unter Konfigurieren von DNS-Routing für eine neue Domäne und Erstellen einer neuen gehosteten Zone für eine Unterdomäne. Weitere Anbieter finden Sie in der entsprechenden Dokumentation.

Erstellen Sie einen -CNAME-Datensatz, der den benutzerdefinierten Endpunkt auf den automatisch generierten Domain-Endpunkt verweist. Wenn es sich bei Ihrer Domain um einen Dual-Stack handelt, können Sie Ihren CNAME-Eintrag auf einen der beiden vom Dienst generierten Endpunkte verweisen. Die Dual-Stack-Fähigkeit Ihres benutzerdefinierten Endpunkts hängt von dem vom Dienst generierten Endpunkt ab, auf den Sie den CNAME-Eintrag verweisen. Der benutzerdefinierte Endpunkt-Hostname ist der Name des CNAME-Datensatzes und der Hostname des Domain-Endpunkts ist der Wert des CNAME-Datensatzes.

Wenn Sie SAML-Authentifizierung für OpenSearch Dashboards verwenden, müssen Sie Ihren IdP mit der neuen SSO-URL aktualisieren.

Sie können Amazon Route 53 verwenden, um einen Aliasdatensatztyp zu erstellen, um den benutzerdefinierten Endpunkt Ihrer Domäne auf einen Dual-Stack-Suchendpunkt zu verweisen. Um einen Alias-Eintragstyp zu erstellen, müssen Sie Ihre Domain so konfigurieren, dass sie den Dual-Stack-IP-Adresstyp verwendet. Sie können dies über die Route-53-APIs tun.

Um mithilfe der Route 53-API einen Alias-Datensatztyp zu erstellen, geben Sie das Alias-Ziel Ihrer Domain an. Sie finden das Alias-Ziel Ihrer Domain im Feld Hosted Zone (Dual Stack) im Abschnitt „Benutzerdefinierter Endpunkt“ der OpenSearch Service-Konsole oder indem Sie die `DescribeDomain` API verwenden und den Wert von kopieren`DomainEndpointV2HostedZoneId`.

Automatische Optimierung für Amazon Service OpenSearch

Die automatische Optimierung in Amazon OpenSearch Service verwendet Leistungs- und Nutzungsmetriken Ihres OpenSearch Clusters, um speicherbezogene Konfigurationsänderungen vorzuschlagen, einschließlich Warteschlangen- und Cache-Größen und virtuelle Java-Maschinen- (JVM) -Einstellungen auf Ihren Knoten. Diese optionalen Änderungen verbessern die Clustergeschwindigkeit und -stabilität.

Einige Änderungen werden sofort bereitgestellt, während Sie für Ihre Domäne außerhalb der Spitzenzeiten planen. Sie können jederzeit auf die OpenSearch Service-Standardeinstellungen zurückgreifen. Während die automatische Optimierung Leistungsmetriken für Ihre Domäne sammelt und analysiert, können Sie die Empfehlungen in der OpenSearch Service-Konsole auf der Seite Benachrichtigungen anzeigen.

Die automatische Optimierung ist in kommerziellen AWS-Regionen auf Domänen verfügbar, auf denen eine beliebige OpenSearch Version oder Elasticsearch 6.7 oder höher mit einem unterstützten Instance-Typ ausgeführt wird.

Änderungsarten

Die automatische Optimierung hat zwei große Kategorien von Änderungen:

- Unterbrechungsfreie Änderungen, die bei der Ausführung des Clusters angewendet werden
- Änderungen, für die eine blaue/grüne Bereitstellung erforderlich ist, die dann angewendet wird, wenn die Domain nicht in Spitzenzeiten arbeitet.

Basierend auf den Leistungsmetriken Ihrer Domain kann die automatische Optimierung Anpassungen an den folgenden Einstellungen vorschlagen:

Änderungstyp	Kategorie	Beschreibung
JVM-Heap-Größe	Blau/Grün	Standardmäßig verwendet OpenSearch Service 50% des RAM einer Instance für den JVM-Heap bis zu einer Heap-Größe von 32 GiB. Durch Erhöhen dieses Prozentsatzes wird OpenSearch mehr Speicher gegeben, aber weniger für das Betriebssystem und andere Prozesse. Größere Werte können die Anzahl der Garbage-Collection-Pausen verringern, aber die Länge dieser Pausen erhöhen.
JVM-Einstellungen für junge Generation	Blau/Grün	JVM-„junge Generation“-Einstellungen beeinflussen die Häufigkeit von kleineren Garbage Collections. Häufigere kleinere Sammlungen können die Anzahl der großen Sammlungen und Pausen verringern.
Warteschlangengröße	Unterbrechungsfrei	Standardmäßig ist die Größe der Suchwarteschlange `1000` und die Größe der Schreibwarteschlange `10000`. Die automatische Optimierung skaliert automatisch die Such- und Schreibwarteschlangen, wenn zusätzlicher Heap zur Bearbeitung von Anforderungen verfügbar ist.
Cache-Größe	Unterbrechungsfrei	Die Feld-Cache überwacht Datenstrukturen auf Heap. Daher ist es wichtig, die Verwendung des Caches zu überwachen. Die automatische Optimierung skaliert die Größe des Felddaten-Caches, um Probleme mit dem Arbeitsspeicher und dem Leistungsschalter zu vermeiden. Die Shard-Anforderungs-Cache wird auf Knotenebene verwaltet und hat eine standardmäßige maximale Größe von 1 % des Heaps. Die automatische Optimierung skaliert die Größe des Shard-Anforderungscaches, um mehr Such- und Indexanforderungen zu akzeptieren, als das, was der konfigurierte Cluster verarbeiten kann.

Änderungstyp	Kategorie	Beschreibung
Anforderungsgröße	Unterbrechungsfrei	Wenn die aggregierte Größe von in der Übertragung befindlichen Anforderungen 10% der gesamten JVM übersteigt (2% für `t2` Instance-Typen und 1% für`t3.small`), werden standardmäßig alle neuen `_bulk` AND-Anfragen OpenSearch gedrosselt, bis die bestehenden Anforderung `_search` abgeschlossen sind. Die automatische Optimierung optimiert diesen Schwellenwert automatisch, normalerweise zwischen 5 und 15 %, basierend auf der Menge an JVM, die derzeit auf dem System belegt ist. Wenn beispielsweise der JVM-Speicherdruck hoch ist, kann Auto-Tune den Schwellenwert auf 5 % reduzieren und sie erhalten dann möglicherweise mehr Ablehnungen, bis sich der Cluster stabilisiert hat und der Schwellenwert steigt.

Aktivieren oder Deaktivieren der automatischen Optimierung

OpenSearch Service aktiviert standardmäßig die automatische Optimierung für neue Domains. Um die automatische Optimierung auf vorhandenen Domänen zu aktivieren oder zu deaktivieren, wird empfohlen, die Konsole zu verwenden, was den Vorgang vereinfacht. Aktivieren der automatischen Optimierung verursacht keine Blau/Grün-Bereitstellung.

Sie können die automatische Optimierung derzeit mit AWS CloudFormation nicht aktivieren oder deaktivieren.

Konsole

Um Auto-Tune auf einer vorhandenen Domain zu aktivieren

1. Öffnen Sie die Amazon OpenSearch Service-Konsole zu https://console.aws.amazon.com/aos/Hause.
2. Wählen Sie im Navigationsbereich unter Domänen den Namen der Domain, um die Clusterkonfiguration zu öffnen.
3. Wählen Sie Einschalten, falls Auto-Tune noch nicht aktiviert ist.

4. Wählen Sie optional Zeitfenster außerhalb der Spitzenzeiten aus, um Optimierungen zu planen, die eine blaue/grüne Bereitstellung während des für die Domain konfigurierten Zeitfensters außerhalb der Spitzenzeiten erfordern. Weitere Informationen finden Sie unter the section called “Automatische Optimierung”.
5. Wählen Sie Änderungen speichern aus.

CLI

Um Auto-Tune mit dem zu aktivieren, senden Sie eine Anfrage AWS CLI: UpdateDomainConfig

```
aws opensearch update-domain-config \
  --domain-name my-domain \
  --auto-tune-options DesiredState=ENABLED
```

Automatische Optimierung

Vor dem 16. Februar 2023 nutzte Auto-Tune Wartungsfenster, um Änderungen zu planen, die eine blaue/grüne Implementierung erforderten. Wartungsfenster werden jetzt nicht mehr unterstützt, sondern das Zeitfenster außerhalb der Spitzenzeiten. Dabei handelt es sich um einen täglichen Zeitblock von 10 Stunden, in dem Ihre Domain in der Regel wenig Traffic verzeichnet. Sie können die Standardstartzeit für das Fenster außerhalb der Spitzenzeiten ändern, aber Sie können die Länge nicht ändern.

Alle Domains, für die Auto-Tune-Wartungsfenster vor der Einführung von Zeitfenstern außerhalb der Spitzenzeiten am 16. Februar 2023 aktiviert waren, können ältere Wartungsfenster weiterhin ohne Unterbrechung verwenden. Wir empfehlen Ihnen jedoch, Ihre bestehenden Domains zu migrieren, um stattdessen das Zeitfenster außerhalb der Spitzenzeiten für die Domainwartung zu nutzen. Detaillierte Anweisungen finden Sie unter the section called “Migration von Auto-Tune-Wartungsfenstern”.

Konsole

Um Auto-Tune-Aktionen außerhalb der Spitzenzeiten zu planen

1. Öffnen Sie die Amazon OpenSearch Service-Konsole zu https://console.aws.amazon.com/aos/Hause.
2. Wählen Sie im Navigationsbereich unter Domänen den Namen der Domain, um die Clusterkonfiguration zu öffnen.

3. Gehen Sie zur Registerkarte Auto-Tune und wählen Sie Bearbeiten aus.
4. Wählen Sie Einschalten, falls Auto-Tune noch nicht aktiviert ist.
5. Wählen Sie unter Optimierungen außerhalb der Spitzenzeiten planen die Option Zeitfenster außerhalb der Spitzenzeiten aus.
6. Wählen Sie Änderungen speichern aus.

CLI

Um Ihre Domain so zu konfigurieren, dass Auto-Tune-Aktionen während des konfigurierten Zeitfensters außerhalb der Spitzenzeiten geplant werden, fügen Sie der Anfrage Folgendes bei: `UseOffPeakWindow` UpdateDomainConfig

```
aws opensearch update-domain-config \
  --domain-name my-domain \
  --auto-tune-options
 DesiredState=ENABLED,UseOffPeakWindow=true,MaintenanceSchedules=null
```

Automatische Optimierung

Sie können Auto-Tune-Statistiken in überwachen. Amazon CloudWatch Eine vollständige Liste der Metriken finden Sie unter the section called “Automatische Optimierung”.

OpenSearch Der Service sendet Auto-Tune-Ereignisse an Amazon EventBridge. Sie können EventBridge sie verwenden, um Regeln zu konfigurieren, die eine E-Mail senden oder eine bestimmte Aktion ausführen, wenn ein Ereignis empfangen wird. Informationen zum Format der einzelnen Ereignisse, an die gesendet werden EventBridge, finden Sie unterthe section called “Automatische Optimierung von Ereignissen”.

Markierung von OpenSearch Amaz-Service-Domänen

Mit Tags können Sie einer OpenSearch Amazon-Domäne beliebige Informationen zuweisen, damit Sie diese Informationen kategorisieren und filtern können. Ein -Tag ist ein Schlüssel-Wert-Paar, das Sie definieren und mit einer OpenSearch Service-Domäne verknüpfen. Sie können Tags auch verwenden, um Kosten zu verfolgen, indem Ausgaben für ähnlich getaggte Ressourcen gruppiert werden. AWS ordnet Ihren Tags keine semantische Bedeutung zu. Tags werden streng als Zeichenfolgen interpretiert. Alle Tags haben die folgenden Elemente:

Tag-Element	Beschreibung	Erforderlich
Tag-Schlüssel	Der Tag-Schlüssel ist der Name des Markierungen. Schlüssel müssen für die OpenSearch Service-Domäne, der sie zugeordnet sind, eindeutig sein. Eine Liste der grundlegenden Einschränkungen auf Tag-Schlüsseln und -Werten finden Sie unter Einschränkungen benutzerdefinierter Tags.	Ja
Tag-Wert	Der Tag-Wert ist der Zeichenfolgenwert des Tags. Tag-Werte können `null` sein und müssen in einem Tag-Satz nicht einzigartig sein. Sie können beispielsweise ein Schlüssel-Wert-Paar in einem Tag-Satz von project/Trinity and cost-center/Trinity Eine Liste der grundlegenden Einschränkungen auf Tag-Schlüsseln und -Werten finden Sie unter Einschränkungen benutzerdefinierter Tags.	Nein

Jede OpenSearch Service-Domäne verfügt über einen Tag-Satz, der alle Tags enthält, die dieser OpenSearch -Domäne zugewiesen sind. AWS weist den OpenSearch Dienstdomänen nicht automatisch irgendwelche Tags zu. Ein Tag-Satz kann zwischen 0 und 50 Tags enthalten. Wenn Sie einer Domäne einen Tag mit demselben Schlüssel wie ein vorhandenes Tag hinzufügen, wird der alte Wert vom neuen Wert überschrieben.

Tag-Beispiel

Sie können einen Schlüssel verwenden, um eine Kategorie zu definieren, und der Wert könnte ein Element in dieser Kategorie sein. Sie können beispielsweise den Tag-Schlüssel `project` und den Tag-Wert von definieren. Dies bedeutet`Salix`, dass die Domäne OpenSearch Service dem Projekt Salix zugewiesen ist. Sie können mit Tags auch OpenSearch Dienstdomänen kennzeichnen, die zu Test- oder Produktionszwecken verwendet werden, indem Sie einen Schlüssel wie `environment=test` oder `environment=production` Wir empfehlen, einheitliche Tag-Schlüssel zu verwenden, um die mit OpenSearch Service-Domänen verknüpften Metadaten einfacher verfolgen zu können.

Sie können Tags auch verwenden, um Ihre AWS -Rechnung zu organisieren, um Ihre eigene Kostenstruktur darzustellen. Dazu müssen Sie sich registrieren, um Ihre AWS-Konto -Rechnung mit Tag-Schlüsselwerten zu erhalten. Um dann die Kosten kombinierter Ressourcen anzuzeigen, organisieren Sie Ihre Fakturierungsinformationen nach Ressourcen mit gleichen Tag-

Schlüsselwerten. Sie können beispielsweise mehrere OpenSearch Service-Domänen mit Schlüssel-Wert-Paare markieren und dann Ihre Abrechnungsinformationen organisieren, um die Gesamtkosten für die einzelnen Domänen über mehrere Services anzuzeigen. Weitere Informationen finden Sie unter Verwendung von Kostenzuordnungs-Tags in der AWS -Fakturierungs- und Kostenverwaltungs-Dokumentation.

> **Note**
>
> Tags werden für Autorisierungszwecke im Cache gespeichert. Daher können Ergänzungen und Aktualisierungen an Tags für Tags in OpenSearch Service-Domänen einige Minuten in Anspruch nehmen, bevor sie verfügbar sind.

Markierung von Domänen (Konsole)

Die Konsole ist die einfachste Möglichkeit, eine Domäne zu markieren.

So erstellen Sie ein Tag (Konsole)

1. Melden Sie sich bei der https://aws.amazon.com an und wählen Sie dann Sign In to the Console (Bei der Konsole anmelden) aus.
2. Wählen Sie unter Analytics Amazon OpenSearch Service aus.
3. Wählen Sie die Domäne aus, zu der Sie Tags hinzufügen möchten und gehen Sie zur Registerkarte Tags.
4. Wählen Sie Verwalten und neues Tag hinzufügen.
5. Geben Sie einen Tag-Schlüssel und einen optionalen Wert ein.
6. Wählen Sie Speichern.

Um ein Tag zu löschen, führen Sie die gleichen Schritte aus und wählen Sie Entfernen auf der Seite Tags verwalten.

Weitere Informationen zur Verwendung der Konsole für die Arbeit mit Tags finden Sie unter Tag Editor im AWS Handbuch „Erste Schritte“ der Managementkonsole.

Domains taggen ()AWS CLI

Sie können Ressourcen-Tags AWS CLI mit dem --add-tags Befehl erstellen.

Syntax

```
add-tags --arn=<domain_arn> --tag-list Key=<key>,Value=<value>
```

Parameter	Beschreibung
`--arn`	Amazon-Ressourcennamen für die OpenSearch Service-Domäne, der das Tag zugewiesen ist.
`--tag-list`	Satz an durch Leerzeichen getrennten Schlüssel-Wert-Paaren im folgendem Format: `Key=<key>,Value=<value>`

Beispiel

Im folgenden Beispiel werden zwei Tags für die logs-Domäne erstellt:

```
aws opensearch add-tags --arn arn:aws:es:us-east-1:379931976431:domain/logs --tag-list
 Key=service,Value=OpenSearch Key=instances,Value=m3.2xlarge
```

Sie können Tags aus einer OpenSearch Service-Domäne mit dem --remove-tags Befehl entfernen.

Syntax

```
remove-tags --arn=<domain_arn> --tag-keys Key=<key>,Value=<value>
```

Parameter	Beschreibung
`--arn`	OpenSearch Amazon-Ressourcennamen (ARN)
`--tag-keys`	Satz an durch Leerzeichen getrennten Schlüssel-Wert-Paaren, die Sie aus der OpenSearch Domäne Service entfernen möchten

Beispiel

Das folgende Beispiel entfernt zwei Tags aus der logs-Domäne, die im vorherigen Beispiel erstellt wurden:

```
aws opensearch remove-tags --arn arn:aws:es:us-east-1:379931976431:domain/logs --tag-
keys service instances
```

Sie können die vorhandenen Tags für eine OpenSearch Service-Domäne mit dem --list-tags folgenden Befehl anzeigen:

Syntax

```
list-tags --arn=<domain_arn>
```

Parameter	Beschreibung
`--arn`	OpenSearch Amazon-Ressourcennamen (ARN)

Beispiel

Im folgenden Beispiel werden alle Ressourcen-Tags für die logs-Domäne aufgelistet:

```
aws opensearch list-tags --arn arn:aws:es:us-east-1:379931976431:domain/logs
```

Domains taggen ()AWS SDKs

Die AWS SDKs (außer Android und iOS SDKs) unterstützen alle in der Amazon OpenSearch Service API-Referenz definierten Aktionen, einschließlich der `RemoveTags` Operationen `AddTags`, `ListTags`, und. Weitere Informationen über die AWS SDKs Installation und Verwendung von AWS

Python

In diesem Beispiel verwenden wir OpenSearchServiceden Python-Client aus dem AWS SDK für Python (Boto), um einer Domäne ein Tag hinzuzufügen, das an die Domäne angehängte Tag aufzulisten und ein Tag aus der Domäne zu entfernen. Sie müssen Werte für `DOMAIN_ARN`, `TAG_KEY` und `TAG_VALUE` angeben.

```
import boto3
from botocore.config import Config  # import configuration

DOMAIN_ARN = ''  # ARN for the domain. i.e "arn:aws:es:us-east-1:123456789012:domain/
my-domain
TAG_KEY = ''  # The name of the tag key. i.e 'Smileyface'
TAG_VALUE = ''  # The value assigned to the tag. i.e 'Practicetag'
```

```
# defines the configurations parameters such as region

my_config = Config(region_name='us-east-1')
client = boto3.client('opensearch', config=my_config)


# defines the client variable

def addTags():
    """Adds tags to the domain"""

    response = client.add_tags(ARN=DOMAIN_ARN,
                               TagList=[{'Key': TAG_KEY,
                                         'Value': TAG_VALUE}])

    print(response)


def listTags():
    """List tags that have been added to the domain"""

    response = client.list_tags(ARN=DOMAIN_ARN)
    print(response)


def removeTags():
    """Remove tags that have been added to the domain"""

    response = client.remove_tags(ARN=DOMAIN_ARN, TagKeys=[TAG_KEY])

    print('Tag removed')
    return response
```

Ausführen von administrativen Aktionen OpenSearch

Amazon OpenSearch Service bietet mehrere Verwaltungsoptionen, mit denen Sie detailliert steuern können, ob Sie Probleme mit Ihrer Domain beheben müssen. Zu diesen Optionen gehören die Möglichkeit, den OpenSearch Prozess auf einem Datenknoten neu zu starten, und die Möglichkeit, einen Datenknoten neu zu starten.

OpenSearch Der Service überwacht die Integritätsparameter des Knotens und ergreift bei Anomalien Korrekturmaßnahmen, um die Domänen stabil zu halten. Mit den administrativen Optionen zum

Neustarten des OpenSearch Prozesses auf einem Knoten und zum Neustarten eines Knotens selbst haben Sie die Kontrolle über einige dieser Abhilfemaßnahmen.

Sie können das AWS Management Console AWS CLI, oder das AWS SDK verwenden, um diese Aktionen durchzuführen. In den folgenden Abschnitten wird beschrieben, wie Sie diese Aktionen mit der Konsole ausführen.

Den OpenSearch Prozess auf einem Knoten in Amazon OpenSearch Service neu starten

Um den OpenSearch Prozess auf einem Knoten neu zu starten

1. Navigieren Sie zur OpenSearch Servicekonsole unterhttps://console.aws.amazon.com/aos/.
2. Wählen Sie im linken Navigationsbereich die Option Domains aus. Wählen Sie den Namen der Domain aus, die Sie an ein anderes übertragen möchten.
3. Nachdem die Seite mit den Domänendetails geöffnet wurde, navigieren Sie zur Registerkarte Instanzstatus.
4. Wählen Sie das + neben dem Knoten aus, für den Sie die Registrierung aufheben möchten.
5. Wählen Sie das Drop-down-Menü Aktionen aus und wählen Sie Restart OpenSearch / Elasticsearch-Prozess aus.
6. Wählen Sie im Modal die Option Bestätigen aus.
7. Um den Status der von Ihnen initiierten Aktion zu sehen, wählen Sie den Namen des Knotens aus. Nachdem die Seite mit den Knotendetails geöffnet wurde, wählen Sie unter dem Namen des Knotens die Registerkarte Ereignisse aus, um eine Liste der mit diesem Knoten verknüpften Ereignisse anzuzeigen.

Einen Datenknoten in Amazon Service neu starten OpenSearch

Um einen Datenknoten neu zu starten

1. Navigieren Sie zur OpenSearch Servicekonsole unterhttps://console.aws.amazon.com/aos/.
2. Wählen Sie im linken Navigationsbereich die Option Domains aus. Wählen Sie den Namen der Domain aus, die Sie an ein anderes übertragen möchten.
3. Nachdem die Seite mit den Domänendetails geöffnet wurde, navigieren Sie zur Registerkarte Instanzstatus.

4. Wählen Sie das + neben dem Knoten aus, für den Sie die Registrierung aufheben möchten.
5. Wählen Sie das Drop-down-Menü Aktionen aus und wählen Sie Knoten neu starten aus.
6. Wählen Sie im Modal die Option Bestätigen aus.
7. Um den Status der von Ihnen initiierten Aktion zu sehen, wählen Sie den Namen des Knotens aus. Nachdem die Seite mit den Knotendetails geöffnet wurde, wählen Sie unter dem Namen des Knotens die Registerkarte Ereignisse aus, um eine Liste der mit diesem Knoten verknüpften Ereignisse anzuzeigen.

Den OpenSearch Dashboard-Prozess auf einem Knoten in Amazon Service neu starten OpenSearch

Sie können den OpenSearch Dashboard-Prozess (früher Kibana) neu starten, um Probleme wie eine eingefrorene Benutzeroberfläche, Ladefehler oder nicht reagierende Visualisierungen zu beheben. Die Option zum Neustarten von OpenSearch Dashboards ist nur für den Knoten verfügbar, auf dem der Dashboard-Prozess aktiv ausgeführt wird. In den meisten OpenSearch Dienstdomänen läuft dieser Prozess auf dedizierten Koordinatorknoten, nicht auf Datenknoten. Wenn Sie das Drop-down-Menü Aktionen in der Konsole öffnen, wird die Option daher normalerweise nur für Koordinatorknoten angezeigt. Weitere Informationen finden Sie unter the section called “Dedizierte Koordinatorknoten”.

Dieses Verhalten hängt davon ab, wie Ihre Domain konfiguriert ist.

- Domänen mit dedizierten Koordinatorknoten — Der Dashboard-Prozess wird ausschließlich auf diesen Knoten ausgeführt, und nur dort wird die Neustartoption angezeigt.
- Domänen ohne dedizierte Koordinatorknoten — In einfacheren oder älteren Setups werden Dashboards möglicherweise stattdessen auf einem Datenknoten ausgeführt, und die Neustartoption wird dort angezeigt.
- Master-Knoten — Diese Knoten dienen ausschließlich der Verwaltung des Clusterstatus und der Wahlen. Sie führen keine Dashboards aus und zeigen auch nie die Neustartoption an.

Um festzustellen, auf welchem Knoten der Dashboard-Prozess ausgeführt wird, navigieren Sie zum Abschnitt Cluster-Konfiguration Ihrer Domain und überprüfen Sie die Knotenrollen. Die Option zum Neustart ist nur für den Knoten verfügbar, der den Dashboard-Prozess hostet.

Um den Dashboard-Prozess auf einem Knoten neu zu starten

1. Navigieren Sie zur OpenSearch Servicekonsole unter https://console.aws.amazon.com/aos/.

2. Wählen Sie im linken Navigationsbereich die Option Domains aus. Wählen Sie den Namen der Domain aus, die Sie an ein anderes übertragen möchten.
3. Nachdem die Seite mit den Domänendetails geöffnet wurde, navigieren Sie zur Registerkarte Instanzstatus.
4. Wählen Sie im Abschnitt für die Knoten, auf denen der Dashboard-Prozess ausgeführt wird, die Schaltfläche neben dem Knoten aus, auf dem Sie den Prozess neu starten möchten.
5. Wählen Sie das Drop-down-Menü Aktionen aus und wählen Sie Dashboard/Kibana-Prozess neu starten aus.
6. Wählen Sie im Modal die Option Bestätigen aus.
7. Um den Status der von Ihnen initiierten Aktion zu sehen, wählen Sie den Namen des Knotens aus. Nachdem die Seite mit den Knotendetails geöffnet wurde, wählen Sie unter dem Namen des Knotens die Registerkarte Ereignisse aus, um eine Liste der mit diesem Knoten verknüpften Ereignisse anzuzeigen.

Einschränkungen

EFAs haben die folgenden Einschränkungen:

- Verwaltungsoptionen werden auf Elasticsearch-Versionen 7.x und höher unterstützt.
- Administrative Optionen unterstützen keine Domains mit Multi-AZ und aktiviertem Standby.
- Der OpenSearch Neustart des Elasticsearch-Prozesses und der Neustart des Datenknotens werden auf Domains mit drei oder mehr Datenknoten unterstützt.
- Die Prozessunterstützung für Dashboards und Kibana wird auf Domains mit zwei oder mehr Datenknoten unterstützt.
- Um den OpenSearch Prozess auf einem Knoten neu zu starten oder einen Knoten neu zu starten, darf sich die Domain nicht im roten Status befinden und für alle Indizes müssen Replikate konfiguriert sein.

Arbeiten mit direkten Anfragen von Amazon OpenSearch Service

Verwenden Sie Amazon OpenSearch Service Direct Query, um Daten in Amazon CloudWatch Logs, Amazon S3 und Amazon Security Lake zu analysieren, ohne Datenerfassungspipelines zu erstellen. Mit dieser Zero-ETL-Integration können Sie Daten direkt mit OpenSearch SQL oder PPL abfragen und sie in Discover untersuchen.

Konfigurieren Sie zunächst Ihre Datenquelle in der OpenSearch Servicekonsole. Verwenden Sie für Amazon S3 Domänenverbindungen und erstellen Sie Tabellen mit SQL in Query Workbench. CloudWatch Logs und Security Lake verwenden vorkonfigurierte Quellen und AWS Glue Data Catalog Tabellen.

Preisgestaltung bei Direktabfrage

Wenn Sie OpenSearch Service Direct Queries verwenden, fallen separate Gebühren für OpenSearch Service und die Ressourcen an, die für die Verarbeitung und Speicherung Ihrer Daten auf Amazon S3, Amazon CloudWatch Logs und Amazon Security Lake verwendet werden. Wenn Sie direkte Abfragen ausführen, werden Ihnen Gebühren für OpenSearch Recheneinheiten (OCUs) pro Stunde angezeigt, die auf Ihrer Rechnung als DirectQuery OCU-Nutzungsart aufgeführt sind.

Es gibt zwei Arten von direkten Abfragen: interaktive Abfragen und Abfragen mit indizierter Ansicht.

- Interaktive Abfragen werden verwendet, um die Datenauswahl zu füllen und Analysen Ihrer Daten in S3, CloudWatch Logs oder Security Lake durchzuführen.

  Wenn Sie bei direkten Amazon S3 S3-Abfragen eine neue Abfrage von Discover aus ausführen, startet OpenSearch Service eine neue Sitzung, die mindestens drei Minuten dauert. OpenSearch Der Service hält diese Sitzung aktiv, um sicherzustellen, dass nachfolgende Abfragen schnell ausgeführt werden.

  Bei CloudWatch Logs- und Security Lake-Abfragen verarbeitet der OpenSearch Service jede Abfrage mit einem separaten, vorgewärmten Job, ohne dass eine längere Sitzung aufrechterhalten wird.
- Abfragen mit indizierten Ansichten verwenden Compute, um indizierte Ansichten im Service zu verwalten. OpenSearch Diese Abfragen dauern in der Regel länger, da sie eine unterschiedliche Datenmenge in einen benannten Index aufnehmen. Durch die Indizierung von Daten können Sie

dafür sorgen, dass future interaktive Abfragen schneller ausgeführt werden, oder Sie können erweiterte Analysefunktionen wie Dashboards oder Benachrichtigungen nutzen, für deren Referenzierung ein Index erforderlich ist.

Bei Amazon S3 S3-Datenquellen werden die indizierten Daten in einer Domain gespeichert, die auf einem gekauften Instance-Typ basiert. Bei mit CloudWatch Logs und Security Lake verbundenen Datenquellen werden die indizierten Daten in einer OpenSearch serverlosen Sammlung gespeichert, bei der Ihnen die indexierten Daten (IndexingOCU), die durchsuchten Daten (searchOCU) und die in GB gespeicherten Daten in Rechnung gestellt werden.

Weitere Informationen finden Sie in den Abschnitten Direct Query und Serverless unter Amazon OpenSearch Service Pricing.

Einschränkungen bei Direktabfragen

Allgemeine Einschränkungen

Die folgenden Einschränkungen gelten für OpenSearch Service-Direktanfragen.

- Einige Datentypen werden nicht unterstützt. Die unterstützten Datentypen sind auf Parquet, CSV und JSON beschränkt.
- Wenn sich die Struktur Ihrer Daten im Laufe der Zeit ändert, müssen Sie Ihre indizierten Ansichten oder out-of-the-box Integrationen aktualisieren, um den Änderungen der Datenstruktur Rechnung zu tragen.
- AWS CloudFormation Vorlagen werden noch nicht unterstützt.
- OpenSearch SQL- und OpenSearch PPL-Anweisungen haben bei der Arbeit mit OpenSearch Indizes andere Einschränkungen als bei der Verwendung von Direktabfragen. Direct Query unterstützt erweiterte Befehle wie JOINs Unterabfragen und Suchvorgänge, während diese Befehle in OpenSearch Indizes nur begrenzt oder gar nicht unterstützt werden. Weitere Informationen finden Sie unter the section called “Unterstützte SQL- und PPL-Befehle”.

Einschränkungen für Amazon S3

Wenn Sie Daten direkt in Amazon S3 abfragen, gelten die folgenden zusätzlichen Einschränkungen:

- Direct Query für S3 ist nur für OpenSearch Service-Domains verfügbar, auf denen OpenSearch Version 2.13 oder höher ausgeführt wird, und erfordert Zugriff auf. AWS Glue Data Catalog

Bestehende AWS Glue Data Catalog Tabellen müssen mit SQL in OpenSearch Query Workbench neu erstellt werden.

- Bei Direct Query for S3 müssen Sie einen Checkpoint-Bucket auf Amazon S3 angeben. Dieser Bucket behält den Status Ihrer indizierten Ansichten bei, einschließlich der letzten Aktualisierungszeit und der zuletzt aufgenommenen Daten.
- Ihre OpenSearch Domain und AWS Glue Data Catalog müssen sich in derselben befinden. AWS-Konto Ihr S3-Bucket kann sich in einem anderen Konto befinden (erfordert, dass die Bedingung zu Ihrer IAM-Richtlinie hinzugefügt wird), muss sich aber in derselben Domain befinden AWS-Region wie Ihre Domain.
- OpenSearch Direkte Serviceabfragen mit S3 unterstützen nur Spark-Tabellen, die mit Query Workbench generiert wurden. In AWS Glue Data Catalog oder Athena generierte Tabellen werden vom Spark-Streaming nicht unterstützt, das für die Verwaltung indizierter Ansichten erforderlich ist.
- OpenSearch Instance-Typen haben Netzwerknutzlastbeschränkungen von entweder 10 MiB oder 100 MiB, je nachdem, welchen Instance-Typ Sie wählen.

Einschränkungen für Amazon CloudWatch Logs

Wenn Sie Daten direkt in CloudWatch Logs abfragen, gelten die folgenden zusätzlichen Einschränkungen:

- Die direkte Abfrageintegration mit CloudWatch Logs ist nur in OpenSearch Servicesammlungen und auf der OpenSearch Benutzeroberfläche verfügbar.
- OpenSearch Serverlose Sammlungen haben Netzwerknutzlastbeschränkungen von 100 MiB.
- CloudWatch Logs unterstützt VPC Flow- und AWS WAF Dashboard-Integrationen CloudTrail, die über die Konsole installiert werden.

Einschränkungen für Amazon Security Lake

Wenn Sie Daten direkt in Security Lake abfragen, gelten die folgenden zusätzlichen Einschränkungen:

- Die direkte Abfrageintegration mit Security Lake ist nur für OpenSearch Servicesammlungen und die OpenSearch Benutzeroberfläche verfügbar.
- OpenSearch Serverlose Sammlungen haben Netzwerknutzlastbeschränkungen von 100 MiB.
- Die Tabellenverwaltung für Security Lake erfolgt in Lake Formation.

- Security Lake unterstützt nur materialisierte Ansichten als indizierte Ansichten. Verdeckende Indizes werden nicht unterstützt.

Empfehlungen für die Verwendung von Direktabfragen in Amazon OpenSearch Service

Diese Seite enthält Empfehlungen für die Verwendung von Amazon OpenSearch Service Direct Queries zur Analyse von Daten aus CloudWatch Logs, Amazon S3 und Amazon Security Lake. Diese bewährten Methoden helfen Ihnen dabei, die Leistung zu optimieren und effiziente Abfragen zu gewährleisten, ohne dass Daten aufgenommen oder dupliziert werden müssen.

Themen

- Allgemeine Empfehlungen
- Amazon S3 S3-Empfehlungen
- CloudWatch Protokolliert Empfehlungen
- Empfehlungen von Security Lake

Allgemeine Empfehlungen

Wir empfehlen Ihnen, bei der Verwendung von Direct Query wie folgt vorzugehen:

- Verwenden Sie die `COALESCE SQL` Funktion, um fehlende Spalten zu behandeln und sicherzustellen, dass Ergebnisse zurückgegeben werden.

- Verwenden Sie Grenzwerte für Ihre Abfragen, um sicherzustellen, dass Sie nicht zu viele Daten zurückholen.
- Wenn Sie vorhaben, denselben Datensatz mehrmals zu analysieren, erstellen Sie eine indizierte Ansicht, in der die Daten vollständig aufgenommen, indexiert OpenSearch und nach Abschluss der Analyse gelöscht werden.
- Löschen Sie Beschleunigungsjobs und Indizes, wenn sie nicht mehr benötigt werden.
- Abfragen mit Feldnamen, die identisch sind, sich aber nur in der Groß- und Kleinschreibung unterscheiden (z. B. `field1` und`FIELD1`), werden nicht unterstützt.

  Beispielsweise werden die folgenden Abfragen nicht unterstützt:

```
Select AWSAccountId, AwsAccountId from LogGroup
Select a.@LogStream, b.@logStream from Table A INNER Join Table B ona.id = b.id
```

Die folgende Abfrage wird jedoch unterstützt, da der Feldname (@logStream) in beiden Protokollgruppen identisch ist:

```
Select a.@logStream, b.@logStream from Table A INNER Join Table B on a.id = b.id
```

- Funktionen und Ausdrücke müssen mit Feldnamen arbeiten und Teil einer `SELECT` Anweisung mit einer in der `FROM` Klausel angegebenen Protokollgruppe sein.

  Diese Abfrage wird beispielsweise nicht unterstützt:

  ```
  SELECT cos(10) FROM LogGroup
  ```

  Diese Abfrage wird unterstützt:

  ```
  SELECT cos(field1) FROM LogGroup
  ```

Amazon S3 S3-Empfehlungen

Wenn Sie Amazon OpenSearch Service verwenden, um Daten direkt in Amazon S3 abzufragen, empfehlen wir außerdem Folgendes:

- Nehmen Sie Daten mithilfe der Partitionsformate Jahr, Monat, Tag und Stunde in Amazon S3 auf, um Abfragen zu beschleunigen.
- Wenn Sie Skipping-Indizes erstellen, verwenden Sie Bloom-Filter für Felder mit hoher Kardinalität und min/max Indizes für Felder mit großen Wertebereichen. Für Felder mit hoher Kardinalität sollten Sie erwägen, einen wertebasierten Ansatz zu verwenden, um die Abfrageeffizienz zu verbessern.
- Verwenden Sie Index State Management, um Speicherplatz für materialisierte Ansichten und umfassende Indizes bereitzustellen.

CloudWatch Protokolliert Empfehlungen

Wenn Sie Amazon OpenSearch Service verwenden, um Daten direkt in CloudWatch Logs abzufragen, empfehlen wir außerdem Folgendes:

- Wenn Sie mehrere Protokollgruppen in einer Abfrage durchsuchen, verwenden Sie die entsprechende Syntax. Weitere Informationen finden Sie unter the section called “Gruppenfunktionen mit mehreren Protokollen”.
- Wenn Sie SQL- oder PPL-Befehle verwenden, schließen Sie bestimmte Felder in Backticks ein, um sie erfolgreich abzufragen. Backticks werden für Felder mit Sonderzeichen (nicht alphabetisch und nicht numerisch) benötigt. Zum Beispiel „einschließen`@message`“ und „in Backticks“. `Operation.Export, Test::Field` Sie müssen Spalten mit rein alphabetischen Namen nicht in Backticks einschließen.

  Beispielabfrage mit einfachen Feldern:

  ```
  SELECT SessionToken, Operation, StartTime  FROM `LogGroup-A`
  LIMIT 1000;
  ```

  Ähnliche Abfrage mit angehängten Backticks:

  ```
  SELECT `@SessionToken`, `@Operation`, `@StartTime` FROM `LogGroup-A`
  LIMIT 1000;
  ```

Empfehlungen von Security Lake

Wenn Sie Amazon OpenSearch Service verwenden, um Daten direkt in Security Lake abzufragen, empfehlen wir außerdem Folgendes:

- Überprüfen Sie Ihren Security Lake-Status und stellen Sie sicher, dass er problemlos läuft. Ausführliche Schritte zur Fehlerbehebung finden Sie unter Fehlerbehebung beim Data Lake-Status im Amazon Security Lake-Benutzerhandbuch.
- Überprüfen Sie Ihren Abfragezugriff:
  - Wenn Sie Security Lake von einem anderen Konto als dem delegierten Security Lake-Administratorkonto aus abfragen, richten Sie in Security Lake einen Abonnenten mit Abfragezugriff ein.

  - Wenn Sie Security Lake von demselben Konto aus abfragen, suchen Sie in Security Lake nach Nachrichten über die Registrierung Ihrer verwalteten S3-Buckets bei. LakeFormation
- Erkunden Sie die Abfragevorlagen und vorgefertigten Dashboards, um Ihre Analyse zu beschleunigen.
- Machen Sie sich mit Open Cybersecurity Schema Framework (OCSF) und Security Lake vertraut:
  - Sehen Sie sich die Beispiele für Schemazuordnungen für AWS Quellen im GitHub OCSF-Repository an
  - Erfahren Sie, wie Sie Security Lake effektiv abfragen können, indem Sie Security Lake-Abfragen für AWS Quellversion 2 (OCSF 1.1.0) besuchen
  - Verbessern Sie die Abfrageleistung mithilfe der Partitionen:`accountid`, und `region` `time_dt`
- Machen Sie sich mit der SQL-Syntax vertraut, die Security Lake für Abfragen unterstützt. Weitere Informationen finden Sie unter the section called “Unterstützte SQL-Befehle”.

Kontingente für direkte Abfragen

Ihr Konto hat die folgenden Kontingente für direkte Anfragen von OpenSearch Diensten.

Kontingente für Amazon S3

Jedes Mal, wenn Sie eine Abfrage an eine Amazon S3 S3-Datenquelle starten, öffnet OpenSearch Service eine Sitzung und hält sie mindestens drei Minuten lang aufrecht. Dadurch wird die Abfragelatenz reduziert, da die Startzeit der Sitzung bei nachfolgenden Abfragen entfällt.

Beschreibung	Maximum	Kann überschrieben werden
Verbindungen pro Domain	10	Ja
Datenquellen pro Domain	20	Ja
Indizes pro Domain	5	Ja
Gleichzeitige Sitzungen pro Datenquelle	10	Ja
Maximale OCU pro Abfrage	60	Ja

Beschreibung	Maximum	Kann überschrieben werden
Maximale Ausführungszeit für Abfragen (Minuten)	30	Ja
Maximum OCUs pro Beschleunigung	20	Ja
Maximaler kurzlebiger Speicher	20	Ja

Kontingente für Protokolle CloudWatch

> **Note**
>
> Wenn Sie direkte Abfragen mithilfe von CloudWatch Logs Insights durchführen möchten, stellen Sie sicher, dass Sie sich auf Folgendes the section called “CloudWatch Logs Insights” beziehen:

Beschreibung	Wert	Weicher Grenzwe?	Hinweise
TPS-Limit auf Kontoebene für direkte Abfragen APIs	3 TPS	Ja	
Maximale Anzahl von Datenquellen	20	Ja	Das Limit ist pro AWS-Konto.
Maximale Anzahl von Indizes oder materialisierten Ansichten mit automatischer Aktualisierung	30	Ja	Das Limit gilt pro Datenquelle.

Beschreibung	Wert	Weicher Grenzwe?	Hinweise
Maximale Anzahl gleichzeitiger Abfragen	15	Ja	Das Limit gilt für Abfragen im Status „Ausstehend“ oder „Wird ausgeführt“. Umfasst interaktive Abfragen (z. B. Befehle zum Datenabruf wie`SELECT`) und Indexabfragen (z. B. Operationen wie`CREATE/ALTER/DROP`).
Maximale gleichzeitige OCU pro Abfrage	512	Ja	OpenSearch Recheneinheiten (OCU). Das Limit basiert auf 15 Executoren und einem Treiber mit jeweils 16 vCPU und 32 GB Arbeitsspeicher. Steht für gleichzeitige Rechenleistung.
Maximale Ausführungszeit für Abfragen in Minuten	60	Nein	Das Limit gilt für OpenSearch PPL/SQL-Abfragen in CloudWatch Logs Insights.
Zeitraum für das Löschen veralteter Abfragen IDs	90 Tage	Ja	Dies ist der Zeitraum, nach dem der OpenSearch Service Abfrage-Metadaten für ältere Einträge löscht. Beispielsweise schlägt der Anruf GetDirectQuery bei Abfragen GetDirectQueryResult fehl, die älter als 90 Tage sind.

Kontingente für Security Lake

Beschreibung	Wert	Weiches Limit?	Hinweise
TPS-Limit auf Kontoebene für direkte Abfragen APIs	3 TPS	Ja	
Maximale Anzahl von Datenquellen	20	Ja	Das Limit ist pro AWS-Konto.

Beschreibung	Wert	Weiches Limit?	Hinweise
Maximale Anzahl von Indizes oder materialisierten Ansichten mit automatischer Aktualisierung	30	Ja	Das Limit gilt pro Datenquelle. Schließt nur Indizes und materialisierte Ansichten (MVs) ein, bei denen die automatische Aktualisierung auf true gesetzt ist.
Maximale Anzahl gleichzeitiger Abfragen	30	Ja	Das Limit gilt für Abfragen im Status „Ausstehend“ oder „Wird ausgeführt“. Umfasst interaktive Abfragen (z. B. Befehle zum Datenabruf wie`SELECT`) und Indexabfragen (z. B. Operationen wie`CREATE/ALTER/DROP`).
Maximale gleichzeitige OCU pro Abfrage	512	Ja	OpenSearch Recheneinheiten (OCU). Das Limit basiert auf 15 Executoren und einem Treiber mit jeweils 16 vCPU und 32 GB Arbeitsspeicher. Steht für gleichzeitige Rechenleistung.
Maximale Ausführungszeit für Abfragen in Minuten	30	Nein	Gilt nur für interaktive Abfragen (z. B. Befehle zum Datenabruf wie`SELECT`). Für `REFRESH` Abfragen liegt das Limit bei 6 Stunden.
Zeitraum für das Löschen veralteter Abfragen IDs	90 Tage	Ja	Dies ist der Zeitraum, nach dem der OpenSearch Service Abfrage-Metadaten für ältere Einträge löscht. Beispielsweise schlägt der Anruf GetDirectQuery bei Abfragen GetDirectQueryResult fehl, die älter als 90 Tage sind.

Unterstützt AWS-Regionen

Folgendes AWS-Regionen wird für direkte OpenSearch Serviceabfragen in Amazon S3, CloudWatch Logs und Security Lake unterstützt:

Verfügbar AWS-Regionen für Amazon S3

- Asien-Pazifik (Hongkong)
- Asien-Pazifik (Mumbai)
- Asia Pacific (Seoul)
- Asien-Pazifik (Singapur)
- Asien-Pazifik (Sydney)
- Asien-Pazifik (Tokio)
- Canada (Central)
- Europe (Frankfurt)
- Europa (Irland)
- Europa (Stockholm)
- USA Ost (Nord-Virginia)
- USA Ost (Ohio)
- USA West (Oregon)

Verfügbar AWS-Regionen für CloudWatch Protokolle

- Asien-Pazifik (Mumbai)
- Asien-Pazifik (Hongkong)
- Asien-Pazifik (Singapur)
- Asien-Pazifik (Sydney)
- Asien-Pazifik (Tokio)
- Canada (Central)
- Europe (Frankfurt)
- Europa (Irland)
- Europa (Stockholm)
- USA Ost (Nord-Virginia)
- USA Ost (Ohio)
- USA West (Oregon)
- Europa (Paris)

- Europa (London)
- Südamerika (São Paulo)

Verfügbar AWS-Regionen für Security Lake

- Asia Pacific (Mumbai)
- Asien-Pazifik (Singapur)
- Asien-Pazifik (Sydney)
- Asien-Pazifik (Tokio)
- Canada (Central)
- Europe (Frankfurt)
- Europa (Irland)
- Europa (Stockholm)
- USA Ost (Nord-Virginia)
- USA Ost (Ohio)
- USA West (Oregon)
- Europa (Paris)
- Europa (London)
- Südamerika (São Paulo)

Direktes Abfragen von Amazon S3 S3-Daten im Service OpenSearch

Dieser Abschnitt führt Sie durch den Prozess der Erstellung und Konfiguration einer Datenquellenintegration in Amazon OpenSearch Service, sodass Sie Ihre in Amazon S3 gespeicherten Daten effizient abfragen und analysieren können.

Auf den folgenden Seiten erfahren Sie, wie Sie eine Amazon S3 S3-Datenquelle für direkte Abfragen einrichten, sich mit den erforderlichen Voraussetzungen vertraut machen und die step-by-step Verfahren sowohl mit der als auch mit der AWS Management Console OpenSearch Service-API befolgen. Außerdem werden wichtige nächste Schritte behandelt, darunter die Zuordnung von AWS Glue Data Catalog Rollen und die Konfiguration der Zugriffskontrollen in OpenSearch Dashboards.

Themen

- Erstellen einer Amazon S3 S3-Datenquellenintegration in OpenSearch Service
- Konfiguration und Abfrage einer S3-Datenquelle in Dashboards OpenSearch

Erstellen einer Amazon S3 S3-Datenquellenintegration in OpenSearch Service

Sie können eine neue Amazon S3 S3-Direktabfrage-Datenquelle für OpenSearch Service über die AWS Management Console oder die API erstellen. Jede neue Datenquelle verwendet die, um Tabellen AWS Glue Data Catalog zu verwalten, die Amazon S3 S3-Buckets darstellen.

Themen

- Voraussetzungen
- Verfahren
- Nächste Schritte
- Ordnen Sie die Rolle zu AWS Glue Data Catalog
- Weitere Ressourcen

Voraussetzungen

Bevor Sie beginnen, stellen Sie sicher, dass Sie die folgende Dokumentation gelesen haben:

- the section called “Einschränkungen für Amazon S3”
- the section called “Amazon S3 S3-Empfehlungen”
- the section called “Kontingente für Amazon S3”

Bevor Sie eine Datenquelle erstellen können, müssen Sie über die folgenden Ressourcen verfügen AWS-Konto:

- Eine OpenSearch Domäne mit Version 2.13 oder höher. Dies ist die Grundlage für die Einrichtung der Direktabfrageintegration. Anweisungen zur Einrichtung finden Sie unterthe section called “ OpenSearch Dienstdomänen erstellen”.
- Ein oder mehrere S3-Buckets. Sie müssen die Buckets angeben, die Daten enthalten, die Sie abfragen möchten, und einen Bucket, in dem Ihre Abfrage-Checkpoints gespeichert werden sollen.

Anweisungen zum Erstellen eines S3-Buckets finden Sie unter Erstellen eines Buckets im Amazon S3 S3-Benutzerhandbuch.

- (Optional) Eine oder mehrere AWS Glue Tabellen.Um Daten auf Amazon S3 abzufragen, müssen Sie Tabellen eingerichtet haben, die AWS Glue Data Catalog auf die S3-Daten verweisen. Sie müssen die Tabellen mit OpenSearch Query Workbench erstellen. Bestehende Hive-Tabellen sind nicht kompatibel.

  Wenn Sie zum ersten Mal eine Amazon S3 S3-Datenquelle einrichten, müssen Sie eine Admin-Datenquelle erstellen, um all Ihre AWS Glue Data Catalog Tabellen zu konfigurieren. Sie können dies tun, indem Sie OpenSearch out-of-the-box Integrationen installieren oder OpenSearch Query Workbench verwenden, um benutzerdefinierte SQL-Tabellen für erweiterte Anwendungsfälle zu erstellen. Beispiele für das Erstellen von Tabellen für VPC CloudTrail - und AWS WAF-Protokolle finden Sie in der Dokumentation GitHub für VPC,, CloudTrailund. AWS WAF Nachdem Sie Ihre Tabellen erstellt haben, können Sie neue Amazon S3 S3-Datenquellen erstellen und den Zugriff auf eingeschränkte Tabellen einschränken.
- (Optional) Eine manuell erstellte IAM-Rolle.Sie können diese Rolle verwenden, um den Zugriff auf Ihre Datenquelle zu verwalten. Alternativ können Sie OpenSearch Service automatisch eine Rolle mit den erforderlichen Berechtigungen für Sie erstellen lassen. Wenn Sie sich dafür entscheiden, eine manuell erstellte IAM-Rolle zu verwenden, folgen Sie den Anweisungen unterthe section called “Erforderliche Berechtigungen für manuell erstellte IAM-Rollen”.

Verfahren

Sie können eine Datenquelle für direkte Abfragen in einer Domain mit der AWS Management Console oder der OpenSearch Service-API einrichten.

Um eine Datenquelle mit dem einzurichten AWS Management Console

1. Navigieren Sie zur Amazon OpenSearch Service-Konsole unterhttps://console.aws.amazon.com/aos/.
2. Wählen Sie im linken Navigationsbereich die Option Domains aus.
3. Wählen Sie die Domain aus, für die Sie eine neue Datenquelle einrichten möchten. Dadurch wird die Detailseite der Domain geöffnet.
4. Wählen Sie die Registerkarte Verbindungen unter den allgemeinen Domänendetails und suchen Sie den Abschnitt Direkte Abfrage.
5. Wählen Sie Datenquelle konfigurieren aus.

6. Geben Sie einen Namen und eine optionale Beschreibung für Ihre neue Datenquelle ein.
7. Wählen Sie Amazon S3 mit AWS Glue Data Catalog.
8. Wählen Sie unter Einstellungen für den Zugriff auf IAM-Berechtigungen aus, wie der Zugriff verwaltet werden soll.

   a. Gehen Sie folgendermaßen vor, wenn Sie automatisch eine Rolle für diese Datenquelle erstellen möchten:

      i. Wählen Sie Neue Rolle erstellen aus.

      ii. Geben Sie einen Namen für die IAM-Rolle ein.

      iii. Wählen Sie einen oder mehrere S3-Buckets aus, die Daten enthalten, die Sie abfragen möchten.

      iv. Wählen Sie einen Checkpoint-S3-Bucket aus, in dem Abfrage-Checkpoints gespeichert werden sollen.

      v. Wählen Sie eine oder mehrere AWS Glue Datenbanken oder Tabellen aus, um zu definieren, welche Daten abgefragt werden können. Wenn noch keine Tabellen erstellt wurden, gewähren Sie Zugriff auf die Standarddatenbank.

   b. Wenn Sie eine bestehende Rolle verwenden möchten, die Sie selbst verwalten, gehen Sie wie folgt vor:

      i. Wählen Sie Eine vorhandene Rolle verwenden aus.

      ii. Wählen Sie eine bestehende Rolle aus dem Drop-down-Menü aus.

> **Note**
>
> Wenn Sie Ihre eigene Rolle verwenden, müssen Sie sicherstellen, dass sie über alle erforderlichen Berechtigungen verfügt, indem Sie die erforderlichen Richtlinien von der IAM-Konsole aus anhängen. Weitere Informationen finden Sie in der Beispielrichtlinie unter. the section called “Erforderliche Berechtigungen für manuell erstellte IAM-Rollen”

9. Wählen Sie Konfigurieren aus. Dadurch wird der Bildschirm mit den Datenquellendetails mit einer OpenSearch Dashboard-URL geöffnet. Sie können zu dieser URL navigieren, um die nächsten Schritte abzuschließen.

OpenSearch Service-API

Verwenden Sie den AddDataSourceAPI-Vorgang, um eine neue Datenquelle in Ihrer Domain zu erstellen.

```
POST https://es.region.amazonaws.com/2021-01-01/opensearch/domain/domain-name/
dataSource

{
   "DataSourceType": {
        "S3GlueDataCatalog": {
            "RoleArn": "arn:aws:iam::account-id:role/role-name"
        }
    }
   "Description": "data-source-description",
   "Name": "my-data-source"
}
```

Nächste Schritte

Besuchen Sie OpenSearch Dashboards

Nachdem Sie eine Datenquelle erstellt haben, stellt Ihnen OpenSearch Service einen Link zu OpenSearch Dashboards zur Verfügung. Sie können damit die Zugriffskontrolle konfigurieren, Tabellen definieren, out-of-the-box Integrationen installieren und Ihre Daten abfragen.

Weitere Informationen finden Sie unter the section called “Konfiguration einer S3-Datenquelle”.

Ordnen Sie die Rolle zu AWS Glue Data Catalog

Wenn Sie nach dem Erstellen einer Datenquelle eine differenzierte Zugriffskontrolle aktiviert haben, müssen Sie Benutzer ohne Administratorrechte einer IAM-Rolle mit AWS Glue Data Catalog Zugriff zuordnen, um direkte Abfragen ausführen zu können. Gehen Sie wie folgt vor, um manuell eine `glue_access` Back-End-Rolle zu erstellen, die Sie der IAM-Rolle zuordnen können:

> **Note**
>
> Indizes werden für alle Abfragen der Datenquelle verwendet. Ein Benutzer mit Lesezugriff auf den Anforderungsindex für eine bestimmte Datenquelle kann alle Abfragen für diese Datenquelle lesen. Ein Benutzer mit Lesezugriff auf den Ergebnisindex kann Ergebnisse für alle Abfragen dieser Datenquelle lesen.

1. Wählen Sie im Hauptmenü der OpenSearch Dashboards Sicherheit, Rollen und Rollen erstellen aus.
2. Nennen Sie die Rolle glue_access.
3. Wählen Sie für Clusterberechtigungen,`indices:data/write/bulk*`, `indices:data/read/scroll` aus. `indices:data/read/scroll/clear`
4. Geben Sie für Index die folgenden Indizes ein, auf die Sie dem Benutzer mit der Rolle Zugriff gewähren möchten:
   - `.query_execution_request_`*`<name of data source>`*
   - `query_execution_result_`*`<name of data source>`*
   - `.async-query-scheduler`
   - `flint_*`
5. Wählen Sie für Indexberechtigungen die Option aus`indices_all`.
6. Wählen Sie Erstellen aus.
7. Wählen Sie Zugeordnete Benutzer, Mapping verwalten.
8. Fügen Sie unter Backend-Rollen den ARN der AWS Glue Rolle hinzu, für die eine Berechtigung zum Aufrufen Ihrer Domain erforderlich ist.

   ```
   arn:aws:iam::account-id:role/role-name
   ```
9. Wählen Sie Map aus und vergewissern Sie sich, dass die Rolle unter Zugeordnete Benutzer angezeigt wird.

Weitere Informationen zum Zuordnen von Rollen finden Sie unterthe section called “Rollen an Benutzer zuweisen”.

Weitere Ressourcen

Erforderliche Berechtigungen für manuell erstellte IAM-Rollen

Wenn Sie eine Datenquelle für Ihre Domain erstellen, wählen Sie eine IAM-Rolle aus, um den Zugriff auf Ihre Daten zu verwalten. Sie haben hierfür zwei Möglichkeiten:

1. Erstellen Sie automatisch eine neue IAM-Rolle
2. Verwenden Sie eine vorhandene IAM-Rolle, die Sie manuell erstellt haben

Wenn Sie eine manuell erstellte Rolle verwenden, müssen Sie der Rolle die richtigen Berechtigungen zuordnen. Die Berechtigungen müssen den Zugriff auf die spezifische Datenquelle ermöglichen und es dem OpenSearch Service ermöglichen, die Rolle zu übernehmen. Dies ist erforderlich, damit der OpenSearch Dienst sicher auf Ihre Daten zugreifen und mit ihnen interagieren kann.

Die folgende Beispielrichtlinie zeigt die Berechtigungen mit den geringsten Rechten, die zum Erstellen und Verwalten einer Datenquelle erforderlich sind. Wenn Sie über umfassendere Berechtigungen verfügen, wie z. `s3:*` B. die `AdminstratorAccess` Richtlinie, umfassen diese Berechtigungen die Berechtigungen mit den geringsten Rechten in der Beispielrichtlinie.

Ersetzen Sie in der folgenden Beispielrichtlinie die durch Ihre eigenen *`placeholder text`* Informationen.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"HttpActionsForOpenSearchDomain",
         "Effect":"Allow",
         "Action":"es:ESHttp*",
         "Resource":"arn:aws:es:region:account:domain/<domain_name>/*"
      },
      {
         "Sid":"AmazonOpenSearchS3GlueDirectQueryReadAllS3Buckets",
         "Effect":"Allow",
         "Action":[
            "s3:GetObject",
            "s3:GetObjectVersion",
            "s3:ListBucket"
         ],
         "Condition":{
            "StringEquals":{
               "aws:ResourceAccount":"account"
            }
         },
         "Resource":"*"
      },
      {
         "Sid":"AmazonOpenSearchDirectQueryGlueCreateAccess",
         "Effect":"Allow",
```

```
            "Action":[
               "glue:CreateDatabase",
               "glue:CreatePartition",
               "glue:CreateTable",
               "glue:BatchCreatePartition"
            ],
            "Resource":"*"
         },
         {
            "Sid":"AmazonOpenSearchS3GlueDirectQueryModifyAllGlueResources",
            "Effect":"Allow",
            "Action":[
               "glue:DeleteDatabase",
               "glue:DeletePartition",
               "glue:DeleteTable",
               "glue:GetDatabase",
               "glue:GetDatabases",
               "glue:GetPartition",
               "glue:GetPartitions",
               "glue:GetTable",
               "glue:GetTableVersions",
               "glue:GetTables",
               "glue:UpdateDatabase",
               "glue:UpdatePartition",
               "glue:UpdateTable",
               "glue:BatchGetPartition",
               "glue:BatchDeletePartition",
               "glue:BatchDeleteTable"
            ],
            "Resource":[
               "arn:aws:glue:us-east-1:account:table/*",
               "arn:aws:glue:us-east-1:account:database/*",
               "arn:aws:glue:us-east-1:account:catalog",
               "arn:aws:es:region:account:domain/domain_name"
            ],
            "Condition":{
               "StringEquals":{
                  "aws:ResourceAccount":"account"
               }
            }
         },
         {
            "Sid":"ReadAndWriteActionsForS3CheckpointBucket",
            "Effect":"Allow",
```

```
         "Action":[
            "s3:ListMultipartUploadParts",
            "s3:DeleteObject",
            "s3:GetObject",
            "s3:PutObject",
            "s3:GetBucketLocation",
            "s3:ListBucket"
         ],
         "Condition":{
            "StringEquals":{
               "aws:ResourceAccount":"account"
            }
         },
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-bucket",
            "arn:aws:s3:::amzn-s3-demo-bucket/*"
         ]
      }
   ]
}
```

Um Amazon S3 S3-Buckets in verschiedenen Konten zu unterstützen, müssen Sie eine Bedingung in die Amazon S3 S3-Richtlinie aufnehmen und das entsprechende Konto hinzufügen.

Ersetzen Sie im folgenden Beispielzustand die *placeholder text* durch Ihre eigenen Informationen.

```
"Condition": {
               "StringEquals": {
                   "aws:ResourceAccount": "{{accountId}}"
               }
```

Die Rolle muss außerdem über die folgende Vertrauensrichtlinie verfügen, in der die Ziel-ID angegeben ist.

JSON

```
{
    "Version":"2012-10-17",
    "Statement":[
       {
```

```
            "Effect":"Allow",
            "Principal":{
               "Service": "directquery.opensearchservice.amazonaws.com"
            },
            "Action":"sts:AssumeRole"
         }
      ]
}
```

Anweisungen zum Erstellen der Rolle finden Sie unter Erstellen einer Rolle mit benutzerdefinierten Vertrauensrichtlinien.

Wenn Sie in OpenSearch Service eine differenzierte Zugriffskontrolle aktiviert haben, wird automatisch eine neue OpenSearch differenzierte Zugriffssteuerungsrolle für Ihre Datenquelle erstellt. Der Name der neuen detaillierten Zugriffskontrollrolle lautet. `AWS OpenSearchDirectQuery <name of data source>`

Standardmäßig hat die Rolle nur Zugriff auf Datenquellenindizes für direkte Abfragen. Sie können die Rolle zwar so konfigurieren, dass der Zugriff auf Ihre Datenquelle eingeschränkt oder gewährt wird, es wird jedoch empfohlen, den Zugriff dieser Rolle nicht anzupassen. Wenn Sie die Datenquelle löschen, wird diese Rolle gelöscht. Dadurch wird allen anderen Benutzern der Zugriff entzogen, sofern sie der Rolle zugeordnet sind.

Konfiguration und Abfrage einer S3-Datenquelle in Dashboards OpenSearch

Nachdem Sie Ihre Datenquelle erstellt haben, können Sie Sicherheitseinstellungen konfigurieren, Ihre Amazon S3 S3-Tabellen definieren oder eine beschleunigte Datenindizierung einrichten. In diesem Abschnitt werden Sie durch verschiedene Anwendungsfälle mit Ihrer Datenquelle in OpenSearch Dashboards geführt, bevor Sie Ihre Daten abfragen.

Um die folgenden Abschnitte zu konfigurieren, müssen Sie zunächst in OpenSearch Dashboards zu Ihrer Datenquelle navigieren. Wählen Sie in der linken Navigationsleiste unter Verwaltung die Option Datenquellen aus. Wählen Sie unter Datenquellen verwalten den Namen der Datenquelle aus, die Sie in der Konsole erstellt haben.

Erstellen Sie Spark-Tabellen mit Query Workbench

Direkte Abfragen von OpenSearch Service an Amazon S3 verwenden Spark-Tabellen innerhalb von AWS Glue Data Catalog. Sie können Tabellen in der Query Workbench erstellen, ohne die OpenSearch Dashboards verlassen zu müssen.

Um bestehende Datenbanken und Tabellen in Ihrer Datenquelle zu verwalten oder neue Tabellen zu erstellen, für die Sie direkte Abfragen verwenden möchten, wählen Sie Query Workbench aus der linken Navigationsleiste und wählen Sie die Amazon S3 S3-Datenquelle aus der Dropdownliste Datenquelle aus.

Führen Sie die folgende Abfrage aus, um eine Tabelle für in S3 gespeicherte VPC Flow-Protokolle im Parquet-Format einzurichten:

```
CREATE TABLE
datasourcename.gluedatabasename.vpclogstable (version INT, account_id STRING,
 interface_id STRING,
srcaddr STRING, dstaddr STRING, srcport INT, dstport INT, protocol INT, packets
 BIGINT,
bytes BIGINT, start BIGINT, end BIGINT, action STRING, log_status STRING,
`aws-account-id` STRING, `aws-service` STRING, `aws-region` STRING, year STRING,
month STRING, day STRING, hour STRING)

USING parquet PARTITIONED BY (aws-account-id, aws-service, aws-region, year, month,
day, hour)

LOCATION "s3://accountnum-vpcflow/AWSLogs"
```

Führen Sie nach dem Erstellen der Tabelle die folgende Abfrage aus, um sicherzustellen, dass sie mit direkten Abfragen kompatibel ist:

```
MSCK REPAIR TABLE  datasourcename.databasename.vpclogstable
```

Richten Sie Integrationen für beliebte AWS Protokolltypen ein

Sie können in Amazon S3 gespeicherte AWS Protokolltypen in OpenSearch Service integrieren. Verwenden Sie OpenSearch Dashboards, um Integrationen zu installieren, die AWS Glue Data Catalog Tabellen, gespeicherte Abfragen und Dashboards erstellen. Diese Integrationen verwenden indizierte Ansichten, um die Dashboards auf dem neuesten Stand zu halten.

Anweisungen zur Installation einer Integration finden Sie in der Dokumentation unter Installation eines Integrations-Assets. OpenSearch

Wenn Sie eine Integration auswählen, stellen Sie sicher, dass sie über das `S3 Glue` Tag verfügt.

Wenn Sie die Integration einrichten, geben Sie S3 Connection als Verbindungstyp an. Wählen Sie dann die Datenquelle für die Integration, den Amazon S3 S3-Speicherort der Daten, den Checkpoint für die Verwaltung der Beschleunigungsindizierung und die für Ihren Anwendungsfall erforderlichen Ressourcen aus.

> **Note**
>
> Stellen Sie sicher, dass der S3-Bucket für Ihren Checkpoint über Schreibberechtigungen für den Checkpoint-Standort verfügt. Ohne diese Berechtigungen schlagen die Beschleunigungen der Integration fehl.

Einrichten der Zugriffssteuerung

Suchen Sie auf der Detailseite für Ihre Datenquelle den Abschnitt Zugriffskontrollen und wählen Sie Bearbeiten aus. Wenn für die Domain eine differenzierte Zugriffskontrolle aktiviert ist, wählen Sie Eingeschränkt aus und wählen Sie aus, welchen Rollen Sie Zugriff auf die neue Datenquelle gewähren möchten. Sie können auch Nur Administrator wählen, wenn Sie möchten, dass der Administrator nur Zugriff auf die Datenquelle hat.

> **Important**
>
> Indizes werden für alle Abfragen der Datenquelle verwendet. Ein Benutzer mit Lesezugriff auf den Anforderungsindex für eine bestimmte Datenquelle kann alle Abfragen für diese Datenquelle lesen. Ein Benutzer mit Lesezugriff auf den Ergebnisindex kann Ergebnisse für alle Abfragen dieser Datenquelle lesen.

Abfragen von S3-Daten in Discover OpenSearch

Nachdem Sie Ihre Tabellen eingerichtet und die gewünschte optionale Abfragebeschleunigung konfiguriert haben, können Sie mit der Analyse Ihrer Daten beginnen. Um Ihre Daten abzufragen, wählen Sie Ihre Datenquelle aus dem Drop-down-Menü aus. Wenn Sie Amazon S3 und OpenSearch Dashboards verwenden, gehen Sie zu Discover und wählen Sie den Namen der Datenquelle aus.

Wenn Sie einen Skipping-Index verwenden oder noch keinen Index erstellt haben, können Sie SQL oder PPL verwenden, um Ihre Daten abzufragen. Wenn Sie eine materialisierte Ansicht oder einen Deckindex konfiguriert haben, verfügen Sie bereits über einen Index und können die Dashboards Query Language (DQL) in allen Dashboards verwenden. Sie können PPL auch mit dem Observability-Plugin und SQL mit dem Query Workbench-Plugin verwenden. Derzeit unterstützen nur die Observability- und Query Workbench-Plugins PPL und SQL. Informationen zum Abfragen von Daten mithilfe der OpenSearch Service-API finden Sie in der Async-API-Dokumentation.

> **Note**
>
> Nicht alle SQL- und PPL-Anweisungen, Befehle und Funktionen werden unterstützt. Eine Liste der unterstützten Befehle finden Sie unterthe section called “Unterstützte SQL- und PPL-Befehle”.
> Wenn Sie eine materialisierte Ansicht oder einen umfassenden Index erstellt haben, können Sie Ihre Daten mithilfe von DQL abfragen, sofern Sie sie darin indexiert haben.

Fehlerbehebung

Es kann vorkommen, dass die Ergebnisse nicht wie erwartet zurückgegeben werden. Wenn Sie Probleme haben, stellen Sie sicher, dass Sie die befolgenthe section called “Empfehlungen”.

Direktes Abfragen von Amazon CloudWatch Logs-Daten im Service OpenSearch

Dieser Abschnitt führt Sie durch den Prozess der Erstellung und Konfiguration einer Datenquellenintegration in Amazon OpenSearch Service, sodass Sie Ihre in CloudWatch Logs gespeicherten Daten effizient abfragen und analysieren können.

Auf den folgenden Seiten erfahren Sie, wie Sie eine CloudWatch Logs-Datenquelle für direkte Abfragen einrichten, sich mit den erforderlichen Voraussetzungen vertraut machen und die step-by-step Verfahren mithilfe von befolgen. AWS Management Console

Themen

- Eine Amazon CloudWatch Logs-Datenquellenintegration in OpenSearch Service erstellen
- Konfiguration und Abfrage einer CloudWatch Logs-Datenquelle in Dashboards OpenSearch

Eine Amazon CloudWatch Logs-Datenquellenintegration in OpenSearch Service erstellen

Wenn Sie Amazon OpenSearch Serverless für Ihre Observability-Anforderungen verwenden, können Sie jetzt Ihre CloudWatch Amazon-Logs analysieren, ohne die Daten kopieren oder in Service aufnehmen zu müssen. OpenSearch Diese Funktion nutzt direkte Abfragen zum Abfragen von Daten, ähnlich der Analyse von Daten in Amazon S3 von OpenSearch Service. Sie können beginnen, indem Sie in der AWS Management Console eine neue verbundene Datenquelle erstellen.

Sie können eine neue Datenquelle zur Analyse von CloudWatch Logs-Daten erstellen, ohne Amazon OpenSearch Serverless für die direkte Abfrage von Betriebsprotokollen in CloudWatch Logs einrichten zu müssen. Auf diese Weise können Sie Ihre abgerufenen Betriebsdaten analysieren, die sich außerhalb von OpenSearch Service befinden. Durch Abfragen in OpenSearch Service und CloudWatch Logs können Sie mit der Analyse von Protokollen in CloudWatch Logs beginnen und dann zur Überwachung der Datenquellen zurückkehren, OpenSearch ohne zwischen Tools wechseln zu müssen.

Um diese Funktion nutzen zu können, erstellen Sie über die AWS Management Console eine CloudWatch Logs-Direktabfrage-Datenquelle für OpenSearch Service.

Themen

- Voraussetzungen
- Verfahren
- Nächste Schritte
- Weitere Ressourcen

Voraussetzungen

Bevor Sie beginnen, stellen Sie sicher, dass Sie die folgende Dokumentation gelesen haben:

- the section called “Einschränkungen für Amazon CloudWatch Logs”
- the section called “CloudWatch Protokolliert Empfehlungen”
- the section called “Kontingente für Protokolle CloudWatch ”

Bevor Sie eine Datenquelle erstellen können, müssen Sie über die folgenden Ressourcen verfügen AWS-Konto:

- Aktivieren Sie CloudWatch Protokolle. Konfigurieren Sie CloudWatch Logs so, dass Logs auf derselben Ressource gesammelt AWS-Konto werden wie Ihre OpenSearch Ressource. Anweisungen finden Sie unter Erste Schritte mit CloudWatch Logs im Amazon CloudWatch Logs-Benutzerhandbuch.
- Eine oder mehrere CloudWatch Protokollgruppen.Sie können die Protokollgruppen angeben, die Daten enthalten, die Sie abfragen möchten. Anweisungen zum Erstellen einer Protokollgruppe finden Sie unter Erstellen einer Protokollgruppe in CloudWatch Logs im Amazon CloudWatch Logs-Benutzerhandbuch.
- (Optional) Eine manuell erstellte IAM-Rolle.Sie können diese Rolle verwenden, um den Zugriff auf Ihre Datenquelle zu verwalten. Alternativ können Sie OpenSearch Service automatisch eine Rolle mit den erforderlichen Berechtigungen für Sie erstellen lassen. Wenn Sie sich dafür entscheiden, eine manuell erstellte IAM-Rolle zu verwenden, folgen Sie den Anweisungen unterthe section called “Erforderliche Berechtigungen für manuell erstellte IAM-Rollen”.

Verfahren

Mit dem können Sie eine Abfragedatenquelle auf Sammlungsebene einrichten. AWS Management Console

Um eine Datenquelle auf Sammlungsebene einzurichten, verwenden Sie AWS Management Console

1. Navigieren Sie zur Amazon OpenSearch Service-Konsole unterhttps://console.aws.amazon.com/aos/.
2. Gehen Sie im linken Navigationsbereich zu Central Management und wählen Sie Verbundene Datenquellen aus.
3. Wählen Sie Connect aus.
4. Wählen Sie CloudWatchals Datenquellentyp aus.
5. Wählen Sie Weiter aus.
6. Geben Sie unter Datenverbindungsdetails einen Namen und eine optionale Beschreibung ein.
7. Wählen Sie unter IAM-Rollen aus, wie der Zugriff auf die Protokollgruppen verwaltet werden soll.

    a. Gehen Sie folgendermaßen vor, wenn Sie automatisch eine Rolle für diese Datenquelle erstellen möchten:

        i. Wählen Sie Neue Rolle erstellen aus.

        ii. Geben Sie einen Namen für die IAM-Rolle ein.

iii. Wählen Sie eine oder mehrere Protokollgruppen aus, um zu definieren, welche Daten abgefragt werden können.

b. Wenn Sie eine bestehende Rolle verwenden möchten, die Sie selbst verwalten, gehen Sie wie folgt vor:

i. Wählen Sie Eine vorhandene Rolle verwenden aus.

ii. Wählen Sie eine bestehende Rolle aus dem Drop-down-Menü aus.

> **Note**
>
> Wenn Sie Ihre eigene Rolle verwenden, müssen Sie sicherstellen, dass sie über alle erforderlichen Berechtigungen verfügt, indem Sie die erforderlichen Richtlinien von der IAM-Konsole aus anhängen. Weitere Informationen finden Sie unter the section called “Erforderliche Berechtigungen für manuell erstellte IAM-Rollen”.

8. (Optional) Fügen Sie Ihrer Datenquelle unter Tags Tags hinzu.
9. Wählen Sie Weiter aus.
10. Wählen Sie unter Einrichten aus OpenSearch, wie die Einrichtung erfolgen soll OpenSearch.

a. Verwenden Sie die Standardeinstellungen:

- Überprüfen Sie die standardmäßigen Ressourcennamen und Datenaufbewahrungseinstellungen. Wir empfehlen Ihnen, benutzerdefinierte Namen zu verwenden.

  Wenn Sie die Standardeinstellungen verwenden, werden ohne zusätzliche Kosten eine neue OpenSearch Anwendung und ein neuer Essentials-Arbeitsbereich für Sie erstellt. OpenSearch ermöglicht es Ihnen, mehrere Datenquellen zu analysieren. Es umfasst Arbeitsbereiche, die maßgeschneiderte Erlebnisse für beliebte Anwendungsfälle bieten. Workspaces unterstützen die Zugriffskontrolle, sodass Sie private Bereiche für Ihre Anwendungsfälle einrichten und diese nur mit Ihren Mitarbeitern teilen können.

b. Verwenden Sie benutzerdefinierte Einstellungen:

i. Wählen Sie Anpassen aus.

ii. Bearbeiten Sie den Namen der Sammlung und die Einstellungen für die Datenspeicherung nach Bedarf.

iii. Wählen Sie die OpenSearch Anwendung und den Workspace aus, die Sie verwenden möchten.

11. Wählen Sie Weiter aus.
12. Überprüfen Sie Ihre Auswahl und wählen Sie Bearbeiten, falls Sie Änderungen vornehmen müssen.
13. Wählen Sie Connect, um die Datenquelle einzurichten. Bleiben Sie auf dieser Seite, während Ihre Datenquelle erstellt wird. Wenn sie fertig ist, werden Sie zur Seite mit den Datenquellendetails weitergeleitet.

Nächste Schritte

Besuchen Sie OpenSearch Dashboards

Nachdem Sie eine Datenquelle erstellt haben, stellt Ihnen OpenSearch Service eine OpenSearch Dashboard-URL zur Verfügung. Sie verwenden diese, um die Zugriffskontrolle zu konfigurieren, Tabellen zu definieren, protokollbasierte Dashboards für gängige Protokolltypen einzurichten und Ihre Daten mit SQL oder PPL abzufragen.

Weitere Informationen finden Sie unter the section called “Konfiguration einer CloudWatch Logs-Datenquelle”.

Weitere Ressourcen

Erforderliche Berechtigungen für manuell erstellte IAM-Rollen

Beim Erstellen einer Datenquelle wählen Sie eine IAM-Rolle aus, um den Zugriff auf Ihre Daten zu verwalten. Sie haben hierfür zwei Möglichkeiten:

1. Erstellen Sie automatisch eine neue IAM-Rolle
2. Verwenden Sie eine vorhandene IAM-Rolle, die Sie manuell erstellt haben

Wenn Sie eine manuell erstellte Rolle verwenden, müssen Sie der Rolle die richtigen Berechtigungen zuordnen. Die Berechtigungen müssen den Zugriff auf die spezifische Datenquelle ermöglichen und es dem OpenSearch Service ermöglichen, die Rolle zu übernehmen. Dies ist erforderlich, damit der OpenSearch Dienst sicher auf Ihre Daten zugreifen und mit ihnen interagieren kann.

Die folgende Beispielrichtlinie zeigt die Berechtigungen mit den geringsten Rechten, die zum Erstellen und Verwalten einer Datenquelle erforderlich sind. Wenn Sie über umfassendere

Berechtigungen verfügen, wie z. `logs:*` B. die `AdminstratorAccess` Richtlinie, umfassen diese Berechtigungen die Berechtigungen mit den geringsten Rechten in der Beispielrichtlinie.

Ersetzen Sie in der folgenden Beispielrichtlinie die durch Ihre eigenen *`placeholder text`* Informationen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonOpenSearchDirectQueryAllLogsAccess",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeLogGroups",
                "logs:StartQuery",
                "logs:GetLogGroupFields"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "accountId"
                }
            },
            "Resource": [
                "arn:aws:logs:region:accountId:log-group:*"
            ]
        }
    ]
}

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonOpenSearchDirectQueryServerlessAccess",
            "Effect": "Allow",
            "Action": [
                "aoss:APIAccessAll",
                "aoss:DashboardsAccessAll"
            ],
            "Resource": [
                "arn:aws:aoss:region:accountId:collection/ARN/*",
                "arn:aws:aoss:region:accountId:collection/ARN"
            ]
```

```
        }
    ]
}
```

Die Rolle muss außerdem über die folgende Vertrauensrichtlinie verfügen, in der die Ziel-ID angegeben ist.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "TrustPolicyForAmazonOpenSearchDirectQueryService",
            "Effect": "Allow",
            "Principal": {
                "Service": "directquery.opensearchservice.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn":
 "arn:aws:opensearch:region:accountId:datasource/rolename"
                }
            }
        }
    ]
}
```

Anweisungen zum Erstellen der Rolle finden Sie unter Erstellen einer Rolle mit benutzerdefinierten Vertrauensrichtlinien.

Standardmäßig hat die Rolle nur Zugriff auf Datenquellenindizes für direkte Abfragen. Sie können die Rolle zwar so konfigurieren, dass der Zugriff auf Ihre Datenquelle eingeschränkt oder gewährt wird, es wird jedoch empfohlen, den Zugriff dieser Rolle nicht anzupassen. Wenn Sie die Datenquelle löschen, wird diese Rolle gelöscht. Dadurch wird allen anderen Benutzern der Zugriff entzogen, sofern sie der Rolle zugeordnet sind.

Konfiguration und Abfrage einer CloudWatch Logs-Datenquelle in Dashboards OpenSearch

Nachdem Sie Ihre Datenquelle erstellt haben, können Sie mit den Dashboards beginnen. OpenSearch In diesem Abschnitt werden Sie durch verschiedene Anwendungsfälle mit Ihrer Datenquelle in OpenSearch Dashboards geführt.

Fragen Sie Loggruppen von der Discover-Seite aus ab

Auf der OpenSearch Discover-Seite können Sie die neue Direktabfrage-Datenquelle verwenden, die Sie konfiguriert haben, um Ihre CloudWatch Logs-Protokollgruppen abzufragen. Wählen Sie dazu „Protokolle durchsuchen“ und verwenden Sie dann die Suchleiste, um Ihre Abfrage mithilfe von SQL oder PPL zu erstellen. Sie können die von Ihren Protokollgruppen zurückgegebenen Daten filtern, sortieren und visualisieren. Informationen darüber, welche Anweisungen, Befehle und Einschränkungen für die CloudWatch Logs-Integration unterstützt werden, finden Sie unterthe section called “Unterstützte SQL- und PPL-Befehle”.

Erstellen Sie eine Dashboard-Ansicht für Ihre Datenquelle

Wenn Sie OpenSearch Service verwenden, können Sie beliebte AWS Protokolltypen mithilfe von vorgefertigten Dashboard-Vorlagen schnell analysieren. Für CloudWatch Logs gibt es Vorlagen für VPC- CloudTrail und WAF-Logs. Mit diesen Vorlagen können Sie schnell ein Dashboard erstellen, das auf Ihre spezifischen Daten zugeschnitten ist. Sie enthalten Dashboards, die auf diesen speziellen Protokolltyp zugeschnitten sind. Auf diese Weise können Sie schnell mit der Analyse dieser beliebten AWS Protokollquellen beginnen, ohne alles von Grund auf neu erstellen zu müssen.

> **Note**
>
> Dashboards verwenden indizierte Ansichten, die Daten aus CloudWatch Protokollen mithilfe von OpenSearch Recheneinheiten (OCUs) für direkte Abfragen sowie serverlose IndexierungOCUs, Suche und Speicherung von Sammlungen aufnehmen. OCUs

Gehen Sie wie folgt vor, um mithilfe einer dieser vorgefertigten Vorlagen ein Dashboard zu erstellen, sodass Sie sofort mit der Erkundung und Analyse Ihrer Daten beginnen können.

Um eine Dashboard-Ansicht zu erstellen

1. Navigieren Sie zur Amazon OpenSearch Service-Konsole unterhttps://console.aws.amazon.com/aos/.
2. Wählen Sie im linken Navigationsbereich Zentrale Verwaltung und dann Verbundene Datenquellen aus.
3. Wählen Sie die Datenquelle aus, um die Detailseite zu öffnen.
4. Klicken Sie auf Dashboard erstellen.
5. Wählen Sie aus, welche Art von Dashboard Sie erstellen möchten.
6. Geben Sie einen Namen für Ihr Dashboard ein.
7. Geben Sie eine optionale Beschreibung für Ihr Dashboard ein.
8. Wählen Sie eine oder mehrere Protokollgruppen aus, die Sie auf Ihrem Dashboard anzeigen möchten.
9. Wählen Sie aus, wie oft Sie die Daten in Ihrem Dashboard aktualisieren möchten.
10. Wählen Sie aus, welchen OpenSearch Workspace Sie verwenden möchten.
    a. Um einen neuen Workspace zu erstellen, wähle Neuen Workspace erstellen und gib einen Namen ein.
    b. Um einen vorhandenen Workspace zu verwenden, wähle Bestehenden Workspace auswählen aus.
11. Klicken Sie auf Dashboard erstellen.

Abfragen von CloudWatch Protokolldaten in Discover OpenSearch

Um Ihre Daten abzufragen, wählen Sie Ihre Datenquelle aus dem Drop-down-Menü aus. Wenn Sie CloudWatch Logs verwenden, navigieren Sie in Ihrem Essentials-Arbeitsbereich zu Discover und beginnen Sie, Daten mit OpenSearch SQL oder Piped Processing Language (PPL) abzufragen. Eine Liste der unterstützten Befehle finden Sie unter. the section called “Unterstützte SQL- und PPL-Befehle”

> **Note**
>
> Wenn Sie eine materialisierte Ansicht erstellt haben, können Sie Ihre Daten mithilfe von DQL abfragen, sofern Sie sie darin indexiert haben.

Fehlerbehebung

Es kann vorkommen, dass die Ergebnisse nicht wie erwartet zurückgegeben werden. Wenn Sie Probleme haben, stellen Sie sicher, dass Sie die befolgenthe section called “Empfehlungen”.

Direktes Abfragen von Amazon Security Lake-Daten im Service OpenSearch

Dieser Abschnitt führt Sie durch den Prozess der Erstellung und Konfiguration einer Datenquellenintegration in Amazon OpenSearch Service, sodass Sie Ihre in Security Lake gespeicherten Daten effizient abfragen und analysieren können.

Auf den folgenden Seiten erfahren Sie, wie Sie eine Security Lake-Datenquelle für direkte Abfragen einrichten, sich mit den erforderlichen Voraussetzungen vertraut machen und die step-by-step Verfahren mithilfe von befolgen. AWS Management Console

Themen

- Erstellen einer Amazon Security Lake-Datenquellenintegration in OpenSearch Service
- Konfiguration und Abfrage einer Security Lake-Datenquelle in Dashboards OpenSearch

Erstellen einer Amazon Security Lake-Datenquellenintegration in OpenSearch Service

Sie können Amazon OpenSearch Serverless verwenden, um Sicherheitsdaten direkt in Amazon Security Lake abzufragen. Zu diesem Zweck erstellen Sie eine Datenquelle, mit der Sie OpenSearch Zero-ETL-Funktionen für Security Lake-Daten verwenden können. Wenn Sie eine Datenquelle erstellen, können Sie die in Security Lake gespeicherten Daten direkt durchsuchen, Erkenntnisse daraus gewinnen und sie analysieren. Sie können Ihre Abfrageleistung beschleunigen und mithilfe der On-Demand-Indizierung erweiterte OpenSearch Analysen für ausgewählte Security Lake-Datensätze verwenden.

Themen

- Voraussetzungen
- Verfahren
- Nächste Schritte

- Weitere Ressourcen

Voraussetzungen

Bevor Sie beginnen, stellen Sie sicher, dass Sie die folgende Dokumentation gelesen haben:

- the section called “Einschränkungen für Amazon Security Lake”
- the section called “Empfehlungen von Security Lake”
- the section called “Kontingente für Security Lake”

Bevor Sie eine Datenquelle erstellen können, führen Sie die folgenden Aktionen in Security Lake durch:

- Aktivieren Sie Security Lake. Konfigurieren Sie Security Lake so, dass es Protokolle auf derselben Ressource sammelt AWS-Region wie Ihre OpenSearch Ressource. Anweisungen finden Sie unter Erste Schritte mit Amazon Security Lake im Amazon Security Lake-Benutzerhandbuch.
- Richten Sie Security Lake-Berechtigungen ein. Vergewissern Sie sich, dass Sie die mit dem Dienst verknüpften Rollenberechtigungen für die Ressourcenverwaltung akzeptiert haben und dass in der Konsole auf der Seite Probleme keine Probleme angezeigt werden. Weitere Informationen finden Sie unter Servicebezogene Rolle für Security Lake im Amazon Security Lake-Benutzerhandbuch.
- Teilen Sie Security Lake-Datenquellen. Wenn Sie über dasselbe Konto wie Security Lake zugreifen, stellen Sie sicher, dass OpenSearch in der Security Lake-Konsole keine Meldung zur Registrierung Ihrer Security Lake-Buckets bei Lake Formation angezeigt wird. Für den kontoübergreifenden OpenSearch Zugriff richten Sie in der Security Lake-Konsole einen Abonnenten für Lake Formation Query ein. Verwenden Sie das Ihrer OpenSearch Ressource zugeordnete Konto als Abonnent. Weitere Informationen finden Sie unter Abonnentenverwaltung in Security Lake im Amazon Security Lake-Benutzerhandbuch.

Darüber hinaus müssen Sie über die folgenden Ressourcen verfügen AWS-Konto:

- (Optional) Eine manuell erstellte IAM-Rolle. Sie können diese Rolle verwenden, um den Zugriff auf Ihre Datenquelle zu verwalten. Alternativ können Sie OpenSearch Service automatisch eine Rolle mit den erforderlichen Berechtigungen für Sie erstellen lassen. Wenn Sie sich dafür entscheiden, eine manuell erstellte IAM-Rolle zu verwenden, folgen Sie den Anweisungen unterthe section called “Erforderliche Berechtigungen für manuell erstellte IAM-Rollen”.

Verfahren

Sie können eine Datenquelle einrichten, um von der aus eine Verbindung mit einer Security Lake-Datenbank herzustellen. AWS Management Console

Um eine Datenquelle mit dem einzurichten AWS Management Console

1. Navigieren Sie zur Amazon OpenSearch Service-Konsole unterhttps://console.aws.amazon.com/aos/.
2. Gehen Sie im linken Navigationsbereich zu Central Management und wählen Sie Verbundene Datenquellen aus.
3. Wählen Sie Connect aus.
4. Wählen Sie Security Lake als Datenquellentyp aus.
5. Wählen Sie Weiter aus.
6. Geben Sie unter Datenverbindungsdetails einen Namen und eine optionale Beschreibung ein.
7. Wählen Sie unter Einstellungen für den Zugriff auf IAM-Berechtigungen aus, wie der Zugriff auf Ihre Datenquelle verwaltet werden soll.

   a. Gehen Sie folgendermaßen vor, wenn Sie automatisch eine Rolle für diese Datenquelle erstellen möchten:

      i. Wählen Sie Neue Rolle erstellen aus.

      ii. Geben Sie einen Namen für die IAM-Rolle ein.

      iii. Wählen Sie eine oder mehrere AWS Glue Tabellen aus, um zu definieren, welche Daten abgefragt werden können.

   b. Wenn Sie eine bestehende Rolle verwenden möchten, die Sie selbst verwalten, gehen Sie wie folgt vor:

      i. Wählen Sie Eine vorhandene Rolle verwenden aus.

      ii. Wählen Sie eine bestehende Rolle aus dem Drop-down-Menü aus.

> **Note**
>
> Wenn Sie Ihre eigene Rolle verwenden, müssen Sie sicherstellen, dass sie über alle erforderlichen Berechtigungen verfügt, indem Sie die erforderlichen Richtlinien von der

IAM-Konsole aus anhängen. Weitere Informationen finden Sie unter the section called “Erforderliche Berechtigungen für manuell erstellte IAM-Rollen”.

8. (Optional) Fügen Sie Ihrer Datenquelle unter Tags Tags hinzu.
9. Wählen Sie Weiter aus.
10. Wählen Sie unter Einrichten aus OpenSearch, wie die Einrichtung erfolgen soll OpenSearch.

    - Überprüfen Sie die standardmäßigen Ressourcennamen und Datenaufbewahrungseinstellungen.

      Wenn Sie die Standardeinstellungen verwenden, werden ohne zusätzliche Kosten eine neue OpenSearch Anwendung und ein neuer Essentials-Arbeitsbereich für Sie erstellt. OpenSearch ermöglicht es Ihnen, mehrere Datenquellen zu analysieren. Es umfasst Arbeitsbereiche, die maßgeschneiderte Erlebnisse für beliebte Anwendungsfälle bieten. Workspaces unterstützen die Zugriffskontrolle, sodass Sie private Bereiche für Ihre Anwendungsfälle einrichten und diese nur mit Ihren Mitarbeitern teilen können.

11. Verwenden Sie benutzerdefinierte Einstellungen:

    a. Wählen Sie Anpassen aus.
    b. Bearbeiten Sie den Namen der Sammlung und die Einstellungen für die Datenspeicherung nach Bedarf.
    c. Wählen Sie die OpenSearch Anwendung und den Workspace aus, die Sie verwenden möchten.

12. Wählen Sie Weiter aus.
13. Überprüfen Sie Ihre Auswahl und wählen Sie Bearbeiten, falls Sie Änderungen vornehmen müssen.
14. Wählen Sie Connect, um die Datenquelle einzurichten. Bleiben Sie auf dieser Seite, während Ihre Datenquelle erstellt wird. Wenn sie fertig ist, werden Sie zur Seite mit den Datenquellendetails weitergeleitet.

Nächste Schritte

Besuchen Sie OpenSearch Dashboards und erstellen Sie ein Dashboard

Nachdem Sie eine Datenquelle erstellt haben, stellt Ihnen OpenSearch Service eine OpenSearch Dashboard-URL zur Verfügung. Sie verwenden diese, um Ihre Daten mit SQL oder PPL abzufragen.

Die Security Lake-Integration enthält vorkonfigurierte Abfragevorlagen für SQL und PPL, mit denen Sie mit der Analyse Ihrer Protokolle beginnen können.

Weitere Informationen finden Sie unter the section called “Konfiguration einer Security Lake-Datenquelle”.

Weitere Ressourcen

Erforderliche Berechtigungen für manuell erstellte IAM-Rollen

Beim Erstellen einer Datenquelle wählen Sie eine IAM-Rolle aus, um den Zugriff auf Ihre Daten zu verwalten. Sie haben hierfür zwei Möglichkeiten:

1. Erstellen Sie automatisch eine neue IAM-Rolle
2. Verwenden Sie eine vorhandene IAM-Rolle, die Sie manuell erstellt haben

Wenn Sie eine manuell erstellte Rolle verwenden, müssen Sie der Rolle die richtigen Berechtigungen zuordnen. Die Berechtigungen müssen den Zugriff auf die spezifische Datenquelle ermöglichen und es dem OpenSearch Service ermöglichen, die Rolle zu übernehmen. Dies ist erforderlich, damit der OpenSearch Dienst sicher auf Ihre Daten zugreifen und mit ihnen interagieren kann.

Die folgende Beispielrichtlinie zeigt die Berechtigungen mit den geringsten Rechten, die zum Erstellen und Verwalten einer Datenquelle erforderlich sind. Wenn Sie über umfassendere Berechtigungen verfügen, wie z. B. die `AdminstratorAccess` Richtlinie, umfassen diese Berechtigungen die Berechtigungen mit den geringsten Rechten in der Beispielrichtlinie.

Ersetzen Sie in der folgenden Beispielrichtlinie die durch Ihre eigenen *`placeholder text`* Informationen.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonOpenSearchDirectQueryServerlessAccess",
            "Effect": "Allow",
            "Action": [
                "aoss:APIAccessAll",
                "aoss:DashboardsAccessAll"
```

```
            ],
            "Resource": "arn:aws:aoss:region:account:collection/collectionname/*"
        },
        {
            "Sid": "AmazonOpenSearchDirectQueryGlueAccess",
            "Effect": "Allow",
            "Action": [
                "glue:GetDatabase",
                "glue:GetDatabases",
                "glue:GetPartition",
                "glue:GetPartitions",
                "glue:GetTable",
                "glue:GetTableVersions",
                "glue:GetTables",
                "glue:SearchTables",
                "glue:BatchGetPartition"
            ],
            "Resource": [
                "arn:aws:glue:region:account:table/databasename/*",
                "arn:aws:glue:region:account:database/databasename",
                "arn:aws:glue:region:account:catalog",
                "arn:aws:glue:region:account:database/default"
            ]
        },
        {
            "Sid": "AmazonOpenSearchDirectQueryLakeFormationAccess",
            "Effect": "Allow",
            "Action": [
                "lakeformation:GetDataAccess"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

Die Rolle muss außerdem über die folgende Vertrauensrichtlinie verfügen, in der die Ziel-ID angegeben ist.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "directquery.opensearchservice.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Anweisungen zum Erstellen der Rolle finden Sie unter Erstellen einer Rolle mit benutzerdefinierten Vertrauensrichtlinien.

Standardmäßig hat die Rolle nur Zugriff auf Datenquellenindizes für direkte Abfragen. Sie können die Rolle zwar so konfigurieren, dass der Zugriff auf Ihre Datenquelle eingeschränkt oder gewährt wird, es wird jedoch empfohlen, den Zugriff dieser Rolle nicht anzupassen. Wenn Sie die Datenquelle löschen, wird diese Rolle gelöscht. Dadurch wird allen anderen Benutzern der Zugriff entzogen, sofern sie der Rolle zugeordnet sind.

Abfragen von Security Lake-Daten, die mit einem vom Kunden verwalteten Schlüssel verschlüsselt sind

Wenn der mit der Datenverbindung verknüpfte Security Lake-Bucket mit serverseitiger Verschlüsselung verschlüsselt ist und ein Kunde verwaltet wird AWS KMS key, müssen Sie die LakeFormation Servicerolle zur Schlüsselrichtlinie hinzufügen. Dadurch kann der Service auf die Daten für Ihre Abfragen zugreifen und diese lesen.

Ersetzen Sie in der folgenden Beispielrichtlinie die *placeholder text* durch Ihre eigenen Informationen.

```
{
    "Sid": "Allow LakeFormation to access the key",
    "Effect": "Allow",
    "Principal": {
```

```
        "AWS": "arn:aws:iam::account:role/aws-service-role/lakeformation.amazonaws.com/
AWSServiceRoleForLakeFormationDataAccess"
    },
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource": "*"
}
```

Konfiguration und Abfrage einer Security Lake-Datenquelle in Dashboards OpenSearch

Nachdem Sie Ihre Datenquelle erstellt haben, können Sie sie in OpenSearch Dashboards einrichten.

In diesem Abschnitt werden Sie durch verschiedene Anwendungsfälle mit Ihrer Datenquelle in OpenSearch Dashboards geführt, bevor Sie Ihre Daten abfragen. Um zu beginnen, müssen Sie in OpenSearch Dashboards zu Ihrer Datenquelle navigieren. Wählen Sie im Menü auf der linken Seite unter Verwaltung die Option Datenquellen aus. Wählen Sie dann den Namen der Datenquelle aus, die Sie zuvor in der OpenSearch Servicekonsole erstellt haben.

Fragen Sie Security Lake-Tabellen in Discover ab

Wenn Sie Tabellen auf der Grundlage Ihrer Security Lake-Protokolle erstellt haben, können Sie diese Tabellen jetzt direkt von OpenSearch Discover aus abfragen. Auf diese Weise können Sie direkt über die vertraute Discover-Oberfläche nahtlos auf die in Security Lake gespeicherten Daten zugreifen und diese analysieren. Indem Sie Security Lake direkt von Discover aus abfragen, müssen Sie die Daten nicht manuell extrahieren, transformieren und in einen separaten Suchindex laden. Damit Sie schnell mit der Analyse Ihrer Logs beginnen können, enthält Discover eine Reihe von gespeicherten PPL- und SQL-Abfragen.

Wählen Sie zunächst die Datenquelle aus, die Sie konfiguriert haben. Wählen Sie die zugehörige Datenbank und Tabelle aus, die Sie abfragen möchten, und verwenden Sie dann die Suchleiste, um Abfragen für Ihre Tabellen zu schreiben. Informationen darüber, welche Anweisungen, Befehle und Einschränkungen für die Security Lake-Integration unterstützt werden, finden Sie unterthe section called “Unterstützte SQL- und PPL-Befehle”.

Um die Vorteile der vorgefertigten Abfragen zu nutzen, die für Security Lake verfügbar sind, gehen Sie zu... wählen Sie oben rechts in Discover die Option Abfrage öffnen und dann Vorlagen aus. Es gibt viele vorgefertigte Abfragen für Protokollquellen, die in Security Lake unterstützt werden. Suchen Sie nach den Vorlagen, die Ihrem Anwendungsfall entsprechen, kopieren Sie die zu verwendende Abfrage in die Suchleiste und ersetzen Sie vordefinierte Felder (wie Region und Aktion) durch Ihre eigenen Informationen.

Beschleunigen Sie Daten aus Discover

Um die Leistung zu verbessern und nachfolgende Abfragen und Analysen zu beschleunigen OpenSearch, können Sie die Ergebnisse Ihrer Abfrage aus Discover in eine OpenSearch indizierte Ansicht aufnehmen.

Um eine indizierte Ansicht zu erstellen

1. Wählen Sie in Discover die Option Indizierte Ansicht erstellen aus.
2. Geben Sie im Abfrage-Editor die gewünschte Abfrage ein. Sie können hier eine neue Abfrage erstellen oder eine bestehende aus Ihren vorherigen Suchanfragen verwenden.
3. Geben Sie einen Namen für Ihre neue indizierte Ansicht ein. Wählen Sie einen aussagekräftigen Namen, anhand dessen Sie die Ansicht später leichter identifizieren können.
4. Konfigurieren Sie die Datenaufbewahrungseinstellungen für Ihre indizierte Ansicht. Sie können angeben, wie lange die Daten im Index aufbewahrt werden sollen, sodass Sie ein ausgewogenes Verhältnis zwischen Leistung und Speicherkosten herstellen können.
5. Erstellen Sie die indizierte Ansicht. Nach der Erstellung steht Ihre indizierte Ansicht für schnellere Abfragen und Analysen zur Verfügung.

Wenn Sie zuvor indizierte Ansichten erstellt haben, können Sie über Discover darauf zugreifen.

Um eine bestehende Indexansicht zu verwenden

1. Wählen Sie in Discover die Option Indexierte Ansicht auswählen aus, um eine Liste Ihrer vorhandenen indizierten Ansichten für Security Lake anzuzeigen.
2. Wählen Sie die indizierte Ansicht aus, die Sie verwenden möchten. Dadurch wird die Ansicht auf Ihre aktuelle Abfrage angewendet, wodurch der Datenabruf und die Datenanalyse möglicherweise erheblich beschleunigt werden.

Erstellen Sie eine Dashboard-Ansicht für Ihre Datenquelle

Wenn Sie OpenSearch Service verwenden, können Sie beliebte AWS Protokolltypen mithilfe vorgefertigter Dashboard-Vorlagen analysieren. Für Security Lake gibt es Vorlagen für VPC-CloudTrail und WAF-Logs. Mit diesen Vorlagen können Sie ein Dashboard erstellen, das auf Ihre spezifischen Daten zugeschnitten ist. Sie enthalten vorgefertigte Abfragen und Dashboards, die auf diesen speziellen Protokolltyp zugeschnitten sind. Auf diese Weise können Sie schnell mit der Analyse dieser beliebten AWS Protokollquellen beginnen, ohne alles von Grund auf neu erstellen zu müssen.

> **Note**
>
> Dashboards verwenden indizierte Ansichten, die Daten aus Security Lake aufnehmen und zur direkten Abfrage und Erfassung von Daten beitragen.

Gehen Sie wie folgt vor, um mithilfe einer dieser vorgefertigten Vorlagen ein Dashboard zu erstellen, sodass Sie sofort mit der Erkundung und Analyse Ihrer Daten beginnen können.

Um eine Dashboard-Ansicht zu erstellen

1. Navigieren Sie zur Amazon OpenSearch Service-Konsole unterhttps://console.aws.amazon.com/aos/.
2. Wählen Sie im linken Navigationsbereich Zentrale Verwaltung und dann Verbundene Datenquellen aus.
3. Wählen Sie die Datenquelle aus, um die Detailseite zu öffnen.
4. Klicken Sie auf Dashboard erstellen.
5. Wählen Sie aus, welche Art von Dashboard Sie erstellen möchten.
6. Geben Sie einen Namen für Ihr Dashboard ein.
7. Geben Sie eine optionale Beschreibung für Ihr Dashboard ein.
8. Wählen Sie eine oder mehrere AWS Glue-Tabellen aus, um sie auf Ihrem Dashboard anzuzeigen.
9. Wählen Sie aus, wie oft Sie die Daten in Ihrem Dashboard aktualisieren möchten.
10. Wählen Sie aus, welchen OpenSearch Workspace Sie verwenden möchten.

    a. Um einen neuen Workspace zu erstellen, wähle Neuen Workspace erstellen.

b. Um einen vorhandenen Workspace zu verwenden, wähle Bestehenden Workspace auswählen aus.

11. Gib einen Namen für deinen Workspace ein.
12. Klicken Sie auf Dashboard erstellen.

Fehlerbehebung

Es kann vorkommen, dass die Ergebnisse nicht wie erwartet zurückgegeben werden. Wenn Sie Probleme haben, stellen Sie sicher, dass Sie die befolgenthe section called “Empfehlungen”.

Verwaltung einer Datenquelle in Amazon OpenSearch Service

Die Verwaltung Ihrer Datenquelle ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung von Datenquellen für Direktabfragen und Ihrer anderen AWS Lösungen. AWS stellt die folgenden Tools bereit, um Fehler zu überwachen, zu melden und gegebenenfalls automatische Maßnahmen zu ergreifen.

Themen

- Überwachung mit CloudWatch Metrik-Datenquellen
- Datenquellen aktivieren und deaktivieren
- Überwachung mit Budget AWS
- Löschen einer Datenquelle

Überwachung mit CloudWatch Metrik-Datenquellen

Sie können die Direktabfrage überwachen mit CloudWatch. CloudWatch sammelt Rohdaten und verarbeitet sie zu lesbaren Metriken, die nahezu in Echtzeit verfügbar sind. Diese Statistiken werden 15 Monate gespeichert, damit Sie auf Verlaufsinformationen zugreifen können und einen besseren Überblick darüber erhalten, wie Ihre Webanwendung oder der Service ausgeführt werden.

Sie können auch Alarme einrichten, um bestimmte Schwellenwerte zu überwachen und Benachrichtigungen zu senden oder Maßnahmen zu ergreifen, wenn diese Schwellenwerte erreicht werden. Weitere Informationen finden Sie unter Was ist Amazon CloudWatch.

Amazon S3 meldet die folgenden Metriken:

Metrik	Beschreibung
AsyncQueryCreateAPI	Die Gesamtzahl der Anfragen, die an die API gestellt wurden, um asynchrone Abfragen zu erstellen. Relevante Statistiken: Durchschnitt, Maximum, Summe Abmessungen:`ClientId`, `DomainName` Frequenz: 60 Sekunden
AsyncQueryGetApiRequestCount	Die Gesamtzahl der Anfragen an die API zum Abrufen asynchroner Abfrageergebnisse. Relevante Statistiken: Durchschnitt, Maximum, Summe Abmessungen:, `ClientId` `DomainName` Frequenz: 60 Sekunden
AsyncQueryCancelApiRequestCount	Die Gesamtzahl der Anfragen, die an die API gestellt wurden, um asynchrone Abfragen abzubrechen. Relevante Statistiken: Durchschnitt, Maximum, Summe Abmessungen:, `ClientId` `DomainName` Frequenz: 60 Sekunden
AsyncQueryGetApiFailedRequestCusErrCount	Die Anzahl der fehlgeschlagenen Anfragen beim Abrufen asynchroner Abfrageergebnisse aufgrund von kundenbezogenen Fehlern (z. B. ungültige Abfrage-ID). Relevante Statistiken: Durchschnitt, Maximum, Summe Abmessungen:, `ClientId` `DomainName` Frequenz: 60 Sekunden

Metrik	Beschreibung
AsyncQueryCancelApiFailedRequestCusErrCount	Die Anzahl der fehlgeschlagenen Anfragen beim Abrufen asynchroner Abfrageergebnisse aufgrund von kundenbezogenen Fehlern (z. B. ungültige Abfrage-ID). Relevante Statistiken: Durchschnitt, Maximum, Summe Abmessungen:, `ClientId` `DomainName` Frequenz: 60 Sekunden
AsyncQueryCancelApiFailedRequestSysErrCount	Die Anzahl der fehlgeschlagenen Anfragen bei der Erstellung asynchroner Abfragen aufgrund von kundenbezogenen Fehlern. Relevante Statistiken: Durchschnitt, Maximum, Summe Abmessungen:, `ClientId` `DomainName` Frequenz: 60 Sekunden
AsyncQueryGetApiFailedRequestSysErrCount	Die Anzahl der fehlgeschlagenen Anfragen beim Abrufen asynchroner Abfrageergebnisse aufgrund systembedingter Fehler. Relevante Statistiken: Durchschnitt, Maximum, Summe Abmessungen:, `ClientId` `DomainName` Frequenz: 60 Sekunden

CloudWatch Logs und Security Lake melden die folgenden Kennzahlen:

Metrik	Beschreibung
DirectQueryRate	Die Rate der Anfragen an die Datenquellen. Relevante Statistiken: Summe, Maximum, Minimum, Durchschnitt

Metrik	Beschreibung
	Dimensionen: `DataSourceName` Frequenz: 60 Sekunden
DirectQueryLatency	Die Latenz, die bei der Ausführung von Abfragen in den Datenquellen beobachtet wurde. Relevante Statistiken: Durchschnitt, P90, P99, Summe, Minimum, Maximum Dimensionen: `DataSourceName` Frequenz: 60 Sekunden
FailedDirectQueries	Die Gesamtzahl der Abfragefehler, die bei den Datenquel lenabfragen beobachtet wurden. Relevante Statistiken: Summe, Maximum, Minimum, Durchschnitt Dimensionen: `DataSourceName` Frequenz: 60 Sekunden
DirectQueryConsumedOCU	Die Anzahl davon OCUs , die für die Ausführung der Abfragen in den Datenquellen verbraucht werden. Relevante Statistiken: Durchschnitt, P90, P99, Summe, Minimum, Maximum Dimensionen: `DataSourceName` Frequenz: 60 Sekunden

Datenquellen aktivieren und deaktivieren

> **Note**
>
> Die folgenden Informationen gelten nur für Amazon S3 S3-Datenquellen.

Für Situationen, in denen Sie die direkte Abfrageverwendung für eine Datenquelle beenden möchten, können Sie sich dafür entscheiden, die Datenquelle zu deaktivieren. Durch das Deaktivieren einer Datenquelle wird die Ausführung vorhandener Abfragen abgeschlossen und die Ausführung aller neuen Abfragen angehalten.

Die Einrichtung von Beschleunigungen zur Steigerung der Abfrageleistung, z. B. das Überspringen von Indizes, materialisierten Ansichten und das Abdecken von Indizes, wird auf manuell gesetzt, sobald eine Datenquelle deaktiviert wird. Sobald eine Datenquelle nach der Deaktivierung auf aktiv gesetzt wurde, werden Benutzerabfragen wie erwartet ausgeführt. Beschleunigungen, die zuvor eingerichtet und auf manuell eingestellt waren, müssen manuell konfiguriert werden, damit sie wieder nach einem Zeitplan ausgeführt werden.

Überwachung mit Budget AWS

Amazon OpenSearch Service füllt OCU-Nutzungsdaten auf Kontoebene in den Cost Explorer von Billing and Cost Management ein. Sie können die OCU-Nutzung auf Kontoebene berücksichtigen und Schwellenwerte sowie Warnmeldungen festlegen, wenn Schwellenwerte überschritten werden.

Das Format des Verwendungstyps, nach dem im Cost Explorer gefiltert werden soll, sieht wie folgt aus: DirectQuery OCU (RegionCodeOCU-Stunden). Wenn Sie benachrichtigt werden möchten, wenn DirectQuery die OCU-Nutzung (OCU-Stunden) Ihren Schwellenwert erreicht, können Sie ein AWS Budgets-Konto erstellen und eine Warnung konfigurieren, die auf dem von Ihnen festgelegten Schwellenwert basiert. Optional können Sie für Amazon S3 ein Amazon SNS SNS-Thema einrichten, das eine Datenquelle ausschaltet, falls ein Schwellenwertkriterium erfüllt wird.

> **Note**
>
> Die Nutzungsdaten in AWS Budgets sind nicht in Echtzeit verfügbar und können sich um bis zu 8 Stunden verzögern.

Löschen einer Datenquelle

Wenn Sie eine Datenquelle löschen, entfernt Amazon OpenSearch Service sie aus Ihrer Domain oder Ihrer Sammlung. OpenSearch Service entfernt auch Indizes, die mit der Datenquelle verknüpft sind. Ihre Transaktionsdaten werden nicht aus dem anderen gelöscht AWS-Service, aber der andere sendet AWS-Service keine neuen Daten an Service. OpenSearch

Sie können eine Datenquellenintegration mithilfe der AWS Management Console oder der OpenSearch Service-API löschen.

AWS Management Console

Um eine Amazon S3 S3-Datenquelle zu löschen

1. Navigieren Sie zur Amazon OpenSearch Service-Konsole unterhttps://console.aws.amazon.com/aos/.
2. Wählen Sie im linken Navigationsbereich Domains aus.
3. Wählen Sie die Domäne aus, für die Sie eine Datenquelle löschen möchten. Dadurch wird die Detailseite der Domain geöffnet. Wählen Sie die Registerkarte Verbindungen unter den allgemeinen Informationen und suchen Sie den Abschnitt Direkte Abfrage.
4. Wählen Sie die Datenquelle aus, die Sie löschen möchten, wählen Sie Löschen und bestätigen Sie den Löschvorgang.

Um eine CloudWatch Logs- oder Security Lake-Datenquelle zu löschen

1. Navigieren Sie zur Amazon OpenSearch Service-Konsole unterhttps://console.aws.amazon.com/aos/.
2. Wählen Sie im linken Navigationsbereich Zentrale Verwaltung und dann Verbundene Datenquellen aus.
3. Wählen Sie die Datenquelle aus, die Sie löschen möchten, wählen Sie Löschen und bestätigen Sie den Löschvorgang.

OpenSearch Service-API

Verwenden Sie den DeleteDataSourceAPI-Vorgang, um eine Amazon S3 S3-Datenquelle zu löschen.

```
POST https://es.region.amazonaws.com/2021-01-01/opensearch/domain/domain-name/
dataSource/data-source-name
```

Verwenden Sie den DeleteDirectQueryDataSourceAPI-Vorgang, um eine CloudWatch Logs- oder Security Lake-Datenquelle zu löschen.

Optimierung der Abfrageleistung für Amazon OpenSearch Service-Datenquellen

Die Abfrageleistung in Amazon OpenSearch Service kann sich verlangsamen, wenn Sie auf externe Datenquellen zugreifen. Dies kann auf Faktoren wie Netzwerklatenz, Datentransformation oder große Datenmengen zurückzuführen sein. Um die Leistung zu verbessern, sollten Sie je nach Anwendungsfall die Indizierung bestimmter Datenmengen in Betracht ziehen:

- Schnellere direkte Abfragen auf Amazon S3 (Index überspringen)
- Erstellung von Dashboard-Visualisierungen auf und Security Lake (materialisierte Ansichten)
- Erfassung von Abfrageergebnissen mithilfe indizierter Ansichten zur Offline-Überprüfung oder zur Leistungssteigerung auf Security Lake (materialisierte Ansichten)

Eine vollständige Dokumentation zu beschleunigten Abfragen, einschließlich Beispielabfragen, finden Sie in der Open-Source-Dokumentation unter Optimieren der Abfrageleistung mithilfe der OpenSearch Indizierung.

Themen

- Indizes überspringen
- Materialisierte Ansichten
- Erläuterung von Indizes

Indizes überspringen

Ein Skipping-Index nimmt nur die Metadaten der in Amazon S3 gespeicherten Daten auf. Wenn Sie eine Tabelle mit einem Übersprungindex abfragen, verwendet der Abfrageplaner den Index, um die Abfrage neu zu schreiben und so den Speicherort der Daten effizient zu identifizieren, ohne alle Partitionen und Dateien zu scannen. Dieser Ansatz hilft dabei, den genauen Speicherort der gespeicherten Daten einzugrenzen.

Es gibt zwei Möglichkeiten, einen Skipping-Index zu erstellen. Die erste Möglichkeit besteht darin, den Übersprungindex aus den Datenquellendetails heraus automatisch zu generieren. Die zweite Möglichkeit besteht darin, Query Workbench zu verwenden, um den Skipping-Index mithilfe einer SQL-Anweisung manuell zu erstellen.

Um einen Skipping-Index aus Ihrer Datenquelle automatisch zu generieren, gehen Sie zu Dashboard-Verwaltung und Accelerate data und wählen Sie dann Ihre Datenbank und Tabelle aus (Sie müssen möglicherweise aktualisieren, um die neuesten Datenbanken und Tabellen zu erhalten). Sie können dann Generieren wählen, um einen Übersprungindex automatisch zu generieren, oder jedes Feld, das Sie indizieren möchten, manuell auswählen und die Beschleunigung angeben (Typ des Übersprungsindexes). Wählen Sie abschließend „Beschleunigung erstellen“, um einen wiederkehrenden Job zu erstellen, der den neuen Sprungindex auffüllt.

Das Überspringen von Indizes wird nur für Amazon S3 S3-Datenquellen unterstützt.

Weitere Informationen zum Einrichten von Übersprungsindizes mit Query Workbench finden Sie in der Dokumentation unter Überspringen von Indizes. OpenSearch

Materialisierte Ansichten

Materialisierte Ansichten verwenden komplexe Abfragen wie Aggregationen, um Dashboard-Visualisierungen zu unterstützen. OpenSearch Sie nehmen eine Teilmenge Ihrer Daten auf der Grundlage der Abfrage auf und speichern sie in einem Index. OpenSearch Sie können diesen Index dann verwenden, um Visualisierungen zu erstellen.

Materialisierte Ansichten werden für Amazon S3- und Security Lake-Datenquellen unterstützt.

Weitere Informationen zum Einrichten von materialisierten Ansichten mit Query Workbench finden Sie in der Dokumentation unter Materialized Views. OpenSearch

Erläuterung von Indizes

Ein Deckindex nimmt Daten aus einer bestimmten Spalte in einer Tabelle auf und OpenSearch erstellt auf der Grundlage dieser Daten einen neuen Index. Sie können diesen neuen Index für Visualisierungen und andere OpenSearch Funktionen wie die Erkennung von Anomalien oder Geodatenanalysen verwenden.

Deckindizes werden nur für Amazon S3 S3-Datenquellen unterstützt.

Weitere Informationen zur Einrichtung von Deckungsindizes finden Sie in der Dokumentation unter Covering Indexes. OpenSearch

Unterstützte SQL- und PPL-Befehle

OpenSearch SQL und OpenSearch Pipeline Processing Language (PPL) sind Sprachen zum Abfragen, Analysieren und Verarbeiten von Daten in OpenSearch CloudWatch Logs Insights und Security Lake. Sie können OpenSearch SQL und OpenSearch PPL in OpenSearch Discover verwenden, um Daten in CloudWatch Logs, Amazon S3 oder Security Lake abzufragen. CloudWatch Logs Insights unterstützt neben Logs Insights OpenSearch QL, einer speziell entwickelten Abfragesprache für die Analyse von Logs, auch sowohl PPL- als auch SQL-Abfragesprachen. OpenSearch CloudWatch

- OpenSearch SQL: OpenSearch SQL bietet eine vertraute Option, wenn Sie es gewohnt sind, mit relationalen Datenbanken zu arbeiten. OpenSearch SQL bietet einen Teil der SQL-Funktionalität und ist daher eine gute Wahl für die Ausführung von Ad-hoc-Abfragen und Datenanalyseaufgaben. Mit OpenSearch SQL können Sie Befehle wie SELECT, FROM, WHERE, GROUP BY, HAVING und verschiedene andere in SQL verfügbare SQL-Befehle und -Funktionen verwenden. Sie können JOINs tabellenübergreifend (oder Protokollgruppen) ausführen, Daten tabellenübergreifend (oder Protokollgruppen) mithilfe von Unterabfragen korrelieren und die umfangreiche Palette an JSON-, mathematischen, Zeichenketten-, bedingten und anderen SQL-Funktionen verwenden, um leistungsstarke Analysen von Protokoll- und Sicherheitsdaten durchzuführen.
- OpenSearch PPL (Piped Processing Language): Mit OpenSearch PPL können Sie Daten mithilfe von in der Pipeline hinterlegten Befehlen abrufen, abfragen und analysieren, was das Verständnis und die Erstellung komplexer Abfragen erleichtert. Die Syntax basiert auf Unix-Pipes und ermöglicht die Verkettung von Befehlen zur Transformation und Verarbeitung von Daten. Mit PPL können Sie Daten filtern und aggregieren und Befehle wie JOINs Unterabfragen, LOOKUP und eine Vielzahl von mathematischen Funktionen, Zeichenketten-, Datums-, Bedingungs- und anderen Funktionen für Analysen verwenden.

Obwohl die meisten Befehle in OpenSearch PPL- und OpenSearch SQL-Abfragesprachen in CloudWatch Logs üblich sind OpenSearch, gibt es einige Unterschiede darin, welche Befehle und Funktionen in den einzelnen Diensten unterstützt werden. Weitere Einzelheiten finden Sie in den Tabellen auf den folgenden Seiten.

- the section called “Unterstützte SQL-Befehle”
  - the section called “CloudWatch Logs Insights”
  - the section called “Allgemeine SQL-Einschränkungen”

- the section called “Unterstützte PPL-Befehle”
  - the section called “Zusätzliche Informationen für CloudWatch Logs Insights-Benutzer, die OpenSearch PPL verwenden”

Unterstützte OpenSearch SQL-Befehle und -Funktionen

Die folgenden Referenztabellen zeigen, welche SQL-Befehle in OpenSearch Discover für die Abfrage von Daten in Amazon S3, Security Lake oder CloudWatch Logs unterstützt werden und welche SQL-Befehle in CloudWatch Logs Insights unterstützt werden. Die in CloudWatch Logs Insights unterstützte SQL-Syntax und die in OpenSearch Discover für die Abfrage von CloudWatch Logs unterstützte SQL-Syntax sind identisch und werden in den folgenden CloudWatch Tabellen als Logs bezeichnet.

> **Note**
>
> OpenSearch bietet außerdem SQL-Unterstützung für die Abfrage von Daten, die in Indizes aufgenommen OpenSearch und in Indizes gespeichert werden. Dieser SQL-Dialekt unterscheidet sich von dem bei Direktabfragen verwendeten SQL und wird bei Indizes als OpenSearch SQL bezeichnet.

Themen

- Befehle
- Funktionen
- Allgemeine SQL-Einschränkungen
- Zusätzliche Informationen für CloudWatch Logs Insights-Benutzer, die OpenSearch SQL verwenden

Befehle

> **Note**
>
> Ersetzen Sie in der Spalte mit den Beispielbefehlen nach *<tableName/logGroup>* Bedarf, je nachdem, welche Datenquelle Sie abfragen.
>
> - Beispielbefehl: `SELECT Body , Operation FROM` **`<tableName/logGroup>`**

- Wenn Sie Amazon S3 oder Security Lake abfragen, verwenden Sie: `SELECT Body , Operation FROM table_name`
- Wenn Sie CloudWatch Logs abfragen, verwenden Sie: `SELECT Body , Operation FROM `LogGroupA``

Befehl	Beschreibung	CloudWatch Logs	Amazon S3	Security Lake	-Beispielbefehl
the section called “SELECT-Klausel”	Zeigt projizierte Werte an.	U zt	U zt	U zt	`SELECT method, status FROM <tableName/logGroup>`
the section called “WHERE-Klausel”	Filtert Protokollereignisse auf der Grundlage der angegebenen Feldkriterien.	U zt	U zt	U zt	`SELECT * FROM <tableName/logGroup> WHERE status = 100`
the section called “GROUP BY-Klausel”	Gruppenprotokollieren Ereignisse nach Kategorien und ermitteln anhand	U zt	U zt	U zt	`SELECT method, status, COUNT(*) AS request_count, SUM(bytes) AS total_bytes FROM <tableName/logGroup> GROUP BY method, status`

Befehl	Beschreibung	CloudWatch Logs	Amazon S3	Security Lake	-Beispielbefehl
	von Statistiken den Durchschnitt.				
the section called “HAVING-Klausel”	Filtert die Ergebnisse auf der Grundlage von Gruppierungsbedingungen.	U zt	U zt	U zt	`SELECT method, status, COUNT(*) AS request_count, SUM(bytes) AS total_bytes FROM <tableName/logGroup> GROUP BY method, status HAVING COUNT(*) > 5`

Befehl	Beschreibung	CloudWatch Logs	Amazon S3	Security Lake	-Beispielbefehl
the section called “ORDER BY-Klausel”	Sortiert die Ergebnisse auf der Grundlage der Felder in der Order-Klausel. Sie können entweder in absteigender oder aufsteigender Reihenfolge sortieren.	Unterstützt	Unterstützt	Unterstützt	`SELECT * FROM <tableName/logGroup> ORDER BY status DESC`

Befehl	Beschreibung	CloudWatch Logs	Amazon S3	Security Lake	-Beispielbefehl

the section called “JOIN-Klausel”
 	
(INNER | CROSS | LEFT OUTER)
	Verbindet die Ergebnisse für zwei Tabellen auf der Grundlage gemeinsamer Felder.	Unterstützt (für den Join müssen Left Outer Schlüsselwörter Inner und -Schlüsselwörter verwendet werden; in einer SELECT Anweisung wird nur ein JOIN-Vorgang unterstützt)	Unterstützt (für die Verknüpfung müssen die Schlüsselwörter Inner, Left Outer und Cross verwendet werden)	Unterstützt (für die Verknüpfung müssen die Schlüsselwörter Inner, Left Outer und Cross verwendet werden)	`SELECT`
					`  A.Body,`
					`  B.Timestamp`
					`FROM`
					`  <tableNameA/logGroupA>  AS A`
					`INNER JOIN`
					`  <tableNameB/logGroupB>  AS B`
					`  ON A.`requestId` = B.`requestId``

Befehl	Beschreibung	CloudWatch Logs	Amazon S3	Security Lake	-Beispielbefehl
the section called “LIMIT-Klausel”	Beschränkt die Ergebnisse auf die ersten N Zeilen.	U zt	U zt	U zt	`SELECT * FROM <tableName/logGroup> LIMIT 10`

Befehl	Beschreibung	CloudWatch Logs	Amazon S3	Security Lake	-Beispielbefehl
the section called “CASE-Klausel”	Wertet Bedingungen aus und gibt einen Wert zurück, wenn die erste Bedingung erfüllt ist.	U zt	U zt	U zt	SELECT method, status, CASE WHEN status BETWEEN 100 AND 199 THEN 'Informational' WHEN status BETWEEN 200 AND 299 THEN 'Success' WHEN status BETWEEN 300 AND 399 THEN 'Redirection' WHEN status BETWEEN 400 AND 499 THEN 'Client Error' WHEN status BETWEEN 500 AND 599 THEN 'Server Error' ELSE 'Unknown Status' END AS status_category, CASE method WHEN 'GET' THEN 'Read Operation' WHEN 'POST' THEN 'Create Operation' WHEN 'PUT' THEN 'Update Operation' WHEN 'PATCH' THEN 'Partial Update Operation' WHEN 'DELETE' THEN 'Delete Operation' ELSE 'Other Operation' END AS operation_type, bytes, datetime FROM *<tableName/logGroup>*

Befehl	Beschrei ung	CloudWa h Logs	Amazon S3	Security Lake	-Beispielbefehl
the section called “Gemeinsa mer Tabellena usdruck”	Erstellt eine benannte temporäi Ergebnis enge innerhalb einer SELECT INSERT- UPDATE DELETE oder MERGE- Anw eisung.	W nicht unterstüt zt	U zt	U zt	`WITH RequestStats AS ( SELECT method, status, bytes, COUNT(*) AS request_count FROM tableName GROUP BY method, status, bytes ) SELECT method, status, bytes, request_count FROM RequestStats WHERE bytes > 1000`

Befehl	Beschreibung	CloudWatch Logs	Amazon S3	Security Lake	-Beispielbefehl
the section called “EXPLAIN	Zeigt den Ausführungsplan einer SQL-Anweisung an, ohne sie tatsächlich auszuführen.	W nicht unterstützt	U zt	U zt	`EXPLAIN SELECT k, SUM(v) FROM VALUES (1, 2), (1, 3) AS t(k, v) GROUP BY k`

Befehl	Beschreibung	CloudWatch Logs	Amazon S3	Security Lake	-Beispielbefehl
the section called “LATERAL SUBQUERY Klausel”	Ermöglicht einer Unterabfrage in der FROM-Klausel, auf Spalten aus vorherigen Elementen in derselben FROM-Klausel zu verweisen.	W nicht unterstützt	U zt	U zt	`SELECT * FROM tableName LATERAL ( SELECT * FROM t2 WHERE t1.c1 = t2.c1 )`

Befehl	Beschreibung	CloudWatch Logs	Amazon S3	Security Lake	-Beispielbefehl
the section called “Klausel LATERAL VIEW”	Generiert eine virtuelle Tabelle, indem eine Funktion zum Generieren von Tabellen auf jede Zeile einer Basistabelle angewendet wird.	Wird nicht unterstützt	Unterstützt	Unterstützt	`SELECT * FROM tableName LATERAL VIEW EXPLODE(ARRAY(30, 60)) tableName AS c_age LATERAL VIEW EXPLODE(ARRAY(40, 80)) AS d_age`
the section called “LIKE-Prädikat”	Ordnet eine Zeichenfolge einem Muster unter Verwendung von Platzhalterzeichen zu.	Unterstützt	Unterstützt	Unterstützt	`SELECT method, status, request, host FROM <tableName/logGroup> WHERE method LIKE 'D%'`

Befehl	Beschrei ung	CloudWa h Logs	Amazon S3	Security Lake	-Beispielbefehl
the section called “OFFSET”	Gibt die Anzahl der Zeilen an, die übersprungen werden sollen, bevor mit der Rückgab von Zeilen aus der Abfrage begonne wird.	W unterstüt zt, wenn es in Verbindu g mit einer LIMIT Klausel in einer Abfrage verwend wird. Zum Beispiel: • Unters zt: SELEC * FROM Table LIMIT 100 OFFSE 10 • Nicht unters zt: SELEC *	U zt	U zt	SELECT method, status, bytes, datetime FROM *<tableName/logGroup>* ORDER BY datetime OFFSET 10

Befehl	Beschrei ung	CloudWa h Logs	Amazon S3	Security Lake	-Beispielbefehl
		FROM Table OFFSE 10			
the section called “PIVOT-Klausel”	Transfor iert Zeilen in Spalten und rotiert Daten von einem zeilenba ierten Format in ein spaltenb siertes Format.	W nicht unterstüt zt	U zt	U zt	SELECT * FROM (SELECT method, status, bytes FROM *<tableName/logGroup>*) AS SourceTable PIVOT (SUM(bytes) FOR method IN ('GET', 'POST', 'PATCH', 'PUT', 'DELETE')) AS PivotTable

Befehl	Beschrei ung	CloudWa h Logs	Amazon S3	Security Lake	-Beispielbefehl

the section called “Satzoperatoren”	Kombinie t die Ergebnis e von zwei oder mehr SELECT An weisung (z. B. UNION, INTERSI , EXCEPT	U zt	U zt	U zt	`SELECT method, status, bytes FROM <tableName/logGroup> WHERE status = '416'`
					
					`UNION`
					
					`SELECT method, status, bytes FROM <tableName/logGroup> WHERE bytes > 20000`

the section called “SORT BY-Klausel”	Gibt die Reihenfo ge an, in der die Abfragee gebnisse zurückge eben werden sollen.	U zt	U zt	U zt	`SELECT method, status, bytes FROM <tableName/logGroup> SORT BY bytes DESC`

Befehl	Beschrei ung	CloudWa h Logs	Amazon S3	Security Lake	-Beispielbefehl
the section called “UNPIVOT	Wandelt Spalten in Zeilen um und rotiert Daten von einem spaltenb sierten Format in ein zeilenba iertes Format.	W nicht unterstüt zt	U zt	U zt	`SELECT status, REPLACE(method, '_bytes', '') AS request_method, bytes, datetime FROM PivotedData UNPIVOT ( bytes FOR method IN ( GET_bytes, POST_bytes, PATCH_bytes, PUT_bytes, DELETE_bytes ) ) AS UnpivotedData`

Funktionen

> **Note**
>
> Ersetzen Sie in der Spalte mit den Beispielbefehlen nach *<tableName/logGroup>* Bedarf, je nachdem, welche Datenquelle Sie abfragen.
>
> - Beispielbefehl: `SELECT Body , Operation FROM` **`<tableName/logGroup>`**
> - Wenn Sie Amazon S3 oder Security Lake abfragen, verwenden Sie: `SELECT Body , Operation FROM` **`table_name`**
> - Wenn Sie CloudWatch Logs abfragen, verwenden Sie: `SELECT Body , Operation FROM` **`` `LogGroupA` ``**

Verfügbare SQL-Grammatik	Beschreibung	CloudWatch Logs	Amazon S3	Security Lake	-Beispielbefehl
the section called “Zeichenfolgenfunktionen”	Integrierte Funktionen, mit denen Zeichenketten- und Textdaten in SQL-Abfragen bearbeitet und transformiert werden können. Zum Beispiel das Konvertieren von Groß- und Kleinschreibung, das Kombinieren von Zeichenketten, das Extrahieren von Teilen und das Bereinigen von Text.	Unterstützt	Unterstützt	Unterstützt	`SELECT UPPER(method) AS upper_method, LOWER(host) AS lower_host FROM <tableName/logGroup>`

Verfügbare SQL-Grammatik	Beschreibung	CloudWatch Logs	Amazon S3	Security Lake	-Beispielbefehl
the section called “Datum und Zeitfunktionen”	Integrierte Funktionen für die Verarbeitung und Transformation von Datums- und Zeitstempeldaten in Abfragen. Zum Beispiel date_add, date_format, datediff und current_date.	U zt	U zt	U zt	`SELECT TO_TIMESTAMP(datetime) AS timestamp, TIMESTAMP_SECONDS(UNIX_TIMESTAMP(datetime)) AS from_seconds, UNIX_TIMESTAMP(datetime) AS to_unix, FROM_UTC_TIMESTAMP(datetime, 'PST') AS to_pst, TO_UTC_TIMESTAMP(datetime, 'EST') AS from_est FROM <tableName/logGroup>`

Verfügbare SQL-Grammatik	Beschreibung	CloudWatch Logs	Amazon S3	Security Lake	-Beispielbefehl
the section called “Aggregationsfunktionen”	Integrierte Funktionen, die Berechnungen für mehrere Zeilen durchführen, um einen einzigen zusammengefassten Wert zu erzeugen. Zum Beispiel Summe, Anzahl, Durchschnitt, Maximum und Min.	U zt	U zt	U zt	`SELECT COUNT(*) AS total_records, COUNT(DISTINCT method) AS unique_methods, SUM(bytes) AS total_bytes, AVG(bytes) AS avg_bytes, MIN(bytes) AS min_bytes, MAX(bytes) AS max_bytes FROM <tableName/logGroup>`

Verfügbare SQL-Grammatik	Beschreibung	CloudWatch Logs	Amazon S3	Security Lake	-Beispielbefehl
the section called “Konditionale Funktion”	Integrierte Funktionen, die Aktionen auf der Grundlage bestimmter Bedingungen ausführen oder Ausdrücke bedingt auswerten. Zum Beispiel CASE und IF.	U zt	U zt	U zt	`SELECT CASE WHEN method = 'GET' AND bytes < 1000 THEN 'Small Read' WHEN method = 'POST' AND bytes > 10000 THEN 'Large Write' WHEN status >= 400 OR bytes = 0 THEN 'Problem' ELSE 'Normal' END AS request_type FROM <tableName/logGroup>`

Verfügbare SQL-Grammatik	Beschreibung	CloudWatch Logs	Amazon S3	Security Lake	-Beispielbefehl
the section called “JSON-Funktionen	Integrierte Funktionen zum Parsen, Extrahieren, Ändern und Abfragen von Daten im JSON-Format innerhalb von SQL-Abfragen (z. B. from_json, to_json, get_json_object, json_tuple), die die Manipulation von JSON-Strukturen in Datensätzen ermöglichen.	Wird unterstützt	Unterstützt	Unterstützt	`SELECT FROM_JSON( @message, 'STRUCT< host: STRING, user-identifier: STRING, datetime: STRING, method: STRING, status: INT, bytes: INT >' ) AS parsed_json FROM <tableName/logGroup>`

Verfügbare SQL-Grammatik	Beschreibung	CloudWatch Logs	Amazon S3	Security Lake	-Beispielbefehl
the section called “Array-Funktionen”	Integrierte Funktionen für die Arbeit mit Spalten vom Typ Array in SQL-Abfragen, die Operationen wie Zugriff, Änderung und Analyse von Array-Daten (z. B. size, explode, array_contains) ermöglichen.	Unterstützt	Unterstützt	Unterstützt	`SELECT scores, size(scores) AS length, array_contains(scores, 90) AS has_90 FROM <tableName/logGroup>`

Verfügbare SQL-Grammatik	Beschreibung	CloudWatch Logs	Amazon S3	Security Lake	-Beispielbefehl
the section called “Fensterfunktionen” -	Integrierte Funktionen, die Berechnungen für einen bestimmten Satz von Zeilen durchführen, die sich auf die aktuelle Zeile (Fenster) beziehen, wodurch Operationen wie Rangfolge, Gesamtwerte und gleitende Durchschnitte (z. B. ROW_NUMBER, RANK, LAG, LEAD) ermöglicht werden	Wird unterstützt	Unterstützt	Unterstützt	`SELECT field1, field2, RANK() OVER (ORDER BY field2 DESC) AS field2Rank FROM <tableName/logGroup>`

Verfügbare SQL-Grammatik	Beschreibung	CloudWatch Logs	Amazon S3	Security Lake	-Beispielbefehl
the section called “Konvertierungsfunktionen”	Integrierte Funktionen zum Konvertieren von Daten von einem Typ in einen anderen innerhalb von SQL-Abfragen, die Datentyptransformationen und Formatkonvertierungen ermöglichen (z. B. CAST, TO_DATE, TO_TIMESTAMP, BINARY)	Unterstützt	Unterstützt	Unterstützt	`SELECT CAST('123' AS INT) AS converted_number, CAST(123 AS STRING) AS converted_string FROM <tableName/logGroup>`

Verfügbare SQL-Grammatik	Beschreibung	CloudWatch Logs	Amazon S3	Security Lake	-Beispielbefehl
the section called “Prädikatsfunktionen”	Integrierte Funktionen, die Bedingungen auswerten und boolesche Werte (true/false) basierend auf bestimmten Kriterien oder Mustern zurückgeben (z. B. IN, LIKE, BETWEEN, IS NULL, EXISTS)	Wird unterstützt	Unterstützt	Unterstützt	`SELECT * FROM <tableName/logGroup> WHERE id BETWEEN 50000 AND 75000`

Verfügbare SQL-Grammatik	Beschreibung	CloudWatch Logs	Amazon S3	Security Lake	-Beispielbefehl
the section called “Funktionen zuordnen	Wendet eine angegebene Funktion auf jedes Element in einer Sammlung an und wandelt die Daten in einen neuen Satz von Werten um.	Wird nicht unterstützt	Unterstützt	Unterstützt	`SELECT MAP_FILTER( MAP( 'method', method, 'status', CAST(status AS STRING), 'bytes', CAST(bytes AS STRING) ), (k, v) -> k IN ('method', 'status') AND v != 'null' ) AS filtered_map FROM <tableName/logGroup> WHERE status = 100`

Verfügbare SQL-Grammatik	Beschreibung	CloudWatch Logs	Amazon S3	Security Lake	-Beispielbefehl
the section called “Mathematische Funktionen”	Führt mathematische Operationen mit numerischen Daten aus, z. B. die Berechnung von Durchschnittswerten, Summen oder trigonometrischen Werten.	Unterstützt	Unterstützt	Unterstützt	`SELECT bytes, bytes + 1000 AS added, bytes - 1000 AS subtracted, bytes * 2 AS doubled, bytes / 1024 AS kilobytes, bytes % 1000 AS remainder FROM <tableName/logGroup>`
the section called “Gruppunktion mit mehreren Protokollen”	Ermöglicht Benutzern, mehrere Protokollgruppen in einer SQL SELECT-Anweisung anzugeben	Wird unterstützt	Nicht zutreffend	Nicht zutreffend	`SELECT lg1.Column1, lg1.Column2 FROM `logGroups(logGroupIdentifier: ['LogGroup1', 'LogGroup2'])` AS lg1 WHERE lg1.Column3 = "Success"`

Verfügbare SQL-Grammatik	Beschreibung	CloudWatch Logs	Amazon S3	Security Lake	-Beispielbefehl
the section called “Generatorfunktionen”	Erzeugt ein Iterator-Objekt, das eine Folge von Werten liefert und so eine effiziente Speichernutzung in großen Datensätzen ermöglicht.	Wird nicht unterstützt	Unterstützt	Unterstützt	`SELECT explode(array(10, 20))`

Allgemeine SQL-Einschränkungen

Die folgenden Einschränkungen gelten bei der Verwendung von OpenSearch SQL with CloudWatch Logs, Amazon S3 und Security Lake.

1. Sie können in einer SELECT-Anweisung nur eine JOIN-Operation verwenden.
2. Es wird nur eine Ebene verschachtelter Unterabfragen unterstützt.
3. Abfragen mit mehreren Anweisungen, die durch Semikolons getrennt sind, werden nicht unterstützt.
4. Abfragen mit Feldnamen, die identisch sind, sich aber nur in der Groß- und Kleinschreibung unterscheiden (wie Feld1 und FIELD1), werden nicht unterstützt.

   Beispielsweise werden die folgenden Abfragen nicht unterstützt:

   ```
   Select AWSAccountId, awsaccountid from LogGroup
   ```

Die folgende Abfrage ist jedoch darauf zurückzuführen, dass der Feldname (@logStream) in beiden Protokollgruppen identisch ist:

```
Select a.`@logStream`, b.`@logStream` from Table A INNER Join Table B on a.id = b.id
```

5. Funktionen und Ausdrücke müssen mit Feldnamen arbeiten und Teil einer SELECT-Anweisung mit einer in der FROM-Klausel angegebenen Protokollgruppe sein.

   Diese Abfrage wird beispielsweise nicht unterstützt:

   ```
   SELECT cos(10) FROM LogGroup
   ```

   Diese Abfrage wird unterstützt:

   ```
   SELECT cos(field1) FROM LogGroup
   ```

Zusätzliche Informationen für CloudWatch Logs Insights-Benutzer, die OpenSearch SQL verwenden

CloudWatch Logs unterstützt OpenSearch SQL-Abfragen in der Logs Insights-Konsole, API und CLI. Es unterstützt die meisten Befehle, einschließlich SELECT, FROM, WHERE, GROUP BY, HAVING, JOINS und verschachtelte Abfragen sowie JSON-, Math-, Zeichenketten- und Bedingungsfunktionen. CloudWatch Logs unterstützt jedoch nur Lesevorgänge, sodass DDL- oder DML-Anweisungen nicht zulässig sind. Eine vollständige Liste der unterstützten Befehle und Funktionen finden Sie in den Tabellen in den vorherigen Abschnitten.

Gruppenfunktionen mit mehreren Protokollen

CloudWatch Logs Insights unterstützt die Möglichkeit, mehrere Protokollgruppen abzufragen. Um diesen Anwendungsfall in SQL zu behandeln, können Sie den `logGroups` Befehl verwenden. Dieser Befehl ist spezifisch für das Abfragen von Daten in CloudWatch Logs Insights, an denen eine oder mehrere Protokollgruppen beteiligt sind. Verwenden Sie diese Syntax, um mehrere Protokollgruppen abzufragen, indem Sie sie im Befehl angeben, anstatt eine Abfrage für jede der Protokollgruppen zu schreiben und sie mit einem `UNION` Befehl zu kombinieren.

Syntax:

```
`logGroups(
```

```
    logGroupIdentifier: ['LogGroup1','LogGroup2', ...'LogGroupn']
)
```

In dieser Syntax können Sie bis zu 50 Protokollgruppen im `logGroupIndentifier` Parameter angeben. Wenn Sie in einem Monitoring-Konto auf Protokollgruppen verweisen möchten, verwenden Sie ARNs anstelle von `LogGroup` Namen.

Beispielabfrage:

```
SELECT LG1.Column1, LG1.Column2 from `logGroups(
    logGroupIdentifier: ['LogGroup1', 'LogGroup2']
)` as LG1
WHERE LG1.Column1 = 'ABC'
```

Die folgende Syntax mit mehreren Protokollgruppen nach der `FROM` Anweisung wird bei der Abfrage von CloudWatch Logs nicht unterstützt:

```
SELECT Column1, Column2 FROM 'LogGroup1', 'LogGroup2', ...'LogGroupn'
WHERE Column1 = 'ABC'
```

Einschränkungen

Wenn Sie SQL- oder PPL-Befehle verwenden, schließen Sie bestimmte Felder in Backticks ein, um sie abzufragen. Backticks sind für Felder mit Sonderzeichen (nicht alphabetisch und nicht numerisch) erforderlich. Zum Beispiel „einschließen`@message`“ und „in Backticks“. `Operation.Export, Test::Field` Sie müssen Spalten mit rein alphabetischen Namen nicht in Backticks einschließen.

Beispielabfrage mit einfachen Feldern:

```
SELECT SessionToken, Operation, StartTime  FROM `LogGroup-A`
LIMIT 1000;
```

Dieselbe Abfrage mit angehängten Backticks:

```
SELECT `SessionToken`, `Operation`, `StartTime`  FROM `LogGroup-A`
LIMIT 1000;
```

Weitere allgemeine Einschränkungen, die nicht spezifisch für CloudWatch Protokolle sind, finden Sie unter. the section called “Allgemeine SQL-Einschränkungen”

Beispielabfragen und Kontingente

> **Note**
>
> Das Folgende gilt sowohl für CloudWatch Logs Insights-Benutzer als auch für OpenSearch Benutzer, die CloudWatch Daten abfragen.

Beispiele für SQL-Abfragen, die Sie in CloudWatch Logs verwenden können, finden Sie unter Gespeicherte Abfragen und Beispielabfragen in der Amazon CloudWatch Logs Insights-Konsole.

Informationen zu den Beschränkungen, die bei der Abfrage von CloudWatch Logs from OpenSearch Service gelten, finden Sie unter CloudWatch Log-Kontingente im Amazon CloudWatch Logs-Benutzerhandbuch. Die Beschränkungen betreffen die Anzahl der CloudWatch Protokollgruppen, die Sie abfragen können, die maximale Anzahl gleichzeitiger Abfragen, die Sie ausführen können, die maximale Ausführungszeit von Abfragen und die maximale Anzahl von Zeilen, die in Ergebnissen zurückgegeben werden. Die Grenzwerte sind dieselben, unabhängig davon, welche Sprache Sie für die Abfrage von CloudWatch Logs verwenden (nämlich OpenSearch PPL, SQL und Logs Insights).

SQL-Befehle

Themen

- Zeichenfolgenfunktionen
- Datums- und Zeitfunktionen
- Aggregationsfunktionen
- Konditionale Funktionen
- JSON-Funktionen
- Array-Funktionen
- Fensterfunktionen
- Konvertierungs-Funktionen
- Prädikatsfunktionen
- Funktionen zuordnen
- Mathematische Funktionen
- Generatorfunktionen
- SELECT-Klausel

- WHERE-Klausel
- GROUP BY-Klausel
- HAVING-Klausel
- ORDER BY-Klausel
- JOIN-Klausel
- LIMIT-Klausel
- CASE-Klausel
- Gemeinsamer Tabellenausdruck
- EXPLAIN
- LATERALE SUBQUERY-Klausel
- Klausel LATERAL VIEW
- LIKE-Prädikat
- OFFSET
- PIVOT-Klausel
- Satzoperatoren
- SORT BY-Klausel
- UNPIVOT

Zeichenfolgenfunktionen

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen SQL-Befehl unterstützen, finden Sie unter. the section called “Unterstützte SQL-Befehle”

Funktion	Beschreibung
ascii (str)	Gibt den numerischen Wert des ersten Zeichens von zurück. `str`
base64 (bin)	Konvertiert das Argument von einer Binärdatei `bin` in eine Base-64-Zeichenfolge.

Funktion	Beschreibung
bit_length (expr)	Gibt die Bitlänge von Zeichenkettendaten oder die Anzahl der Bits von Binärdaten zurück.
btrim (str)	Entfernt die führenden und nachfolgenden Leerzeichen von. `str`
btrim (str, trimStr)	Entferne die führenden und nachfolgenden `trimStr` Zeichen von. `str`
char (Ausdruck)	Gibt das ASCII-Zeichen zurück, dessen binäre Entsprechung zu ist. `expr` Wenn n größer als 256 ist, entspricht das Ergebnis chr (n% 256)
Zeichenlänge (Ausdruck)	Gibt die Zeichenlänge von Zeichenkettendaten oder die Anzahl der Byte von Binärdaten zurück. Die Länge von Zeichenkettendaten schließt die abschließenden Leerzeichen ein. Die Länge von Binärdaten beinhaltet binäre Nullen.
Zeichenlänge (expr)	Gibt die Zeichenlänge von Zeichenkettendaten oder die Anzahl der Byte von Binärdaten zurück. Die Länge von Zeichenkettendaten schließt die abschließenden Leerzeichen ein. Die Länge von Binärdaten beinhaltet binäre Nullen.
chr (expr)	Gibt das ASCII-Zeichen zurück, dessen binäre Entsprechung zu ist. `expr` Wenn n größer als 256 ist, entspricht das Ergebnis chr (n% 256)
concat_ws (sep [, str | array (str)] +)	Gibt die Verkettung der Zeichenketten zurück, getrennt durch, wobei Nullwerte übersprungen werden. `sep`

Funktion	Beschreibung
enthält (links, rechts)	Gibt einen booleschen Wert zurück. Der Wert ist True, wenn rechts innerhalb von links gefunden wird. Gibt NULL zurück, wenn einer der Eingabeausdrücke NULL ist. Andernfalls wird False zurückgegeben. Sowohl links als auch rechts müssen vom Typ STRING oder BINARY sein.
dekodieren (bin, Zeichensatz)	Dekodiert das erste Argument mit dem Zeichensatz des zweiten Arguments.
dekodieren (expr, search, result [, search, result]... [, default])	Vergleicht expr der Reihe nach mit jedem Suchwert. Wenn expr einem Suchwert entspricht, gibt decode das entsprechende Ergebnis zurück. Wenn keine Übereinst immung gefunden wird, wird die Standarde instellung zurückgegeben. Wenn Standard weggelassen wird, wird Null zurückgegeben.
elt (n, Eingabe1, Eingabe2,...)	Gibt n die -te Eingabe zurück, gibt z. B. zurück, `input2` wenn n 2 ist.
kodieren (str, Zeichensatz)	Kodiert das erste Argument mit dem Zeichensa tz des zweiten Arguments.
endet mit (links, rechts)	Gibt einen booleschen Wert zurück. Der Wert ist True, wenn links mit rechts endet. Gibt NULL zurück, wenn einer der Eingabeau sdrücke NULL ist. Andernfalls wird False zurückgegeben. Sowohl links als auch rechts müssen vom Typ STRING oder BINARY sein.

Funktion	Beschreibung
find_in_set (str, str_array)	Gibt den Index (1-basiert) der angegebenen Zeichenfolge () in der kommagetrennten Liste (`str`) zurück. `str_array` Gibt 0 zurück, wenn die Zeichenfolge nicht gefunden wurde oder wenn die angegebene Zeichenfolge () `str` ein Komma enthält.
format_number (expr1, expr2)	Formatiert die Zahl `expr1` wie '#, ###, ###.##', auf Dezimalstellen gerundet. `expr2` Wenn 0 `expr2` ist, hat das Ergebnis weder einen Dezimalpunkt noch einen Bruchteil. `expr2`akzeptiert auch ein benutzerdefinierte s Format. Das soll wie FORMAT von MySQL funktionieren.
format_string (strfmt, obj,...)	Gibt eine formatierte Zeichenfolge aus Formatzeichenketten im Printf-Stil zurück.
initcap (str)	Gibt zurück, `str` wobei der erste Buchstabe jedes Worts in Großbuchstaben geschrieb en wird. Alle anderen Buchstaben werden in Kleinbuchstaben geschrieben. Wörter werden durch Leerraum getrennt.
instr (str, substr)	Gibt den (1-basierten) Index des ersten Vorkommens von in zurück. `substr` `str`
lcase (str)	Gibt zurück, `str` bei der alle Zeichen in Kleinbuchstaben geändert wurden.
links (str, len)	Gibt die am weitesten links stehenden Zeichen `len` (`len`kann vom Typ Zeichenfolge sein) aus der Zeichenfolge zurück. Wenn sie kleiner oder gleich 0 `len` ist`str`, ist das Ergebnis eine leere Zeichenfolge.

Funktion	Beschreibung
len (expr)	Gibt die Zeichenlänge von Zeichenkettendaten oder die Anzahl der Byte von Binärdaten zurück. Die Länge von Zeichenkettendaten schließt die abschließenden Leerzeichen ein. Die Länge von Binärdaten beinhaltet binäre Nullen.
Länge (expr)	Gibt die Zeichenlänge von Zeichenkettendaten oder die Anzahl der Byte von Binärdaten zurück. Die Länge von Zeichenkettendaten schließt die abschließenden Leerzeichen ein. Die Länge von Binärdaten beinhaltet binäre Nullen.
levenshtein (str1, str2 [, Schwellenwert])	Gibt den Levenshtein-Abstand zwischen den beiden angegebenen Zeichenketten zurück. Wenn der Schwellenwert gesetzt ist und die Entfernung größer ist, wird -1 zurückgegeben.
lokalisieren (substr, str [, pos])	Gibt die Position des ersten Vorkommens von `substr` in `str` nach der Position `pos` zurück. Der angegebene Wert `pos` und der Rückgabewert basieren auf 1.
niedriger (str)	Gibt zurück, `str` bei der alle Zeichen in Kleinbuchstaben geändert wurden.
lpad (str, len [, pad])	Gibt zurück`str`, links aufgefüllt mit `pad` bis zu einer Länge von. `len` Wenn `str` ist länger als`len`, wird der Rückgabewert auf `len` Zeichen oder Byte gekürzt. Wenn `pad` nicht angegeben, `str` wird es nach links mit Leerzeichen aufgefüllt, wenn es sich um eine Zeichenfolge handelt, und mit Nullen, wenn es sich um eine Bytefolge handelt.

Funktion	Beschreibung
ltrim (str)	Entfernt die führenden Leerzeichen von`str`.
luhn_check (str)	Überprüft, ob eine Ziffernfolge gemäß dem Luhn-Algorithmus gültig ist. Diese Prüfsumme nfunktion wird häufig bei Kreditkartennummer n und behördlichen Identifikationsnummern angewendet, um gültige Zahlen von falsch eingegebenen Zahlen zu unterscheiden.
Maske (Eingabe [, UpperChar, LowerChar, DigitChar, OtherChar])	maskiert den angegebenen Zeichenkettenwert. Die Funktion ersetzt Zeichen durch 'X' oder 'x' und Zahlen durch 'n'. Dies kann nützlich sein, um Kopien von Tabellen zu erstellen, bei denen vertrauliche Informationen entfernt wurden.
octet_length (expr)	Gibt die Bytelänge von Zeichenkettendaten oder die Anzahl der Byte von Binärdaten zurück.
Überlagerung (Eingabe, Ersetzen, Pos [, Len])	Ersetze durch `input` `replace` das, was bei der Länge beginnt `pos` und eine Länge `len` hat.
position (substr, str [, pos])	Gibt die Position des ersten Vorkommens von `substr` in `str` nach Position `pos` zurück. Der angegebene Wert `pos` und der Rückgabewert basieren auf 1.
printf (strfmt, obj,...)	Gibt eine formatierte Zeichenfolge aus Formatzeichenketten im Printf-Stil zurück.
regexp_count (str, regexp)	Gibt zurück, wie oft das Muster `regexp` eines regulären Ausdrucks in der Zeichenfolge übereinstimmt. `str`

Funktion	Beschreibung
regexp_extract (str, regexp [, idx])	Extrahieren Sie die erste Zeichenfolge in der`str`, die dem `regexp` Ausdruck entspricht und dem Regex-Gruppenindex entspricht.
regexp_extract_all (str, regexp [, idx])	Extrahiert alle Zeichenketten in der`str`, die dem Ausdruck entsprechen und dem Regex-Gruppenindex entsprechen. `regexp`
regexp_instr (str, regexp)	Durchsucht eine Zeichenfolge nach einem regulären Ausdruck und gibt eine Ganzzahl zurück, die die Anfangsposition der übereinst immenden Teilzeichenfolge angibt. Positione n basieren auf 1, nicht auf 0. Wenn keine Übereinstimmung gefunden wird, wird 0 zurückgegeben.
regexp_replace (str, regexp, rep [, position])	Ersetzt alle Teilstrings dieses Matches durch. `str` `regexp` `rep`
regexp_substr (str, regexp)	Gibt die Teilzeichenfolge zurück, die dem regulären Ausdruck innerhalb der Zeichenfo lge entspricht. `regexp` `str` Wenn der reguläre Ausdruck nicht gefunden wird, ist das Ergebnis Null.
wiederhole (str, n)	Gibt die Zeichenfolge zurück, die den angegebenen Zeichenkettenwert n-mal wiederholt.
ersetzen (str, suche [, ersetzen])	Ersetzt alle Vorkommen von `search` mit`replace`.

Funktion	Beschreibung
rechts (str, len)	Gibt die am weitesten rechts stehenden Zeichen `len` (`len`kann vom Typ Zeichenfo lge sein) aus der Zeichenfolge zurück. Wenn sie kleiner oder gleich 0 `len` ist`str`, ist das Ergebnis eine leere Zeichenfolge.
rpad (str, len [, pad])	Gibt zurück`str`, nach rechts aufgefüllt mit `pad` bis zu einer Länge von. `len` Wenn `str` ist länger als`len`, wird der Rückgabewert auf `len` Zeichen gekürzt. Wenn `pad` nicht angegeben , `str` wird es nach rechts mit Leerzeichen aufgefüllt, wenn es sich um eine Zeichenfolge handelt, und mit Nullen, wenn es sich um eine binäre Zeichenfolge handelt.
rtrim (str)	Entfernt die abschließenden Leerzeichen von. `str`
Sätze (str [, lang, country])	Teilt sich `str` in eine Reihe von Wörtern auf.
Soundex (str)	Gibt den Soundex-Code der Zeichenfolge zurück.
Leerzeichen (n)	Gibt eine Zeichenfolge zurück, die aus n Leerzeichen besteht.
split (str, regex, limit)	Teilt `str` übereinstimmende Vorkommen auf `regex` und gibt ein Array mit einer Länge von höchstens `limit`

Funktion	Beschreibung
split_part (str, delimiter, partNum)	Teilt `str` nach Trennzeichen auf und gibt den angeforderten Teil der Aufteilung zurück (1-basiert). Wenn eine Eingabe Null ist, wird Null zurückgegeben. Liegt eine Eingabe außerhalb des Bereichs der geteilten Teile, `partNum` wird eine leere Zeichenfolge zurückgegeben. Wenn 0 `partNum` ist, wird ein Fehler ausgegebe n. Wenn negativ `partNum` ist, werden die Teile vom Ende der Zeichenfolge rückwärts gezählt. Wenn `delimiter` es sich um eine leere Zeichenfolge handelt, `str` wird die nicht aufgeteilt.
beginnt mit (links, rechts)	Gibt einen booleschen Wert zurück. Der Wert ist True, wenn links mit rechts beginnt. Gibt NULL zurück, wenn einer der Eingabeau sdrücke NULL ist. Andernfalls wird False zurückgegeben. Sowohl links als auch rechts müssen vom Typ STRING oder BINARY sein.
substr (str, pos [, len])	Gibt den Teilstring zurück`str`, der bei der Länge beginnt `pos` und die Länge hat`len`, oder den Teil des Byte-Arrays, der bei beginnt `pos` und die Länge hat. `len`
substr (str VON pos [FÜR len]])	Gibt den Teilstring zurück`str`, der bei der Länge beginnt `pos` und die Länge hat`len`, oder den Teil eines Byte-Arrays, der mit der Länge beginnt `pos` und die Länge hat. `len`
Teilzeichenfolge (str, pos [, len])	Gibt die Teilzeichenfolge zurück`str`, die bei der Länge beginnt `pos` und die Länge hat`len`, oder den Teil des Byte-Arrays, der bei beginnt `pos` und die Länge hat. `len`

Funktion	Beschreibung
Teilzeichenfolge (str FROM pos [FÜR LEN]])	Gibt den Teilstring zurück`str`, der bei der Länge beginnt `pos` und die Länge hat`len`, oder den Teil eines Byte-Arrays, der bei der Länge beginnt `pos` und diese hat. `len`
substring_index (str, delim, count)	Gibt die Teilzeichenfolge zurück, die `str` vor `count` dem Auftreten des Trennzeichens entstanden ist. `delim` Falls positiv, `count` wird alles zurückgegeben, was sich links vom letzten Trennzeichen befindet (von links gezählt). Wenn negativ `count` ist, wird alles zurückgegeben, was sich rechts vom letzten Trennzeichen befindet (von rechts gezählt). Die Funktion substring_index führt bei der Suche nach eine Übereinstimmung zwischen Groß- und Kleinschreibung durch. `delim`
to_binary (str [, fmt])	Konvertiert die Eingabe in einen Binärwert `str`, der auf dem angegebenen Wert basiert. `fmt` `fmt`kann ein Zeichenkettenliteral von „hex“, „utf-8", „utf8" oder „base64" sein, das Groß- und Kleinschreibung nicht berücksic htigt. Standardmäßig ist das Binärformat für die Konvertierung „hex“, wenn es weggelassen wird. `fmt` Die Funktion gibt NULL zurück, wenn mindestens einer der Eingabeparameter NULL ist.

Funktion	Beschreibung
to_char (NumberExpr, FormatExpr)	Konvertiert in eine Zeichenfolge, `numberExpr` die auf dem basiert. `formatExpr` Löst eine Ausnahme aus, wenn die Konvertierung fehlschlägt. Das Format kann ohne Berücksichtigung der Groß- und Kleinschreibung aus den folgenden Zeichen bestehen: '0' oder '9': Gibt eine erwartete Ziffer zwischen 0 und 9 an. Eine Folge von 0 oder 9 in der Formatzeichenfolge entspricht einer Ziffernfolge im Eingabewert, wodurch eine Ergebniszeichenfolge mit derselben Länge wie die entsprechende Sequenz in der Formatzeichenfolge generiert wird. Die Ergebniszeichenfolge wird links mit Nullen aufgefüllt, wenn die 0/9-Sequenz mehr Ziffern umfasst als der entsprechende Teil des Dezimalwerts, mit 0 beginnt und vor dem Dezimalpunkt liegt. Andernfalls wird sie mit Leerzeichen aufgefüllt. '.' oder 'D': Gibt die Position des Dezimaltrennzeichens an (optional, nur einmal zulässig). ',' oder 'G': Gibt die Position des Gruppierungstrennzeichens (Tausende) an (,). Links und rechts von jedem Gruppierungstrennzeichen muss eine 0 oder 9 stehen. '

Funktion	Beschreibung
to_number (expr, fmt)	Konvertiert die Zeichenfolge 'expr' in eine Zahl, die auf dem Zeichenkettenformat 'fmt' basiert. Löst eine Ausnahme aus, wenn die Konvertierung fehlschlägt. Das Format kann ohne Berücksichtigung der Groß- und Kleinschreibung aus den folgenden Zeichen bestehen: '0' oder '9': Gibt eine erwartete Ziffer zwischen 0 und 9 an. Eine Folge von 0 oder 9 in der Formatzeichenfolge entspricht einer Ziffernfolge in der Eingabezeichenfolge. Wenn die 0/9-Sequenz mit 0 beginnt und vor dem Dezimaltrennzeichen liegt, kann sie nur einer Ziffernfolge derselben Größe entsprechen. Andernfalls, wenn die Sequenz mit 9 beginnt oder nach dem Dezimalpunkt liegt, kann sie einer Ziffernfolge entsprechen, die dieselbe oder eine kleinere Größe hat. '.' oder 'D': Gibt die Position des Dezimaltrennzeichens an (optional, nur einmal zulässig). ',' oder 'G': Gibt die Position des Gruppierungstrennz eichens (Tausend) an (,). Links und rechts von jedem Gruppierungstrennzeichen muss eine 0 oder 9 stehen. 'expr' muss mit dem Gruppieru ngstrennzeichen übereinstimmen, das für die Größe der Zahl relevant ist. '

Funktion	Beschreibung
to_varchar (NumberExpr, FormatExpr)	Konvertiert in `numberExpr` eine Zeichenfolge, die auf dem basiert. `formatExpr` Löst eine Ausnahme aus, wenn die Konvertierung fehlschlägt. Das Format kann ohne Berücksichtigung der Groß- und Kleinschreibung aus den folgenden Zeichen bestehen: '0' oder '9': Gibt eine erwartete Ziffer zwischen 0 und 9 an. Eine Folge von 0 oder 9 in der Formatzeichenfolge entspricht einer Ziffernfolge im Eingabewert, wodurch eine Ergebniszeichenfolge mit derselben Länge wie die entsprechende Sequenz in der Formatzeichenfolge generiert wird. Die Ergebniszeichenfolge wird links mit Nullen aufgefüllt, wenn die 0/9-Sequenz mehr Ziffern umfasst als der entsprechende Teil des Dezimalwerts, mit 0 beginnt und vor dem Dezimalpunkt liegt. Andernfalls wird sie mit Leerzeichen aufgefüllt. '.' oder 'D': Gibt die Position des Dezimaltrennzeichens an (optional, nur einmal zulässig). ',' oder 'G': Gibt die Position des Gruppierungstrennzeichens (Tausende) an (,). Links und rechts von jedem Gruppierungstrennzeichen muss eine 0 oder 9 stehen. '
übersetzen (Eingabe, von, nach)	Übersetzt die `input` Zeichenfolge, indem die in der `from` Zeichenfolge vorhandenen Zeichen durch die entsprechenden Zeichen in der `to` Zeichenfolge ersetzt werden.
trim (str)	Entfernt die führenden und abschließenden Leerzeichen von`str`.
trim (BEIDE VON str)	Entfernt die führenden und nachfolgenden Leerzeichen von`str`.

Funktion	Beschreibung
trim (FÜHREND VON str)	Entfernt die führenden Leerzeichen von`str`.
trim (NACHFOLGEND VON str)	Entfernt die abschließenden Leerzeichen von. `str`
trim (trimStr VON str)	Entferne die führenden und nachfolgenden Zeichen von. `trimStr` `str`
trim (BEIDE trimStr VON str)	Entferne die führenden und nachfolgenden Zeichen von. `trimStr` `str`
trim (FÜHRENDES TrimStr VON str)	Entferne die führenden `trimStr` Zeichen von. `str`
trim (ABSCHLIESSENDES TrimStr VON str)	Entferne die nachfolgenden `trimStr` Zeichen von. `str`
try_to_binary (str [, fmt])	Dies ist eine spezielle Version von`to_binary` , die dieselbe Operation ausführt, aber einen NULL-Wert zurückgibt, anstatt einen Fehler auszulösen, wenn die Konvertierung nicht durchgeführt werden kann.
try_to_number (expr, fmt)	Konvertiert die Zeichenfolge 'expr' in eine Zahl, die auf dem Zeichenkettenformat basiert. `fmt` Gibt NULL zurück, wenn die Zeichenfolge 'expr' nicht dem erwarteten Format entspricht. Das Format folgt derselben Semantik wie die Funktion to_number.
ucase (str)	Gibt zurück, `str` bei der alle Zeichen in Großbuchstaben geändert wurden.
unbase64 (str)	Konvertiert das Argument von einer Base-64-Z eichenfolge in eine `str` Binärdatei.

Funktion	Beschreibung
oberer Wert (str)	Gibt zurück, `str` bei der alle Zeichen in Großbuchstaben geändert wurden.

Beispiele

```
-- ascii
SELECT ascii('222');
+----------+
|ascii(222)|
+----------+
|        50|
+----------+
SELECT ascii(2);
+--------+
|ascii(2)|
+--------+
|      50|
+--------+
-- base64
SELECT base64('Feathers');
+-----------------+
|base64(Feathers)|
+-----------------+
|     RmVhdGhlcnM=|
+-----------------+
SELECT base64(x'537061726b2053514c');
+----------------------------+
|base64(X'537061726B2053514C')|
+----------------------------+
|                 U3BhcmsgU1FM|
+----------------------------+
-- bit_length
SELECT bit_length('Feathers');
+---------------------+
|bit_length(Feathers)|
+---------------------+
|                   64|
+---------------------+
SELECT bit_length(x'537061726b2053514c');
```

```
+--------------------------------+
|bit_length(X'537061726B2053514C')|
+--------------------------------+
|                              72|
+--------------------------------+
-- btrim
SELECT btrim('    Feathers   ');
+----------------------+
|btrim(    Feathers   )|
+----------------------+
|              Feathers|
+----------------------+
SELECT btrim(encode('    Feathers   ', 'utf-8'));
+-----------------------------------+
|btrim(encode(    Feathers   , utf-8))|
+-----------------------------------+
|                           Feathers|
+-----------------------------------+
SELECT btrim('Feathers', 'Fe');
+---------------------+
|btrim(Alphabet, Al)|
+---------------------+
|               athers|
+---------------------+
SELECT btrim(encode('Feathers', 'utf-8'), encode('Al', 'utf-8'));
+-------------------------------------------------+
|btrim(encode(Feathers, utf-8), encode(Al, utf-8))|
+-------------------------------------------------+
|                                           athers|
+-------------------------------------------------+
-- char
SELECT char(65);
+--------+
|char(65)|
+--------+
|       A|
+--------+
-- char_length
SELECT char_length('Feathers ');
+-----------------------+
|char_length(Feathers )|
+-----------------------+
|                      9 |
+-----------------------+
```

```
SELECT char_length(x'537061726b2053514c');
+---------------------------------+
|char_length(X'537061726B2053514C')|
+---------------------------------+
|                                9|
+---------------------------------+
SELECT CHAR_LENGTH('Feathers ');
+-----------------------+
|char_length(Feathers )|
+-----------------------+
|                     9|
+-----------------------+
SELECT CHARACTER_LENGTH('Feathers ');
+----------------------------+
|character_length(Feathers )|
+----------------------------+
|                           9|
+----------------------------+
-- character_length
SELECT character_length('Feathers ');
+----------------------------+
|character_length(Feathers )|
+----------------------------+
|                           9|
+----------------------------+
SELECT character_length(x'537061726b2053514c');
+-------------------------------------+
|character_length(X'537061726B2053514C')|
+-------------------------------------+
|                                    9|
+-------------------------------------+
SELECT CHAR_LENGTH('Feathers ');
+-----------------------+
|char_length(Feathers )|
+-----------------------+
|                     9|
+-----------------------+
SELECT CHARACTER_LENGTH('Feathers ');
+----------------------------+
|character_length(Feathers )|
+----------------------------+
|                           9|
+----------------------------+
-- chr
```

```
SELECT chr(65);
+-------+
|chr(65)|
+-------+
|      A|
+-------+
-- concat_ws
SELECT concat_ws(' ', 'Fea', 'thers');
+------------------------+
|concat_ws( , Fea, thers)|
+------------------------+
|               Feathers|
+------------------------+
SELECT concat_ws('s');
+------------+
|concat_ws(s)|
+------------+
|            |
+------------+
SELECT concat_ws('/', 'foo', null, 'bar');
+----------------------------+
|concat_ws(/, foo, NULL, bar)|
+----------------------------+
|                     foo/bar|
+----------------------------+
SELECT concat_ws(null, 'Fea', 'thers');
+--------------------------+
|concat_ws(NULL, Fea, thers)|
+--------------------------+
|                      NULL|
+--------------------------+
-- contains
SELECT contains('Feathers', 'Fea');
+-------------------------+
|contains(Feathers, Fea)|
+-------------------------+
|                     true|
+-------------------------+
SELECT contains('Feathers', 'SQL');
+-------------------------+
|contains(Feathers, SQL)|
+-------------------------+
|                     false|
+-------------------------+
```

```
SELECT contains('Feathers', null);
+-------------------------+
|contains(Feathers, NULL)|
+-------------------------+
|                     NULL|
+-------------------------+
SELECT contains(x'537061726b2053514c', x'537061726b');
+-----------------------------------------------+
|contains(X'537061726B2053514C', X'537061726B')|
+-----------------------------------------------+
|                                           true|
+-----------------------------------------------+
-- decode
SELECT decode(encode('abc', 'utf-8'), 'utf-8');
+---------------------------------+
|decode(encode(abc, utf-8), utf-8)|
+---------------------------------+
|                              abc|
+---------------------------------+
SELECT decode(2, 1, 'Southlake', 2, 'San Francisco', 3, 'New Jersey', 4, 'Seattle',
 'Non domestic');
+-------------------------------------------------------------------------------+
|decode(2, 1, Southlake, 2, San Francisco, 3, New Jersey, 4, Seattle, Non domestic)|
+-------------------------------------------------------------------------------+
|                                                                  San Francisco|
+-------------------------------------------------------------------------------+
SELECT decode(6, 1, 'Southlake', 2, 'San Francisco', 3, 'New Jersey', 4, 'Seattle',
 'Non domestic');
+-------------------------------------------------------------------------------+
|decode(6, 1, Southlake, 2, San Francisco, 3, New Jersey, 4, Seattle, Non domestic)|
+-------------------------------------------------------------------------------+
|                                                                   Non domestic|
+-------------------------------------------------------------------------------+
SELECT decode(6, 1, 'Southlake', 2, 'San Francisco', 3, 'New Jersey', 4, 'Seattle');
+-----------------------------------------------------------------+
|decode(6, 1, Southlake, 2, San Francisco, 3, New Jersey, 4, Seattle)|
+-----------------------------------------------------------------+
|                                                             NULL|
+-----------------------------------------------------------------+
SELECT decode(null, 6, 'Fea', NULL, 'thers', 4, 'rock');
+----------------------------------------+
|decode(NULL, 6, Fea, NULL, thers, 4, rock)|
+----------------------------------------+
|                                   thers|
```

```
+----------------------------------------+
-- elt
SELECT elt(1, 'scala', 'java');
+------------------+
|elt(1, scala, java)|
+------------------+
|              scala|
+------------------+
SELECT elt(2, 'a', 1);
+------------+
|elt(2, a, 1)|
+------------+
|           1|
+------------+
-- encode
SELECT encode('abc', 'utf-8');
+------------------+
|encode(abc, utf-8)|
+------------------+
|        [61 62 63]|
+------------------+
-- endswith
SELECT endswith('Feathers', 'ers');
+------------------------+
|endswith(Feathers, ers)|
+------------------------+
|                    true|
+------------------------+
SELECT endswith('Feathers', 'SQL');
+-------------------------+
|endswith(Feathers, SQL)|
+-------------------------+
|                     false|
+-------------------------+
SELECT endswith('Feathers', null);
+-------------------------+
|endswith(Feathers, NULL)|
+-------------------------+
|                     NULL|
+-------------------------+
SELECT endswith(x'537061726b2053514c', x'537061726b');
+-----------------------------------------------+
|endswith(X'537061726B2053514C', X'537061726B')|
+-----------------------------------------------+
```

```
|                                           false|
+--------------------------------------------+
SELECT endswith(x'537061726b2053514c', x'53514c');
+----------------------------------------+
|endswith(X'537061726B2053514C', X'53514C')|
+----------------------------------------+
|                                    true|
+----------------------------------------+
-- find_in_set
SELECT find_in_set('ab','abc,b,ab,c,def');
+------------------------------+
|find_in_set(ab, abc,b,ab,c,def)|
+------------------------------+
|                             3|
+------------------------------+
-- format_number
SELECT format_number(12332.123456, 4);
+------------------------------+
|format_number(12332.123456, 4)|
+------------------------------+
|                  12,332.1235|
+------------------------------+
SELECT format_number(12332.123456, '##################.###');
+---------------------------------------------------+
|format_number(12332.123456, ##################.###)|
+---------------------------------------------------+
|                                          12332.123|
+---------------------------------------------------+
-- format_string
SELECT format_string("Hello World %d %s", 100, "days");
+-----------------------------------------+
|format_string(Hello World %d %s, 100, days)|
+-----------------------------------------+
|                      Hello World 100 days|
+-----------------------------------------+
-- initcap
SELECT initcap('Feathers');
+------------------+
|initcap(Feathers)|
+------------------+
|         Feathers|
+------------------+
-- instr
SELECT instr('Feathers', 'ers');
```

```
+--------------------+
|instr(Feathers, ers)|
+--------------------+
|                   6|
+--------------------+
-- lcase
SELECT lcase('Feathers');
+---------------+
|lcase(Feathers)|
+---------------+
|       feathers|
+---------------+
-- left
SELECT left('Feathers', 3);
+------------------+
|left(Feathers, 3)|
+------------------+
|               Fea|
+------------------+
SELECT left(encode('Feathers', 'utf-8'), 3);
+---------------------------------+
|left(encode(Feathers, utf-8), 3)|
+---------------------------------+
|                         [RmVh]|
+---------------------------------+
-- len
SELECT len('Feathers ');
+---------------+
|len(Feathers )|
+---------------+
|             9|
+---------------+
SELECT len(x'537061726b2053514c');
+--------------------------+
|len(X'537061726B2053514C')|
+--------------------------+
|                         9|
+--------------------------+
SELECT CHAR_LENGTH('Feathers ');
+-----------------------+
|char_length(Feathers )|
+-----------------------+
|                      9|
+-----------------------+
```

```
SELECT CHARACTER_LENGTH('Feathers ');
+---------------------------+
|character_length(Feathers )|
+---------------------------+
|                          9|
+---------------------------+
-- length
SELECT length('Feathers ');
+------------------+
|length(Feathers )|
+------------------+
|                9|
+------------------+
SELECT length(x'537061726b2053514c');
+-----------------------------+
|length(X'537061726B2053514C')|
+-----------------------------+
|                            9|
+-----------------------------+
SELECT CHAR_LENGTH('Feathers ');
+-----------------------+
|char_length(Feathers )|
+-----------------------+
|                      9|
+-----------------------+
SELECT CHARACTER_LENGTH('Feathers ');
+---------------------------+
|character_length(Feathers )|
+---------------------------+
|                          9|
+---------------------------+
-- levenshtein
SELECT levenshtein('kitten', 'sitting');
+---------------------------+
|levenshtein(kitten, sitting)|
+---------------------------+
|                           3|
+---------------------------+
SELECT levenshtein('kitten', 'sitting', 2);
+-------------------------------+
|levenshtein(kitten, sitting, 2)|
+-------------------------------+
|                             -1|
+-------------------------------+
```

```
-- locate
SELECT locate('bar', 'foobarbar');
+-------------------------+
|locate(bar, foobarbar, 1)|
+-------------------------+
|                        4|
+-------------------------+
SELECT locate('bar', 'foobarbar', 5);
+-------------------------+
|locate(bar, foobarbar, 5)|
+-------------------------+
|                        7|
+-------------------------+
SELECT POSITION('bar' IN 'foobarbar');
+-------------------------+
|locate(bar, foobarbar, 1)|
+-------------------------+
|                        4|
+-------------------------+
-- lower
SELECT lower('Feathers');
+---------------+
|lower(Feathers)|
+---------------+
|       feathers|
+---------------+
-- lpad
SELECT lpad('hi', 5, '??');
+---------------+
|lpad(hi, 5, ??)|
+---------------+
|          ???hi|
+---------------+
SELECT lpad('hi', 1, '??');
+---------------+
|lpad(hi, 1, ??)|
+---------------+
|              h|
+---------------+
SELECT lpad('hi', 5);
+--------------+
|lpad(hi, 5,  )|
+--------------+
|            hi|
```

```
+--------------+
SELECT hex(lpad(unhex('aabb'), 5));
+-------------------------------+
|hex(lpad(unhex(aabb), 5, X'00'))|
+-------------------------------+
|                     000000AABB|
+-------------------------------+
SELECT hex(lpad(unhex('aabb'), 5, unhex('1122')));
+-------------------------------------+
|hex(lpad(unhex(aabb), 5, unhex(1122)))|
+-------------------------------------+
|                           112211AABB|
+-------------------------------------+
-- ltrim
SELECT ltrim('    Feathers   ');
+----------------------+
|ltrim(    Feathers   )|
+----------------------+
|           Feathers   |
+----------------------+
-- luhn_check
SELECT luhn_check('8112189876');
+----------------------+
|luhn_check(8112189876)|
+----------------------+
|                  true|
+----------------------+
SELECT luhn_check('79927398713');
+-----------------------+
|luhn_check(79927398713)|
+-----------------------+
|                   true|
+-----------------------+
SELECT luhn_check('79927398714');
+-----------------------+
|luhn_check(79927398714)|
+-----------------------+
|                  false|
+-----------------------+
-- mask
SELECT mask('abcd-EFGH-8765-4321');
+----------------------------------------+
|mask(abcd-EFGH-8765-4321, X, x, n, NULL)|
+----------------------------------------+
```

```
|                    xxxx-XXXX-nnnn-nnnn|
+---------------------------------------+
SELECT mask('abcd-EFGH-8765-4321', 'Q');
+---------------------------------------+
|mask(abcd-EFGH-8765-4321, Q, x, n, NULL)|
+---------------------------------------+
|                    xxxx-QQQQ-nnnn-nnnn|
+---------------------------------------+
SELECT mask('AbCD123-@$#', 'Q', 'q');
+--------------------------------+
|mask(AbCD123-@$#, Q, q, n, NULL)|
+--------------------------------+
|                    QqQQnnn-@$#|
+--------------------------------+
SELECT mask('AbCD123-@$#');
+--------------------------------+
|mask(AbCD123-@$#, X, x, n, NULL)|
+--------------------------------+
|                    XxXXnnn-@$#|
+--------------------------------+
SELECT mask('AbCD123-@$#', 'Q');
+--------------------------------+
|mask(AbCD123-@$#, Q, x, n, NULL)|
+--------------------------------+
|                    QxQQnnn-@$#|
+--------------------------------+
SELECT mask('AbCD123-@$#', 'Q', 'q');
+--------------------------------+
|mask(AbCD123-@$#, Q, q, n, NULL)|
+--------------------------------+
|                    QqQQnnn-@$#|
+--------------------------------+
SELECT mask('AbCD123-@$#', 'Q', 'q', 'd');
+--------------------------------+
|mask(AbCD123-@$#, Q, q, d, NULL)|
+--------------------------------+
|                    QqQQddd-@$#|
+--------------------------------+
SELECT mask('AbCD123-@$#', 'Q', 'q', 'd', 'o');
+-----------------------------+
|mask(AbCD123-@$#, Q, q, d, o)|
+-----------------------------+
|                 QqQQdddoooo|
+-----------------------------+
```

```
SELECT mask('AbCD123-@$#', NULL, 'q', 'd', 'o');
+--------------------------------+
|mask(AbCD123-@$#, NULL, q, d, o)|
+--------------------------------+
|                     AqCDdddoooo|
+--------------------------------+
SELECT mask('AbCD123-@$#', NULL, NULL, 'd', 'o');
+-----------------------------------+
|mask(AbCD123-@$#, NULL, NULL, d, o)|
+-----------------------------------+
|                        AbCDdddoooo|
+-----------------------------------+
SELECT mask('AbCD123-@$#', NULL, NULL, NULL, 'o');
+--------------------------------------+
|mask(AbCD123-@$#, NULL, NULL, NULL, o)|
+--------------------------------------+
|                           AbCD123oooo|
+--------------------------------------+
SELECT mask(NULL, NULL, NULL, NULL, 'o');
+--------------------------------+
|mask(NULL, NULL, NULL, NULL, o)|
+--------------------------------+
|                           NULL|
+--------------------------------+
SELECT mask(NULL);
+-------------------------+
|mask(NULL, X, x, n, NULL)|
+-------------------------+
|                     NULL|
+-------------------------+
SELECT mask('AbCD123-@$#', NULL, NULL, NULL, NULL);
+-----------------------------------------+
|mask(AbCD123-@$#, NULL, NULL, NULL, NULL)|
+-----------------------------------------+
|                              AbCD123-@$#|
+-----------------------------------------+
-- octet_length
SELECT octet_length('Feathers');
+----------------------+
|octet_length(Feathers)|
+----------------------+
|                     8|
+----------------------+
SELECT octet_length(x'537061726b2053514c');
```

```
+----------------------------------+
|octet_length(X'537061726B2053514C')|
+----------------------------------+
|                                 9|
+----------------------------------+
-- overlay
SELECT overlay('Feathers' PLACING '_' FROM 6);
+---------------------------+
|overlay(Feathers, _, 6, -1)|
+---------------------------+
|                  Feathe_ers|
+---------------------------+
SELECT overlay('Feathers' PLACING 'ures' FROM 5);
+-----------------------------+
|overlay(Feathers, ures, 5, -1)|
+-----------------------------+
|                     Features  |
+-----------------------------+
-- position
SELECT position('bar', 'foobarbar');
+---------------------------+
|position(bar, foobarbar, 1)|
+---------------------------+
|                          4|
+---------------------------+
SELECT position('bar', 'foobarbar', 5);
+---------------------------+
|position(bar, foobarbar, 5)|
+---------------------------+
|                          7|
+---------------------------+
SELECT POSITION('bar' IN 'foobarbar');
+-------------------------+
|locate(bar, foobarbar, 1)|
+-------------------------+
|                        4|
+-------------------------+
-- printf
SELECT printf("Hello World %d %s", 100, "days");
+-----------------------------------+
|printf(Hello World %d %s, 100, days)|
+-----------------------------------+
|               Hello World 100 days|
+-----------------------------------+
```

```
-- regexp_count
SELECT regexp_count('Steven Jones and Stephen Smith are the best players', 'Ste(v|
ph)en');
+-------------------------------------------------------------------------------+
|regexp_count(Steven Jones and Stephen Smith are the best players, Ste(v|ph)en)|
+-------------------------------------------------------------------------------+
|                                                                              2|
+-------------------------------------------------------------------------------+
SELECT regexp_count('abcdefghijklmnopqrstuvwxyz', '[a-z]{3}');
+--------------------------------------------------+
|regexp_count(abcdefghijklmnopqrstuvwxyz, [a-z]{3})|
+--------------------------------------------------+
|                                                 8|
+--------------------------------------------------+
-- regexp_extract
SELECT regexp_extract('100-200', '(\\d+)-(\\d+)', 1);
+--------------------------------------+
|regexp_extract(100-200, (\d+)-(\d+), 1)|
+--------------------------------------+
|                                   100|
+--------------------------------------+
-- regexp_extract_all
SELECT regexp_extract_all('100-200, 300-400', '(\\d+)-(\\d+)', 1);
+-----------------------------------------------------+
|regexp_extract_all(100-200, 300-400, (\d+)-(\d+), 1)|
+-----------------------------------------------------+
|                                           [100, 300]|
+-----------------------------------------------------+
-- regexp_instr
SELECT regexp_instr('user@opensearch.org', '@[^.]*');
+-----------------------------------------------+
|regexp_instr(user@opensearch.org, @[^.]*, 0)|
+-----------------------------------------------+
|                                              5|
+-----------------------------------------------+
-- regexp_replace
SELECT regexp_replace('100-200', '(\\d+)', 'num');
+--------------------------------------+
|regexp_replace(100-200, (\d+), num, 1)|
+--------------------------------------+
|                               num-num|
+--------------------------------------+
-- regexp_substr
```

```
SELECT regexp_substr('Steven Jones and Stephen Smith are the best players', 'Ste(v|
ph)en');
+-----------------------------------------------------------------------------+
|regexp_substr(Steven Jones and Stephen Smith are the best players, Ste(v|ph)en)|
+-----------------------------------------------------------------------------+
|                                                                        Steven|
+-----------------------------------------------------------------------------+
SELECT regexp_substr('Steven Jones and Stephen Smith are the best players', 'Jeck');
+-----------------------------------------------------------------------+
|regexp_substr(Steven Jones and Stephen Smith are the best players, Jeck)|
+-----------------------------------------------------------------------+
|                                                                   NULL|
+-----------------------------------------------------------------------+
-- repeat
SELECT repeat('123', 2);
+--------------+
|repeat(123, 2)|
+--------------+
|        123123|
+--------------+
-- replace
SELECT replace('ABCabc', 'abc', 'DEF');
+-------------------------+
|replace(ABCabc, abc, DEF)|
+-------------------------+
|                   ABCDEF|
+-------------------------+
-- right
SELECT right('Feathers', 3);
+-------------------+
|right(Feathers, 3)|
+-------------------+
|                ers|
+-------------------+
-- rpad
SELECT rpad('hi', 5, '??');
+---------------+
|rpad(hi, 5, ??)|
+---------------+
|          hi???|
+---------------+
SELECT rpad('hi', 1, '??');
+---------------+
|rpad(hi, 1, ??)|
```

```
+---------------+
|              h|
+---------------+
SELECT rpad('hi', 5);
+--------------+
|rpad(hi, 5,  )|
+--------------+
|         hi   |
+--------------+
SELECT hex(rpad(unhex('aabb'), 5));
+--------------------------------+
|hex(rpad(unhex(aabb), 5, X'00'))|
+--------------------------------+
|                      AABB000000|
+--------------------------------+
SELECT hex(rpad(unhex('aabb'), 5, unhex('1122')));
+-------------------------------------+
|hex(rpad(unhex(aabb), 5, unhex(1122)))|
+-------------------------------------+
|                            AABB112211|
+-------------------------------------+
-- rtrim
SELECT rtrim('    Feathers   ');
+----------------------+
|rtrim(    Feathers   )|
+----------------------+
|              Feathers|
+----------------------+
-- sentences
SELECT sentences('Hi there! Good morning.');
+-------------------------------------+
|sentences(Hi there! Good morning., , )|
+-------------------------------------+
|                  [[Hi, there], [Go...|
+-------------------------------------+
-- soundex
SELECT soundex('Miller');
+---------------+
|soundex(Miller)|
+---------------+
|           M460|
+---------------+
-- space
SELECT concat(space(2), '1');
```

```
+-------------------+
|concat(space(2), 1)|
+-------------------+
|                  1|
+-------------------+
-- split
SELECT split('oneAtwoBthreeC', '[ABC]');
+--------------------------------+
|split(oneAtwoBthreeC, [ABC], -1)|
+--------------------------------+
|             [one, two, three, ]|
+--------------------------------+
SELECT split('oneAtwoBthreeC', '[ABC]', -1);
+--------------------------------+
|split(oneAtwoBthreeC, [ABC], -1)|
+--------------------------------+
|             [one, two, three, ]|
+--------------------------------+
SELECT split('oneAtwoBthreeC', '[ABC]', 2);
+-------------------------------+
|split(oneAtwoBthreeC, [ABC], 2)|
+-------------------------------+
|              [one, twoBthreeC]|
+-------------------------------+
-- split_part
SELECT split_part('11.12.13', '.', 3);
+--------------------------+
|split_part(11.12.13, ., 3)|
+--------------------------+
|                        13|
+--------------------------+
-- startswith
SELECT startswith('Feathers', 'Fea');
+---------------------------+
|startswith(Feathers, Fea)|
+---------------------------+
|                       true|
+---------------------------+
SELECT startswith('Feathers', 'SQL');
+--------------------------+
|startswith(Feathers, SQL)|
+--------------------------+
|                      false|
+--------------------------+
```

```
SELECT startswith('Feathers', null);
+--------------------------+
|startswith(Feathers, NULL)|
+--------------------------+
|                      NULL|
+--------------------------+
SELECT startswith(x'537061726b2053514c', x'537061726b');
+-------------------------------------------------+
|startswith(X'537061726B2053514C', X'537061726B')|
+-------------------------------------------------+
|                                             true|
+-------------------------------------------------+
SELECT startswith(x'537061726b2053514c', x'53514c');
+-----------------------------------------+
|startswith(X'537061726B2053514C', X'53514C')|
+-----------------------------------------+
|                                    false|
+-----------------------------------------+
-- substr
SELECT substr('Feathers', 5);
+-------------------------------+
|substr(Feathers, 5, 2147483647)|
+-------------------------------+
|                          hers |
+-------------------------------+
SELECT substr('Feathers', -3);
+-------------------------------+
|substr(Feathers, -3, 2147483647)|
+-------------------------------+
|                             ers|
+-------------------------------+
SELECT substr('Feathers', 5, 1);
+----------------------+
|substr(Feathers, 5, 1)|
+----------------------+
|                     h|
+----------------------+
SELECT substr('Feathers' FROM 5);
+---------------------------------+
|substring(Feathers, 5, 2147483647)|
+---------------------------------+
|                             hers |
+---------------------------------+
SELECT substr('Feathers' FROM -3);
```

```
+-----------------------------------+
|substring(Feathers, -3, 2147483647)|
+-----------------------------------+
|                                ers|
+-----------------------------------+
SELECT substr('Feathers' FROM 5 FOR 1);
+-------------------------+
|substring(Feathers, 5, 1)|
+-------------------------+
|                        h|
+-------------------------+
-- substring
SELECT substring('Feathers', 5);
+----------------------------------+
|substring(Feathers, 5, 2147483647)|
+----------------------------------+
|                             hers |
+----------------------------------+
SELECT substring('Feathers', -3);
+-----------------------------------+
|substring(Feathers, -3, 2147483647)|
+-----------------------------------+
|                                ers|
+-----------------------------------+
SELECT substring('Feathers', 5, 1);
+-------------------------+
|substring(Feathers, 5, 1)|
+-------------------------+
|                        h|
+-------------------------+
SELECT substring('Feathers' FROM 5);
+----------------------------------+
|substring(Feathers, 5, 2147483647)|
+----------------------------------+
|                             hers |
+----------------------------------+
SELECT substring('Feathers' FROM -3);
+-----------------------------------+
|substring(Feathers, -3, 2147483647)|
+-----------------------------------+
|                                ers|
+-----------------------------------+
SELECT substring('Feathers' FROM 5 FOR 1);
+-------------------------+
```

```
|substring(Feathers, 5, 1)|
+-------------------------+
|                        h|
+-------------------------+
-- substring_index
SELECT substring_index('www.apache.org', '.', 2);
+-----------------------------------+
|substring_index(www.apache.org, ., 2)|
+-----------------------------------+
|                         www.apache|
+-----------------------------------+
-- to_binary
SELECT to_binary('abc', 'utf-8');
+---------------------+
|to_binary(abc, utf-8)|
+---------------------+
|           [61 62 63]|
+---------------------+
-- to_char
SELECT to_char(454, '999');
+-----------------+
|to_char(454, 999)|
+-----------------+
|              454|
+-----------------+
SELECT to_char(454.00, '000D00');
+-----------------------+
|to_char(454.00, 000D00)|
+-----------------------+
|                 454.00|
+-----------------------+
SELECT to_char(12454, '99G999');
+----------------------+
|to_char(12454, 99G999)|
+----------------------+
|                12,454|
+----------------------+
SELECT to_char(78.12, '$99.99');
+----------------------+
|to_char(78.12, $99.99)|
+----------------------+
|                $78.12|
+----------------------+
SELECT to_char(-12454.8, '99G999D9S');
```

```
+---------------------------+
|to_char(-12454.8, 99G999D9S)|
+---------------------------+
|                  12,454.8-|
+---------------------------+
-- to_number
SELECT to_number('454', '999');
+-------------------+
|to_number(454, 999)|
+-------------------+
|               454|
+-------------------+
SELECT to_number('454.00', '000.00');
+-------------------------+
|to_number(454.00, 000.00)|
+-------------------------+
|                   454.00|
+-------------------------+
SELECT to_number('12,454', '99,999');
+-------------------------+
|to_number(12,454, 99,999)|
+-------------------------+
|                    12454|
+-------------------------+
SELECT to_number('$78.12', '$99.99');
+-------------------------+
|to_number($78.12, $99.99)|
+-------------------------+
|                    78.12|
+-------------------------+
SELECT to_number('12,454.8-', '99,999.9S');
+-------------------------------+
|to_number(12,454.8-, 99,999.9S)|
+-------------------------------+
|                       -12454.8|
+-------------------------------+
-- to_varchar
SELECT to_varchar(454, '999');
+-----------------+
|to_char(454, 999)|
+-----------------+
|              454|
+-----------------+
SELECT to_varchar(454.00, '000D00');
```

```
+-----------------------+
|to_char(454.00, 000D00)|
+-----------------------+
|                 454.00|
+-----------------------+
SELECT to_varchar(12454, '99G999');
+----------------------+
|to_char(12454, 99G999)|
+----------------------+
|               12,454|
+----------------------+
SELECT to_varchar(78.12, '$99.99');
+----------------------+
|to_char(78.12, $99.99)|
+----------------------+
|               $78.12|
+----------------------+
SELECT to_varchar(-12454.8, '99G999D9S');
+----------------------------+
|to_char(-12454.8, 99G999D9S)|
+----------------------------+
|                  12,454.8-|
+----------------------------+
-- translate
SELECT translate('AaBbCc', 'abc', '123');
+---------------------------+
|translate(AaBbCc, abc, 123)|
+---------------------------+
|                     A1B2C3|
+---------------------------+
-- try_to_binary
SELECT try_to_binary('abc', 'utf-8');
+-------------------------+
|try_to_binary(abc, utf-8)|
+-------------------------+
|              [61 62 63]|
+-------------------------+
select try_to_binary('a!', 'base64');
+-------------------------+
|try_to_binary(a!, base64)|
+-------------------------+
|                     NULL|
+-------------------------+
select try_to_binary('abc', 'invalidFormat');
```

```
+--------------------------------+
|try_to_binary(abc, invalidFormat)|
+--------------------------------+
|                            NULL|
+--------------------------------+
-- try_to_number
SELECT try_to_number('454', '999');
+----------------------+
|try_to_number(454, 999)|
+----------------------+
|                   454|
+----------------------+
SELECT try_to_number('454.00', '000.00');
+----------------------------+
|try_to_number(454.00, 000.00)|
+----------------------------+
|                      454.00|
+----------------------------+
SELECT try_to_number('12,454', '99,999');
+----------------------------+
|try_to_number(12,454, 99,999)|
+----------------------------+
|                       12454|
+----------------------------+
SELECT try_to_number('$78.12', '$99.99');
+----------------------------+
|try_to_number($78.12, $99.99)|
+----------------------------+
|                       78.12|
+----------------------------+
SELECT try_to_number('12,454.8-', '99,999.9S');
+---------------------------------+
|try_to_number(12,454.8-, 99,999.9S)|
+---------------------------------+
|                         -12454.8|
+---------------------------------+
-- ucase
SELECT ucase('Feathers');
+--------------+
|ucase(Feathers)|
+--------------+
|       FEATHERS|
+--------------+
-- unbase64
```

```
SELECT unbase64('U3BhcmsgU1FM');
+----------------------+
|unbase64(U3BhcmsgU1FM)|
+----------------------+
|  [53 70 61 72 6B 2...|
+----------------------+
-- upper
SELECT upper('Feathers');
+---------------+
|upper(Feathers)|
+---------------+
|       FEATHERS|
+---------------+
```

Datums- und Zeitfunktionen

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen SQL-Befehl unterstützen, finden Sie unter. the section called “Unterstützte SQL-Befehle”

Funktion	Beschreibung
add_months (Startdatum, Anzahl_Monate)	Gibt das Datum zurück, das danach liegt. `num_months start_date`
convert_timezone ([QuellTZ,] ZielTZ, QuellTS)	Konvertiert den Zeitstempel ohne Zeitzone von der Zeitzone in. `sourceTs sourceTz targetTz`
kurieren ()	Gibt das aktuelle Datum zu Beginn der Abfrageauswertung zurück. Alle Aufrufe von curdate innerhalb derselben Abfrage geben denselben Wert zurück.
aktuelles_Datum ()	Gibt das aktuelle Datum zu Beginn der Abfrageauswertung zurück. Alle Aufrufe von

Funktion	Beschreibung
	current_date innerhalb derselben Abfrage geben denselben Wert zurück.
current_date	Gibt das aktuelle Datum zu Beginn der Abfrageauswertung zurück.
current_timestamp ()	Gibt den aktuellen Zeitstempel zu Beginn der Abfrageauswertung zurück. Alle Aufrufe von current_timestamp innerhalb derselben Abfrage geben denselben Wert zurück.
current_timestamp	Gibt den aktuellen Zeitstempel zu Beginn der Abfrageauswertung zurück.
current_timezone ()	Gibt die lokale Zeitzone der aktuellen Sitzung zurück.
date_add (Startdatum, Anzahl_Tage)	Gibt das Datum zurück, das danach liegt. `num_days` `start_date`
date_diff (Enddatum, Startdatum)	Gibt die Anzahl der Tage von bis zurück. `startDate` `endDate`
date_format (Zeitstempel, fmt)	Konvertiert `timestamp` in einen Zeichenketten wert in dem durch das Datumsformat angegebenen Format. `fmt`
date_from_unix_date (Tage)	Erzeugt ein Datum aus der Anzahl der Tage seit dem 01.01.1970.
date_part (Feld, Quelle)	Extrahiert einen Teil der Quelle date/timestamp oder des Intervalls.
date_sub (Startdatum, Anzahl_Tage)	Gibt das Datum zurück, das davor liegt. `num_days` `start_date`

Funktion	Beschreibung
date_trunc (fmt, ts)	Gibt den Zeitstempel zurück, der auf die im Formatmodell angegebene Einheit `ts` gekürzt wurde. `fmt`
dateadd (Startdatum, Anzahl_Tage)	Gibt das Datum zurück, das danach liegt. `num_days` `start_date`
datediff (EndDate, StartDate)	Gibt die Anzahl der Tage von bis zurück. `startDate endDate`
Datepart (Feld, Quelle)	Extrahiert einen Teil der Quelle date/timestamp oder des Intervalls.
Tag (Datum)	Gibt den Tag des Monats zurück, an dem das Datum/der Zeitstempel angegeben wurde.
Tag des Monats (Datum)	Gibt den Tag des Monats zurück, an dem das Datum/der Zeitstempel angegeben wurde.
Wochentag (Datum)	Gibt den Wochentag für date/timestamp (1 = Sonntag, 2 = Montag,..., 7 = Samstag) zurück.
TagOfYear (Datum)	Gibt den Tag des Jahres des Datums/Ze itstempels zurück.
extrahieren (Feld AUS der Quelle)	Extrahiert einen Teil der Quelle date/timestamp oder des Intervalls.
from_unixtime (unix_time [, fmt])	Gibt im `unix_time` angegebenen Wert `fmt` zurück.
from_utc_timestamp (Zeitstempel, Zeitzone)	Ein gegebener Zeitstempel wie '2017-07-14 02:40:00.0 'interpretiert ihn als eine Zeit in UTC und rendert diese Zeit als Zeitstempel in der angegebenen Zeitzone. Zum Beispiel würde 'GMT+1' den Wert '2017-07-14 03:40:00.0 'ergeben.

Funktion	Beschreibung
Stunde (Zeitstempel)	Gibt die Stundenkomponente der Zeichenkette/des Zeitstempels zurück.
last_day (Datum)	Gibt den letzten Tag des Monats zurück, zu dem das Datum gehört.
localtimestamp ()	Gibt den aktuellen Zeitstempel ohne Zeitzone zu Beginn der Abfrageauswertung zurück. Alle Aufrufe von localtimestamp innerhalb derselben Abfrage geben denselben Wert zurück.
lokaler Zeitstempel	Gibt das aktuelle lokale Datum und die Uhrzeit in der Zeitzone der Sitzung zu Beginn der Abfrageauswertung zurück.
make_date (Jahr, Monat, Tag)	Erstellen Sie ein Datum aus den Feldern Jahr, Monat und Tag.
make_dt_interval ([Tage [, Stunden [, Minuten [, Sekunden]]]])	Stellen Sie die DayTimeIntervalType Dauer aus Tagen, Stunden, Minuten und Sekunden zusammen.
make_interval ([Jahre [, Monate [, Wochen [, Tage [, Stunden [, Minuten [, Sekunden]]]]]]])	Erstelle ein Intervall aus Jahren, Monaten, Wochen, Tagen, Stunden, Minuten und Sekunden.
make_timestamp (Jahr, Monat, Tag, Stunde, Minute, Sekunde [, Zeitzone])	Erstellen Sie einen Zeitstempel aus den Feldern Jahr, Monat, Tag, Stunde, Minute, Sekunde und Zeitzone.
make_timestamp_ltz (Jahr, Monat, Tag, Stunde, Minute, Sekunde [, Zeitzone])	Erstellt den aktuellen Zeitstempel mit der lokalen Zeitzone aus den Feldern Jahr, Monat, Tag, Stunde, Minute, Sekunde und Zeitzone.

Funktion	Beschreibung
make_timestamp_ntz (Jahr, Monat, Tag, Stunde, Minute, Sekunde)	Erstellen Sie lokale Datums-/Uhrzeitangaben aus den Feldern Jahr, Monat, Tag, Stunde, Minute und Sekunde.
make_ym_interval ([Jahre [, Monate]])	Erstelle das Jahres-Monats-Intervall aus Jahren, Monaten.
Minute (Zeitstempel)	Gibt die Minutenkomponente der Zeichenkette/des Zeitstempels zurück.
Monat (Datum)	Gibt die Monatskomponente des Datums-/Zeitstempels zurück.
months_between (timestamp1, timestamp2 [, RoundOff])	Wenn es später ist als, dann ist das Ergebnis positiv. `timestamp1` `timestamp2` Wenn `timestamp1` und `timestamp2` am selben Tag des Monats liegen oder beide der letzte Tag des Monats sind, wird die Uhrzeit ignoriert. Andernfalls wird die Differenz auf der Grundlage von 31 Tagen pro Monat berechnet und auf 8 Ziffern gerundet, es sei denn, RoundOff=False.
nächster Tag (Startdatum, Wochentag)	Gibt das erste Datum zurück, das später ist und wie angegeben benannt ist. `start_date` Die Funktion gibt NULL zurück, wenn mindestens einer der Eingabeparameter NULL ist.
jetzt ()	Gibt den aktuellen Zeitstempel zu Beginn der Abfrageauswertung zurück.
Quartal (Datum)	Gibt das Quartal des Jahres für das Datum im Bereich 1 bis 4 zurück.

Funktion	Beschreibung
Sekunde (Zeitstempel)	Gibt die zweite Komponente der Zeichenkette/des Zeitstempels zurück.
session_window (Zeitspalte, Gap_Duration)	Generiert ein Sitzungsfenster anhand eines Zeitstempels, der die Spalten- und Lückendauer angibt. Ausführliche Erläuterungen und Beispiele finden Sie im Dokument „Arten von Zeitfenstern“ im Dokument „Strukturiertes Streaming“.
timestamp_micros (Mikrosekunden)	Erzeugt einen Zeitstempel aus der Anzahl der Mikrosekunden seit der UTC-Epoche.
timestamp_millis (Millisekunden)	Erzeugt einen Zeitstempel aus der Anzahl der Millisekunden seit der UTC-Epoche.
timestamp_seconds (Sekunden)	Erzeugt einen Zeitstempel aus der Anzahl der Sekunden (kann Bruchteile sein) seit der UTC-Epoche.
to_date (date_str [, fmt])	Analysiert den `date_str` Ausdruck mit dem Ausdruck bis zu einem Datum. `fmt` Gibt bei ungültiger Eingabe Null zurück. Standardmäßig folgt es den Umwandlungsregeln für ein Datum, wenn das weggelassen `fmt` wird.
to_timestamp (timestamp_str [, fmt])	Analysiert den Ausdruck mit dem Ausdruck bis zu einem Zeitstempel. `timestamp_str` `fmt` Gibt bei ungültiger Eingabe Null zurück. Standardmäßig folgt es den Umwandlungsregeln in einen Zeitstempel, wenn der weggelassen `fmt` wird.

Funktion	Beschreibung
to_timestamp_ltz (timestamp_str [, fmt])	Analysiert den Ausdruck mit dem Ausdruck bis zu einem Zeitstempel mit lokaler Zeitzone. `timestamp_str` `fmt` Gibt bei ungültiger Eingabe Null zurück. Standardmäßig folgt es den Umwandlungsregeln in einen Zeitstempel, wenn der weggelassen `fmt` wird.
to_timestamp_ntz (timestamp_str [, fmt])	Analysiert den Ausdruck mit dem Ausdruck bis zu einem Zeitstempel ohne Zeitzone. `timestamp_str` `fmt` Gibt bei ungültiger Eingabe Null zurück. Standardmäßig folgt es den Umwandlungsregeln in einen Zeitstempel, wenn der weggelassen `fmt` wird.
to_unix_timestamp (TimeExp [, fmt])	Gibt den UNIX-Zeitstempel der angegebenen Zeit zurück.
to_utc_timestamp (Zeitstempel, Zeitzone)	Ein gegebener Zeitstempel wie '2017-07-14 02:40:00.0 'interpretiert ihn als eine Zeit in der angegebenen Zeitzone und rendert diese Zeit als Zeitstempel in UTC. Zum Beispiel würde 'GMT+1' den Wert '2017-07-14 01:40:00.0 'ergeben.
trunc (Datum, FMT)	Gibt zurück, `date` wobei der Zeitteil des Tages auf die im Formatmodell angegebene Einheit gekürzt wird. `fmt`
try_to_timestamp (timestamp_str [, fmt])	Analysiert den Ausdruck mit dem Ausdruck bis zu einem Zeitstempel. `timestamp_str` `fmt`
unix_date (Datum)	Gibt die Anzahl der Tage seit dem 01.01.1970 zurück.
unix_micros (Zeitstempel)	Gibt die Anzahl der Mikrosekunden seit 1970-01-01 00:00:00 UTC zurück.

Funktion	Beschreibung
unix_millis (Zeitstempel)	Gibt die Anzahl der Millisekunden seit 1970-01-01 00:00:00 UTC zurück. Kürzt höhere Genauigkeitsstufen.
unix_seconds (Zeitstempel)	Gibt die Anzahl der Sekunden seit 1970-01-01 00:00:00 UTC zurück. Kürzt höhere Genauigke itsstufen.
unix_timestamp ([TimeExp [, fmt]])	Gibt den UNIX-Zeitstempel der aktuellen oder angegebenen Zeit zurück.
Wochentag (Datum)	Gibt den Wochentag für date/timestamp (0 = Montag, 1 = Dienstag,..., 6 = Sonntag) zurück.
Woche des Jahres (Datum)	Gibt die Woche des Jahres des angegebenen Datums zurück. Es wird davon ausgegangen, dass eine Woche an einem Montag beginnt und Woche 1 ist die erste Woche mit >3 Tagen.
window (time_column, window_duration [, slide_duration [, start_time]])	Ordnet Zeilen anhand eines Zeitstempels, der die Spalte spezifiziert, in ein oder mehrere Zeitfenster. Fensteranfänge sind inklusiv, aber die Fensterenden sind exklusiv, z. B. 12:05 Uhr wird im Fenster [12:05,12:10) sein, aber nicht in [12:00,12:05). Windows kann eine Genauigkeit im Mikrosekundenbereich unterstützen. Windows in der Reihenfolge der Monate wird nicht unterstützt. Ausführli che Erläuterungen und Beispiele finden Sie im Dokument „Fensteroperationen bei Event Time“ im Dokument „Structured Streaming Guide“.

Funktion	Beschreibung
Fensterzeit (Fensterspalte)	Extrahieren Sie den Zeitwert aus der time/session Fensterspalte, der als Ereigniszeitwert des Fensters verwendet werden kann. Die extrahierte Zeit ist (window.end — 1), was die Tatsache widerspiegelt, dass die aggregierten Fenster eine exklusive Obergrenze haben — [Start, Ende). Ausführliche Erläuterungen und Beispiele finden Sie unter „Fensteroperationen bei Event Time“ im Dokument Structured Streaming Guide.
Jahr (Datum)	Gibt die Jahreskomponente des Datums-/Zeitstempels zurück.

Beispiele

```
-- add_months
SELECT add_months('2016-08-31', 1);
+-------------------------+
|add_months(2016-08-31, 1)|
+-------------------------+
|               2016-09-30|
+-------------------------+
-- convert_timezone
SELECT convert_timezone('Europe/Brussels', 'America/Los_Angeles',
 timestamp_ntz'2021-12-06 00:00:00');
+-----------------------------------------------------------------------------------------------
+
|convert_timezone(Europe/Brussels, America/Los_Angeles, TIMESTAMP_NTZ '2021-12-06
 00:00:00')|
+-----------------------------------------------------------------------------------------------
+
|                                                                                 2021-12-05
 15:00:00|
+-----------------------------------------------------------------------------------------------
+
SELECT convert_timezone('Europe/Brussels', timestamp_ntz'2021-12-05 15:00:00');
```

```
+------------------------------------------------------------------------------------------------
+
|convert_timezone(current_timezone(), Europe/Brussels, TIMESTAMP_NTZ '2021-12-05
 15:00:00')|
+------------------------------------------------------------------------------------------------
+
|                                                                              2021-12-05
 07:00:00|
+------------------------------------------------------------------------------------------------
+
-- curdate
SELECT curdate();
+--------------+
|current_date()|
+--------------+
|    2024-02-24|
+--------------+
-- current_date
SELECT current_date();
+--------------+
|current_date()|
+--------------+
|    2024-02-24|
+--------------+
SELECT current_date;
+--------------+
|current_date()|
+--------------+
|    2024-02-24|
+--------------+
-- current_timestamp
SELECT current_timestamp();
+--------------------+
| current_timestamp()|
+--------------------+
|2024-02-24 16:36:...|
+--------------------+
SELECT current_timestamp;
+--------------------+
| current_timestamp()|
+--------------------+
|2024-02-24 16:36:...|
+--------------------+
-- current_timezone
```

```
SELECT current_timezone();
+------------------+
|current_timezone()|
+------------------+
|        Asia/Seoul|
+------------------+
-- date_add
SELECT date_add('2016-07-30', 1);
+----------------------+
|date_add(2016-07-30, 1)|
+----------------------+
|             2016-07-31|
+----------------------+
-- date_diff
SELECT date_diff('2009-07-31', '2009-07-30');
+---------------------------------+
|date_diff(2009-07-31, 2009-07-30)|
+---------------------------------+
|                                1|
+---------------------------------+
SELECT date_diff('2009-07-30', '2009-07-31');
+---------------------------------+
|date_diff(2009-07-30, 2009-07-31)|
+---------------------------------+
|                               -1|
+---------------------------------+
-- date_format
SELECT date_format('2016-04-08', 'y');
+--------------------------+
|date_format(2016-04-08, y)|
+--------------------------+
|                      2016|
+--------------------------+
-- date_from_unix_date
SELECT date_from_unix_date(1);
+----------------------+
|date_from_unix_date(1)|
+----------------------+
|            1970-01-02|
+----------------------+
-- date_part
SELECT date_part('YEAR', TIMESTAMP '2019-08-12 01:00:00.123456');
+-------------------------------------------------------+
|date_part(YEAR, TIMESTAMP '2019-08-12 01:00:00.123456')|
```

```
+-----------------------------------------------------+
|                                                 2019|
+-----------------------------------------------------+
SELECT date_part('week', timestamp'2019-08-12 01:00:00.123456');
+-----------------------------------------------------+
|date_part(week, TIMESTAMP '2019-08-12 01:00:00.123456')|
+-----------------------------------------------------+
|                                                   33|
+-----------------------------------------------------+
SELECT date_part('doy', DATE'2019-08-12');
+--------------------------------+
|date_part(doy, DATE '2019-08-12')|
+--------------------------------+
|                             224|
+--------------------------------+
SELECT date_part('SECONDS', timestamp'2019-10-01 00:00:01.000001');
+------------------------------------------------------------+
|date_part(SECONDS, TIMESTAMP '2019-10-01 00:00:01.000001')|
+------------------------------------------------------------+
|                                                  1.000001|
+------------------------------------------------------------+
SELECT date_part('days', interval 5 days 3 hours 7 minutes);
+-------------------------------------------------+
|date_part(days, INTERVAL '5 03:07' DAY TO MINUTE)|
+-------------------------------------------------+
|                                                5|
+-------------------------------------------------+
SELECT date_part('seconds', interval 5 hours 30 seconds 1 milliseconds 1 microseconds);
+-----------------------------------------------------------------+
|date_part(seconds, INTERVAL '05:00:30.001001' HOUR TO SECOND)|
+-----------------------------------------------------------------+
|                                                       30.001001|
+-----------------------------------------------------------------+
SELECT date_part('MONTH', INTERVAL '2021-11' YEAR TO MONTH);
+-------------------------------------------------+
|date_part(MONTH, INTERVAL '2021-11' YEAR TO MONTH)|
+-------------------------------------------------+
|                                               11|
+-------------------------------------------------+
SELECT date_part('MINUTE', INTERVAL '123 23:55:59.002001' DAY TO SECOND);
+-----------------------------------------------------------------+
|date_part(MINUTE, INTERVAL '123 23:55:59.002001' DAY TO SECOND)|
+-----------------------------------------------------------------+
|                                                               55|
```

```
+------------------------------------------------------------+
-- date_sub
SELECT date_sub('2016-07-30', 1);
+----------------------+
|date_sub(2016-07-30, 1)|
+----------------------+
|             2016-07-29|
+----------------------+
-- date_trunc
SELECT date_trunc('YEAR', '2015-03-05T09:32:05.359');
+---------------------------------------+
|date_trunc(YEAR, 2015-03-05T09:32:05.359)|
+---------------------------------------+
|                      2015-01-01 00:00:00|
+---------------------------------------+
SELECT date_trunc('MM', '2015-03-05T09:32:05.359');
+--------------------------------------+
|date_trunc(MM, 2015-03-05T09:32:05.359)|
+--------------------------------------+
|                    2015-03-01 00:00:00|
+--------------------------------------+
SELECT date_trunc('DD', '2015-03-05T09:32:05.359');
+--------------------------------------+
|date_trunc(DD, 2015-03-05T09:32:05.359)|
+--------------------------------------+
|                    2015-03-05 00:00:00|
+--------------------------------------+
SELECT date_trunc('HOUR', '2015-03-05T09:32:05.359');
+---------------------------------------+
|date_trunc(HOUR, 2015-03-05T09:32:05.359)|
+---------------------------------------+
|                      2015-03-05 09:00:00|
+---------------------------------------+
SELECT date_trunc('MILLISECOND', '2015-03-05T09:32:05.123456');
+-----------------------------------------------------+
|date_trunc(MILLISECOND, 2015-03-05T09:32:05.123456)|
+-----------------------------------------------------+
|                               2015-03-05 09:32:...|
+-----------------------------------------------------+
-- dateadd
SELECT dateadd('2016-07-30', 1);
+----------------------+
|date_add(2016-07-30, 1)|
+----------------------+
```

```
|             2016-07-31|
+-----------------------+
-- datediff
SELECT datediff('2009-07-31', '2009-07-30');
+--------------------------------+
|datediff(2009-07-31, 2009-07-30)|
+--------------------------------+
|                               1|
+--------------------------------+
SELECT datediff('2009-07-30', '2009-07-31');
+--------------------------------+
|datediff(2009-07-30, 2009-07-31)|
+--------------------------------+
|                              -1|
+--------------------------------+
-- datepart
SELECT datepart('YEAR', TIMESTAMP '2019-08-12 01:00:00.123456');
+-----------------------------------------------------------+
|datepart(YEAR FROM TIMESTAMP '2019-08-12 01:00:00.123456')|
+-----------------------------------------------------------+
|                                                       2019|
+-----------------------------------------------------------+
SELECT datepart('week', timestamp'2019-08-12 01:00:00.123456');
+-----------------------------------------------------------+
|datepart(week FROM TIMESTAMP '2019-08-12 01:00:00.123456')|
+-----------------------------------------------------------+
|                                                         33|
+-----------------------------------------------------------+
SELECT datepart('doy', DATE'2019-08-12');
+----------------------------------+
|datepart(doy FROM DATE '2019-08-12')|
+----------------------------------+
|                               224|
+----------------------------------+
SELECT datepart('SECONDS', timestamp'2019-10-01 00:00:01.000001');
+-------------------------------------------------------------+
|datepart(SECONDS FROM TIMESTAMP '2019-10-01 00:00:01.000001')|
+-------------------------------------------------------------+
|                                                     1.000001|
+-------------------------------------------------------------+
SELECT datepart('days', interval 5 days 3 hours 7 minutes);
+---------------------------------------------------+
|datepart(days FROM INTERVAL '5 03:07' DAY TO MINUTE)|
+---------------------------------------------------+
```

```
|                                                     5|
+------------------------------------------------------+
SELECT datepart('seconds', interval 5 hours 30 seconds 1 milliseconds 1 microseconds);
+-----------------------------------------------------------------+
|datepart(seconds FROM INTERVAL '05:00:30.001001' HOUR TO SECOND)|
+-----------------------------------------------------------------+
|                                                        30.001001|
+-----------------------------------------------------------------+
SELECT datepart('MONTH', INTERVAL '2021-11' YEAR TO MONTH);
+-------------------------------------------------------+
|datepart(MONTH FROM INTERVAL '2021-11' YEAR TO MONTH)|
+-------------------------------------------------------+
|                                                     11|
+-------------------------------------------------------+
SELECT datepart('MINUTE', INTERVAL '123 23:55:59.002001' DAY TO SECOND);
+-------------------------------------------------------------------+
|datepart(MINUTE FROM INTERVAL '123 23:55:59.002001' DAY TO SECOND)|
+-------------------------------------------------------------------+
|                                                                 55|
+-------------------------------------------------------------------+
-- day
SELECT day('2009-07-30');
+---------------+
|day(2009-07-30)|
+---------------+
|             30|
+---------------+
-- dayofmonth
SELECT dayofmonth('2009-07-30');
+----------------------+
|dayofmonth(2009-07-30)|
+----------------------+
|                    30|
+----------------------+
-- dayofweek
SELECT dayofweek('2009-07-30');
+---------------------+
|dayofweek(2009-07-30)|
+---------------------+
|                    5|
+---------------------+
-- dayofyear
SELECT dayofyear('2016-04-09');
+---------------------+
```

```
|dayofyear(2016-04-09)|
+---------------------+
|                  100|
+---------------------+
-- extract
SELECT extract(YEAR FROM TIMESTAMP '2019-08-12 01:00:00.123456');
+-----------------------------------------------------------+
|extract(YEAR FROM TIMESTAMP '2019-08-12 01:00:00.123456')|
+-----------------------------------------------------------+
|                                                       2019|
+-----------------------------------------------------------+
SELECT extract(week FROM timestamp'2019-08-12 01:00:00.123456');
+-----------------------------------------------------------+
|extract(week FROM TIMESTAMP '2019-08-12 01:00:00.123456')|
+-----------------------------------------------------------+
|                                                         33|
+-----------------------------------------------------------+
SELECT extract(doy FROM DATE'2019-08-12');
+----------------------------------+
|extract(doy FROM DATE '2019-08-12')|
+----------------------------------+
|                               224|
+----------------------------------+
SELECT extract(SECONDS FROM timestamp'2019-10-01 00:00:01.000001');
+-------------------------------------------------------------+
|extract(SECONDS FROM TIMESTAMP '2019-10-01 00:00:01.000001')|
+-------------------------------------------------------------+
|                                                     1.000001|
+-------------------------------------------------------------+
SELECT extract(days FROM interval 5 days 3 hours 7 minutes);
+---------------------------------------------------+
|extract(days FROM INTERVAL '5 03:07' DAY TO MINUTE)|
+---------------------------------------------------+
|                                                  5|
+---------------------------------------------------+
SELECT extract(seconds FROM interval 5 hours 30 seconds 1 milliseconds 1 microseconds);
+-----------------------------------------------------------------+
|extract(seconds FROM INTERVAL '05:00:30.001001' HOUR TO SECOND)|
+-----------------------------------------------------------------+
|                                                        30.001001|
+-----------------------------------------------------------------+
SELECT extract(MONTH FROM INTERVAL '2021-11' YEAR TO MONTH);
+-----------------------------------------------------+
|extract(MONTH FROM INTERVAL '2021-11' YEAR TO MONTH)|
```

```
+-----------------------------------------------------+
|                                                   11|
+-----------------------------------------------------+
SELECT extract(MINUTE FROM INTERVAL '123 23:55:59.002001' DAY TO SECOND);
+-------------------------------------------------------------------+
|extract(MINUTE FROM INTERVAL '123 23:55:59.002001' DAY TO SECOND)|
+-------------------------------------------------------------------+
|                                                                 55|
+-------------------------------------------------------------------+
-- from_unixtime
SELECT from_unixtime(0, 'yyyy-MM-dd HH:mm:ss');
+-------------------------------------+
|from_unixtime(0, yyyy-MM-dd HH:mm:ss)|
+-------------------------------------+
|                  1970-01-01 09:00:00|
+-------------------------------------+
SELECT from_unixtime(0);
+-------------------------------------+
|from_unixtime(0, yyyy-MM-dd HH:mm:ss)|
+-------------------------------------+
|                  1970-01-01 09:00:00|
+-------------------------------------+
-- from_utc_timestamp
SELECT from_utc_timestamp('2016-08-31', 'Asia/Seoul');
+-----------------------------------------+
|from_utc_timestamp(2016-08-31, Asia/Seoul)|
+-----------------------------------------+
|                      2016-08-31 09:00:00|
+-----------------------------------------+
-- hour
SELECT hour('2009-07-30 12:58:59');
+-------------------------+
|hour(2009-07-30 12:58:59)|
+-------------------------+
|                       12|
+-------------------------+
-- last_day
SELECT last_day('2009-01-12');
+--------------------+
|last_day(2009-01-12)|
+--------------------+
|          2009-01-31|
+--------------------+
-- localtimestamp
```

```
SELECT localtimestamp();
+--------------------+
|    localtimestamp()|
+--------------------+
|2024-02-24 16:36:...|
+--------------------+
-- make_date
SELECT make_date(2013, 7, 15);
+----------------------+
|make_date(2013, 7, 15)|
+----------------------+
|            2013-07-15|
+----------------------+
SELECT make_date(2019, 7, NULL);
+------------------------+
|make_date(2019, 7, NULL)|
+------------------------+
|                    NULL|
+------------------------+
-- make_dt_interval
SELECT make_dt_interval(1, 12, 30, 01.001001);
+-------------------------------------+
|make_dt_interval(1, 12, 30, 1.001001)|
+-------------------------------------+
|                 INTERVAL '1 12:30...|
+-------------------------------------+
SELECT make_dt_interval(2);
+---------------------------------+
|make_dt_interval(2, 0, 0, 0.000000)|
+---------------------------------+
|               INTERVAL '2 00:00...|
+---------------------------------+
SELECT make_dt_interval(100, null, 3);
+---------------------------------------+
|make_dt_interval(100, NULL, 3, 0.000000)|
+---------------------------------------+
|                                   NULL|
+---------------------------------------+
-- make_interval
SELECT make_interval(100, 11, 1, 1, 12, 30, 01.001001);
+-----------------------------------------------+
|make_interval(100, 11, 1, 1, 12, 30, 1.001001)|
+-----------------------------------------------+
|                         100 years 11 mont...|
```

```
+-----------------------------------------------+
SELECT make_interval(100, null, 3);
+-----------------------------------------------+
|make_interval(100, NULL, 3, 0, 0, 0, 0.000000)|
+-----------------------------------------------+
|                                           NULL|
+-----------------------------------------------+
SELECT make_interval(0, 1, 0, 1, 0, 0, 100.000001);
+-----------------------------------------------+
|make_interval(0, 1, 0, 1, 0, 0, 100.000001)|
+-----------------------------------------------+
|                      1 months 1 days 1...|
+-----------------------------------------------+
-- make_timestamp
SELECT make_timestamp(2014, 12, 28, 6, 30, 45.887);
+-----------------------------------------+
|make_timestamp(2014, 12, 28, 6, 30, 45.887)|
+-----------------------------------------+
|                     2014-12-28 06:30:...|
+-----------------------------------------+
SELECT make_timestamp(2014, 12, 28, 6, 30, 45.887, 'CET');
+-------------------------------------------------+
|make_timestamp(2014, 12, 28, 6, 30, 45.887, CET)|
+-------------------------------------------------+
|                           2014-12-28 14:30:...|
+-------------------------------------------------+
SELECT make_timestamp(2019, 6, 30, 23, 59, 60);
+---------------------------------------+
|make_timestamp(2019, 6, 30, 23, 59, 60)|
+---------------------------------------+
|                    2019-07-01 00:00:00|
+---------------------------------------+
SELECT make_timestamp(2019, 6, 30, 23, 59, 1);
+---------------------------------------+
|make_timestamp(2019, 6, 30, 23, 59, 1)|
+---------------------------------------+
|                   2019-06-30 23:59:01|
+---------------------------------------+
SELECT make_timestamp(null, 7, 22, 15, 30, 0);
+---------------------------------------+
|make_timestamp(NULL, 7, 22, 15, 30, 0)|
+---------------------------------------+
|                                   NULL|
+---------------------------------------+
```

```
-- make_timestamp_ltz
SELECT make_timestamp_ltz(2014, 12, 28, 6, 30, 45.887);
+----------------------------------------------+
|make_timestamp_ltz(2014, 12, 28, 6, 30, 45.887)|
+----------------------------------------------+
|                          2014-12-28 06:30:...|
+----------------------------------------------+
SELECT make_timestamp_ltz(2014, 12, 28, 6, 30, 45.887, 'CET');
+-------------------------------------------------------+
|make_timestamp_ltz(2014, 12, 28, 6, 30, 45.887, CET)|
+-------------------------------------------------------+
|                               2014-12-28 14:30:...|
+-------------------------------------------------------+
SELECT make_timestamp_ltz(2019, 6, 30, 23, 59, 60);
+-----------------------------------------+
|make_timestamp_ltz(2019, 6, 30, 23, 59, 60)|
+-----------------------------------------+
|                      2019-07-01 00:00:00|
+-----------------------------------------+
SELECT make_timestamp_ltz(null, 7, 22, 15, 30, 0);
+---------------------------------------+
|make_timestamp_ltz(NULL, 7, 22, 15, 30, 0)|
+---------------------------------------+
|                                   NULL|
+---------------------------------------+
-- make_timestamp_ntz
SELECT make_timestamp_ntz(2014, 12, 28, 6, 30, 45.887);
+----------------------------------------------+
|make_timestamp_ntz(2014, 12, 28, 6, 30, 45.887)|
+----------------------------------------------+
|                          2014-12-28 06:30:...|
+----------------------------------------------+
SELECT make_timestamp_ntz(2019, 6, 30, 23, 59, 60);
+-----------------------------------------+
|make_timestamp_ntz(2019, 6, 30, 23, 59, 60)|
+-----------------------------------------+
|                      2019-07-01 00:00:00|
+-----------------------------------------+
SELECT make_timestamp_ntz(null, 7, 22, 15, 30, 0);
+---------------------------------------+
|make_timestamp_ntz(NULL, 7, 22, 15, 30, 0)|
+---------------------------------------+
|                                   NULL|
+---------------------------------------+
```

```
-- make_ym_interval
SELECT make_ym_interval(1, 2);
+---------------------+
|make_ym_interval(1, 2)|
+---------------------+
|  INTERVAL '1-2' YE...|
+---------------------+
SELECT make_ym_interval(1, 0);
+---------------------+
|make_ym_interval(1, 0)|
+---------------------+
|  INTERVAL '1-0' YE...|
+---------------------+
SELECT make_ym_interval(-1, 1);
+----------------------+
|make_ym_interval(-1, 1)|
+----------------------+
|   INTERVAL '-0-11' ...|
+----------------------+
SELECT make_ym_interval(2);
+---------------------+
|make_ym_interval(2, 0)|
+---------------------+
|  INTERVAL '2-0' YE...|
+---------------------+
-- minute
SELECT minute('2009-07-30 12:58:59');
+--------------------------+
|minute(2009-07-30 12:58:59)|
+--------------------------+
|                        58|
+--------------------------+
-- month
SELECT month('2016-07-30');
+-----------------+
|month(2016-07-30)|
+-----------------+
|                7|
+-----------------+
-- months_between
SELECT months_between('1997-02-28 10:30:00', '1996-10-30');
+----------------------------------------------------+
|months_between(1997-02-28 10:30:00, 1996-10-30, true)|
+----------------------------------------------------+
```

```
|                                              3.94959677|
+------------------------------------------------------+
SELECT months_between('1997-02-28 10:30:00', '1996-10-30', false);
+------------------------------------------------------+
|months_between(1997-02-28 10:30:00, 1996-10-30, false)|
+------------------------------------------------------+
|                                  3.9495967741935485|
+------------------------------------------------------+
-- next_day
SELECT next_day('2015-01-14', 'TU');
+-----------------------+
|next_day(2015-01-14, TU)|
+-----------------------+
|             2015-01-20|
+-----------------------+
-- now
SELECT now();
+--------------------+
|               now()|
+--------------------+
|2024-02-24 16:36:...|
+--------------------+
-- quarter
SELECT quarter('2016-08-31');
+-------------------+
|quarter(2016-08-31)|
+-------------------+
|                  3|
+-------------------+
-- second
SELECT second('2009-07-30 12:58:59');
+---------------------------+
|second(2009-07-30 12:58:59)|
+---------------------------+
|                         59|
+---------------------------+
-- session_window
SELECT a, session_window.start, session_window.end, count(*) as cnt FROM VALUES ('A1',
 '2021-01-01 00:00:00'), ('A1', '2021-01-01 00:04:30'), ('A1', '2021-01-01 00:10:00'),
 ('A2', '2021-01-01 00:01:00') AS tab(a, b) GROUP by a, session_window(b, '5 minutes')
 ORDER BY a, start;
+---+-------------------+-------------------+---+
|  a|              start|                end|cnt|
+---+-------------------+-------------------+---+
```

```
| A1|2021-01-01 00:00:00|2021-01-01 00:09:30|  2|
| A1|2021-01-01 00:10:00|2021-01-01 00:15:00|  1|
| A2|2021-01-01 00:01:00|2021-01-01 00:06:00|  1|
+---+-------------------+-------------------+---+
SELECT a, session_window.start, session_window.end, count(*) as cnt FROM VALUES ('A1',
 '2021-01-01 00:00:00'), ('A1', '2021-01-01 00:04:30'), ('A1', '2021-01-01 00:10:00'),
 ('A2', '2021-01-01 00:01:00'), ('A2', '2021-01-01 00:04:30') AS tab(a, b) GROUP by a,
 session_window(b, CASE WHEN a = 'A1' THEN '5 minutes' WHEN a = 'A2' THEN '1 minute'
 ELSE '10 minutes' END) ORDER BY a, start;
+---+-------------------+-------------------+---+
|  a|              start|                end|cnt|
+---+-------------------+-------------------+---+
| A1|2021-01-01 00:00:00|2021-01-01 00:09:30|  2|
| A1|2021-01-01 00:10:00|2021-01-01 00:15:00|  1|
| A2|2021-01-01 00:01:00|2021-01-01 00:02:00|  1|
| A2|2021-01-01 00:04:30|2021-01-01 00:05:30|  1|
+---+-------------------+-------------------+---+
-- timestamp_micros
SELECT timestamp_micros(1230219000123123);
+----------------------------------+
|timestamp_micros(1230219000123123)|
+----------------------------------+
|              2008-12-26 00:30:...|
+----------------------------------+
-- timestamp_millis
SELECT timestamp_millis(1230219000123);
+-------------------------------+
|timestamp_millis(1230219000123)|
+-------------------------------+
|           2008-12-26 00:30:...|
+-------------------------------+
-- timestamp_seconds
SELECT timestamp_seconds(1230219000);
+----------------------------+
|timestamp_seconds(1230219000)|
+----------------------------+
|          2008-12-26 00:30:00|
+----------------------------+
SELECT timestamp_seconds(1230219000.123);
+---------------------------------+
|timestamp_seconds(1230219000.123)|
+---------------------------------+
|             2008-12-26 00:30:...|
+---------------------------------+
```

```
-- to_date
SELECT to_date('2009-07-30 04:17:52');
+----------------------------+
|to_date(2009-07-30 04:17:52)|
+----------------------------+
|                  2009-07-30|
+----------------------------+
SELECT to_date('2016-12-31', 'yyyy-MM-dd');
+-------------------------------+
|to_date(2016-12-31, yyyy-MM-dd)|
+-------------------------------+
|                     2016-12-31|
+-------------------------------+
-- to_timestamp
SELECT to_timestamp('2016-12-31 00:12:00');
+---------------------------------+
|to_timestamp(2016-12-31 00:12:00)|
+---------------------------------+
|              2016-12-31 00:12:00|
+---------------------------------+
SELECT to_timestamp('2016-12-31', 'yyyy-MM-dd');
+-----------------------------------+
|to_timestamp(2016-12-31, yyyy-MM-dd)|
+-----------------------------------+
|                 2016-12-31 00:00:00|
+-----------------------------------+
-- to_timestamp_ltz
SELECT to_timestamp_ltz('2016-12-31 00:12:00');
+-------------------------------------+
|to_timestamp_ltz(2016-12-31 00:12:00)|
+-------------------------------------+
|                  2016-12-31 00:12:00|
+-------------------------------------+
SELECT to_timestamp_ltz('2016-12-31', 'yyyy-MM-dd');
+---------------------------------------+
|to_timestamp_ltz(2016-12-31, yyyy-MM-dd)|
+---------------------------------------+
|                     2016-12-31 00:00:00|
+---------------------------------------+
-- to_timestamp_ntz
SELECT to_timestamp_ntz('2016-12-31 00:12:00');
+-------------------------------------+
|to_timestamp_ntz(2016-12-31 00:12:00)|
+-------------------------------------+
```

```
|                  2016-12-31 00:12:00|
+-------------------------------------+
SELECT to_timestamp_ntz('2016-12-31', 'yyyy-MM-dd');
+---------------------------------------+
|to_timestamp_ntz(2016-12-31, yyyy-MM-dd)|
+---------------------------------------+
|                     2016-12-31 00:00:00|
+---------------------------------------+
-- to_unix_timestamp
SELECT to_unix_timestamp('2016-04-08', 'yyyy-MM-dd');
+---------------------------------------+
|to_unix_timestamp(2016-04-08, yyyy-MM-dd)|
+---------------------------------------+
|                                1460041200|
+---------------------------------------+
-- to_utc_timestamp
SELECT to_utc_timestamp('2016-08-31', 'Asia/Seoul');
+---------------------------------------+
|to_utc_timestamp(2016-08-31, Asia/Seoul)|
+---------------------------------------+
|                     2016-08-30 15:00:00|
+---------------------------------------+
-- trunc
SELECT trunc('2019-08-04', 'week');
+-----------------------+
|trunc(2019-08-04, week)|
+-----------------------+
|             2019-07-29|
+-----------------------+
SELECT trunc('2019-08-04', 'quarter');
+-------------------------+
|trunc(2019-08-04, quarter)|
+-------------------------+
|                2019-07-01|
+-------------------------+
SELECT trunc('2009-02-12', 'MM');
+---------------------+
|trunc(2009-02-12, MM)|
+---------------------+
|           2009-02-01|
+---------------------+
SELECT trunc('2015-10-27', 'YEAR');
+-----------------------+
|trunc(2015-10-27, YEAR)|
```

```
+-----------------------+
|             2015-01-01|
+-----------------------+
-- try_to_timestamp
SELECT try_to_timestamp('2016-12-31 00:12:00');
+-------------------------------------+
|try_to_timestamp(2016-12-31 00:12:00)|
+-------------------------------------+
|                  2016-12-31 00:12:00|
+-------------------------------------+
SELECT try_to_timestamp('2016-12-31', 'yyyy-MM-dd');
+---------------------------------------+
|try_to_timestamp(2016-12-31, yyyy-MM-dd)|
+---------------------------------------+
|                     2016-12-31 00:00:00|
+---------------------------------------+
SELECT try_to_timestamp('foo', 'yyyy-MM-dd');
+---------------------------------+
|try_to_timestamp(foo, yyyy-MM-dd)|
+---------------------------------+
|                             NULL|
+---------------------------------+
-- unix_date
SELECT unix_date(DATE("1970-01-02"));
+---------------------+
|unix_date(1970-01-02)|
+---------------------+
|                    1|
+---------------------+
-- unix_micros
SELECT unix_micros(TIMESTAMP('1970-01-01 00:00:01Z'));
+--------------------------------+
|unix_micros(1970-01-01 00:00:01Z)|
+--------------------------------+
|                         1000000|
+--------------------------------+
-- unix_millis
SELECT unix_millis(TIMESTAMP('1970-01-01 00:00:01Z'));
+--------------------------------+
|unix_millis(1970-01-01 00:00:01Z)|
+--------------------------------+
|                            1000|
+--------------------------------+
-- unix_seconds
```

```
SELECT unix_seconds(TIMESTAMP('1970-01-01 00:00:01Z'));
+---------------------------------+
|unix_seconds(1970-01-01 00:00:01Z)|
+---------------------------------+
|                                1|
+---------------------------------+
-- unix_timestamp
SELECT unix_timestamp();
+-------------------------------------------------------+
|unix_timestamp(current_timestamp(), yyyy-MM-dd HH:mm:ss)|
+-------------------------------------------------------+
|                                             1708760216|
+-------------------------------------------------------+
SELECT unix_timestamp('2016-04-08', 'yyyy-MM-dd');
+--------------------------------------+
|unix_timestamp(2016-04-08, yyyy-MM-dd)|
+--------------------------------------+
|                            1460041200|
+--------------------------------------+
-- weekday
SELECT weekday('2009-07-30');
+-------------------+
|weekday(2009-07-30)|
+-------------------+
|                  3|
+-------------------+
-- weekofyear
SELECT weekofyear('2008-02-20');
+----------------------+
|weekofyear(2008-02-20)|
+----------------------+
|                     8|
+----------------------+
-- window
SELECT a, window.start, window.end, count(*) as cnt FROM VALUES ('A1', '2021-01-01
 00:00:00'), ('A1', '2021-01-01 00:04:30'), ('A1', '2021-01-01 00:06:00'), ('A2',
 '2021-01-01 00:01:00') AS tab(a, b) GROUP by a, window(b, '5 minutes') ORDER BY a,
 start;
+---+-------------------+-------------------+---+
|  a|              start|                end|cnt|
+---+-------------------+-------------------+---+
| A1|2021-01-01 00:00:00|2021-01-01 00:05:00|  2|
| A1|2021-01-01 00:05:00|2021-01-01 00:10:00|  1|
| A2|2021-01-01 00:00:00|2021-01-01 00:05:00|  1|
```

```
+---+------------------+------------------+---+
SELECT a, window.start, window.end, count(*) as cnt FROM VALUES ('A1', '2021-01-01
 00:00:00'), ('A1', '2021-01-01 00:04:30'), ('A1', '2021-01-01 00:06:00'), ('A2',
 '2021-01-01 00:01:00') AS tab(a, b) GROUP by a, window(b, '10 minutes', '5 minutes')
 ORDER BY a, start;
+---+------------------+------------------+---+
|  a|             start|               end|cnt|
+---+------------------+------------------+---+
| A1|2020-12-31 23:55:00|2021-01-01 00:05:00|  2|
| A1|2021-01-01 00:00:00|2021-01-01 00:10:00|  3|
| A1|2021-01-01 00:05:00|2021-01-01 00:15:00|  1|
| A2|2020-12-31 23:55:00|2021-01-01 00:05:00|  1|
| A2|2021-01-01 00:00:00|2021-01-01 00:10:00|  1|
+---+------------------+------------------+---+
-- window_time
SELECT a, window.start as start, window.end as end, window_time(window), cnt FROM
 (SELECT a, window, count(*) as cnt FROM VALUES ('A1', '2021-01-01 00:00:00'), ('A1',
 '2021-01-01 00:04:30'), ('A1', '2021-01-01 00:06:00'), ('A2', '2021-01-01 00:01:00')
 AS tab(a, b) GROUP by a, window(b, '5 minutes') ORDER BY a, window.start);
+---+------------------+------------------+-------------------+---+
|  a|             start|               end| window_time(window)|cnt|
+---+------------------+------------------+-------------------+---+
| A1|2021-01-01 00:00:00|2021-01-01 00:05:00|2021-01-01 00:04:...|  2|
| A1|2021-01-01 00:05:00|2021-01-01 00:10:00|2021-01-01 00:09:...|  1|
| A2|2021-01-01 00:00:00|2021-01-01 00:05:00|2021-01-01 00:04:...|  1|
+---+------------------+------------------+-------------------+---+
-- year
SELECT year('2016-07-30');
+----------------+
|year(2016-07-30)|
+----------------+
|            2016|
+----------------+
```

Aggregationsfunktionen

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen SQL-Befehl unterstützen, finden Sie unter. the section called “Unterstützte SQL-Befehle”

Aggregatfunktionen verarbeiten Werte in mehreren Zeilen, um mathematische Berechnungen wie Summe, Durchschnitt, Zählung, minimum/maximum Werte, Standardabweichung und Schätzung sowie einige nichtmathematische Operationen durchzuführen.

Syntax

```
aggregate_function(input1 [, input2, ...]) FILTER (WHERE boolean_expression)
```

Parameter

- `boolean_expression`- Gibt einen beliebigen Ausdruck an, der zu einem booleschen Ergebnistyp ausgewertet wird. Zwei oder mehr Ausdrücke können mithilfe der logischen Operatoren (AND, OR) miteinander kombiniert werden.

Aggregatfunktionen mit geordneten Mengen

Diese Aggregatfunktionen verwenden eine andere Syntax als die anderen Aggregatfunktionen, um einen Ausdruck (normalerweise einen Spaltennamen) anzugeben, nach dem die Werte sortiert werden sollen.

Syntax

```
{ PERCENTILE_CONT | PERCENTILE_DISC }(percentile) WITHIN GROUP (ORDER BY
 { order_by_expression [ ASC | DESC ] [ NULLS { FIRST | LAST } ] [ , ... ] }) FILTER
 (WHERE boolean_expression)
```

Parameter

- `percentile`- Das Perzentil des Werts, den Sie finden möchten. Das Perzentil muss eine Konstante zwischen 0,0 und 1,0 sein.
- `order_by_expression`- Der Ausdruck (normalerweise ein Spaltenname), nach dem die Werte sortiert werden sollen, bevor sie aggregiert werden.
- `boolean_expression`- Gibt einen beliebigen Ausdruck an, der zu einem booleschen Ergebnistyp ausgewertet wird. Zwei oder mehr Ausdrücke können mithilfe der logischen Operatoren (AND, OR) miteinander kombiniert werden.

Beispiele

```
CREATE OR REPLACE TEMPORARY VIEW basic_pays AS SELECT * FROM VALUES
```

```
('Jane Doe','Accounting',8435),
('Akua Mansa','Accounting',9998),
('John Doe','Accounting',8992),
('Juan Li','Accounting',8870),
('Carlos Salazar','Accounting',11472),
('Arnav Desai','Accounting',6627),
('Saanvi Sarkar','IT',8113),
('Shirley Rodriguez','IT',5186),
('Nikki Wolf','Sales',9181),
('Alejandro Rosalez','Sales',9441),
('Nikhil Jayashankar','Sales',6660),
('Richard Roe','Sales',10563),
('Pat Candella','SCM',10449),
('Gerard Hernandez','SCM',6949),
('Pamela Castillo','SCM',11303),
('Paulo Santos','SCM',11798),
('Jorge Souza','SCM',10586)
AS basic_pays(employee_name, department, salary);
SELECT * FROM basic_pays;
+------------------+----------+------+
|    employee_name  |department|salary|
+------------------+----------+------+
| Arnav Desai       |Accounting|  6627|
| Jorge Souza       |       SCM| 10586|
| Jane Doe          |Accounting|  8435|
| Nikhil Jayashankar|     Sales|  6660|
| Diego Vanauf      |     Sales| 10563|
| Carlos Salazar    |Accounting| 11472|
| Gerard Hernandez  |       SCM|  6949|
| John Doe          |Accounting|  8992|
| Nikki Wolf        |     Sales|  9181|
| Paulo Santos      |       SCM| 11798|
| Saanvi Sarkar     |        IT|  8113|
| Shirley Rodriguez |        IT|  5186|
| Pat Candella      |       SCM| 10449|
| Akua Mansa        |Accounting|  9998|
| Pamela Castillo   |       SCM| 11303|
| Alejandro Rosalez |     Sales|  9441|
| Juan Li           |Accounting|  8870|
+------------------+----------+------+
SELECT
department,
percentile_cont(0.25) WITHIN GROUP (ORDER BY salary) AS pc1,
```

```
percentile_cont(0.25) WITHIN GROUP (ORDER BY salary) FILTER (WHERE employee_name LIKE
 '%Bo%') AS pc2,
percentile_cont(0.25) WITHIN GROUP (ORDER BY salary DESC) AS pc3,
percentile_cont(0.25) WITHIN GROUP (ORDER BY salary DESC) FILTER (WHERE employee_name
 LIKE '%Bo%') AS pc4,
percentile_disc(0.25) WITHIN GROUP (ORDER BY salary) AS pd1,
percentile_disc(0.25) WITHIN GROUP (ORDER BY salary) FILTER (WHERE employee_name LIKE
 '%Bo%') AS pd2,
percentile_disc(0.25) WITHIN GROUP (ORDER BY salary DESC) AS pd3,
percentile_disc(0.25) WITHIN GROUP (ORDER BY salary DESC) FILTER (WHERE employee_name
 LIKE '%Bo%') AS pd4
FROM basic_pays
GROUP BY department
ORDER BY department;
+----------+-------+--------+-------+--------+-----+-----+-----+-----+
|department|    pc1|     pc2|    pc3|     pc4|  pd1|  pd2|  pd3|  pd4|
+----------+-------+--------+-------+--------+-----+-----+-----+-----+
|Accounting|8543.75| 7838.25| 9746.5|10260.75| 8435| 6627| 9998|11472|
|        IT|5917.75|    NULL|7381.25|    NULL| 5186| NULL| 8113| NULL|
|     Sales|8550.75|    NULL| 9721.5|    NULL| 6660| NULL|10563| NULL|
|       SCM|10449.0|10786.25|11303.0|11460.75|10449|10449|11303|11798|
+----------+-------+--------+-------+--------+-----+-----+-----+-----+
```

Konditionale Funktionen

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen SQL-Befehl unterstützen, finden Sie unterthe section called “Unterstützte SQL-Befehle”.

Funktion	Beschreibung
verschmelzen (Ausdruck1, Ausdruck2,...)	Gibt das erste Argument zurück, das nicht Null ist, falls vorhanden. Andernfalls NULL.
wenn (Ausdruck1, Ausdruck2, Ausdruck3)	Wenn das Ergebnis wahr ist`expr1`, wird zurückgegeben; andernfalls wird zurückgeg eben. `expr2` `expr3`

Funktion	Beschreibung
wenn null (Ausdruck1, Ausdruck2)	Gibt zurück, `expr2` ob Null `expr1` ist oder nicht. `expr1`
nanvl (Ausdruck1, Ausdruck2)	Gibt zurück`expr1`, ob es nicht NaN oder `expr2` anders ist.
null (Ausdruck1, Ausdruck2)	Gibt null zurück, wenn gleich oder anders. `expr1` `expr2` `expr1`
nvl (Ausdruck1, Ausdruck2)	Gibt zurück, `expr2` ob Null `expr1` ist oder nicht. `expr1`
nvl2 (Ausdruck1, Ausdruck2, Ausdruck3)	Gibt zurück`expr2`, ob nicht Null ist oder nicht. `expr1` `expr3`
FALL WENN Ausdruck1 DANN Ausdruck2 [WENN Ausdruck3 DANN Ausdruck4] * [SONST Ausdruck5] ENDE	Wenn `expr1` = wahr, kehrt zurück; andernfalls wenn = wahr, kehrt zurück`expr2`; sonst kehrt zurück. `expr3` `expr4` `expr5`

Beispiele

```
-- coalesce
SELECT coalesce(NULL, 1, NULL);
+----------------------+
|coalesce(NULL, 1, NULL)|
+----------------------+
|                     1|
+----------------------+
-- if
SELECT if(1 < 2, 'a', 'b');
+------------------+
|(IF((1 < 2), a, b))|
+------------------+
|                 a|
+------------------+
-- ifnull
SELECT ifnull(NULL, array('2'));
+---------------------+
```

```
|ifnull(NULL, array(2))|
+----------------------+
|                   [2]|
+----------------------+
-- nanvl
SELECT nanvl(cast('NaN' as double), 123);
+-------------------------------+
|nanvl(CAST(NaN AS DOUBLE), 123)|
+-------------------------------+
|                          123.0|
+-------------------------------+
-- nullif
SELECT nullif(2, 2);
+------------+
|nullif(2, 2)|
+------------+
|        NULL|
+------------+
-- nvl
SELECT nvl(NULL, array('2'));
+------------------+
|nvl(NULL, array(2))|
+------------------+
|               [2]|
+------------------+
-- nvl2
SELECT nvl2(NULL, 2, 1);
+----------------+
|nvl2(NULL, 2, 1)|
+----------------+
|               1|
+----------------+
-- when
SELECT CASE WHEN 1 > 0 THEN 1 WHEN 2 > 0 THEN 2.0 ELSE 1.2 END;
+-----------------------------------------------------------+
|CASE WHEN (1 > 0) THEN 1 WHEN (2 > 0) THEN 2.0 ELSE 1.2 END|
+-----------------------------------------------------------+
|                                                        1.0|
+-----------------------------------------------------------+
SELECT CASE WHEN 1 < 0 THEN 1 WHEN 2 > 0 THEN 2.0 ELSE 1.2 END;
+-----------------------------------------------------------+
|CASE WHEN (1 < 0) THEN 1 WHEN (2 > 0) THEN 2.0 ELSE 1.2 END|
+-----------------------------------------------------------+
|                                                        2.0|
```

```
+-----------------------------------------------------------+
SELECT CASE WHEN 1 < 0 THEN 1 WHEN 2 < 0 THEN 2.0 END;
+-------------------------------------------------+
|CASE WHEN (1 < 0) THEN 1 WHEN (2 < 0) THEN 2.0 END|
+-------------------------------------------------+
|                                             NULL|
+-------------------------------------------------+
```

JSON-Funktionen

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen SQL-Befehl unterstützen, finden Sie unterthe section called “Unterstützte SQL-Befehle”.

Funktion	Beschreibung
from_json (JsonStr, Schema [, Optionen])	Gibt einen Strukturwert mit den angegebenen Werten `JsonStr` und `schema` zurück.
get_json_ object (json_txt, Pfad)	Extrahiert ein JSON-Objekt aus `path`.
json_arra y_length (JsonArray)	Gibt die Anzahl der Elemente im äußersten JSON-Array zurück.
json_obje ct_keys (json_object)	Gibt alle Schlüssel des äußersten JSON-Objekts als Array zurück.

Funktion	Beschreibung
json_tuple (JsonStr, p1, p2,..., pn)	Gibt ein Tupel wie die Funktion get_json_object zurück, benötigt aber mehrere Namen. Alle Eingabeparameter und Ausgabespaltentypen sind Zeichenketten.
schema_of _json (json [, Optionen])	Gibt das Schema im DDL-Format der JSON-Zeichenfolge zurück.
to_json (expr [, Optionen])	Gibt eine JSON-Zeichenfolge mit einem bestimmten Strukturwert zurück

Beispiele

```
-- from_json
SELECT from_json('{"a":1, "b":0.8}', 'a INT, b DOUBLE');
+---------------------------+
| from_json({"a":1, "b":0.8}) |
+---------------------------+
| {1, 0.8}                  |
+---------------------------+

SELECT from_json('{"time":"26/08/2015"}', 'time Timestamp', map('timestampFormat', 'dd/
MM/yyyy'));
+--------------------------------+
| from_json({"time":"26/08/2015"}) |
+--------------------------------+
| {2015-08-26 00:00...           |
+--------------------------------+

SELECT from_json('{"teacher": "Alice", "student": [{"name": "Bob", "rank": 1}, {"name":
 "Charlie", "rank": 2}]}', 'STRUCT<teacher: STRING, student: ARRAY<STRUCT<name: STRING,
 rank: INT>>>');
+-------------------------------------------------------------------------------------------------------
+
| from_json({"teacher": "Alice", "student": [{"name": "Bob", "rank": 1}, {"name":
 "Charlie", "rank": 2}]}) |
+-------------------------------------------------------------------------------------------------------
+
```

```
| {Alice, [{Bob, 1}...
                  |
+-------------------------------------------------------------------------------------------------------------------
+

-- get_json_object
SELECT get_json_object('{"a":"b"}', '$.a');
+-------------------------------+
| get_json_object({"a":"b"}, $.a) |
+-------------------------------+
| b                             |
+-------------------------------+

-- json_array_length
SELECT json_array_length('[1,2,3,4]');
+----------------------------+
| json_array_length([1,2,3,4]) |
+----------------------------+
| 4                          |
+----------------------------+

SELECT json_array_length('[1,2,3,{"f1":1,"f2":[5,6]},4]');
+-------------------------------------------------+
| json_array_length([1,2,3,{"f1":1,"f2":[5,6]},4]) |
+-------------------------------------------------+
| 5                                               |
+-------------------------------------------------+

SELECT json_array_length('[1,2');
+-----------------------+
| json_array_length([1,2) |
+-----------------------+
| NULL                  |
+-----------------------+

-- json_object_keys
SELECT json_object_keys('{}');
+--------------------+
| json_object_keys({}) |
+--------------------+
| []                 |
+--------------------+

SELECT json_object_keys('{"key": "value"}');
```

```
+---------------------------------+
| json_object_keys({"key": "value"}) |
+---------------------------------+
| [key]                           |
+---------------------------------+

SELECT json_object_keys('{"f1":"abc","f2":{"f3":"a", "f4":"b"}}');
+-----------------------------------------------------------+
| json_object_keys({"f1":"abc","f2":{"f3":"a", "f4":"b"}}) |
+-----------------------------------------------------------+
| [f1, f2]                                                  |
+-----------------------------------------------------------+

-- json_tuple
SELECT json_tuple('{"a":1, "b":2}', 'a', 'b');
+---+---+
| c0| c1|
+---+---+
|  1|  2|
+---+---+

-- schema_of_json
SELECT schema_of_json('[{"col":0}]');
+---------------------------+
| schema_of_json([{"col":0}]) |
+---------------------------+
| ARRAY<STRUCT<col:...      |
+---------------------------+

SELECT schema_of_json('[{"col":01}]', map('allowNumericLeadingZeros', 'true'));
+---------------------------+
| schema_of_json([{"col":01}]) |
+---------------------------+
| ARRAY<STRUCT<col:...       |
+---------------------------+

-- to_json
SELECT to_json(named_struct('a', 1, 'b', 2));
+---------------------------------+
| to_json(named_struct(a, 1, b, 2)) |
+---------------------------------+
| {"a":1,"b":2}                   |
+---------------------------------+
```

```
SELECT to_json(named_struct('time', to_timestamp('2015-08-26', 'yyyy-MM-dd')),
 map('timestampFormat', 'dd/MM/yyyy'));
+--------------------------------------------------------------------+
| to_json(named_struct(time, to_timestamp(2015-08-26, yyyy-MM-dd))) |
+--------------------------------------------------------------------+
| {"time":"26/08/20...                                               |
+--------------------------------------------------------------------+

SELECT to_json(array(named_struct('a', 1, 'b', 2)));
+----------------------------------------+
| to_json(array(named_struct(a, 1, b, 2))) |
+----------------------------------------+
| [{"a":1,"b":2}]                        |
+----------------------------------------+

SELECT to_json(map('a', named_struct('b', 1)));
+-----------------------------------+
| to_json(map(a, named_struct(b, 1))) |
+-----------------------------------+
| {"a":{"b":1}}                     |
+-----------------------------------+

SELECT to_json(map(named_struct('a', 1),named_struct('b', 2)));
+-------------------------------------------------------+
| to_json(map(named_struct(a, 1), named_struct(b, 2))) |
+-------------------------------------------------------+
| {"[1]":{"b":2}}                                       |
+-------------------------------------------------------+

SELECT to_json(map('a', 1));
+------------------+
| to_json(map(a, 1)) |
+------------------+
| {"a":1}          |
+------------------+

SELECT to_json(array(map('a', 1)));
+-------------------------+
| to_json(array(map(a, 1))) |
+-------------------------+
| [{"a":1}]               |
+-------------------------+
```

Array-Funktionen

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen SQL-Befehl unterstützen, finden Sie unterthe section called “Unterstützte SQL-Befehle”.

Funktion	Beschreibung
Array (expr,...)	Gibt ein Array mit den angegebenen Elementen zurück.
array_append (Array, Element)	Fügt das Element am Ende des als erstes Argument übergebenen Arrays hinzu. Der Typ des Elements sollte dem Typ der Elemente des Arrays ähneln. Das Null-Element wird ebenfalls an das Array angehängt. Aber wenn das Array übergeben wurde, ist die Ausgabe NULL
array_compact (Array)	Entfernt Nullwerte aus dem Array.
array_contains (Array, Wert)	Gibt true zurück, wenn das Array den Wert enthält.
array_distinct (Array)	Entfernt doppelte Werte aus dem Array.
array_except (Matrix1, Matrix2)	Gibt ein Array der Elemente in Array1, aber nicht in Array2, ohne Duplikate zurück.
array_insert (x, pos, wert)	Platziert val in den Index Pos von Array x. Array-Indizes beginnen bei 1. Der maximale negative Index ist -1, für den die Funktion ein neues Element nach dem aktuellen letzten Element einfügt. Bei einem Index über der Arraygröße werden dem Array oder, falls der Index negativ ist, dem Array „Null“ -Elemente vorangestellt.

Funktion	Beschreibung
array_intersect (Matrix1, Matrix2)	Gibt ein Array der Elemente im Schnittpunkt von array1 und array2 zurück, ohne Duplikate.
array_join (Array, Trennzeichen [, NullReplacement])	Verkettet die Elemente des angegebenen Arrays mithilfe des Trennzeichens und einer optionalen Zeichenfolge, um Nullen zu ersetzen. Wenn kein Wert für NullReplacement festgelegt ist, wird jeder Nullwert gefiltert.
array_max (Array)	Gibt den Maximalwert im Array zurück. NaN ist größer als alle Nicht-NaN-Elemente für den double/float Typ. NULL-Elemente werden übersprungen.
array_min (Array)	Gibt den Minimalwert im Array zurück. NaN ist größer als alle Nicht-NaN-Elemente für den double/float Typ. NULL-Elemente werden übersprungen.
array_position (Array, Element)	Gibt den (1-basierten) Index des ersten passenden Elements des Arrays als Long zurück oder 0, wenn keine Übereinstimmung gefunden wurde.
array_prepend (Array, Element)	Fügt das Element am Anfang des als erstes Argument übergebenen Arrays hinzu. Der Typ des Elements sollte dem Typ der Elemente des Arrays entsprechen. Das Null-Element wird dem Array ebenfalls vorangestellt. Aber wenn das übergebene Array NULL ist, ist die Ausgabe NULL
array_remove (Array, Element)	Entferne alle Elemente, die dem Element entsprechen, aus dem Array.

Funktion	Beschreibung
array_repeat (Element, Anzahl)	Gibt das Array zurück, das die Anzahl der Elemente enthält.
array_union (Matrix1, Matrix2)	Gibt ein Array der Elemente in der Vereinigung von array1 und array2 zurück, ohne Duplikate.
arrays_overlap (a1, a2)	Gibt true zurück, wenn a1 mindestens ein Nicht-Null-Element enthält, das auch in a2 vorhanden ist. Wenn die Arrays kein gemeinsames Element haben und beide nicht leer sind und eines von ihnen ein Null-Element enthält, wird Null zurückgegeben, andernfalls False.
arrays_zip (a1, a2,...)	Gibt ein zusammengeführtes Array von Strukturen zurück, in dem die N-te Struktur alle N-ten Werte der Eingabearrays enthält.
arrayOfArraysabflachen ()	Transformiert ein Array von Arrays in ein einzelnes Array.
get (Array, Index)	Gibt das Element eines Arrays an einem angegebenen (0-basierten) Index zurück. Wenn der Index außerhalb der Array-Grenzen zeigt, gibt diese Funktion NULL zurück.

Funktion	Beschreibung
Reihenfolge (Start, Stopp, Schritt)	Generiert eine Reihe von Elementen von Anfang bis Ende (einschließlich), die schrittweise inkrementiert werden. Der Typ der zurückgegebenen Elemente entspricht dem Typ der Argumentausdrücke. Unterstützte Typen sind: Byte, Short, Integer, Long, Date, Timestamp. Die Start- und Stoppausdrücke müssen denselben Typ ergeben. Wenn Start- und Stoppausdrücke in den Typ „Datum“ oder „Zeitstempel“ aufgelöst werden, muss der Schrittausdruck in den Typ „Intervall“, „Jahres-Monats-Intervall“ oder „Tages-Zeitintervall“ aufgelöst werden, andernfalls in denselben Typ wie die Start- und Stoppausdrücke.
Shuffle (Array)	Gibt eine zufällige Permutation des angegebenen Arrays zurück.
slice (x, Start, Länge)	Unterteilt Array x, beginnend mit dem Indexstart (Array-Indizes beginnen bei 1 oder beginnen am Ende, wenn Start negativ ist) mit der angegebenen Länge.
sort_array (Array [, aufsteigende Reihenfolge])	Sortiert das Eingabe-Array in aufsteigender oder absteigender Reihenfolge entsprechend der natürlichen Reihenfolge der Array-Elemente. NaN ist größer als alle Nicht-NaN-Elemente für den double/float Typ. Null-Elemente werden in aufsteigender Reihenfolge am Anfang des zurückgegebenen Arrays oder in absteigender Reihenfolge am Ende des zurückgegebenen Arrays platziert.

Beispiele

```
-- array
SELECT array(1, 2, 3);
+--------------+
|array(1, 2, 3)|
+--------------+
|     [1, 2, 3]|
+--------------+
-- array_append
SELECT array_append(array('b', 'd', 'c', 'a'), 'd');
+----------------------------------+
|array_append(array(b, d, c, a), d)|
+----------------------------------+
|                   [b, d, c, a, d]|
+----------------------------------+
SELECT array_append(array(1, 2, 3, null), null);
+---------------------------------------+
|array_append(array(1, 2, 3, NULL), NULL)|
+---------------------------------------+
|                    [1, 2, 3, NULL, N...|
+---------------------------------------+
SELECT array_append(CAST(null as Array<Int>), 2);
+---------------------+
|array_append(NULL, 2)|
+---------------------+
|                 NULL|
+---------------------+
-- array_compact
SELECT array_compact(array(1, 2, 3, null));
+----------------------------------+
|array_compact(array(1, 2, 3, NULL))|
+----------------------------------+
|                          [1, 2, 3]|
+----------------------------------+
SELECT array_compact(array("a", "b", "c"));
+-----------------------------+
|array_compact(array(a, b, c))|
+-----------------------------+
|                    [a, b, c]|
+-----------------------------+
-- array_contains
SELECT array_contains(array(1, 2, 3), 2);
+---------------------------------+
|array_contains(array(1, 2, 3), 2)|
```

```
+--------------------------------+
|                            true|
+--------------------------------+
-- array_distinct
SELECT array_distinct(array(1, 2, 3, null, 3));
+--------------------------------------+
|array_distinct(array(1, 2, 3, NULL, 3))|
+--------------------------------------+
|                       [1, 2, 3, NULL]|
+--------------------------------------+
-- array_except
SELECT array_except(array(1, 2, 3), array(1, 3, 5));
+-------------------------------------------+
|array_except(array(1, 2, 3), array(1, 3, 5))|
+-------------------------------------------+
|                                        [2]|
+-------------------------------------------+
-- array_insert
SELECT array_insert(array(1, 2, 3, 4), 5, 5);
+-----------------------------------+
|array_insert(array(1, 2, 3, 4), 5, 5)|
+-----------------------------------+
|                     [1, 2, 3, 4, 5]|
+-----------------------------------+
SELECT array_insert(array(5, 4, 3, 2), -1, 1);
+-----------------------------------+
|array_insert(array(5, 4, 3, 2), -1, 1)|
+-----------------------------------+
|                      [5, 4, 3, 2, 1]|
+-----------------------------------+
SELECT array_insert(array(5, 3, 2, 1), -4, 4);
+-----------------------------------+
|array_insert(array(5, 3, 2, 1), -4, 4)|
+-----------------------------------+
|                      [5, 4, 3, 2, 1]|
+-----------------------------------+
-- array_intersect
SELECT array_intersect(array(1, 2, 3), array(1, 3, 5));
+-----------------------------------------------+
|array_intersect(array(1, 2, 3), array(1, 3, 5))|
+-----------------------------------------------+
|                                         [1, 3]|
+-----------------------------------------------+
-- array_join
```

```
SELECT array_join(array('hello', 'world'), ' ');
+---------------------------------+
|array_join(array(hello, world),  )|
+---------------------------------+
|                      hello world|
+---------------------------------+
SELECT array_join(array('hello', null ,'world'), ' ');
+--------------------------------------+
|array_join(array(hello, NULL, world),  )|
+--------------------------------------+
|                             hello world|
+--------------------------------------+
SELECT array_join(array('hello', null ,'world'), ' ', ',');
+-----------------------------------------+
|array_join(array(hello, NULL, world),  , ,)|
+-----------------------------------------+
|                              hello , world|
+-----------------------------------------+
-- array_max
SELECT array_max(array(1, 20, null, 3));
+--------------------------------+
|array_max(array(1, 20, NULL, 3))|
+--------------------------------+
|                              20|
+--------------------------------+
-- array_min
SELECT array_min(array(1, 20, null, 3));
+--------------------------------+
|array_min(array(1, 20, NULL, 3))|
+--------------------------------+
|                               1|
+--------------------------------+
-- array_position
SELECT array_position(array(312, 773, 708, 708), 708);
+-----------------------------------------------+
|array_position(array(312, 773, 708, 708), 708)|
+-----------------------------------------------+
|                                              3|
+-----------------------------------------------+
SELECT array_position(array(312, 773, 708, 708), 414);
+-----------------------------------------------+
|array_position(array(312, 773, 708, 708), 414)|
+-----------------------------------------------+
|                                              0|
```

```
+-----------------------------------------------+
-- array_prepend
SELECT array_prepend(array('b', 'd', 'c', 'a'), 'd');
+----------------------------------+
|array_prepend(array(b, d, c, a), d)|
+----------------------------------+
|                    [d, b, d, c, a]|
+----------------------------------+
SELECT array_prepend(array(1, 2, 3, null), null);
+---------------------------------------+
|array_prepend(array(1, 2, 3, NULL), NULL)|
+---------------------------------------+
|                     [NULL, 1, 2, 3, N...|
+---------------------------------------+
SELECT array_prepend(CAST(null as Array<Int>), 2);
+----------------------+
|array_prepend(NULL, 2)|
+----------------------+
|                  NULL|
+----------------------+
-- array_remove
SELECT array_remove(array(1, 2, 3, null, 3), 3);
+---------------------------------------+
|array_remove(array(1, 2, 3, NULL, 3), 3)|
+---------------------------------------+
|                           [1, 2, NULL]|
+---------------------------------------+
-- array_repeat
SELECT array_repeat('123', 2);
+--------------------+
|array_repeat(123, 2)|
+--------------------+
|          [123, 123]|
+--------------------+
-- array_union
SELECT array_union(array(1, 2, 3), array(1, 3, 5));
+-----------------------------------------+
|array_union(array(1, 2, 3), array(1, 3, 5))|
+-----------------------------------------+
|                               [1, 2, 3, 5]|
+-----------------------------------------+
-- arrays_overlap
SELECT arrays_overlap(array(1, 2, 3), array(3, 4, 5));
+-------------------------------------------+
```

```
|arrays_overlap(array(1, 2, 3), array(3, 4, 5))|
+----------------------------------------------+
|                                          true|
+----------------------------------------------+
-- arrays_zip
SELECT arrays_zip(array(1, 2, 3), array(2, 3, 4));
+-----------------------------------------+
|arrays_zip(array(1, 2, 3), array(2, 3, 4))|
+-----------------------------------------+
|                      [{1, 2}, {2, 3}, ...|
+-----------------------------------------+
SELECT arrays_zip(array(1, 2), array(2, 3), array(3, 4));
+-------------------------------------------------+
|arrays_zip(array(1, 2), array(2, 3), array(3, 4))|
+-------------------------------------------------+
|                             [{1, 2, 3}, {2, 3...|
+-------------------------------------------------+
-- flatten
SELECT flatten(array(array(1, 2), array(3, 4)));
+---------------------------------------+
|flatten(array(array(1, 2), array(3, 4)))|
+---------------------------------------+
|                           [1, 2, 3, 4]|
+---------------------------------------+
-- get
SELECT get(array(1, 2, 3), 0);
+----------------------+
|get(array(1, 2, 3), 0)|
+----------------------+
|                     1|
+----------------------+
SELECT get(array(1, 2, 3), 3);
+----------------------+
|get(array(1, 2, 3), 3)|
+----------------------+
|                  NULL|
+----------------------+
SELECT get(array(1, 2, 3), -1);
+----------------------+
|get(array(1, 2, 3), -1)|
+----------------------+
|                   NULL|
+----------------------+
-- sequence
```

```
SELECT sequence(1, 5);
+---------------+
| sequence(1, 5)|
+---------------+
|[1, 2, 3, 4, 5]|
+---------------+
SELECT sequence(5, 1);
+---------------+
| sequence(5, 1)|
+---------------+
|[5, 4, 3, 2, 1]|
+---------------+
SELECT sequence(to_date('2018-01-01'), to_date('2018-03-01'), interval 1 month);
+------------------------------------------------------------------------+
|sequence(to_date(2018-01-01), to_date(2018-03-01), INTERVAL '1' MONTH)|
+------------------------------------------------------------------------+
|                                                    [2018-01-01, 2018...|
+------------------------------------------------------------------------+
SELECT sequence(to_date('2018-01-01'), to_date('2018-03-01'), interval '0-1' year to
 month);
+--------------------------------------------------------------------------------------+
|sequence(to_date(2018-01-01), to_date(2018-03-01), INTERVAL '0-1' YEAR TO MONTH)|
+--------------------------------------------------------------------------------------+
|                                                                  [2018-01-01, 2018...|
+--------------------------------------------------------------------------------------+
-- shuffle
SELECT shuffle(array(1, 20, 3, 5));
+---------------------------+
|shuffle(array(1, 20, 3, 5))|
+---------------------------+
|              [5, 1, 20, 3]|
+---------------------------+
SELECT shuffle(array(1, 20, null, 3));
+------------------------------+
|shuffle(array(1, 20, NULL, 3))|
+------------------------------+
|              [1, NULL, 20, 3]|
+------------------------------+
-- slice
SELECT slice(array(1, 2, 3, 4), 2, 2);
+------------------------------+
|slice(array(1, 2, 3, 4), 2, 2)|
+------------------------------+
|                        [2, 3]|
```

```
+------------------------------+
SELECT slice(array(1, 2, 3, 4), -2, 2);
+------------------------------+
|slice(array(1, 2, 3, 4), -2, 2)|
+------------------------------+
|                        [3, 4]|
+------------------------------+
-- sort_array
SELECT sort_array(array('b', 'd', null, 'c', 'a'), true);
+-----------------------------------------+
|sort_array(array(b, d, NULL, c, a), true)|
+-----------------------------------------+
|                      [NULL, a, b, c, d]|
+-----------------------------------------+
```

Fensterfunktionen

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen SQL-Befehl unterstützen, finden Sie unter. the section called “Unterstützte SQL-Befehle”

Fensterfunktionen arbeiten mit einer Gruppe von Zeilen, die als Fenster bezeichnet werden, und berechnen einen Rückgabewert für jede Zeile auf der Grundlage der Zeilengruppe. Fensterfunktionen sind nützlich, um Aufgaben wie die Berechnung eines gleitenden Durchschnitts, die Berechnung einer kumulativen Statistik oder den Zugriff auf den Wert von Zeilen anhand der relativen Position der aktuellen Zeile auszuführen.

Syntax

```
window_function [ nulls_option ] OVER ( [ { PARTITION | DISTRIBUTE } BY
 partition_col_name = partition_col_val ( [ , ... ] ) ] { ORDER | SORT } BY expression
 [ ASC | DESC ] [ NULLS { FIRST | LAST } ] [ , ... ] [ window_frame ] )
```

Parameter

- Rangfestlegungsfunktionen

  Syntax: `RANK | DENSE_RANK | PERCENT_RANK | NTILE | ROW_NUMBER`

Analytische Funktionen

Syntax: `CUME_DIST | LAG | LEAD | NTH_VALUE | FIRST_VALUE | LAST_VALUE`

Aggregationsfunktionen

Syntax: `MAX | MIN | COUNT | SUM | AVG | ...`

- `nulls_option`- Gibt an, ob Nullwerte bei der Auswertung der Fensterfunktion übersprungen werden sollen oder nicht. NULLS RESPEKTIEREN bedeutet, dass Nullwerte nicht übersprungen werden, NULL-Werte IGNORIEREN bedeutet, dass sie übersprungen werden. Falls nicht angegeben, ist die Standardeinstellung RESPECT NULLS.

  Syntax: `{ IGNORE | RESPECT } NULLS`

  Hinweis: `Only LAG | LEAD | NTH_VALUE FIRST_VALUE | LAST_VALUE` kann mit verwendet werden. `IGNORE NULLS`
- `window_frame`- Gibt an, in welcher Zeile das Fenster beginnen und wo es enden soll.

  Syntax: `{ RANGE | ROWS } { frame_start | BETWEEN frame_start AND frame_end }`

  frame_start und frame_end haben die folgende Syntax:

  Syntax: `UNBOUNDED PRECEDING | offset PRECEDING | CURRENT ROW | offset FOLLOWING | UNBOUNDED FOLLOWING`

  Offset: gibt den Offset von der Position der aktuellen Zeile an.

  Hinweis Wenn frame_end weggelassen wird, wird standardmäßig CURRENT ROW verwendet.

Beispiele

```
CREATE TABLE employees (name STRING, dept STRING, salary INT, age INT);
INSERT INTO employees VALUES ("Lisa", "Sales", 10000, 35);
INSERT INTO employees VALUES ("Evan", "Sales", 32000, 38);
INSERT INTO employees VALUES ("Fred", "Engineering", 21000, 28);
INSERT INTO employees VALUES ("Alex", "Sales", 30000, 33);
INSERT INTO employees VALUES ("Tom", "Engineering", 23000, 33);
INSERT INTO employees VALUES ("Jane", "Marketing", 29000, 28);
INSERT INTO employees VALUES ("Jeff", "Marketing", 35000, 38);
```

```
INSERT INTO employees VALUES ("Paul", "Engineering", 29000, 23);
INSERT INTO employees VALUES ("Chloe", "Engineering", 23000, 25);
SELECT * FROM employees;
+-----+-----------+------+-----+
| name|       dept|salary|  age|
+-----+-----------+------+-----+
|Chloe|Engineering| 23000|   25|
| Fred|Engineering| 21000|   28|
| Paul|Engineering| 29000|   23|
|Helen|  Marketing| 29000|   40|
|  Tom|Engineering| 23000|   33|
| Jane|  Marketing| 29000|   28|
| Jeff|  Marketing| 35000|   38|
| Evan|      Sales| 32000|   38|
| Lisa|      Sales| 10000|   35|
| Alex|      Sales| 30000|   33|
+-----+-----------+------+-----+
SELECT name, dept, salary, RANK() OVER (PARTITION BY dept ORDER BY salary) AS rank FROM
 employees;
+-----+-----------+------+----+
| name|       dept|salary|rank|
+-----+-----------+------+----+
| Lisa|      Sales| 10000|   1|
| Alex|      Sales| 30000|   2|
| Evan|      Sales| 32000|   3|
| Fred|Engineering| 21000|   1|
|  Tom|Engineering| 23000|   2|
|Chloe|Engineering| 23000|   2|
| Paul|Engineering| 29000|   4|
|Helen|  Marketing| 29000|   1|
| Jane|  Marketing| 29000|   1|
| Jeff|  Marketing| 35000|   3|
+-----+-----------+------+----+
SELECT name, dept, salary, DENSE_RANK() OVER (PARTITION BY dept ORDER BY salary ROWS
 BETWEEN
UNBOUNDED PRECEDING AND CURRENT ROW) AS dense_rank FROM employees;
+-----+-----------+------+----------+
| name|       dept|salary|dense_rank|
+-----+-----------+------+----------+
| Lisa|      Sales| 10000|         1|
| Alex|      Sales| 30000|         2|
| Evan|      Sales| 32000|         3|
| Fred|Engineering| 21000|         1|
|  Tom|Engineering| 23000|         2|
```

```
|Chloe|Engineering| 23000|         2|
| Paul|Engineering| 29000|         3|
|Helen|  Marketing| 29000|         1|
| Jane|  Marketing| 29000|         1|
| Jeff|  Marketing| 35000|         2|
+-----+-----------+------+----------+
SELECT name, dept, age, CUME_DIST() OVER (PARTITION BY dept ORDER BY age
RANGE BETWEEN UNBOUNDED PRECEDING AND CURRENT ROW) AS cume_dist FROM employees;
+-----+-----------+------+------------------+
| name|       dept|age   |         cume_dist|
+-----+-----------+------+------------------+
| Alex|      Sales|    33|0.3333333333333333|
| Lisa|      Sales|    35|0.6666666666666666|
| Evan|      Sales|    38|               1.0|
| Paul|Engineering|    23|              0.25|
|Chloe|Engineering|    25|              0.75|
| Fred|Engineering|    28|              0.25|
|  Tom|Engineering|    33|               1.0|
| Jane|  Marketing|    28|0.3333333333333333|
| Jeff|  Marketing|    38|0.6666666666666666|
|Helen|  Marketing|    40|               1.0|
+-----+-----------+------+------------------+
SELECT name, dept, salary, MIN(salary) OVER (PARTITION BY dept ORDER BY salary) AS min
FROM employees;
+-----+-----------+------+-----+
| name|       dept|salary|  min|
+-----+-----------+------+-----+
| Lisa|      Sales| 10000|10000|
| Alex|      Sales| 30000|10000|
| Evan|      Sales| 32000|10000|
|Helen|  Marketing| 29000|29000|
| Jane|  Marketing| 29000|29000|
| Jeff|  Marketing| 35000|29000|
| Fred|Engineering| 21000|21000|
|  Tom|Engineering| 23000|21000|
|Chloe|Engineering| 23000|21000|
| Paul|Engineering| 29000|21000|
+-----+-----------+------+-----+
SELECT name, salary,
LAG(salary) OVER (PARTITION BY dept ORDER BY salary) AS lag,
LEAD(salary, 1, 0) OVER (PARTITION BY dept ORDER BY salary) AS lead
FROM employees;
+-----+-----------+------+-----+-----+
| name|       dept|salary|  lag| lead|
```

```
+-----+-----------+------+-----+-----+
| Lisa|      Sales| 10000|NULL |30000|
| Alex|      Sales| 30000|10000|32000|
| Evan|      Sales| 32000|30000|    0|
| Fred|Engineering| 21000| NULL|23000|
|Chloe|Engineering| 23000|21000|23000|
|  Tom|Engineering| 23000|23000|29000|
| Paul|Engineering| 29000|23000|    0|
|Helen|  Marketing| 29000| NULL|29000|
| Jane|  Marketing| 29000|29000|35000|
| Jeff|  Marketing| 35000|29000|    0|
+-----+-----------+------+-----+-----+
SELECT id, v,
LEAD(v, 0) IGNORE NULLS OVER w lead,
LAG(v, 0) IGNORE NULLS OVER w lag,
NTH_VALUE(v, 2) IGNORE NULLS OVER w nth_value,
FIRST_VALUE(v) IGNORE NULLS OVER w first_value,
LAST_VALUE(v) IGNORE NULLS OVER w last_value
FROM test_ignore_null
WINDOW w AS (ORDER BY id)
ORDER BY id;
+--+----+----+----+---------+-----------+----------+
|id|   v|lead| lag|nth_value|first_value|last_value|
+--+----+----+----+---------+-----------+----------+
| 0|NULL|NULL|NULL|     NULL|       NULL|      NULL|
| 1|   x|   x|   x|     NULL|          x|         x|
| 2|NULL|NULL|NULL|     NULL|          x|         x|
| 3|NULL|NULL|NULL|     NULL|          x|         x|
| 4|   y|   y|   y|        y|          x|         y|
| 5|NULL|NULL|NULL|        y|          x|         y|
| 6|   z|   z|   z|        y|          x|         z|
| 7|   v|   v|   v|        y|          x|         v|
| 8|NULL|NULL|NULL|        y|          x|         v|
+--+----+----+----+---------+-----------+----------+
```

Konvertierungs-Funktionen

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen SQL-Befehl unterstützen, finden Sie unter. the section called “Unterstützte SQL-Befehle”

Funktion	Beschreibung
bigint (Ausdruck)	Wandelt den Wert `expr` in den Zieldatentyp `bigint` um.
binär (expr)	Wandelt den Wert `expr `in den Zieldatentyp `binary` um.
boolescher Wert (expr)	Wandelt den Wert `expr` in den Zieldatentyp `boolean` um.
cast (Typ expr AS)	Wandelt den Wert `expr` in den Zieldatentyp `type` um.
Datum (expr)	Wandelt den Wert `expr` in den Zieldatentyp `date` um.
dezimal (expr)	Wandelt den Wert `expr` in den Zieldatentyp `decimal` um.
doppelt (expr)	Wandelt den Wert `expr `in den Zieldatentyp `double` um.
float (expr)	Wandelt den Wert `expr `in den Zieldatentyp `float` um.
int (Ausdruck)	Wandelt den Wert `expr `in den Zieldatentyp `int` um.
smallint (expr)	Wandelt den Wert `expr` in den Zieldatentyp `smallint` um.
Zeichenfolge (expr)	Wandelt den Wert `expr `in den Zieldatentyp `string` um.
Zeitstempel (expr)	Wandelt den Wert `expr` in den Zieldatentyp `timestamp` um.
tinyint (expr)	Wandelt den Wert `expr` in den Zieldatentyp `tinyint` um.

Beispiele

```
-- cast
SELECT cast(field as int);
+---------------+
|CAST(field AS INT)|
+---------------+
|             10|
+---------------+
```

Prädikatsfunktionen

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen SQL-Befehl unterstützen, finden Sie unter. the section called “Unterstützte SQL-Befehle”

Funktion	Beschreibung
! expr	Logisch nicht.
expr1 < expr2	Gibt true zurück, wenn `expr1` kleiner als `expr2` ist.
Ausdruck1 <= Ausdruck2	Gibt true zurück, wenn `expr1` kleiner oder gleich `expr2` ist.
Ausdruck1 <=> Ausdruck2	Gibt dasselbe Ergebnis zurück wie der EQUAL (=) -Operator für Operanden, die nicht Null sind, gibt aber true zurück, wenn beide Null sind, und false, wenn einer von ihnen Null ist.
Ausdruck1 = Ausdruck2	Gibt true zurück, wenn `expr1` gleich `expr2` ist, andernfalls false.
Ausdruck1 == Ausdruck2	Gibt true zurück, wenn `expr1` gleich `expr2` ist, andernfalls false.
Ausdruck1 > Ausdruck2	Gibt true zurück, wenn `expr1` größer als `expr2` ist.
Ausdruck1 >= Ausdruck2	Gibt true zurück, wenn `expr1` größer oder gleich `expr2` ist.
expr1 und expr2	Logisches UND.
str, ich mag das Muster [ESCAPE Escape].	Gibt true zurück, wenn str zwischen `pattern` und `escape` passt, ohne Berücksichtigung der Groß- und Kleinschreibung, null, wenn irgendwelche Argumente Null sind, andernfalls false.
Ausdruck1 in (Ausdruck2, Ausdruck3,...)	Gibt true zurück, wenn `expr` einem beliebigen Wert von ValN entspricht.
isnan (Ausdruck)	Gibt true zurück, wenn `expr NaN ist, andernfalls false.
ist nicht null (expr)	Gibt true zurück, wenn `expr nicht Null ist, andernfalls false.

Funktion	Beschreibung
ist null (expr)	Gibt true zurück, wenn `expr null ist, andernfalls false.
str ähnliches Muster [ESCAPE Escape]	Gibt true zurück, wenn str `pattern` mit `escape` übereinstimmt, null, wenn irgendwelche Argumente null sind, andernfalls false.
nicht expr	Logisch nicht.
expr1 oder expr2	Logisches ODER.
regexp (str, regexp)	Gibt true zurück, wenn `str` mit `regexp` übereinstimmt, andernfalls false.
regexp_like (str, regexp)	Gibt true zurück, wenn `str` mit `regexp` übereinstimmt, andernfalls false.
rlike (str, regexp)	Gibt true zurück, wenn `str` mit `regexp` übereinstimmt, andernfalls false.

Beispiele

```
-- !
SELECT ! true;
+----------+
|(NOT true)|
+----------+
|     false|
+----------+
SELECT ! false;
+-----------+
|(NOT false)|
+-----------+
|       true|
+-----------+
SELECT ! NULL;
+----------+
|(NOT NULL)|
+----------+
|      NULL|
+----------+
```

```
-- <
SELECT to_date('2009-07-30 04:17:52') < to_date('2009-07-30 04:17:52');
+-------------------------------------------------------------+
|(to_date(2009-07-30 04:17:52) < to_date(2009-07-30 04:17:52))|
+-------------------------------------------------------------+
|                                                        false|
+-------------------------------------------------------------+
SELECT to_date('2009-07-30 04:17:52') < to_date('2009-08-01 04:17:52');
+-------------------------------------------------------------+
|(to_date(2009-07-30 04:17:52) < to_date(2009-08-01 04:17:52))|
+-------------------------------------------------------------+
|                                                         true|
+-------------------------------------------------------------+
SELECT 1 < NULL;
+----------+
|(1 < NULL)|
+----------+
|      NULL|
+----------+
-- <=
SELECT 2 <= 2;
+--------+
|(2 <= 2)|
+--------+
|    true|
+--------+
SELECT 1.0 <= '1';
+----------+
|(1.0 <= 1)|
+----------+
|      true|
+----------+
SELECT to_date('2009-07-30 04:17:52') <= to_date('2009-07-30 04:17:52');
+-------------------------------------------------------------+
|(to_date(2009-07-30 04:17:52) <= to_date(2009-07-30 04:17:52))|
+-------------------------------------------------------------+
|                                                         true|
+-------------------------------------------------------------+
SELECT to_date('2009-07-30 04:17:52') <= to_date('2009-08-01 04:17:52');
+-------------------------------------------------------------+
|(to_date(2009-07-30 04:17:52) <= to_date(2009-08-01 04:17:52))|
+-------------------------------------------------------------+
|                                                         true|
+-------------------------------------------------------------+
```

```
SELECT 1 <= NULL;
+-----------+
|(1 <= NULL)|
+-----------+
|       NULL|
+-----------+
-- <=>
SELECT 2 <=> 2;
+---------+
|(2 <=> 2)|
+---------+
|     true|
+---------+
SELECT 1 <=> '1';
+---------+
|(1 <=> 1)|
+---------+
|     true|
+---------+
SELECT true <=> NULL;
+---------------+
|(true <=> NULL)|
+---------------+
|          false|
+---------------+
SELECT NULL <=> NULL;
+---------------+
|(NULL <=> NULL)|
+---------------+
|           true|
+---------------+
-- =
SELECT 2 = 2;
+-------+
|(2 = 2)|
+-------+
|   true|
+-------+
SELECT 1 = '1';
+-------+
|(1 = 1)|
+-------+
|   true|
+-------+
```

```
SELECT true = NULL;
+-------------+
|(true = NULL)|
+-------------+
|         NULL|
+-------------+
SELECT NULL = NULL;
+-------------+
|(NULL = NULL)|
+-------------+
|         NULL|
+-------------+
-- ==
SELECT 2 == 2;
+-------+
|(2 = 2)|
+-------+
|   true|
+-------+
SELECT 1 == '1';
+-------+
|(1 = 1)|
+-------+
|   true|
+-------+
SELECT true == NULL;
+-------------+
|(true = NULL)|
+-------------+
|         NULL|
+-------------+
SELECT NULL == NULL;
+-------------+
|(NULL = NULL)|
+-------------+
|         NULL|
+-------------+
-- >
SELECT 2 > 1;
+-------+
|(2 > 1)|
+-------+
|   true|
+-------+
```

```
SELECT 2 > 1.1;
+-------+
|(2 > 1)|
+-------+
|   true|
+-------+
SELECT to_date('2009-07-30 04:17:52') > to_date('2009-07-30 04:17:52');
+-------------------------------------------------------------+
|(to_date(2009-07-30 04:17:52) > to_date(2009-07-30 04:17:52))|
+-------------------------------------------------------------+
|                                                        false|
+-------------------------------------------------------------+
SELECT to_date('2009-07-30 04:17:52') > to_date('2009-08-01 04:17:52');
+-------------------------------------------------------------+
|(to_date(2009-07-30 04:17:52) > to_date(2009-08-01 04:17:52))|
+-------------------------------------------------------------+
|                                                        false|
+-------------------------------------------------------------+
SELECT 1 > NULL;
+----------+
|(1 > NULL)|
+----------+
|      NULL|
+----------+
-- >=
SELECT 2 >= 1;
+--------+
|(2 >= 1)|
+--------+
|    true|
+--------+
SELECT 2.0 >= '2.1';
+------------+
|(2.0 >= 2.1)|
+------------+
|       false|
+------------+
SELECT to_date('2009-07-30 04:17:52') >= to_date('2009-07-30 04:17:52');
+-------------------------------------------------------------+
|(to_date(2009-07-30 04:17:52) >= to_date(2009-07-30 04:17:52))|
+-------------------------------------------------------------+
|                                                        true|
+-------------------------------------------------------------+
SELECT to_date('2009-07-30 04:17:52') >= to_date('2009-08-01 04:17:52');
```

```
+------------------------------------------------------------------+
|(to_date(2009-07-30 04:17:52) >= to_date(2009-08-01 04:17:52))|
+------------------------------------------------------------------+
|                                                             false|
+------------------------------------------------------------------+
SELECT 1 >= NULL;
+-----------+
|(1 >= NULL)|
+-----------+
|       NULL|
+-----------+
-- and
SELECT true and true;
+---------------+
|(true AND true)|
+---------------+
|           true|
+---------------+
SELECT true and false;
+----------------+
|(true AND false)|
+----------------+
|           false|
+----------------+
SELECT true and NULL;
+---------------+
|(true AND NULL)|
+---------------+
|           NULL|
+---------------+
SELECT false and NULL;
+----------------+
|(false AND NULL)|
+----------------+
|           false|
+----------------+
-- ilike
SELECT ilike('Wagon', '_Agon');
+-------------------+
|ilike(Wagon, _Agon)|
+-------------------+
|               true|
+-------------------+
SELECT '%SystemDrive%\Users\John' ilike '\%SystemDrive\%\\users%';
```

```
+-----------------------------------------------------------+
|ilike(%SystemDrive%\Users\John, \%SystemDrive\%\\users%)|
+-----------------------------------------------------------+
|                                                       true|
+-----------------------------------------------------------+
SELECT '%SystemDrive%\\USERS\\John' ilike '\%SystemDrive\%\\\\Users%';
+-----------------------------------------------------------+
|ilike(%SystemDrive%\USERS\John, \%SystemDrive\%\\Users%)|
+-----------------------------------------------------------+
|                                                       true|
+-----------------------------------------------------------+
SELECT '%SystemDrive%/Users/John' ilike '/%SYSTEMDrive/%//Users%' ESCAPE '/';
+-----------------------------------------------------------+
|ilike(%SystemDrive%/Users/John, /%SYSTEMDrive/%//Users%)|
+-----------------------------------------------------------+
|                                                       true|
+-----------------------------------------------------------+
-- in
SELECT 1 in(1, 2, 3);
+----------------+
|(1 IN (1, 2, 3))|
+----------------+
|            true|
+----------------+
SELECT 1 in(2, 3, 4);
+----------------+
|(1 IN (2, 3, 4))|
+----------------+
|           false|
+----------------+
SELECT named_struct('a', 1, 'b', 2) in(named_struct('a', 1, 'b', 1), named_struct('a',
 1, 'b', 3));
+-------------------------------------------------------------------------------------+
|(named_struct(a, 1, b, 2) IN (named_struct(a, 1, b, 1), named_struct(a, 1, b, 3)))|
+-------------------------------------------------------------------------------------+
|                                                                                false|
+-------------------------------------------------------------------------------------+
SELECT named_struct('a', 1, 'b', 2) in(named_struct('a', 1, 'b', 2), named_struct('a',
 1, 'b', 3));
+-------------------------------------------------------------------------------------+
|(named_struct(a, 1, b, 2) IN (named_struct(a, 1, b, 2), named_struct(a, 1, b, 3)))|
+-------------------------------------------------------------------------------------+
|                                                                                 true|
+-------------------------------------------------------------------------------------+
```

```
-- isnan
SELECT isnan(cast('NaN' as double));
+--------------------------+
|isnan(CAST(NaN AS DOUBLE))|
+--------------------------+
|                      true|
+--------------------------+
-- isnotnull
SELECT isnotnull(1);
+---------------+
|(1 IS NOT NULL)|
+---------------+
|           true|
+---------------+
-- isnull
SELECT isnull(1);
+-----------+
|(1 IS NULL)|
+-----------+
|      false|
+-----------+
-- like
SELECT like('Wagon', '_Agon');
+----------------+
|Wagon LIKE _Agon|
+----------------+
|            true|
+----------------+
-- not
SELECT not true;
+----------+
|(NOT true)|
+----------+
|     false|
+----------+
SELECT not false;
+-----------+
|(NOT false)|
+-----------+
|       true|
+-----------+
SELECT not NULL;
+----------+
|(NOT NULL)|
```

```
+----------+
|      NULL|
+----------+
-- or
SELECT true or false;
+---------------+
|(true OR false)|
+---------------+
|           true|
+---------------+
SELECT false or false;
+----------------+
|(false OR false)|
+----------------+
|           false|
+----------------+
SELECT true or NULL;
+--------------+
|(true OR NULL)|
+--------------+
|          true|
+--------------+
SELECT false or NULL;
+---------------+
|(false OR NULL)|
+---------------+
|           NULL|
+---------------+
```

Funktionen zuordnen

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen SQL-Befehl unterstützen, finden Sie unterthe section called “Unterstützte SQL-Befehle”.

Funktion	Beschreibung
element_at (Array, Index)	Gibt das Element eines Arrays am angegebenen (1-basierten) Index zurück.

Funktion	Beschreibung
element_at (Karte, Schlüssel)	Gibt den Wert für den angegebenen Schlüssel zurück. Die Funktion gibt NULL zurück, wenn der Schlüssel nicht in der Map enthalten ist.
map (Schlüssel0, Wert0, Schlüssel1, Wert1,...)	Erzeugt eine Map mit den angegebenen Paaren. key/value
map_concat (Karte,...)	Gibt die Vereinigung aller angegebenen Maps zurück
map_contains_key (Karte, Schlüssel)	Gibt true zurück, wenn die Map den Schlüssel enthält.
map_entries (Karte)	Gibt ein ungeordnetes Array aller Einträge in der angegebenen Map zurück.
map_from_arrays (Schlüssel, Werte)	Erzeugt eine Map mit einem Paar der angegebenen Arrays. key/value Alle Elemente in Schlüsseln sollten nicht Null sein
map_from_entries () arrayOfEntries	Gibt eine Map zurück, die aus dem angegeben en Array von Einträgen erstellt wurde.
map_keys (Karte)	Gibt ein ungeordnetes Array zurück, das die Schlüssel der Map enthält.
map_values (Karte)	Gibt ein ungeordnetes Array zurück, das die Werte der Map enthält.
str_to_map (Text [, PairDelim [,]]) keyValueD elim	Erstellt eine Map, nachdem der Text mithilfe von Trennzeichen in Schlüssel/Wert-Paare aufgeteilt wurde. Die Standardtrennzeichen sind ',' für `PairDelim` und ':' für ``. keyValueD elim Sowohl `pairDelim` als auch `` werden als reguläre Ausdrücke behandelt. keyValueDelim

Funktion	Beschreibung
try_element_at (Array, Index)	Gibt das Element eines Arrays am angegebenen (1-basierten) Index zurück. Wenn Index 0 ist, gibt das System einen Fehler aus. Wenn der Index < 0 ist, wird auf Elemente vom letzten bis zum ersten zugegriffen. Die Funktion gibt immer NULL zurück, wenn der Index die Länge des Arrays überschreitet.
try_element_at (Map, Schlüssel)	Gibt den Wert für den angegebenen Schlüssel zurück. Die Funktion gibt immer NULL zurück, wenn der Schlüssel nicht in der Map enthalten ist.

Beispiele

```
-- element_at
SELECT element_at(array(1, 2, 3), 2);
+----------------------------+
|element_at(array(1, 2, 3), 2)|
+----------------------------+
|                           2|
+----------------------------+
SELECT element_at(map(1, 'a', 2, 'b'), 2);
+----------------------------+
|element_at(map(1, a, 2, b), 2)|
+----------------------------+
|                           b|
+----------------------------+
-- map
SELECT map(1.0, '2', 3.0, '4');
+--------------------+
| map(1.0, 2, 3.0, 4)|
+--------------------+
|{1.0 -> 2, 3.0 -> 4}|
+--------------------+
-- map_concat
SELECT map_concat(map(1, 'a', 2, 'b'), map(3, 'c'));
+------------------------------------+
```

```
|map_concat(map(1, a, 2, b), map(3, c))|
+--------------------------------------+
|                  {1 -> a, 2 -> b, ...|
+--------------------------------------+
-- map_contains_key
SELECT map_contains_key(map(1, 'a', 2, 'b'), 1);
+-----------------------------------+
|map_contains_key(map(1, a, 2, b), 1)|
+-----------------------------------+
|                               true|
+-----------------------------------+
SELECT map_contains_key(map(1, 'a', 2, 'b'), 3);
+-----------------------------------+
|map_contains_key(map(1, a, 2, b), 3)|
+-----------------------------------+
|                              false|
+-----------------------------------+
-- map_entries
SELECT map_entries(map(1, 'a', 2, 'b'));
+---------------------------+
|map_entries(map(1, a, 2, b))|
+---------------------------+
|            [{1, a}, {2, b}]|
+---------------------------+
-- map_from_arrays
SELECT map_from_arrays(array(1.0, 3.0), array('2', '4'));
+-------------------------------------------+
|map_from_arrays(array(1.0, 3.0), array(2, 4))|
+-------------------------------------------+
|                        {1.0 -> 2, 3.0 -> 4}|
+-------------------------------------------+
-- map_from_entries
SELECT map_from_entries(array(struct(1, 'a'), struct(2, 'b')));
+---------------------------------------------------+
|map_from_entries(array(struct(1, a), struct(2, b)))|
+---------------------------------------------------+
|                                {1 -> a, 2 -> b}|
+---------------------------------------------------+
-- map_keys
SELECT map_keys(map(1, 'a', 2, 'b'));
+-------------------------+
|map_keys(map(1, a, 2, b))|
+-------------------------+
|                   [1, 2]|
```

```
+-------------------------+
-- map_values
SELECT map_values(map(1, 'a', 2, 'b'));
+-------------------------+
|map_values(map(1, a, 2, b))|
+-------------------------+
|                   [a, b]|
+-------------------------+
-- str_to_map
SELECT str_to_map('a:1,b:2,c:3', ',', ':');
+---------------------------+
|str_to_map(a:1,b:2,c:3, ,, :)|
+---------------------------+
|         {a -> 1, b -> 2, ...|
+---------------------------+
SELECT str_to_map('a');
+-------------------+
|str_to_map(a, ,, :)|
+-------------------+
|        {a -> NULL}|
+-------------------+
-- try_element_at
SELECT try_element_at(array(1, 2, 3), 2);
+---------------------------------+
|try_element_at(array(1, 2, 3), 2)|
+---------------------------------+
|                                2|
+---------------------------------+
SELECT try_element_at(map(1, 'a', 2, 'b'), 2);
+---------------------------------+
|try_element_at(map(1, a, 2, b), 2)|
+---------------------------------+
|                                 b|
+---------------------------------+
```

Mathematische Funktionen

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen SQL-Befehl unterstützen, finden Sie unterthe section called “Unterstützte SQL-Befehle”.

Funktion	Beschreibung
Ausdruck1% Ausdruck2	Gibt den Rest nach `expr1`/`expr2` zurück.
Ausdruck1 * Ausdruck2	Gibt `expr1`*`expr2` zurück.
Ausdruck1 + Ausdruck2	Gibt `expr1`+`expr2` zurück.
Ausdruck1 - Ausdruck2	Gibt `expr1`-`expr2` zurück.
Ausdruck1//Ausdruck2	Gibt `expr1`/`expr2` zurück. Es führt immer eine Gleitkommadivision durch.
abs (expr)	Gibt den absoluten Wert des numerischen Werts oder des Intervallwerts zurück.
acos (expr)	Gibt den inversen Kosinus (auch bekannt als Arkuskosinus) von `expr“ zurück, als ob er von `java.lang.Math.acos` berechnet worden wäre.
acosh (Ausdruck)	Gibt den inversen hyperbolischen Kosinus von `expr` zurück.
asin (expr)	Gibt den Umkehrsinus (auch bekannt als Arkussinus) und den Arkussinus von `expr zurück, als ob er von `java.lang.Math.asin` berechnet worden wäre.
asinh (Ausdruck)	Gibt den inversen hyperbolischen Sinus von `expr` zurück.
Satan (Ausdruck)	Gibt den umgekehrten Tangens (auch bekannt als Arkustangens) von `expr` zurück, als ob er von `java.lang.Math.Atan` berechnet worden wäre
Satan2 (ExprY, ExprX)	Gibt den Winkel im Bogenmaß zwischen der positiven X-Achse einer Ebene und dem durch die Koordinaten (`expRx`, `expRY`)

Funktion	Beschreibung
	angegebenen Punkt zurück, als ob er von `java.lang.Math.atan2` berechnet worden wäre.
atanh (Ausdruck)	Gibt den umgekehrten hyperbolischen Tangens von `expr` zurück.
bin (Ausdruck)	Gibt die Zeichenkettendarstellung des langen Werts `expr `zurück, der binär dargestellt wird.
bround (expr, d)	Gibt `expr` im Rundungsmodus HALF_EVEN auf `d` Dezimalstellen gerundet zurück.
cbrt (Ausdruck)	Gibt die Kubikwurzel von `expr zurück.
ceil (Ausdruck [, Skala])	Gibt nach dem Aufrunden die kleinste Zahl zurück, die nicht kleiner als `expr` ist. Ein optionaler `scale`-Parameter kann angegeben werden, um das Rundungsverhalten zu steuern.
Decke (expr [, scale])	Gibt nach dem Aufrunden die kleinste Zahl zurück, die nicht kleiner als `expr` ist. Ein optionaler `scale`-Parameter kann angegeben werden, um das Rundungsverhalten zu steuern.
conv (Zahl, from_base, to_base)	Konvertiert `num` von `from_base` nach `to_base`.
cos (Ausdruck)	Gibt den Kosinus von `expr zurück, als ob er von `java.lang.Math.cos` berechnet worden wäre.
cosh (expr)	Gibt den hyperbolischen Kosinus von `expr zurück, als ob er von `java.lang.Math.Cosh` berechnet worden wäre.

Funktion	Beschreibung
Kosten (expr)	Gibt den Kotangens von `expr zurück, als ob er von `1/java.lang.Math.TAN` berechnet worden wäre.
csc (expr)	Gibt den Kosekans von `expr zurück, als ob er mit `1/java.lang.Math.sin` berechnet worden wäre.
Grad (expr)	Konvertiert Radiant in Grad.
expr1 div expr2	Dividiere `expr1` durch `expr2`. Es gibt NULL zurück, wenn ein Operand NULL ist oder `expr2` 0 ist. Das Ergebnis wird in Long umgewandelt.
(e)	Gibt die Eulersche Zahl zurück, e.
exp (expr)	Setzt e in die Potenz von `expr zurück.
expm1 (expr) — Gibt exp (`expr) zurück	1
faktoriell (expr)	Gibt den Faktorwert von `expr zurück. `expr` ist [0.. 20]. Andernfalls NULL.
Etage (expr [, Skala])	Gibt nach dem Abrunden die größte Zahl zurück, die nicht größer als `expr ist. Ein optionaler `scale`-Parameter kann angegeben werden, um das Rundungsverhalten zu steuern.
am größten (expr,...)	Gibt den größten Wert aller Parameter zurück, wobei Nullwerte übersprungen werden.
Hexadezimalzahl (Ausdruck)	Konvertiert `expr` nach Hexadezimal.
Hypot (Ausdruck1, Ausdruck2)	Gibt sqrt (`expr1`**2 + `expr2`**2) zurück.

Funktion	Beschreibung
mindestens (expr,...)	Gibt den kleinsten Wert aller Parameter zurück, wobei Nullwerte übersprungen werden.
ln (Ausdruck)	Gibt den natürlichen Logarithmus (Basis e) von `expr zurück.
log (Basis, Ausdruck)	Gibt den Logarithmus von `expr mit `base` zurück.
log10 (Ausdruck)	Gibt den Logarithmus von `expr mit der Basis 10 zurück.
log1p (Ausdruck)	Gibt log (1 + `expr) zurück.
log2 (Ausdruck)	Gibt den Logarithmus von `expr mit der Basis 2 zurück.
Ausdruck1 gegen Ausdruck2	Gibt den Rest nach `expr1`/`expr2` zurück.
negativ (expr)	Gibt den negierten Wert von `expr` zurück.
pi ()	Gibt Pi zurück.
pmod (Ausdruck1, Ausdruck2)	Gibt den positiven Wert von `expr1` mod `expr2` zurück.
positiv (expr)	Gibt den Wert von `expr` zurück.
pow (Ausdruck1, Ausdruck2)	Erhöht `expr1` auf die Potenz von `expr2`.
Leistung (Ausdruck1, Ausdruck2)	Potenziert `expr1` mit `expr2`.
Radiant (expr)	Konvertiert Grad in Radiant.
Rand ([Ausgangswert])	Gibt einen Zufallswert mit unabhängigen und identisch verteilten (i.i.d.) gleichmäßig verteilte n Werten in [0, 1) zurück.

Funktion	Beschreibung
randn ([Geschwindigkeit])	Gibt einen Zufallswert mit unabhängigen und identisch verteilten (i.i.d.) Werten aus der Standardnormalverteilung zurück.
zufällig ([Startwert])	Gibt einen Zufallswert mit unabhängigen und identisch verteilten (i.i.d.) gleichmäßig verteilte n Werten in [0, 1) zurück.
print (Ausdruck)	Gibt den doppelten Wert zurück, dessen Wert dem Argument am nächsten kommt und einer mathematischen Ganzzahl entspricht.
rund (expr, d)	Gibt `expr` im Rundungsmodus HALF_UP auf `d` Dezimalstellen gerundet zurück.
Sekunde (Ausdruck)	Gibt den Sekans von `expr zurück, als ob er von `1/java.lang.Math.cos` berechnet worden wäre.
shiftleft (Basis, Ausdruck)	Bitweises Verschieben nach links.
Zeichen (expr)	Gibt -1,0, 0,0 oder 1,0 zurück, wenn `expr negativ, 0 oder positiv ist.
Signal (Ausdruck)	Gibt -1,0, 0,0 oder 1,0 zurück, wenn `expr negativ, 0 oder positiv ist.
sin (Ausdruck)	Gibt den Sinus von `expr zurück, als ob er von `java.lang.Math.Sin` berechnet worden wäre.
sinh (Ausdruck)	Gibt den hyperbolischen Sinus von `expr zurück, als ob er von `java.lang.Math.Sinh` berechnet worden wäre.
sqrt (Ausdruck)	Gibt die Quadratwurzel von `expr zurück.

Funktion	Beschreibung
tan (expr)	Gibt den Tangens von `expr zurück, als ob er von `java.lang.Math.TAN` berechnet worden wäre.
tanh (expr)	Gibt den hyperbolischen Tangens von `expr zurück, als ob er von `java.lang.Math.Tanh` berechnet worden wäre.
try_add (expr1, expr2)	Gibt die Summe von `expr1` und `expr2` zurück und das Ergebnis ist Null bei Überlauf. Die akzeptierten Eingabetypen sind dieselben wie beim Operator `+`.
try_divide (Dividende, Divisor)	Gibt `dividend`/`divisor` zurück. Es führt immer eine Gleitkommadivision durch. Das Ergebnis ist immer Null, wenn `expr2` 0 ist. `dividend` muss eine Zahl oder ein Intervall sein. `Divisor` muss eine Zahl sein.
try_multiply (Ausdruck1, Ausdruck2)	Gibt `expr1`*`expr2` zurück und das Ergebnis ist Null bei Überlauf. Die akzeptierten Eingabetypen sind dieselben wie beim Operator `*`.
try_subtract (expr1, expr2)	Gibt `expr1`-`expr2` zurück und das Ergebnis ist Null bei Überlauf. Die akzeptierten Eingabetypen sind dieselben wie beim Operator `-`.
unhex (Ausdruck)	Konvertiert das hexadezimale `expr `expr` in ein binäres.
width_bucket (Wert, min_value, max_value, num_bucket)	Gibt die Bucket-Nummer zurück, der `Wert` in einem Äquiwidth-Histogramm mit `num_buck et`-Buckets zugewiesen würde, im Bereich `min_value` bis `max_value`.“

Beispiele

```
-- %
SELECT 2 % 1.8;
+---------+
|(2 % 1.8)|
+---------+
|      0.2|
+---------+
SELECT MOD(2, 1.8);
+-----------+
|mod(2, 1.8)|
+-----------+
|        0.2|
+-----------+
-- *
SELECT 2 * 3;
+-------+
|(2 * 3)|
+-------+
|      6|
+-------+
-- +
SELECT 1 + 2;
+-------+
|(1 + 2)|
+-------+
|      3|
+-------+
-- -
SELECT 2 - 1;
+-------+
|(2 - 1)|
+-------+
|      1|
+-------+
-- /
SELECT 3 / 2;
+-------+
|(3 / 2)|
+-------+
|    1.5|
+-------+
SELECT 2L / 2L;
```

```
+-------+
|(2 / 2)|
+-------+
|    1.0|
+-------+
-- abs
SELECT abs(-1);
+-------+
|abs(-1)|
+-------+
|      1|
+-------+
SELECT abs(INTERVAL -'1-1' YEAR TO MONTH);
+-----------------------------------+
|abs(INTERVAL '-1-1' YEAR TO MONTH)|
+-----------------------------------+
|              INTERVAL '1-1' YE...|
+-----------------------------------+
-- acos
SELECT acos(1);
+-------+
|ACOS(1)|
+-------+
|    0.0|
+-------+
SELECT acos(2);
+-------+
|ACOS(2)|
+-------+
|    NaN|
+-------+
-- acosh
SELECT acosh(1);
+--------+
|ACOSH(1)|
+--------+
|     0.0|
+--------+
SELECT acosh(0);
+--------+
|ACOSH(0)|
+--------+
|     NaN|
+--------+
```

```
-- asin
SELECT asin(0);
+-------+
|ASIN(0)|
+-------+
|    0.0|
+-------+
SELECT asin(2);
+-------+
|ASIN(2)|
+-------+
|    NaN|
+-------+
-- asinh
SELECT asinh(0);
+--------+
|ASINH(0)|
+--------+
|     0.0|
+--------+
-- atan
SELECT atan(0);
+-------+
|ATAN(0)|
+-------+
|    0.0|
+-------+
-- atan2
SELECT atan2(0, 0);
+-----------+
|ATAN2(0, 0)|
+-----------+
|        0.0|
+-----------+
-- atanh
SELECT atanh(0);
+--------+
|ATANH(0)|
+--------+
|     0.0|
+--------+
SELECT atanh(2);
+--------+
|ATANH(2)|
```

```
+--------+
|     NaN|
+--------+
-- bin
SELECT bin(13);
+-------+
|bin(13)|
+-------+
|   1101|
+-------+
SELECT bin(-13);
+--------------------+
|            bin(-13)|
+--------------------+
|1111111111111111...|
+--------------------+
SELECT bin(13.3);
+---------+
|bin(13.3)|
+---------+
|     1101|
+---------+
-- bround
SELECT bround(2.5, 0);
+--------------+
|bround(2.5, 0)|
+--------------+
|             2|
+--------------+
SELECT bround(25, -1);
+--------------+
|bround(25, -1)|
+--------------+
|            20|
+--------------+
-- cbrt
SELECT cbrt(27.0);
+----------+
|CBRT(27.0)|
+----------+
|       3.0|
+----------+
-- ceil
SELECT ceil(-0.1);
```

```
+----------+
|CEIL(-0.1)|
+----------+
|         0|
+----------+
SELECT ceil(5);
+-------+
|CEIL(5)|
+-------+
|      5|
+-------+
SELECT ceil(3.1411, 3);
+---------------+
|ceil(3.1411, 3)|
+---------------+
|          3.142|
+---------------+
SELECT ceil(3.1411, -3);
+----------------+
|ceil(3.1411, -3)|
+----------------+
|            1000|
+----------------+
-- ceiling
SELECT ceiling(-0.1);
+-------------+
|ceiling(-0.1)|
+-------------+
|            0|
+-------------+
SELECT ceiling(5);
+----------+
|ceiling(5)|
+----------+
|         5|
+----------+
SELECT ceiling(3.1411, 3);
+------------------+
|ceiling(3.1411, 3)|
+------------------+
|             3.142|
+------------------+
SELECT ceiling(3.1411, -3);
+------------------+
```

```
|ceiling(3.1411, -3)|
+-------------------+
|               1000|
+-------------------+
-- conv
SELECT conv('100', 2, 10);
+----------------+
|conv(100, 2, 10)|
+----------------+
|               4|
+----------------+
SELECT conv(-10, 16, -10);
+------------------+
|conv(-10, 16, -10)|
+------------------+
|               -16|
+------------------+
-- cos
SELECT cos(0);
+------+
|COS(0)|
+------+
|   1.0|
+------+
-- cosh
SELECT cosh(0);
+-------+
|COSH(0)|
+-------+
|    1.0|
+-------+
-- cot
SELECT cot(1);
+------------------+
|            COT(1)|
+------------------+
|0.6420926159343306|
+------------------+
-- csc
SELECT csc(1);
+------------------+
|            CSC(1)|
+------------------+
|1.1883951057781212|
```

```
+------------------+
-- degrees
SELECT degrees(3.141592653589793);
+--------------------------+
|DEGREES(3.141592653589793)|
+--------------------------+
|                     180.0|
+--------------------------+
-- div
SELECT 3 div 2;
+---------+
|(3 div 2)|
+---------+
|        1|
+---------+
SELECT INTERVAL '1-1' YEAR TO MONTH div INTERVAL '-1' MONTH;
+-----------------------------------------------------------+
|(INTERVAL '1-1' YEAR TO MONTH div INTERVAL '-1' MONTH)|
+-----------------------------------------------------------+
|                                                        -13|
+-----------------------------------------------------------+
-- e
SELECT e();
+-----------------+
|              E()|
+-----------------+
|2.718281828459045|
+-----------------+
-- exp
SELECT exp(0);
+------+
|EXP(0)|
+------+
|   1.0|
+------+
-- expm1
SELECT expm1(0);
+--------+
|EXPM1(0)|
+--------+
|     0.0|
+--------+
-- factorial
SELECT factorial(5);
```

```
+------------+
|factorial(5)|
+------------+
|         120|
+------------+
-- floor
SELECT floor(-0.1);
+-----------+
|FLOOR(-0.1)|
+-----------+
|         -1|
+-----------+
SELECT floor(5);
+--------+
|FLOOR(5)|
+--------+
|       5|
+--------+
SELECT floor(3.1411, 3);
+----------------+
|floor(3.1411, 3)|
+----------------+
|           3.141|
+----------------+
SELECT floor(3.1411, -3);
+-----------------+
|floor(3.1411, -3)|
+-----------------+
|                0|
+-----------------+
-- greatest
SELECT greatest(10, 9, 2, 4, 3);
+------------------------+
|greatest(10, 9, 2, 4, 3)|
+------------------------+
|                      10|
+------------------------+
-- hex
SELECT hex(17);
+-------+
|hex(17)|
+-------+
|     11|
+-------+
```

```
SELECT hex('SQL');
+------------------+
|    hex(SQL)|
+------------------+
|53514C|
+------------------+
-- hypot
SELECT hypot(3, 4);
+-----------+
|HYPOT(3, 4)|
+-----------+
|        5.0|
+-----------+
-- least
SELECT least(10, 9, 2, 4, 3);
+---------------------+
|least(10, 9, 2, 4, 3)|
+---------------------+
|                    2|
+---------------------+
-- ln
SELECT ln(1);
+-----+
|ln(1)|
+-----+
|  0.0|
+-----+
-- log
SELECT log(10, 100);
+------------+
|LOG(10, 100)|
+------------+
|         2.0|
+------------+
-- log10
SELECT log10(10);
+---------+
|LOG10(10)|
+---------+
|      1.0|
+---------+
-- log1p
SELECT log1p(0);
+--------+
```

```
|LOG1P(0)|
+--------+
|     0.0|
+--------+
-- log2
SELECT log2(2);
+-------+
|LOG2(2)|
+-------+
|    1.0|
+-------+
-- mod
SELECT 2 % 1.8;
+---------+
|(2 % 1.8)|
+---------+
|      0.2|
+---------+
SELECT MOD(2, 1.8);
+-----------+
|mod(2, 1.8)|
+-----------+
|        0.2|
+-----------+
-- negative
SELECT negative(1);
+-----------+
|negative(1)|
+-----------+
|         -1|
+-----------+
-- pi
SELECT pi();
+-----------------+
|             PI()|
+-----------------+
|3.141592653589793|
+-----------------+
-- pmod
SELECT pmod(10, 3);
+-----------+
|pmod(10, 3)|
+-----------+
|          1|
```

```
+-----------+
SELECT pmod(-10, 3);
+------------+
|pmod(-10, 3)|
+------------+
|           2|
+------------+
-- positive
SELECT positive(1);
+-----+
|(+ 1)|
+-----+
|    1|
+-----+
-- pow
SELECT pow(2, 3);
+---------+
|pow(2, 3)|
+---------+
|      8.0|
+---------+
-- power
SELECT power(2, 3);
+-----------+
|POWER(2, 3)|
+-----------+
|        8.0|
+-----------+
-- radians
SELECT radians(180);
+-----------------+
|     RADIANS(180)|
+-----------------+
|3.141592653589793|
+-----------------+
-- rand
SELECT rand();
+------------------+
|            rand()|
+------------------+
|0.7211420708112387|
+------------------+
SELECT rand(0);
+------------------+
```

```
|           rand(0)|
+------------------+
|0.7604953758285915|
+------------------+
SELECT rand(null);
+------------------+
|        rand(NULL)|
+------------------+
|0.7604953758285915|
+------------------+
-- randn
SELECT randn();
+-------------------+
|            randn()|
+-------------------+
|-0.8175603217732732|
+-------------------+
SELECT randn(0);
+------------------+
|          randn(0)|
+------------------+
|1.6034991609278433|
+------------------+
SELECT randn(null);
+------------------+
|       randn(NULL)|
+------------------+
|1.6034991609278433|
+------------------+
-- random
SELECT random();
+-----------------+
|           rand()|
+-----------------+
|0.394205008255365|
+-----------------+
SELECT random(0);
+------------------+
|           rand(0)|
+------------------+
|0.7604953758285915|
+------------------+
SELECT random(null);
+------------------+
```

```
|        rand(NULL)|
+------------------+
|0.7604953758285915|
+------------------+
-- rint
SELECT rint(12.3456);
+-------------+
|rint(12.3456)|
+-------------+
|         12.0|
+-------------+
-- round
SELECT round(2.5, 0);
+-------------+
|round(2.5, 0)|
+-------------+
|            3|
+-------------+
-- sec
SELECT sec(0);
+------+
|SEC(0)|
+------+
|   1.0|
+------+
-- shiftleft
SELECT shiftleft(2, 1);
+---------------+
|shiftleft(2, 1)|
+---------------+
|              4|
+---------------+
-- sign
SELECT sign(40);
+--------+
|sign(40)|
+--------+
|     1.0|
+--------+
SELECT sign(INTERVAL -'100' YEAR);
+--------------------------+
|sign(INTERVAL '-100' YEAR)|
+--------------------------+
|                      -1.0|
```

```
+--------------------------+
-- signum
SELECT signum(40);
+----------+
|SIGNUM(40)|
+----------+
|       1.0|
+----------+
SELECT signum(INTERVAL -'100' YEAR);
+----------------------------+
|SIGNUM(INTERVAL '-100' YEAR)|
+----------------------------+
|                        -1.0|
+----------------------------+
-- sin
SELECT sin(0);
+------+
|SIN(0)|
+------+
|   0.0|
+------+
-- sinh
SELECT sinh(0);
+-------+
|SINH(0)|
+-------+
|    0.0|
+-------+
-- sqrt
SELECT sqrt(4);
+-------+
|SQRT(4)|
+-------+
|    2.0|
+-------+
-- tan
SELECT tan(0);
+------+
|TAN(0)|
+------+
|   0.0|
+------+
-- tanh
SELECT tanh(0);
```

```
+-------+
|TANH(0)|
+-------+
|    0.0|
+-------+
-- try_add
SELECT try_add(1, 2);
+-------------+
|try_add(1, 2)|
+-------------+
|            3|
+-------------+
SELECT try_add(2147483647, 1);
+----------------------+
|try_add(2147483647, 1)|
+----------------------+
|                  NULL|
+----------------------+
SELECT try_add(date'2021-01-01', 1);
+-----------------------------+
|try_add(DATE '2021-01-01', 1)|
+-----------------------------+
|                   2021-01-02|
+-----------------------------+
SELECT try_add(date'2021-01-01', interval 1 year);
+---------------------------------------------+
|try_add(DATE '2021-01-01', INTERVAL '1' YEAR)|
+---------------------------------------------+
|                                   2022-01-01|
+---------------------------------------------+
SELECT try_add(timestamp'2021-01-01 00:00:00', interval 1 day);
+-----------------------------------------------------------+
|try_add(TIMESTAMP '2021-01-01 00:00:00', INTERVAL '1' DAY)|
+-----------------------------------------------------------+
|                                        2021-01-02 00:00:00|
+-----------------------------------------------------------+
SELECT try_add(interval 1 year, interval 2 year);
+-----------------------------------------------+
|try_add(INTERVAL '1' YEAR, INTERVAL '2' YEAR)|
+-----------------------------------------------+
|                             INTERVAL '3' YEAR|
+-----------------------------------------------+
-- try_divide
SELECT try_divide(3, 2);
```

```
+----------------+
|try_divide(3, 2)|
+----------------+
|             1.5|
+----------------+
SELECT try_divide(2L, 2L);
+----------------+
|try_divide(2, 2)|
+----------------+
|             1.0|
+----------------+
SELECT try_divide(1, 0);
+----------------+
|try_divide(1, 0)|
+----------------+
|            NULL|
+----------------+
SELECT try_divide(interval 2 month, 2);
+--------------------------------+
|try_divide(INTERVAL '2' MONTH, 2)|
+--------------------------------+
|             INTERVAL '0-1' YE...|
+--------------------------------+
SELECT try_divide(interval 2 month, 0);
+--------------------------------+
|try_divide(INTERVAL '2' MONTH, 0)|
+--------------------------------+
|                            NULL|
+--------------------------------+
-- try_multiply
SELECT try_multiply(2, 3);
+------------------+
|try_multiply(2, 3)|
+------------------+
|                 6|
+------------------+
SELECT try_multiply(-2147483648, 10);
+-----------------------------+
|try_multiply(-2147483648, 10)|
+-----------------------------+
|                         NULL|
+-----------------------------+
SELECT try_multiply(interval 2 year, 3);
+--------------------------------+
```

```
|try_multiply(INTERVAL '2' YEAR, 3)|
+----------------------------------+
|              INTERVAL '6-0' YE...|
+----------------------------------+
-- try_subtract
SELECT try_subtract(2, 1);
+------------------+
|try_subtract(2, 1)|
+------------------+
|                 1|
+------------------+
SELECT try_subtract(-2147483648, 1);
+----------------------------+
|try_subtract(-2147483648, 1)|
+----------------------------+
|                        NULL|
+----------------------------+
SELECT try_subtract(date'2021-01-02', 1);
+----------------------------------+
|try_subtract(DATE '2021-01-02', 1)|
+----------------------------------+
|                        2021-01-01|
+----------------------------------+
SELECT try_subtract(date'2021-01-01', interval 1 year);
+-------------------------------------------------+
|try_subtract(DATE '2021-01-01', INTERVAL '1' YEAR)|
+-------------------------------------------------+
|                                       2020-01-01|
+-------------------------------------------------+
SELECT try_subtract(timestamp'2021-01-02 00:00:00', interval 1 day);
+-----------------------------------------------------------------+
|try_subtract(TIMESTAMP '2021-01-02 00:00:00', INTERVAL '1' DAY)|
+-----------------------------------------------------------------+
|                                              2021-01-01 00:00:00|
+-----------------------------------------------------------------+
SELECT try_subtract(interval 2 year, interval 1 year);
+-------------------------------------------------+
|try_subtract(INTERVAL '2' YEAR, INTERVAL '1' YEAR)|
+-------------------------------------------------+
|                                 INTERVAL '1' YEAR|
+-------------------------------------------------+
-- unhex
SELECT decode(unhex('53514C'), 'UTF-8');
+---------------------------------------+
```

```
|decode(unhex(53514C), UTF-8)|
+----------------------------------------+
|                                     SQL|
+----------------------------------------+
-- width_bucket
SELECT width_bucket(5.3, 0.2, 10.6, 5);
+-------------------------------+
|width_bucket(5.3, 0.2, 10.6, 5)|
+-------------------------------+
|                              3|
+-------------------------------+
SELECT width_bucket(-2.1, 1.3, 3.4, 3);
+-------------------------------+
|width_bucket(-2.1, 1.3, 3.4, 3)|
+-------------------------------+
|                              0|
+-------------------------------+
SELECT width_bucket(8.1, 0.0, 5.7, 4);
+-------------------------------+
|width_bucket(8.1, 0.0, 5.7, 4)|
+-------------------------------+
|                             5|
+-------------------------------+
SELECT width_bucket(-0.9, 5.2, 0.5, 2);
+-------------------------------+
|width_bucket(-0.9, 5.2, 0.5, 2)|
+-------------------------------+
|                              3|
+-------------------------------+
SELECT width_bucket(INTERVAL '0' YEAR, INTERVAL '0' YEAR, INTERVAL '10' YEAR, 10);
+-----------------------------------------------------------------------------+
|width_bucket(INTERVAL '0' YEAR, INTERVAL '0' YEAR, INTERVAL '10' YEAR, 10)|
+-----------------------------------------------------------------------------+
|                                                                            1|
+-----------------------------------------------------------------------------+
SELECT width_bucket(INTERVAL '1' YEAR, INTERVAL '0' YEAR, INTERVAL '10' YEAR, 10);
+-----------------------------------------------------------------------------+
|width_bucket(INTERVAL '1' YEAR, INTERVAL '0' YEAR, INTERVAL '10' YEAR, 10)|
+-----------------------------------------------------------------------------+
|                                                                            2|
+-----------------------------------------------------------------------------+
SELECT width_bucket(INTERVAL '0' DAY, INTERVAL '0' DAY, INTERVAL '10' DAY, 10);
+-------------------------------------------------------------------+
|width_bucket(INTERVAL '0' DAY, INTERVAL '0' DAY, INTERVAL '10' DAY, 10)|
```

```
+-------------------------------------------------------------------------+
|                                                                        1|
+-------------------------------------------------------------------------+
SELECT width_bucket(INTERVAL '1' DAY, INTERVAL '0' DAY, INTERVAL '10' DAY, 10);
+-------------------------------------------------------------------------+
|width_bucket(INTERVAL '1' DAY, INTERVAL '0' DAY, INTERVAL '10' DAY, 10)|
+-------------------------------------------------------------------------+
|                                                                        2|
+-------------------------------------------------------------------------+
```

Generatorfunktionen

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diese SQL-Funktionen unterstützen, finden Sie unterthe section called “Unterstützte SQL-Befehle”.

Funktion	Beschreibung
explodieren (expr)	Teilt die Elemente des Arrays `expr in mehrere Zeilen oder die Elemente der Map `expr in mehrere Zeilen und Spalten auf. Sofern nicht anders angegeben, verwendet es den Standardspaltennamen `col` für Elemente des Arrays oder `key` und `value` für die Elemente der Map.
explode_outer (expr)	Teilt die Elemente des Arrays `expr in mehrere Zeilen oder die Elemente der Map `expr in mehrere Zeilen und Spalten auf. Sofern nicht anders angegeben, verwendet es den Standardspaltennamen `col` für Elemente des Arrays oder `key` und `value` für die Elemente der Map.
inline (expr)	Löst ein Array von Strukturen in eine Tabelle auf. Verwendet standardm äßig die Spaltennamen col1, col2 usw., sofern nicht anders angegeben.
inline_outer (expr)	Löst ein Array von Strukturen in eine Tabelle auf. Verwendet standardm äßig die Spaltennamen col1, col2 usw., sofern nicht anders angegeben.
posexplode (expr)	Teilt die Elemente des Arrays `expr in mehrere Zeilen mit Positionen oder die Elemente der Map `expr in mehrere Zeilen und Spalten mit Positionen auf. Sofern nicht anders angegeben, verwendet es den

Funktion	Beschreibung
	Spaltennamen `pos` für die Position, `col` für Elemente des Arrays oder `key` und `value` für Elemente der Map.
posexplode_outer (expr)	Teilt die Elemente des Arrays `expr in mehrere Zeilen mit Positionen oder die Elemente der Map `expr in mehrere Zeilen und Spalten mit Positionen auf. Sofern nicht anders angegeben, verwendet es den Spaltennamen `pos` für die Position, `col` für Elemente des Arrays oder `key` und `value` für Elemente der Map.
stack (n, expr1,..., exprk)	Teilt `expr1`,..., `exprk` in `n` Zeilen auf. Verwendet standardmäßig die Spaltennamen col0, col1 usw., sofern nicht anders angegeben.

Beispiele

```
-- explode
SELECT explode(array(10, 20));
+---+
|col|
+---+
| 10|
| 20|
+---+

SELECT explode(collection => array(10, 20));
+---+
|col|
+---+
| 10|
| 20|
+---+

SELECT * FROM explode(collection => array(10, 20));
+---+
|col|
+---+
| 10|
| 20|
+---+
```

```
-- explode_outer
SELECT explode_outer(array(10, 20));
+---+
|col|
+---+
| 10|
| 20|
+---+

SELECT explode_outer(collection => array(10, 20));
+---+
|col|
+---+
| 10|
| 20|
+---+

SELECT * FROM explode_outer(collection => array(10, 20));
+---+
|col|
+---+
| 10|
| 20|
+---+

-- inline
SELECT inline(array(struct(1, 'a'), struct(2, 'b')));
+----+----+
|col1|col2|
+----+----+
|   1|   a|
|   2|   b|
+----+----+

-- inline_outer
SELECT inline_outer(array(struct(1, 'a'), struct(2, 'b')));
+----+----+
|col1|col2|
+----+----+
|   1|   a|
|   2|   b|
+----+----+

-- posexplode
```

```
SELECT posexplode(array(10,20));
+---+---+
|pos|col|
+---+---+
|  0| 10|
|  1| 20|
+---+---+

SELECT * FROM posexplode(array(10,20));
+---+---+
|pos|col|
+---+---+
|  0| 10|
|  1| 20|
+---+---+

-- posexplode_outer
SELECT posexplode_outer(array(10,20));
+---+---+
|pos|col|
+---+---+
|  0| 10|
|  1| 20|
+---+---+

SELECT * FROM posexplode_outer(array(10,20));
+---+---+
|pos|col|
+---+---+
|  0| 10|
|  1| 20|
+---+---+

-- stack
SELECT stack(2, 1, 2, 3);
+----+----+
|col0|col1|
+----+----+
|   1|   2|
|   3|NULL|
+----+----+
```

SELECT-Klausel

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen SQL-Befehl unterstützen, finden Sie unter. the section called “Unterstützte SQL-Befehle”

OpenSearch SQL unterstützt eine `SELECT` Anweisung, die zum Abrufen von Ergebnismengen aus einer oder mehreren Tabellen verwendet wird. Im folgenden Abschnitt werden die allgemeine Abfragesyntax und die verschiedenen Konstrukte einer Abfrage beschrieben.

Syntax

```
select_statement
[ { UNION | INTERSECT | EXCEPT } [ ALL | DISTINCT ] select_statement, ... ]
[ ORDER BY
    { expression [ ASC | DESC ] [ NULLS { FIRST | LAST } ]
    [ , ... ]
    }
]
[ SORT BY
    { expression [ ASC | DESC ] [ NULLS { FIRST | LAST } ]
    [ , ... ]
    }
]
[ WINDOW { named_window [ , WINDOW named_window, ... ] } ]
[ LIMIT { ALL | expression } ]
```

While `select_statement` ist definiert als:

```
SELECT [ ALL | DISTINCT ] { [ [ named_expression ] [ , ... ] ] }
FROM { from_item [ , ... ] }
[ PIVOT clause ]
[ UNPIVOT clause ]
[ LATERAL VIEW clause ] [ ... ]
[ WHERE boolean_expression ]
[ GROUP BY expression [ , ... ] ]
[ HAVING boolean_expression ]
```

Parameter

- ALLES

  Wählt alle passenden Zeilen aus der Beziehung aus und ist standardmäßig aktiviert.

- EINDEUTIG

  Wählt alle passenden Zeilen aus der Beziehung aus, nachdem Duplikate in den Ergebnissen entfernt wurden.

- Named_Ausdruck

  Ein Ausdruck mit einem zugewiesenen Namen. Im Allgemeinen bezeichnet es einen Spaltenausdruck.

  Syntax: `expression [[AS] alias]`

- from_item

  Beziehung zur Tabelle

  Beziehung verbinden

  Beziehung ausrichten

  Relation aufheben

  Funktion „Tabellenwert“

  Inline-Tabelle

  ```
  [ LATERAL ] ( Subquery )
  ```

- PIVOT

  Die `PIVOT` Klausel wird für die Datenperspektive verwendet. Sie können die aggregierten Werte auf der Grundlage eines bestimmten Spaltenwerts abrufen.

- UNPIVOT

  Die `UNPIVOT` Klausel wandelt Spalten in Zeilen um. Es ist das Gegenteil von`PIVOT`, mit Ausnahme der Aggregation von Werten.

- SEITLICHE ANSICHT

  Die `LATERAL VIEW` Klausel wird in Verbindung mit Generatorfunktionen wie`EXPLODE`, verwendet, die eine virtuelle Tabelle mit einer oder mehreren Zeilen generieren.

`LATERAL VIEW`wendet die Zeilen auf jede ursprüngliche Ausgabezeile an.

- WO

  Filtert das Ergebnis der `FROM` Klausel auf der Grundlage der angegebenen Prädikate.

- GRUPPIEREN NACH

  Gibt die Ausdrücke an, die zum Gruppieren der Zeilen verwendet werden.

  Dies wird in Verbindung mit Aggregatfunktionen (`MIN`,,, `MAXCOUNT`, usw.) verwendet `SUMAVG`, um Zeilen auf der Grundlage der Gruppierungsausdrücke zu gruppieren und Werte in jeder Gruppe zu aggregieren.

  Wenn eine `FILTER` Klausel an eine Aggregatfunktion angehängt wird, werden nur die entsprechenden Zeilen an diese Funktion übergeben.

- HABEN

  Gibt die Prädikate an, nach denen die von erzeugten Zeilen gefiltert `GROUP BY` werden.

  Die `HAVING` Klausel wird verwendet, um Zeilen zu filtern, nachdem die Gruppierung durchgeführt wurde.

  Wenn ohne angegeben `HAVING` wird`GROUP BY`, bedeutet dies a `GROUP BY` ohne Gruppierungsausdrücke (globales Aggregat).

- SORTIERT NACH

  Gibt eine Reihenfolge der Zeilen der vollständigen Ergebnismenge der Abfrage an.

  Die Ausgabezeilen sind partitionsübergreifend angeordnet.

  Dieser Parameter schließt sich mit `SORT BY` und gegenseitig aus `DISTRIBUTE BY` und kann nicht zusammen angegeben werden.

- SORTIERE NACH

  Gibt eine Reihenfolge an, in der die Zeilen innerhalb jeder Partition angeordnet werden.

  Dieser Parameter schließt sich gegenseitig aus `ORDER BY` und kann nicht zusammen angegeben werden.

- BESCHRÄNKEN

Gibt die maximale Anzahl von Zeilen an, die von einer Anweisung oder Unterabfrage zurückgegeben werden können.

Diese Klausel wird meistens in Verbindung mit verwendet, `ORDER BY` um ein deterministisches Ergebnis zu erzeugen.

- boolescher_Ausdruck

  Gibt einen beliebigen Ausdruck an, der zu einem booleschen Ergebnistyp ausgewertet wird.

  Zwei oder mehr Ausdrücke können mithilfe der logischen Operatoren (`AND`,) miteinander kombiniert werden. `OR`
- Ausdruck

  Gibt eine Kombination aus einem oder mehreren Werten, Operatoren und SQL-Funktionen an, die zu einem Wert ausgewertet werden.
- named_window

  Gibt Aliase für eine oder mehrere Quellfensterspezifikationen an.

  Auf die Spezifikationen des Quellfensters kann in den Fensterdefinitionen in der Abfrage verwiesen werden.

WHERE-Klausel

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen SQL-Befehl unterstützen, finden Sie unterthe section called “Unterstützte SQL-Befehle”.

Die `WHERE` Klausel wird verwendet, um die Ergebnisse der `FROM` Klausel einer Abfrage oder Unterabfrage auf der Grundlage der angegebenen Bedingung einzuschränken.

Syntax

```
WHERE boolean_expression
```

Parameter

- boolescher_Ausdruck

  Gibt einen beliebigen Ausdruck an, der zu einem booleschen Ergebnistyp ausgewertet wird.

  Zwei oder mehr Ausdrücke können mithilfe der logischen Operatoren (AND,) miteinander kombiniert werden. 0R

Beispiele

```
CREATE TABLE person (id INT, name STRING, age INT);
INSERT INTO person VALUES
(100, 'John', 30),
(200, 'Mary', NULL),
(300, 'Mike', 80),
(400, 'Dan',  50);

-- Comparison operator in `WHERE` clause.
SELECT * FROM person WHERE id > 200 ORDER BY id;
+---+----+---+
| id|name|age|
+---+----+---+
|300|Mike| 80|
|400| Dan| 50|
+---+----+---+

-- Comparison and logical operators in `WHERE` clause.
SELECT * FROM person WHERE id = 200 OR id = 300 ORDER BY id;
+---+----+----+
| id|name| age|
+---+----+----+
|200|Mary|null|
|300|Mike|  80|
+---+----+----+

-- IS NULL expression in `WHERE` clause.
SELECT * FROM person WHERE id > 300 OR age IS NULL ORDER BY id;
+---+----+----+
| id|name| age|
+---+----+----+
|200|Mary|null|
|400| Dan|  50|
+---+----+----+
```

```
-- Function expression in `WHERE` clause.
SELECT * FROM person WHERE length(name) > 3 ORDER BY id;
+---+----+----+
| id|name| age|
+---+----+----+
|100|John|  30|
|200|Mary|null|
|300|Mike|  80|
+---+----+----+

-- `BETWEEN` expression in `WHERE` clause.
SELECT * FROM person WHERE id BETWEEN 200 AND 300 ORDER BY id;
+---+----+----+
| id|name| age|
+---+----+----+
|200|Mary|null|
|300|Mike|  80|
+---+----+----+

-- Scalar Subquery in `WHERE` clause.
SELECT * FROM person WHERE age > (SELECT avg(age) FROM person);
+---+----+---+
| id|name|age|
+---+----+---+
|300|Mike| 80|
+---+----+---+

-- Correlated Subquery in `WHERE` clause.
SELECT id FROM person
WHERE exists (SELECT id FROM person where id = 200);
+---+----+----+
|id |name|age |
+---+----+----+
|200|Mary|null|
+---+----+----+
```

GROUP BY-Klausel

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen SQL-Befehl unterstützen, finden Sie unterthe section called “Unterstützte SQL-Befehle”.

Die GROUP BY Klausel wird verwendet, um die Zeilen auf der Grundlage einer Reihe von angegebenen Gruppierungsausdrücken zu gruppieren und Aggregationen für die Gruppe von Zeilen auf der Grundlage einer oder mehrerer spezifizierter Aggregatfunktionen zu berechnen.

Das System führt auch mehrere Aggregationen für denselben Eingabedatensatz mithilfe vonGROUPING SETS,, CUBE -Klauseln durch. ROLLUP Die Gruppierungsausdrücke und erweiterten Aggregationen können in der Klausel gemischt und in einer GROUP BY Klausel verschachtelt werden. GROUPING SETS Weitere Einzelheiten finden Sie im Abschnitt. Mixed/Nested Grouping Analytics

Wenn eine FILTER Klausel an eine Aggregatfunktion angehängt wird, werden nur die entsprechenden Zeilen an diese Funktion übergeben.

Syntax

```
GROUP BY group_expression [ , group_expression [ , ... ] ] [ WITH { ROLLUP | CUBE } ]
GROUP BY { group_expression | { ROLLUP | CUBE | GROUPING SETS } (grouping_set
 [ , ...]) } [ , ... ]
```

Aggregatfunktionen sind zwar wie folgt definiert:

```
aggregate_name ( [ DISTINCT ] expression [ , ... ] ) [ FILTER ( WHERE
 boolean_expression ) ]
```

Parameter

- group_expression

  Gibt die Kriterien an, nach denen die Zeilen gruppiert werden. Die Gruppierung von Zeilen erfolgt auf der Grundlage der Ergebniswerte der Gruppierungsausdrücke.

  Ein Gruppierungsausdruck kann ein Spaltenname wieGROUP BY a, eine Spaltenposition wie oder ein Ausdruck wie GROUP BY 0 sein. GROUP BY a + b
- grouping_set

  Ein Gruppierungssatz wird durch null oder mehr durch Kommas getrennte Ausdrücke in Klammern angegeben. Wenn der Gruppierungssatz nur ein Element enthält, können Klammern weggelassen werden.

  Zum Beispiel ist GROUPING SETS ((a), (b)) identisch zu GROUPING SETS (a, b).

Syntax: `{ ( [ expression [ , ... ] ] ) | expression }`

- GRUPPIERUNGSSÄTZE

  Gruppiert die Zeilen für jeden Gruppierungssatz, der danach angegeben wurde. `GROUPING SETS`

  `GROUP BY GROUPING SETS ((warehouse), (product))`Ist beispielsweise semantisch gleichbedeutend mit der Vereinigung der Ergebnisse von `GROUP BY warehouse` und. `GROUP BY product` Diese Klausel ist eine Abkürzung für UNION ALL, bei der jeder Teil des `UNION ALL` Operators die Aggregation aller in der Klausel angegebenen Gruppierungssätze durchführt. `GROUPING SETS`

  In ähnlicher Weise entspricht sie semantisch der Vereinigung von Ergebnissen von und globalem Aggregat. `GROUP BY GROUPING SETS ((warehouse, product), (product), ())` `GROUP BY warehouse, product, GROUP BY product`

- ROLLUP

  Gibt mehrere Aggregationsebenen in einer einzigen Anweisung an. Diese Klausel wird verwendet, um Aggregationen zu berechnen, die auf mehreren Gruppierungssätzen basieren. `ROLLUP`ist eine Abkürzung für. `GROUPING SETS`

  Beispiel: `GROUP BY warehouse, product WITH ROLLUP or GROUP BY ROLLUP(warehouse, product)` ist gleichbedeutend mit `GROUP BY GROUPING SETS((warehouse, product), (warehouse), ())`.

  `GROUP BY ROLLUP(warehouse, product, (warehouse, location))` ist gleich `GROUP BY GROUPING SETS((warehouse, product, location), (warehouse, product), (warehouse), ())`.

  Die N Elemente einer ROLLUP-Spezifikation ergeben N+1 GROUPING SETS.

- CUBE

  Die CUBE-Klausel wird verwendet, um Aggregationen auf der Grundlage einer Kombination von Gruppierungsspalten durchzuführen, die in der GROUP BY-Klausel angegeben sind. CUBE ist eine Abkürzung für GROUPING SETS.

  Beispiel: `GROUP BY warehouse, product WITH CUBE or GROUP BY CUBE(warehouse, product)` ist gleichbedeutend mit `GROUP BY GROUPING SETS((warehouse, product), (warehouse), (product), ())`.

`GROUP BY CUBE(warehouse, product, (warehouse, location))` ist gleich `GROUP BY GROUPING SETS((warehouse, product, location), (warehouse, product), (warehouse, location), (product, warehouse, location), (warehouse), (product), (warehouse, product), ())`. Die N Elemente einer `CUBE` Spezifikation ergeben 2^N. `GROUPING SETS`

- Analytik für gemischte/verschachtelte Gruppierungen

  Eine `GROUP BY` Klausel kann mehrere group_expressions und mehrere enthalten. `CUBE|ROLLUP|GROUPING SETS` `GROUPING SETS`kann auch verschachtelte `CUBE|ROLLUP|GROUPING SETS` Klauseln enthalten, wie,,. `GROUPING SETS(ROLLUP(warehouse, location)` `CUBE(warehouse, location))` `GROUPING SETS(warehouse, GROUPING SETS(location, GROUPING SETS(ROLLUP(warehouse, location), CUBE(warehouse, location))))`

  `CUBE|ROLLUP`ist nur ein Syntaxzucker für. `GROUPING SETS` In den obigen Abschnitten finden Sie Informationen `CUBE|ROLLUP` zur Übersetzung von`GROUPING SETS`. `group_expression`kann in diesem Kontext als eine einzige Gruppe `GROUPING SETS` behandelt werden.

  Für mehrere Elemente `GROUPING SETS` in der `GROUP BY` Klausel generieren wir eine einzelne, `GROUPING SETS` indem wir ein Kreuzprodukt des Originals erstellen. `GROUPING SETS` Für die `GROUPING SETS` in der `GROUPING SETS` Klausel verschachtelte Klausel nehmen wir einfach ihre Gruppierungssätze und entfernen sie.

  Beispiel: `GROUP BY warehouse, GROUPING SETS((product), ()), GROUPING SETS((location, size), (location), (size), ()) and GROUP BY warehouse, ROLLUP(product), CUBE(location, size)` ist gleichbedeutend mit `GROUP BY GROUPING SETS( (warehouse, product, location, size), (warehouse, product, location), (warehouse, product, size), (warehouse, product), (warehouse, location, size), (warehouse, location), (warehouse, size), (warehouse))`.

  `GROUP BY GROUPING SETS(GROUPING SETS(warehouse), GROUPING SETS((warehouse, product)))` ist gleich `GROUP BY GROUPING SETS((warehouse), (warehouse, product))`.

- aggregate_name

  Gibt den Namen einer Aggregatfunktion an (`MIN`MAX,`COUNT`,`SUM`,`AVG`, usw.).

- DEUTLICH

Entfernt Duplikate in Eingabezeilen, bevor sie an Aggregatfunktionen übergeben werden.

- FILTERN

  Filtert die Eingabezeilen, für die die `boolean_expression` WHERE In-the-Klausel als wahr ausgewertet wird, an die Aggregatfunktion übergeben; andere Zeilen werden verworfen.

Beispiele

```
CREATE TABLE dealer (id INT, city STRING, car_model STRING, quantity INT);
INSERT INTO dealer VALUES
(100, 'Fremont', 'Honda Civic', 10),
(100, 'Fremont', 'Honda Accord', 15),
(100, 'Fremont', 'Honda CRV', 7),
(200, 'Dublin', 'Honda Civic', 20),
(200, 'Dublin', 'Honda Accord', 10),
(200, 'Dublin', 'Honda CRV', 3),
(300, 'San Jose', 'Honda Civic', 5),
(300, 'San Jose', 'Honda Accord', 8);

-- Sum of quantity per dealership. Group by `id`.
SELECT id, sum(quantity) FROM dealer GROUP BY id ORDER BY id;
+---+-------------+
| id|sum(quantity)|
+---+-------------+
|100|           32|
|200|           33|
|300|           13|
+---+-------------+

-- Use column position in GROUP by clause.
SELECT id, sum(quantity) FROM dealer GROUP BY 1 ORDER BY 1;
+---+-------------+
| id|sum(quantity)|
+---+-------------+
|100|           32|
|200|           33|
|300|           13|
+---+-------------+

-- Multiple aggregations.
-- 1. Sum of quantity per dealership.
```

```
-- 2. Max quantity per dealership.
SELECT id, sum(quantity) AS sum, max(quantity) AS max FROM dealer GROUP BY id ORDER BY
 id;
+---+---+---+
| id|sum|max|
+---+---+---+
|100| 32| 15|
|200| 33| 20|
|300| 13|  8|
+---+---+---+

-- Count the number of distinct dealer cities per car_model.
SELECT car_model, count(DISTINCT city) AS count FROM dealer GROUP BY car_model;
+------------+-----+
|   car_model|count|
+------------+-----+
| Honda Civic|    3|
|   Honda CRV|    2|
|Honda Accord|    3|
+------------+-----+

-- Sum of only 'Honda Civic' and 'Honda CRV' quantities per dealership.
SELECT id, sum(quantity) FILTER (
WHERE car_model IN ('Honda Civic', 'Honda CRV')
) AS `sum(quantity)` FROM dealer
GROUP BY id ORDER BY id;
+---+-------------+
| id|sum(quantity)|
+---+-------------+
|100|           17|
|200|           23|
|300|            5|
+---+-------------+

-- Aggregations using multiple sets of grouping columns in a single statement.
-- Following performs aggregations based on four sets of grouping columns.
-- 1. city, car_model
-- 2. city
-- 3. car_model
-- 4. Empty grouping set. Returns quantities for all city and car models.
SELECT city, car_model, sum(quantity) AS sum FROM dealer
GROUP BY GROUPING SETS ((city, car_model), (city), (car_model), ())
ORDER BY city;
+---------+------------+---+
```

```
|     city|   car_model|sum|
+---------+------------+---+
|     null|        null| 78|
|     null| HondaAccord| 33|
|     null|    HondaCRV| 10|
|     null|  HondaCivic| 35|
|   Dublin|        null| 33|
|   Dublin| HondaAccord| 10|
|   Dublin|    HondaCRV|  3|
|   Dublin|  HondaCivic| 20|
|  Fremont|        null| 32|
|  Fremont| HondaAccord| 15|
|  Fremont|    HondaCRV|  7|
|  Fremont|  HondaCivic| 10|
| San Jose|        null| 13|
| San Jose| HondaAccord|  8|
| San Jose|  HondaCivic|  5|
+---------+------------+---+

-- Group by processing with `ROLLUP` clause.
-- Equivalent GROUP BY GROUPING SETS ((city, car_model), (city), ())
SELECT city, car_model, sum(quantity) AS sum FROM dealer
GROUP BY city, car_model WITH ROLLUP
ORDER BY city, car_model;
+---------+------------+---+
|     city|   car_model|sum|
+---------+------------+---+
|     null|        null| 78|
|   Dublin|        null| 33|
|   Dublin| HondaAccord| 10|
|   Dublin|    HondaCRV|  3|
|   Dublin|  HondaCivic| 20|
|  Fremont|        null| 32|
|  Fremont| HondaAccord| 15|
|  Fremont|    HondaCRV|  7|
|  Fremont|  HondaCivic| 10|
| San Jose|        null| 13|
| San Jose| HondaAccord|  8|
| San Jose|  HondaCivic|  5|
+---------+------------+---+

-- Group by processing with `CUBE` clause.
-- Equivalent GROUP BY GROUPING SETS ((city, car_model), (city), (car_model), ())
SELECT city, car_model, sum(quantity) AS sum FROM dealer
```

```
GROUP BY city, car_model WITH CUBE
ORDER BY city, car_model;
+---------+------------+---+
|     city|   car_model|sum|
+---------+------------+---+
|     null|        null| 78|
|     null| HondaAccord| 33|
|     null|    HondaCRV| 10|
|     null|  HondaCivic| 35|
|   Dublin|        null| 33|
|   Dublin| HondaAccord| 10|
|   Dublin|    HondaCRV|  3|
|   Dublin|  HondaCivic| 20|
|  Fremont|        null| 32|
|  Fremont| HondaAccord| 15|
|  Fremont|    HondaCRV|  7|
|  Fremont|  HondaCivic| 10|
| San Jose|        null| 13|
| San Jose| HondaAccord|  8|
| San Jose|  HondaCivic|  5|
+---------+------------+---+

--Prepare data for ignore nulls example
CREATE TABLE person (id INT, name STRING, age INT);
INSERT INTO person VALUES
(100, 'Mary', NULL),
(200, 'John', 30),
(300, 'Mike', 80),
(400, 'Dan', 50);

--Select the first row in column age
SELECT FIRST(age) FROM person;
+--------------------+
| first(age, false)  |
+--------------------+
| NULL               |
+--------------------+

--Get the first row in column `age` ignore nulls,last row in column `id` and sum of
 column `id`.
SELECT FIRST(age IGNORE NULLS), LAST(id), SUM(id) FROM person;
+-------------------+------------------+----------+
| first(age, true)  | last(id, false)  | sum(id)  |
+-------------------+------------------+----------+
```

```
| 30                | 400               | 1000     |
+-------------------+-------------------+----------+
```

HAVING-Klausel

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen SQL-Befehl unterstützen, finden Sie unter. the section called “Unterstützte SQL-Befehle”

Die `HAVING` Klausel wird verwendet, um die Ergebnisse zu filtern, die auf der `GROUP BY` Grundlage der angegebenen Bedingung erzeugt wurden. Sie wird häufig in Verbindung mit einer `GROUP BY` Klausel verwendet.

Syntax

```
HAVING boolean_expression
```

Parameter

- boolescher_Ausdruck

  Gibt einen beliebigen Ausdruck an, der zu einem booleschen Ergebnistyp ausgewertet wird. Zwei oder mehr Ausdrücke können mithilfe der logischen Operatoren (`AND`,) miteinander kombiniert werden. `OR`

  Hinweis Die in der `HAVING` Klausel angegebenen Ausdrücke können sich nur auf Folgendes beziehen:

  1. Konstanten
  2. Ausdrücke, die vorkommen in `GROUP BY`
  3. Aggregationsfunktionen

Beispiele

```
CREATE TABLE dealer (id INT, city STRING, car_model STRING, quantity INT);
INSERT INTO dealer VALUES
(100, 'Fremont', 'Honda Civic', 10),
(100, 'Fremont', 'Honda Accord', 15),
```

```
(100, 'Fremont', 'Honda CRV', 7),
(200, 'Dublin', 'Honda Civic', 20),
(200, 'Dublin', 'Honda Accord', 10),
(200, 'Dublin', 'Honda CRV', 3),
(300, 'San Jose', 'Honda Civic', 5),
(300, 'San Jose', 'Honda Accord', 8);

-- `HAVING` clause referring to column in `GROUP BY`.
SELECT city, sum(quantity) AS sum FROM dealer GROUP BY city HAVING city = 'Fremont';
+-------+---+
|   city|sum|
+-------+---+
|Fremont| 32|
+-------+---+

-- `HAVING` clause referring to aggregate function.
SELECT city, sum(quantity) AS sum FROM dealer GROUP BY city HAVING sum(quantity) > 15;
+-------+---+
|   city|sum|
+-------+---+
| Dublin| 33|
|Fremont| 32|
+-------+---+

-- `HAVING` clause referring to aggregate function by its alias.
SELECT city, sum(quantity) AS sum FROM dealer GROUP BY city HAVING sum > 15;
+-------+---+
|   city|sum|
+-------+---+
| Dublin| 33|
|Fremont| 32|
+-------+---+

-- `HAVING` clause referring to a different aggregate function than what is present in
-- `SELECT` list.
SELECT city, sum(quantity) AS sum FROM dealer GROUP BY city HAVING max(quantity) > 15;
+------+---+
|  city|sum|
+------+---+
|Dublin| 33|
+------+---+

-- `HAVING` clause referring to constant expression.
SELECT city, sum(quantity) AS sum FROM dealer GROUP BY city HAVING 1 > 0 ORDER BY city;
```

```
+--------+---+
|    city|sum|
+--------+---+
|  Dublin| 33|
| Fremont| 32|
|San Jose| 13|
+--------+---+

-- `HAVING` clause without a `GROUP BY` clause.
SELECT sum(quantity) AS sum FROM dealer HAVING sum(quantity) > 10;
+---+
|sum|
+---+
| 78|
+---+
```

ORDER BY-Klausel

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen SQL-Befehl unterstützen, finden Sie unterthe section called “Unterstützte SQL-Befehle”.

Die `ORDER BY` Klausel wird verwendet, um die Ergebniszeilen sortiert in der vom Benutzer angegebenen Reihenfolge zurückzugeben. Im Gegensatz zur SORT BY-Klausel garantiert diese Klausel eine vollständige Reihenfolge in der Ausgabe.

Syntax

```
ORDER BY { expression [ sort_direction | nulls_sort_order ] [ , ... ] }
```

Parameter

- SORTIERT NACH

  Gibt eine durch Kommas getrennte Liste von Ausdrücken zusammen mit optionalen Parametern `sort_direction` an`nulls_sort_order`, die zum Sortieren der Zeilen verwendet werden.

- sort_direction

Gibt optional an, ob die Zeilen in aufsteigender oder absteigender Reihenfolge sortiert werden sollen.

Die gültigen Werte für die Sortierrichtung gelten für aufsteigend und `ASC` `DESC` für absteigend.

Wenn die Sortierrichtung nicht explizit angegeben ist, werden Zeilen standardmäßig aufsteigend sortiert.

Syntax: `[ ASC | DESC ]`

- nulls_sort_order

Gibt optional an, ob `NULL` Werte zurückgegeben werden, die nicht NULL sind. before/after

Wenn null_sort_order nicht angegeben ist, wird zuerst `NULLs` sortiert, wenn die Sortierreihenfolge angegeben ist, `ASC` und NULLS sortiert zuletzt, wenn die Sortierreihenfolge angegeben ist. `DESC`

1. Wenn `NULLS FIRST` angegeben, werden unabhängig von der Sortierreihenfolge zuerst NULL-Werte zurückgegeben.

2. Wenn `NULLS LAST` angegeben, werden NULL-Werte unabhängig von der Sortierreihenfolge zuletzt zurückgegeben.

Syntax: `[ NULLS { FIRST | LAST } ]`

Beispiele

```
CREATE TABLE person (id INT, name STRING, age INT);
INSERT INTO person VALUES
(100, 'John', 30),
(200, 'Mary', NULL),
(300, 'Mike', 80),
(400, 'Jerry', NULL),
(500, 'Dan',  50);

-- Sort rows by age. By default rows are sorted in ascending manner with NULL FIRST.
SELECT name, age FROM person ORDER BY age;
+-----+----+
| name| age|
+-----+----+
|Jerry|null|
```

```
| Mary|null|
| John|  30|
|  Dan|  50|
| Mike|  80|
+-----+----+

-- Sort rows in ascending manner keeping null values to be last.
SELECT name, age FROM person ORDER BY age NULLS LAST;
+-----+----+
| name| age|
+-----+----+
| John|  30|
|  Dan|  50|
| Mike|  80|
| Mary|null|
|Jerry|null|
+-----+----+

-- Sort rows by age in descending manner, which defaults to NULL LAST.
SELECT name, age FROM person ORDER BY age DESC;
+-----+----+
| name| age|
+-----+----+
| Mike|  80|
|  Dan|  50|
| John|  30|
|Jerry|null|
| Mary|null|
+-----+----+

-- Sort rows in ascending manner keeping null values to be first.
SELECT name, age FROM person ORDER BY age DESC NULLS FIRST;
+-----+----+
| name| age|
+-----+----+
|Jerry|null|
| Mary|null|
| Mike|  80|
|  Dan|  50|
| John|  30|
+-----+----+

-- Sort rows based on more than one column with each column having different
-- sort direction.
```

```
SELECT * FROM person ORDER BY name ASC, age DESC;
+---+-----+----+
| id| name| age|
+---+-----+----+
|500|  Dan|  50|
|400|Jerry|null|
|100| John|  30|
|200| Mary|null|
|300| Mike|  80|
+---+-----+----+
```

JOIN-Klausel

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen SQL-Befehl unterstützen, finden Sie unterthe section called “Unterstützte SQL-Befehle”.

Eine SQL-Verknüpfung wird verwendet, um Zeilen aus zwei Beziehungen auf der Grundlage von Verbindungskriterien zu kombinieren. Im folgenden Abschnitt werden die allgemeine Join-Syntax und die verschiedenen Arten von Verknüpfungen zusammen mit Beispielen beschrieben.

Syntax

```
relation INNER JOIN relation [ join_criteria ]
```

Parameter

- Beziehung

  Gibt die Beziehung an, die verbunden werden soll.
- Verbindungstyp

  Gibt den Verbindungstyp an.

  Syntax: `INNER | CROSS | LEFT OUTER`
- join_criteria

  Gibt an, wie die Zeilen einer Beziehung mit den Zeilen einer anderen Beziehung kombiniert werden.

Syntax: `ON boolean_expression | USING ( column_name [ , ... ] )`

- boolescher_Ausdruck

  Gibt einen Ausdruck mit dem Rückgabetyp Boolean an.

Arten von Verbindungen

- Innerer Zusammenschluss

  Der innere Join muss explizit angegeben werden. Es wählt Zeilen aus, die in beiden Beziehungen übereinstimmende Werte haben.

  Syntax: `relation INNER JOIN relation [ join_criteria ]`

- Links verbinden

  Eine linke Verknüpfung gibt alle Werte aus der linken Beziehung und die übereinstimmenden Werte aus der rechten Beziehung zurück oder hängt NULL an, wenn keine Übereinstimmung vorliegt. Sie wird auch als Left Outer Join bezeichnet.

  Syntax: `relation LEFT OUTER JOIN relation [ join_criteria ]`

- Kreuzverknüpfung

  Eine Kreuzverknüpfung gibt das kartesische Produkt zweier Beziehungen zurück.

  Syntax: `relation CROSS JOIN relation [ join_criteria ]`

Beispiele

```
-- Use employee and department tables to demonstrate different type of joins.
SELECT * FROM employee;
+---+-----+------+
| id| name|deptno|
+---+-----+------+
|105|Chloe|     5|
|103| Paul|     3|
|101| John|     1|
|102| Lisa|     2|
|104| Evan|     4|
|106|  Amy|     6|
```

```
+---+-----+------+
SELECT * FROM department;
+------+-----------+
|deptno|   deptname|
+------+-----------+
|     3|Engineering|
|     2|      Sales|
|     1|  Marketing|
+------+-----------+

-- Use employee and department tables to demonstrate inner join.
SELECT id, name, employee.deptno, deptname
FROM employee INNER JOIN department ON employee.deptno = department.deptno;
+---+-----+------+-----------|
| id| name|deptno|   deptname|
+---+-----+------+-----------|
|103| Paul|     3|Engineering|
|101| John|     1|  Marketing|
|102| Lisa|     2|      Sales|
+---+-----+------+-----------|

-- Use employee and department tables to demonstrate left join.
SELECT id, name, employee.deptno, deptname
FROM employee LEFT JOIN department ON employee.deptno = department.deptno;
+---+-----+------+-----------|
| id| name|deptno|   deptname|
+---+-----+------+-----------|
|105|Chloe|     5|       NULL|
|103| Paul|     3|Engineering|
|101| John|     1|  Marketing|
|102| Lisa|     2|      Sales|
|104| Evan|     4|       NULL|
|106|  Amy|     6|       NULL|
+---+-----+------+-----------|

-- Use employee and department tables to demonstrate cross join.
SELECT id, name, employee.deptno, deptname FROM employee CROSS JOIN department;
+---+-----+------+-----------|
| id| name|deptno|   deptname|
+---+-----+------+-----------|
|105|Chloe|     5|Engineering|
|105|Chloe|     5|  Marketing|
|105|Chloe|     5|      Sales|
|103| Paul|     3|Engineering|
```

```
|103| Paul|     3|  Marketing|
|103| Paul|     3|      Sales|
|101| John|     1|Engineering|
|101| John|     1|  Marketing|
|101| John|     1|      Sales|
|102| Lisa|     2|Engineering|
|102| Lisa|     2|  Marketing|
|102| Lisa|     2|      Sales|
|104| Evan|     4|Engineering|
|104| Evan|     4|  Marketing|
|104| Evan|     4|      Sales|
|106|  Amy|     4|Engineering|
|106|  Amy|     4|  Marketing|
|106|  Amy|     4|      Sales|
+---+-----+------+-----------|
```

LIMIT-Klausel

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen SQL-Befehl unterstützen, finden Sie unter. the section called “Unterstützte SQL-Befehle”

Die `LIMIT` Klausel wird verwendet, um die Anzahl der von der Anweisung zurückgegebenen Zeilen einzuschränken. `SELECT` Im Allgemeinen wird diese Klausel in Verbindung mit verwendet, `ORDER BY` um sicherzustellen, dass die Ergebnisse deterministisch sind.

Syntax

```
LIMIT { ALL | integer_expression }
```

Parameter

- ALLE

  Falls angegeben, gibt die Abfrage alle Zeilen zurück. Mit anderen Worten, es wird kein Limit angewendet, wenn diese Option angegeben ist.
- integer_expression

  Gibt einen faltbaren Ausdruck an, der eine Ganzzahl zurückgibt.

Beispiele

```
CREATE TABLE person (name STRING, age INT);
INSERT INTO person VALUES
('Jane Doe', 25),
('Pat C', 18),
('Nikki W', 16),
('John D', 25),
('Juan L', 18),
('Jorge S', 16);

-- Select the first two rows.
SELECT name, age FROM person ORDER BY name LIMIT 2;
+-------+---+
|   name|age|
+-------+---+
|  Pat C| 18|
|Jorge S| 16|
+------+---+

-- Specifying ALL option on LIMIT returns all the rows.
SELECT name, age FROM person ORDER BY name LIMIT ALL;
+--------+---+
|    name|age|
+--------+---+
|   Pat C| 18|
| Jorge S| 16|
|  Juan L| 18|
|  John D| 25|
| Nikki W| 16|
|Jane Doe| 25|
+--------+---+

-- A function expression as an input to LIMIT.
SELECT name, age FROM person ORDER BY name LIMIT length('OPENSEARCH');
+-------+---+
|   name|age|
+-------+---+
|  Pat C| 18|
|Jorge S| 16|
| Juan L| 18|
| John D| 25|
|Nikki W| 16|
```

```
+-------+---+
```

CASE-Klausel

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen SQL-Befehl unterstützen, finden Sie unterthe section called “Unterstützte SQL-Befehle”.

Die CASE Klausel verwendet eine Regel, um ein bestimmtes Ergebnis auf der Grundlage der angegebenen Bedingung zurückzugeben, ähnlich wie if/else-Anweisungen in anderen Programmiersprachen.

Syntax

```
CASE [ expression ] { WHEN boolean_expression THEN then_expression } [ ... ]
[ ELSE else_expression ]
END
```

Parameter

- boolescher_Ausdruck

  Gibt einen beliebigen Ausdruck an, der zu einem booleschen Ergebnistyp ausgewertet wird.

  Zwei oder mehr Ausdrücke können mithilfe der logischen Operatoren (AND,) miteinander kombiniert werden. OR
- then_expression

  Gibt den Ausdruck then auf der Grundlage der boolean_expression-Bedingung an.

  `then_expression`und `else_expression` sollten alle vom gleichen Typ sein oder durch einen gemeinsamen Typ erzwingbar sein.
- else_expression

  Gibt den Standardausdruck an.

  `then_expression`und `else_expression` sollten alle vom gleichen Typ sein oder durch einen gemeinsamen Typ erzwingbar sein.

Beispiele

```
CREATE TABLE person (id INT, name STRING, age INT);
INSERT INTO person VALUES
(100, 'John', 30),
(200, 'Mary', NULL),
(300, 'Mike', 80),
(400, 'Dan', 50);
SELECT id, CASE WHEN id > 200 THEN 'bigger' ELSE 'small' END FROM person;
+------+-----------------------------------------------------+
|  id  | CASE WHEN (id > 200) THEN bigger ELSE small END  |
+------+-----------------------------------------------------+
| 100  | small                                               |
| 200  | small                                               |
| 300  | bigger                                              |
| 400  | bigger                                              |
+------+-----------------------------------------------------+
SELECT id, CASE id WHEN 100 then 'bigger' WHEN  id > 300 THEN '300' ELSE 'small' END
 FROM person;
+------
+-------------------------------------------------------------------------------------------------------
+
|  id  | CASE WHEN (id = 100) THEN bigger WHEN (id = CAST((id > 300) AS INT)) THEN 300
 ELSE small END  |
+------
+-------------------------------------------------------------------------------------------------------
+
| 100  | bigger
                |
| 200  | small
                |
| 300  | small
                |
| 400  | small
                |
+------
+-------------------------------------------------------------------------------------------------------
+
```

Gemeinsamer Tabellenausdruck

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen SQL-Befehl unterstützen, finden Sie unterthe section called “Unterstützte SQL-Befehle”.

Ein allgemeiner Tabellenausdruck (Common Table Expression, CTE) definiert eine temporäre Ergebnismenge, auf die ein Benutzer im Rahmen einer SQL-Anweisung möglicherweise mehrfach verweisen kann. Ein CTE wird hauptsächlich in einer `SELECT` Anweisung verwendet.

Syntax

```
WITH common_table_expression [ , ... ]
```

While `common_table_expression` ist definiert als:

```
Syntexpression_name [ ( column_name [ , ... ] ) ] [ AS ] ( query )
```

Parameter

- Ausdrucksname

  Gibt einen Namen für den allgemeinen Tabellenausdruck an.
- query

  Eine `SELECT` Aussage.

Beispiele

```
-- CTE with multiple column aliases
WITH t(x, y) AS (SELECT 1, 2)
SELECT * FROM t WHERE x = 1 AND y = 2;
+---+---+
|  x|  y|
+---+---+
|  1|  2|
+---+---+
```

```
-- CTE in CTE definition
WITH t AS (
WITH t2 AS (SELECT 1)
SELECT * FROM t2
)
SELECT * FROM t;
+---+
|  1|
+---+
|  1|
+---+

-- CTE in subquery
SELECT max(c) FROM (
WITH t(c) AS (SELECT 1)
SELECT * FROM t
);
+------+
|max(c)|
+------+
|     1|
+------+

-- CTE in subquery expression
SELECT (
WITH t AS (SELECT 1)
SELECT * FROM t
);
+----------------+
|scalarsubquery()|
+----------------+
|               1|
+----------------+

-- CTE in CREATE VIEW statement
CREATE VIEW v AS
WITH t(a, b, c, d) AS (SELECT 1, 2, 3, 4)
SELECT * FROM t;
SELECT * FROM v;
+---+---+---+---+
|  a|  b|  c|  d|
+---+---+---+---+
|  1|  2|  3|  4|
```

```
+---+---+---+---+
```

EXPLAIN

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen SQL-Befehl unterstützen, finden Sie unterthe section called “Unterstützte SQL-Befehle”.

Die `EXPLAIN` Anweisung wird verwendet, um logische/physische Pläne für eine Eingabeanweisung bereitzustellen. Standardmäßig enthält diese Klausel nur Informationen über einen physischen Plan.

Syntax

```
EXPLAIN [ EXTENDED | CODEGEN | COST | FORMATTED ] statement
```

Parameter

- ERWEITERT

  Generiert einen analysierten logischen Plan, einen analysierten logischen Plan, einen optimierten logischen Plan und einen physischen Plan.

  Der analysierte logische Plan ist ein ungelöster Plan, der aus der Abfrage extrahiert wurde.

  Analysierte logische Pläne werden `unresolvedRelation` umgewandelt, was zu vollständig typisierten `unresolvedAttribute` Objekten führt.

  Der optimierte logische Plan wird mithilfe einer Reihe von Optimierungsregeln transformiert, was zum physischen Plan führt.
- CODEGEN

  Generiert Code für die Anweisung, falls vorhanden, und einen physischen Plan.
- KOSTEN

  Wenn Planknotenstatistiken verfügbar sind, generiert es einen logischen Plan und die Statistiken.
- FORMATIERT

  Generiert zwei Abschnitte: eine physische Planskizze und Knotendetails.

- statement

  Gibt eine zu erklärende SQL-Anweisung an.

Beispiele

```
-- Default Output
EXPLAIN select k, sum(v) from values (1, 2), (1, 3) t(k, v) group by k;
+----------------------------------------------------+
|                                                plan|
+----------------------------------------------------+
| == Physical Plan ==
*(2) HashAggregate(keys=[k#33], functions=[sum(cast(v#34 as bigint))])
+- Exchange hashpartitioning(k#33, 200), true, [id=#59]
+- *(1) HashAggregate(keys=[k#33], functions=[partial_sum(cast(v#34 as bigint))])
+- *(1) LocalTableScan [k#33, v#34]
|
+----------------------------------------------------

-- Using Extended
EXPLAIN EXTENDED select k, sum(v) from values (1, 2), (1, 3) t(k, v) group by k;
+----------------------------------------------------+
|                                                plan|
+----------------------------------------------------+
| == Parsed Logical Plan ==
'Aggregate ['k], ['k, unresolvedalias('sum('v), None)]
 +- 'SubqueryAlias `t`
+- 'UnresolvedInlineTable [k, v], [List(1, 2), List(1, 3)]

 == Analyzed Logical Plan ==
 k: int, sum(v): bigint
 Aggregate [k#47], [k#47, sum(cast(v#48 as bigint)) AS sum(v)#50L]
 +- SubqueryAlias `t`
    +- LocalRelation [k#47, v#48]

 == Optimized Logical Plan ==
 Aggregate [k#47], [k#47, sum(cast(v#48 as bigint)) AS sum(v)#50L]
 +- LocalRelation [k#47, v#48]

 == Physical Plan ==
 *(2) HashAggregate(keys=[k#47], functions=[sum(cast(v#48 as bigint))], output=[k#47,
 sum(v)#50L])
+- Exchange hashpartitioning(k#47, 200), true, [id=#79]
```

```
   +- *(1) HashAggregate(keys=[k#47], functions=[partial_sum(cast(v#48 as bigint))],
 output=[k#47, sum#52L])
    +- *(1) LocalTableScan [k#47, v#48]
|
+----------------------------------------------------+

-- Using Formatted
EXPLAIN FORMATTED select k, sum(v) from values (1, 2), (1, 3) t(k, v) group by k;
+----------------------------------------------------+
|                                                plan|
+----------------------------------------------------+
| == Physical Plan ==
 * HashAggregate (4)
 +- Exchange (3)
    +- * HashAggregate (2)
       +- * LocalTableScan (1)


 (1) LocalTableScan [codegen id : 1]
 Output: [k#19, v#20]

 (2) HashAggregate [codegen id : 1]
 Input: [k#19, v#20]

 (3) Exchange
 Input: [k#19, sum#24L]

 (4) HashAggregate [codegen id : 2]
 Input: [k#19, sum#24L]
|
+----------------------------------------------------+
```

LATERALE SUBQUERY-Klausel

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen SQL-Befehl unterstützen, finden Sie unter. the section called “Unterstützte SQL-Befehle”

`LATERAL SUBQUERY`ist eine Unterabfrage, der das Schlüsselwort vorangestellt ist. `LATERAL` Es bietet eine Möglichkeit, auf Spalten in der vorherigen `FROM` Klausel zu verweisen. Ohne das `LATERAL`

Schlüsselwort können Unterabfragen nur auf Spalten in der äußeren Abfrage verweisen, nicht jedoch auf Spalten in der FROM Klausel. LATERAL SUBQUERYmacht die komplizierten Abfragen einfacher und effizienter.

Syntax

```
[ LATERAL ] primary_relation [ join_relation ]
```

Parameter

- primary_relation

  Gibt die primäre Beziehung an. Es kann sich dabei um eines der folgenden handeln:

  1. Beziehung zur Tabelle
  2. Abfrage mit Aliasnamen

     Syntax: `( query ) [ [ AS ] alias ]`
  3. Beziehung mit Aliasnamen

     `Syntax: ( relation ) [ [ AS ] alias ]`

Beispiele

```
CREATE TABLE t1 (c1 INT, c2 INT);
INSERT INTO t1 VALUES (0, 1), (1, 2);
CREATE TABLE t2 (c1 INT, c2 INT);
INSERT INTO t2 VALUES (0, 2), (0, 3);
SELECT * FROM t1,
LATERAL (SELECT * FROM t2 WHERE t1.c1 = t2.c1);
+--------+-------+--------+-------+
|  t1.c1 | t1.c2 |  t2.c1 | t2.c2 |
+-------+--------+--------+-------+
|    0   |   1   |    0   |   3   |
|    0   |   1   |    0   |   2   |
+-------+--------+--------+-------+
SELECT a, b, c FROM t1,
LATERAL (SELECT c1 + c2 AS a),
LATERAL (SELECT c1 - c2 AS b),
LATERAL (SELECT a * b AS c);
+--------+-------+--------+
|    a   |   b   |    c   |
```

```
+-------+--------+--------+
|    3  |  -1    |   -3   |
|    1  |  -1    |   -1   |
+-------+--------+--------+
```

Klausel LATERAL VIEW

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen SQL-Befehl unterstützen, finden Sie unterthe section called “Unterstützte SQL-Befehle”.

Die `LATERAL VIEW` Klausel wird in Verbindung mit Generatorfunktionen wie`EXPLODE`, verwendet, die eine virtuelle Tabelle mit einer oder mehreren Zeilen generieren. `LATERAL VIEW`wendet die Zeilen auf jede ursprüngliche Ausgabezeile an.

Syntax

```
LATERAL VIEW [ OUTER ] generator_function ( expression [ , ... ] ) [ table_alias ] AS
 column_alias [ , ... ]
```

Parameter

- ÄUSSERER

  Falls `OUTER` angegeben, wird Null zurückgegeben, wenn eine Eingabe leer oder Null array/map ist.
- generator_function

  Spezifiziert eine Generatorfunktion (`EXPLODEINLINE`, usw.).
- table_alias

  Der Alias für`generator_function`, der optional ist.
- column_alias

  Listet die Spaltenaliase von auf`generator_function`, die in Ausgabezeilen verwendet werden können.

  Sie können mehrere Aliase verwenden, wenn mehrere `generator_function` Ausgabespalten vorhanden sind.

Beispiele

```
CREATE TABLE person (id INT, name STRING, age INT, class INT, address STRING);
INSERT INTO person VALUES
(100, 'John', 30, 1, 'Street 1'),
(200, 'Mary', NULL, 1, 'Street 2'),
(300, 'Mike', 80, 3, 'Street 3'),
(400, 'Dan', 50, 4, 'Street 4');
SELECT * FROM person
LATERAL VIEW EXPLODE(ARRAY(30, 60)) tableName AS c_age
LATERAL VIEW EXPLODE(ARRAY(40, 80)) AS d_age;
+------+-------+-------+--------+-----------+--------+--------+
|  id  | name  |  age  | class  |  address  | c_age  | d_age  |
+------+-------+-------+--------+-----------+--------+--------+
| 100  | John  | 30    | 1      | Street 1  | 30     | 40     |
| 100  | John  | 30    | 1      | Street 1  | 30     | 80     |
| 100  | John  | 30    | 1      | Street 1  | 60     | 40     |
| 100  | John  | 30    | 1      | Street 1  | 60     | 80     |
| 200  | Mary  | NULL  | 1      | Street 2  | 30     | 40     |
| 200  | Mary  | NULL  | 1      | Street 2  | 30     | 80     |
| 200  | Mary  | NULL  | 1      | Street 2  | 60     | 40     |
| 200  | Mary  | NULL  | 1      | Street 2  | 60     | 80     |
| 300  | Mike  | 80    | 3      | Street 3  | 30     | 40     |
| 300  | Mike  | 80    | 3      | Street 3  | 30     | 80     |
| 300  | Mike  | 80    | 3      | Street 3  | 60     | 40     |
| 300  | Mike  | 80    | 3      | Street 3  | 60     | 80     |
| 400  | Dan   | 50    | 4      | Street 4  | 30     | 40     |
| 400  | Dan   | 50    | 4      | Street 4  | 30     | 80     |
| 400  | Dan   | 50    | 4      | Street 4  | 60     | 40     |
| 400  | Dan   | 50    | 4      | Street 4  | 60     | 80     |
+------+-------+-------+--------+-----------+--------+--------+
SELECT c_age, COUNT(1) FROM person
LATERAL VIEW EXPLODE(ARRAY(30, 60)) AS c_age
LATERAL VIEW EXPLODE(ARRAY(40, 80)) AS d_age
GROUP BY c_age;
+--------+-----------+
| c_age  | count(1)  |
+--------+-----------+
| 60     | 8         |
| 30     | 8         |
+--------+-----------+
SELECT * FROM person
LATERAL VIEW EXPLODE(ARRAY()) tableName AS c_age;
+-----+-------+------+--------+----------+--------+
```

```
| id  | name  | age  | class  | address  | c_age  |
+-----+-------+------+--------+----------+--------+
+-----+-------+------+--------+----------+--------+
SELECT * FROM person
LATERAL VIEW OUTER EXPLODE(ARRAY()) tableName AS c_age;
+------+-------+-------+--------+-----------+--------+
|  id  | name  |  age  | class  |  address  | c_age  |
+------+-------+-------+--------+-----------+--------+
| 100  | John  | 30    | 1      | Street 1  | NULL   |
| 200  | Mary  | NULL  | 1      | Street 2  | NULL   |
| 300  | Mike  | 80    | 3      | Street 3  | NULL   |
| 400  | Dan   | 50    | 4      | Street 4  | NULL   |
+------+-------+-------+--------+-----------+--------+
```

LIKE-Prädikat

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen SQL-Befehl unterstützen, finden Sie unter. the section called “Unterstützte SQL-Befehle”

Ein `LIKE` Prädikat wird verwendet, um nach einem bestimmten Muster zu suchen. Dieses Prädikat unterstützt auch mehrere Muster mit Quantifizierern wie`ANY`, `SOME` und. `ALL`

Syntax

```
[ NOT ] { LIKE search_pattern [ ESCAPE esc_char ] | [ RLIKE | REGEXP ] regex_pattern }
[ NOT ] { LIKE quantifiers ( search_pattern [ , ... ]) }
```

Parameter

- search_pattern

  Gibt ein Zeichenkettenmuster an, das mit der LIKE-Klausel durchsucht werden soll. Sie kann spezielle Zeichen enthalten, die dem Muster entsprechen:

  - %entspricht null oder mehr Zeichen.
  - _entspricht genau einem Zeichen.
- esc_char

  Gibt das Zeichen an, das als Escape-Zeichen verwendet wird. Das Standard-Escape-Zeichen ist. \

- regex_pattern

  Gibt ein Suchmuster für reguläre Ausdrücke an, das mit der OR-Klausel durchsucht werden soll. `RLIKE` `REGEXP`

- Quantifizierer

  Definiert die Prädikat-Quantifizierer include`ANY`, und. `SOME` `ALL`

  `ANY`oder `SOME` bedeutet, wenn eines der Muster mit der Eingabe übereinstimmt, wird „true“ zurückgegeben.

  `ALL`bedeutet, wenn alle Muster mit der Eingabe übereinstimmen, dann wird true zurückgegeben.

Beispiele

```
CREATE TABLE person (id INT, name STRING, age INT);
INSERT INTO person VALUES
(100, 'John', 30),
(200, 'Mary', NULL),
(300, 'Mike', 80),
(400, 'Dan',  50),
(500, 'Evan_w', 16);
SELECT * FROM person WHERE name LIKE 'M%';
+---+----+----+
| id|name| age|
+---+----+----+
|300|Mike|  80|
|200|Mary|null|
+---+----+----+
SELECT * FROM person WHERE name LIKE 'M_ry';
+---+----+----+
| id|name| age|
+---+----+----+
|200|Mary|null|
+---+----+----+
SELECT * FROM person WHERE name NOT LIKE 'M_ry';
+---+------+---+
| id|  name|age|
+---+------+---+
|500|Evan_W| 16|
|300|  Mike| 80|
|100|  John| 30|
```

```
|400|   Dan| 50|
+---+------+---+
SELECT * FROM person WHERE name RLIKE 'M+';
+---+----+----+
| id|name| age|
+---+----+----+
|300|Mike|  80|
|200|Mary|null|
+---+----+----+
SELECT * FROM person WHERE name REGEXP 'M+';
+---+----+----+
| id|name| age|
+---+----+----+
|300|Mike|  80|
|200|Mary|null|
+---+----+----+
SELECT * FROM person WHERE name LIKE '%\_%';
+---+------+---+
| id|  name|age|
+---+------+---+
|500|Evan_W| 16|
+---+------+---+
SELECT * FROM person WHERE name LIKE '%$_%' ESCAPE '$';
+---+------+---+
| id|  name|age|
+---+------+---+
|500|Evan_W| 16|
+---+------+---+
SELECT * FROM person WHERE name LIKE ALL ('%an%', '%an');
+---+----+----+
| id|name| age|
+---+----+----+
|400| Dan|  50|
+---+----+----+
SELECT * FROM person WHERE name LIKE ANY ('%an%', '%an');
+---+------+---+
| id|  name|age|
+---+------+---+
|400|   Dan| 50|
|500|Evan_W| 16|
+---+------+---+
SELECT * FROM person WHERE name LIKE SOME ('%an%', '%an');
+---+------+---+
| id|  name|age|
```

```
+---+------+---+
|400|   Dan| 50|
|500|Evan_W| 16|
+---+------+---+
SELECT * FROM person WHERE name NOT LIKE ALL ('%an%', '%an');
+---+----+----+
| id|name| age|
+---+----+----+
|100|John|  30|
|200|Mary|null|
|300|Mike|  80|
+---+----+----+
SELECT * FROM person WHERE name NOT LIKE ANY ('%an%', '%an');
+---+------+----+
| id|  name| age|
+---+------+----+
|100|  John|  30|
|200|  Mary|null|
|300|  Mike|  80|
|500|Evan_W|  16|
+---+------+----+
SELECT * FROM person WHERE name NOT LIKE SOME ('%an%', '%an');
+---+------+----+
| id|  name| age|
+---+------+----+
|100|  John|  30|
|200|  Mary|null|
|300|  Mike|  80|
|500|Evan_W|  16|
+---+------+----+
```

OFFSET

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen SQL-Befehl unterstützen, finden Sie unterthe section called “Unterstützte SQL-Befehle”.

Die `OFFSET` Klausel wird verwendet, um die Anzahl der Zeilen anzugeben, die übersprungen werden sollen, bevor mit der Rückgabe der von der `SELECT` Anweisung zurückgegebenen Zeilen begonnen

wird. Im Allgemeinen wird diese Klausel in Verbindung mit verwendet, `ORDER BY` um sicherzustellen, dass die Ergebnisse deterministisch sind.

Syntax

```
OFFSET integer_expression
```

Parameter

- integer_expression

  Gibt einen faltbaren Ausdruck an, der eine Ganzzahl zurückgibt.

Beispiele

```
CREATE TABLE person (name STRING, age INT);
INSERT INTO person VALUES
('Jane Doe', 25),
('Pat C', 18),
('Nikki W', 16),
('Juan L', 25),
('John D', 18),
('Jorge S', 16);

-- Skip the first two rows.
SELECT name, age FROM person ORDER BY name OFFSET 2;
+-------+---+
|   name|age|
+-------+---+
| John D| 18|
| Juan L| 25|
|Nikki W| 16|
|Jane Doe| 25|
+-------+---+

-- Skip the first two rows and returns the next three rows.
SELECT name, age FROM person ORDER BY name LIMIT 3 OFFSET 2;
+-------+---+
|   name|age|
+-------+---+
| John D| 18|
| Juan L| 25|
```

```
|Nikki W| 16|
+-------+---+

-- A function expression as an input to OFFSET.
SELECT name, age FROM person ORDER BY name OFFSET length('WAGON');
+-------+---+
|   name|age|
+-------+---+
|Jane Doe| 25|
+-------+---+
```

PIVOT-Klausel

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen SQL-Befehl unterstützen, finden Sie unter. the section called “Unterstützte SQL-Befehle”

Die `PIVOT` Klausel wird für die Datenperspektive verwendet. Wir können die aggregierten Werte auf der Grundlage bestimmter Spaltenwerte abrufen, die dann in mehrere Spalten umgewandelt werden, die in der `SELECT` Klausel verwendet werden. Die `PIVOT` Klausel kann nach dem Tabellennamen oder der Unterabfrage angegeben werden.

Syntax

```
PIVOT ( { aggregate_expression [ AS aggregate_expression_alias ] } [ , ... ] FOR
 column_list IN ( expression_list ) )
```

Parameter

- aggregate_expression

  Gibt einen `(SUM(a) COUNT(DISTINCT b)` Aggregatausdruck usw. an.).
- aggregate_expression_alias

  Gibt einen Alias für den Aggregatausdruck an.
- column_list

  Enthält Spalten in der `FROM` Klausel, die die Spalten angibt, die Sie durch neue Spalten ersetzen möchten. Sie können die Spalten mit Klammern umgeben, z. `(c1, c2)` B.

- expression_list

  Gibt neue Spalten an, die `column_list` als Aggregationsbedingung zum Abgleichen von Werten verwendet werden. Sie können auch Aliase für sie hinzufügen.

Beispiele

```
CREATE TABLE person (id INT, name STRING, age INT, class INT, address STRING);
INSERT INTO person VALUES
(100, 'John', 30, 1, 'Street 1'),
(200, 'Mary', NULL, 1, 'Street 2'),
(300, 'Mike', 80, 3, 'Street 3'),
(400, 'Dan', 50, 4, 'Street 4');
SELECT * FROM person
PIVOT (
SUM(age) AS a, AVG(class) AS c
FOR name IN ('John' AS john, 'Mike' AS mike)
);
+------+-----------+---------+---------+---------+---------+
|  id  |  address  | john_a  | john_c  | mike_a  | mike_c  |
+------+-----------+---------+---------+---------+---------+
| 200  | Street 2  | NULL    | NULL    | NULL    | NULL    |
| 100  | Street 1  | 30      | 1.0     | NULL    | NULL    |
| 300  | Street 3  | NULL    | NULL    | 80      | 3.0     |
| 400  | Street 4  | NULL    | NULL    | NULL    | NULL    |
+------+-----------+---------+---------+---------+---------+
SELECT * FROM person
PIVOT (
SUM(age) AS a, AVG(class) AS c
FOR (name, age) IN (('John', 30) AS c1, ('Mike', 40) AS c2)
);
+------+-----------+-------+-------+-------+-------+
|  id  |  address  | c1_a  | c1_c  | c2_a  | c2_c  |
+------+-----------+-------+-------+-------+-------+
| 200  | Street 2  | NULL  | NULL  | NULL  | NULL  |
| 100  | Street 1  | 30    | 1.0   | NULL  | NULL  |
| 300  | Street 3  | NULL  | NULL  | NULL  | NULL  |
| 400  | Street 4  | NULL  | NULL  | NULL  | NULL  |
+------+-----------+-------+-------+-------+-------+
```

Satzoperatoren

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen SQL-Befehl unterstützen, finden Sie unter. the section called “Unterstützte SQL-Befehle”

Mengenoperatoren werden verwendet, um zwei Eingabebeziehungen zu einer einzigen zu kombinieren. OpenSearch SQL unterstützt drei Arten von Mengenoperatoren:

- `EXCEPT` oder `MINUS`
- `INTERSECT`
- `UNION`

Eingabebeziehungen müssen dieselbe Anzahl von Spalten und kompatible Datentypen für die jeweiligen Spalten haben.

AUSSER

`EXCEPT`und `EXCEPT ALL` gibt die Zeilen zurück, die in einer Beziehung gefunden werden, aber nicht in der anderen. `EXCEPT`(alternativ`EXCEPT DISTINCT`) verwendet nur unterschiedliche Zeilen, entfernt aber `EXCEPT ALL` keine Duplikate aus den Ergebniszeilen. Beachten Sie, dass `MINUS` dies ein Alias für `EXCEPT` ist.

Syntax

```
[ ( ] relation [ ) ] EXCEPT | MINUS [ ALL | DISTINCT ] [ ( ] relation [ ) ]
```

Beispiele

```
-- Use table1 and table2 tables to demonstrate set operators in this page.
SELECT * FROM table1;
+---+
|  c|
+---+
|  3|
|  1|
|  2|
|  2|
```

```
|  3|
|  4|
+---+
SELECT * FROM table2;
+---+
|  c|
+---+
|  5|
|  1|
|  2|
|  2|
+---+
SELECT c FROM table1 EXCEPT SELECT c FROM table2;
+---+
|  c|
+---+
|  3|
|  4|
+---+
SELECT c FROM table1 MINUS SELECT c FROM table2;
+---+
|  c|
+---+
|  3|
|  4|
+---+
SELECT c FROM table1 EXCEPT ALL (SELECT c FROM table2);
+---+
|  c|
+---+
|  3|
|  3|
|  4|
+---+
SELECT c FROM table1 MINUS ALL (SELECT c FROM table2);
+---+
|  c|
+---+
|  3|
|  3|
|  4|
+---+
```

ÜBERSCHNEIDEN

`INTERSECT`und `INTERSECT ALL` gibt die Zeilen zurück, die in beiden Relationen gefunden wurden. `INTERSECT`(alternativ`INTERSECT DISTINCT`) verwendet nur unterschiedliche Zeilen, entfernt aber `INTERSECT ALL` keine Duplikate aus den Ergebniszeilen.

Syntax

```
 [ ( ] relation [ ) ] INTERSECT [ ALL | DISTINCT ] [ ( ] relation [ ) ]
```

Beispiele

```
(SELECT c FROM table1) INTERSECT (SELECT c FROM table2);
+---+
|  c|
+---+
|  1|
|  2|
+---+
(SELECT c FROM table1) INTERSECT DISTINCT (SELECT c FROM table2);
+---+
|  c|
+---+
|  1|
|  2|
+---+
(SELECT c FROM table1) INTERSECT ALL (SELECT c FROM table2);
+---+
|  c|
+---+
|  1|
|  2|
|  2|
+---+
```

VEREINIGUNG

`UNION`und `UNION ALL` gibt die Zeilen zurück, die in einer der beiden Relationen gefunden wurden. `UNION`(alternativ`UNION DISTINCT`) verwendet nur unterschiedliche Zeilen, entfernt aber `UNION ALL` keine Duplikate aus den Ergebniszeilen.

Syntax

```
[ ( ] relation [ ) ] UNION [ ALL | DISTINCT ] [ ( ] relation [ ) ]
```

Beispiele

```
(SELECT c FROM table1) UNION (SELECT c FROM table2);
+---+
|  c|
+---+
|  1|
|  3|
|  5|
|  4|
|  2|
+---+
(SELECT c FROM table1) UNION DISTINCT (SELECT c FROM table2);
+---+
|  c|
+---+
|  1|
|  3|
|  5|
|  4|
|  2|
+---+
SELECT c FROM table1 UNION ALL (SELECT c FROM table2);
+---+
|  c|
+---+
|  3|
|  1|
|  2|
|  2|
|  3|
|  4|
|  5|
|  1|
|  2|
|  2|
+---+
```

SORT BY-Klausel

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen SQL-Befehl unterstützen, finden Sie unterthe section called “Unterstützte SQL-Befehle”.

Die `SORT BY` Klausel wird verwendet, um die Ergebniszeilen innerhalb jeder Partition sortiert in der vom Benutzer angegebenen Reihenfolge zurückzugeben. Wenn es mehr als eine Partition gibt, `SORT BY` kann ein Ergebnis zurückgegeben werden, das teilweise sortiert ist. Dies unterscheidet sich von der `ORDER BY` Klausel, die eine vollständige Reihenfolge der Ausgabe garantiert.

Syntax

```
SORT BY { expression [ sort_direction | nulls_sort_order ] [ , ... ] }
```

Parameter

- SORTIERE NACH

  Gibt eine durch Kommas getrennte Liste von Ausdrücken zusammen mit den optionalen Parametern sort_direction und nulls_sort_order an, die verwendet werden, um die Zeilen innerhalb jeder Partition zu sortieren.

- sort_direction

  Gibt optional an, ob die Zeilen in aufsteigender oder absteigender Reihenfolge sortiert werden sollen.

  Die gültigen Werte für die Sortierrichtung gelten für aufsteigend und `ASC` `DESC` für absteigend.

  Wenn die Sortierrichtung nicht explizit angegeben ist, werden Zeilen standardmäßig aufsteigend sortiert.

  Syntax: `[ ASC | DESC ]`

- nulls_sort_order

  Gibt optional an, ob NULL-Werte vor/nach Nicht-NULL-Werten zurückgegeben werden.

Wenn nicht angegeben, `null_sort_order` wird zuerst NULLs sortiert, wenn die Sortierreihenfolge ist, `ASC` und NULLS sortiert zuletzt, wenn die Sortierreihenfolge ist. `DESC`

1. Wenn `NULLS FIRST` angegeben, werden NULL-Werte unabhängig von der Sortierreihenfolge zuerst zurückgegeben.

2. Wenn `NULLS LAST` angegeben, werden NULL-Werte unabhängig von der Sortierreihenfolge zuletzt zurückgegeben.

Syntax: `[ NULLS { FIRST | LAST } ]`

Beispiele

```
CREATE TABLE person (zip_code INT, name STRING, age INT);
INSERT INTO person VALUES
(94588, 'Shirley Rodriguez', 50),
(94588, 'Juan Li', 18),
(94588, 'Anil K', 27),
(94588, 'John D', NULL),
(94511, 'David K', 42),
(94511, 'Aryan B.', 18),
(94511, 'Lalit B.', NULL);
-- Sort rows by `name` within each partition in ascending manner
SELECT name, age, zip_code FROM person SORT BY name;
+------------------+----+--------+
|              name| age|zip_code|
+------------------+----+--------+
|            Anil K|  27|   94588|
|           Juan Li|  18|   94588|
|            John D|null|   94588|
| Shirley Rodriguez|  50|   94588|
|          Aryan B.|  18|   94511|
|           David K|  42|   94511|
|          Lalit B.|null|   94511|
+------------------+----+--------+
-- Sort rows within each partition using column position.
SELECT name, age, zip_code FROM person SORT BY 1;
+----------------+----+----------+
|              name| age|zip_code|
+------------------+----+--------+
|            Anil K|  27|   94588|
```

```
|           Juan Li|  18|   94588|
|            John D|null|   94588|
| Shirley Rodriguez|  50|   94588|
|          Aryan B.|  18|   94511|
|           David K|  42|   94511|
|          Lalit B.|null|   94511|
+------------------+----+--------+

-- Sort rows within partition in ascending manner keeping null values to be last.
SELECT age, name, zip_code FROM person SORT BY age NULLS LAST;
+----+------------------+--------+
| age|              name|zip_code|
+----+------------------+--------+
|  18|           Juan Li|   94588|
|  27|            Anil K|   94588|
|  50| Shirley Rodriguez|   94588|
|null|            John D|   94588|
|  18|          Aryan B.|   94511|
|  42|           David K|   94511|
|null|          Lalit B.|   94511|
+--------------+--------+--------+

-- Sort rows by age within each partition in descending manner, which defaults to NULL
 LAST.
SELECT age, name, zip_code FROM person SORT BY age DESC;
+----+------------------+--------+
| age|              name|zip_code|
+----+------------------+--------+
|  50|          Shirley Rodriguez|   94588|
|  27|            Anil K|   94588|
|  18|           Juan Li|   94588|
|null|            John D|   94588|
|  42|           David K|   94511|
|  18|          Aryan B.|   94511|
|null|          Lalit B.|   94511|
+----+------------------+--------+

-- Sort rows by age within each partition in descending manner keeping null values to
 be first.
SELECT age, name, zip_code FROM person SORT BY age DESC NULLS FIRST;
+----+------------------+--------+
| age|              name|zip_code|
+----+------------------+--------+
|null|            John D|   94588|
```

```
|  50| Shirley Rodriguez|   94588|
|  27|            Anil K|   94588|
|  18|           Juan Li|   94588|
|null|          Lalit B.|   94511|
|  42|           David K|   94511|
|  18|          Aryan B.|   94511|
+--------------+--------+--------+

-- Sort rows within each partition based on more than one column with each column
 having
-- different sort direction.
SELECT name, age, zip_code FROM person
SORT BY name ASC, age DESC;
+------------------+----+--------+
|              name| age|zip_code|
+------------------+----+--------+
|            Anil K|  27|   94588|
|           Juan Li|  18|   94588|
|            John D|null|   94588|
| Shirley Rodriguez|  50|   94588|
|          Aryan B.|  18|   94511|
|           David K|  42|   94511|
|          Lalit B.|null|   94511|
+------------------+----+--------+
```

UNPIVOT

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen SQL-Befehl unterstützen, finden Sie unterthe section called “Unterstützte SQL-Befehle”.

Die `UNPIVOT` Klausel wandelt mehrere Spalten in mehrere Zeilen um, die in der Klausel verwendet werden. `SELECT` Die `UNPIVOT` Klausel kann nach dem Tabellennamen oder der Unterabfrage angegeben werden.

Syntax

```
UNPIVOT [ { INCLUDE | EXCLUDE } NULLS ] (
    { single_value_column_unpivot | multi_value_column_unpivot }
) [[AS] alias]
```

```
single_value_column_unpivot:
    values_column
    FOR name_column
    IN (unpivot_column [[AS] alias] [, ...])

multi_value_column_unpivot:
    (values_column [, ...])
    FOR name_column
    IN ((unpivot_column [, ...]) [[AS] alias] [, ...])
```

Parameter

- unpivot_column

  Enthält Spalten in der FROM Klausel, die die Spalten angibt, deren Pivotierung aufgehoben werden soll.

- name_column

  Der Name der Spalte, die die Namen der Spalten ohne Pivotierung enthält.

- values_column

  Der Name der Spalte, die die Werte der Spalten ohne Pivotierung enthält.

Beispiele

```
CREATE TABLE sales_quarterly (year INT, q1 INT, q2 INT, q3 INT, q4 INT);
INSERT INTO sales_quarterly VALUES
(2020, null, 1000, 2000, 2500),
(2021, 2250, 3200, 4200, 5900),
(2022, 4200, 3100, null, null);
-- column names are used as unpivot columns
SELECT * FROM sales_quarterly
UNPIVOT (
sales FOR quarter IN (q1, q2, q3, q4)
);
+------+---------+-------+
| year | quarter | sales |
+------+---------+-------+
| 2020 | q2      | 1000  |
| 2020 | q3      | 2000  |
```

```
| 2020 | q4      | 2500  |
| 2021 | q1      | 2250  |
| 2021 | q2      | 3200  |
| 2021 | q3      | 4200  |
| 2021 | q4      | 5900  |
| 2022 | q1      | 4200  |
| 2022 | q2      | 3100  |
+------+---------+-------+
-- NULL values are excluded by default, they can be included
-- unpivot columns can be alias
-- unpivot result can be referenced via its alias
SELECT up.* FROM sales_quarterly
UNPIVOT INCLUDE NULLS (
sales FOR quarter IN (q1 AS Q1, q2 AS Q2, q3 AS Q3, q4 AS Q4)
) AS up;
+------+---------+-------+
| year | quarter | sales |
+------+---------+-------+
| 2020 | Q1      | NULL  |
| 2020 | Q2      | 1000  |
| 2020 | Q3      | 2000  |
| 2020 | Q4      | 2500  |
| 2021 | Q1      | 2250  |
| 2021 | Q2      | 3200  |
| 2021 | Q3      | 4200  |
| 2021 | Q4      | 5900  |
| 2022 | Q1      | 4200  |
| 2022 | Q2      | 3100  |
| 2022 | Q3      | NULL  |
| 2022 | Q4      | NULL  |
+------+---------+-------+
-- multiple value columns can be unpivoted per row
SELECT * FROM sales_quarterly
UNPIVOT EXCLUDE NULLS (
(first_quarter, second_quarter)
FOR half_of_the_year IN (
(q1, q2) AS H1,
(q3, q4) AS H2
)
);
+------+------------------+---------------+----------------+
|  id  | half_of_the_year | first_quarter | second_quarter |
+------+------------------+---------------+----------------+
| 2020 | H1               | NULL          | 1000           |
```

```
| 2020 | H2                | 2000          | 2500           |
| 2021 | H1                | 2250          | 3200           |
| 2021 | H2                | 4200          | 5900           |
| 2022 | H1                | 4200          | 3100           |
+------+-------------------+---------------+----------------+
```

Unterstützte PPL-Befehle

Die folgenden Tabellen zeigen, welche PPL-Befehle OpenSearch Dashboards für die Abfrage von CloudWatch Logs, Amazon S3 oder Security Lake unterstützt und welche Befehle CloudWatch Logs Insights unterstützt. CloudWatch Logs Insights verwendet bei der Abfrage von Logs dieselbe PPL-Syntax wie OpenSearch Dashboards, und in den Tabellen werden beide als CloudWatch Logs bezeichnet. CloudWatch

> **Note**
>
> Wenn Sie Daten außerhalb von OpenSearch Service analysieren, werden Befehle möglicherweise anders ausgeführt als bei Indizes. OpenSearch

Themen

- Befehle
- Funktionen
- Zusätzliche Informationen für CloudWatch Logs Insights-Benutzer, die OpenSearch PPL verwenden

Befehle

PPL-Befehl	Beschreibung	CloudWatch Logs	Amazon S3	Security Lake	-Beispielbefehl
the section called “fields”	Zeigt eine Reihe von Feldern an, die projiziert werden müssen.	U zt	U zt	U zt	`fields field1, field2`

PPL-Befehl	Beschreibung	CloudWatch Logs	Amazon S3	Security Lake	-Beispielbefehl
the section called “where”	Filtert die Daten auf der Grundlage der von Ihnen angegebenen Bedingungen.	U zt	U zt	U zt	`where field1="success" | where field2 != "i-023fe0a90929d8822" | fields field3, col4, col5, col6 | head 1000`
the section called “stats”	Führt Aggregationen und Berechnungen durch.	U zt	U zt	U zt	`stats count(), count(`field1`), min(`field1`), max(`field1`), avg(`field1`) by field2 | head 1000`

PPL-Befehl	Beschreibung	CloudWatch Logs	Amazon S3	Security Lake	-Beispielbefehl
the section called “parse”	Extrahiert ein Muster mit regulären Ausdrücken (Regex) aus einer Zeichenfolge und zeigt das extrahierte Muster an. Das extrahierte Muster kann weiter verwendet werden, um neue Felder zu erstellen oder Daten zu filtern.	U zt	U zt	U zt	`parse `field1` ".*/(?<field2>[^/]+$)" | where field2 = "requestId" | fields field2, `field2` | head 1000`

PPL-Befehl	Beschreibung	CloudWatch Logs	Amazon S3	Security Lake	-Beispielbefehl
the section called “Muster”	Extrahiert Protokollmuster aus einem Textfeld und hängt die Ergebnisse an das Suchergebnis an. Durch die Gruppierung von Protokollen nach ihren Mustern ist es einfacher, Statistiken aus großen Mengen von Protokolldaten zur Analyse und Fehlerbehebung zu aggregieren.	W nicht unterstützt	U zt	U zt	`patterns new_field='no_numbers' pattern='[0-9]' message | fields message, no_numbers`

PPL-Befehl	Beschreibung	CloudWatch Logs	Amazon S3	Security Lake	-Beispielbefehl
the section called “sort”	Sortiert die angezeigten Ergebnisse nach einem Feldnamen . Verwenden Sie sort - FieldName, um in absteigender Reihenfolge zu sortieren.	U zt	U zt	U zt	stats count(), count(`field1`), min(`field1`) as field1Alias, max(`field1`), avg(`field1`) by field2 | sort - field1Alias | head 1000

PPL-Befehl	Beschreibung	CloudWatch Logs	Amazon S3	Security Lake	-Beispielbefehl
the section called “eval”	Ändert oder verarbeitet den Wert eines Felds und speichert ihn in einem anderen Feld. Dies ist nützlich, um eine Spalte mathematisch zu modifizieren, Zeichenkettenfunktionen auf eine Spalte anzuwenden oder Datumsfunktionen auf eine Spalte anzuwenden.	U zt	U zt	U zt	`eval field2 = `field1` * 2 | fields field1, field2 | head 20`
the section called “umbenennen”	Benennt ein oder mehrere Felder im Suchergebnis um.	U zt	U zt	U zt	`rename field2 as field1 | fields field1`
the section called “head”	Beschränkt die angezeigten Abfrageergebnisse auf die ersten N Zeilen.	U zt	U zt	U zt	`fields `@message` | head 20`

PPL-Befehl	Beschreibung	CloudWatch Logs	Amazon S3	Security Lake	-Beispielbefehl
the section called “grok”	Analysiert ein Textfeld mit einem Grok-Muster, das auf einem regulären Ausdruck basiert, und hängt die Ergebnisse an das Suchergebnis an.	U zt	U zt	U zt	`grok email '.+@%{HOSTNAME:host}' | fields email`
the section called “top”	Findet die häufigsten Werte für ein Feld.	U zt	U zt	U zt	`top 2 Field1 by Field2`
the section called “dedup”	Entfernt doppelte Einträge auf der Grundlage der von Ihnen angegebenen Felder.	U zt	U zt	U zt	`dedup field1 | fields field1, field2, field3`
the section called “join”	Verbindet zwei Datensätze miteinander.	U zt	U zt	U zt	`source=customer | join ON c_custkey = o_custkey orders | head 10`

PPL-Befehl	Beschreibung	CloudWatch Logs	Amazon S3	Security Lake	-Beispielbefehl
the section called “Nachschlagen”	Bereichert Ihre Suchdaten durch Hinzufügen oder Ersetzen von Daten aus einem Nachschlageindex (Dimensionstabelle). Sie können Felder eines Index um Werte aus einer Dimensionstabelle erweitern und Werte anhängen oder ersetzen, wenn die Suchbedingung erfüllt ist	W nicht unterstützt	U zt	U zt	`where orderType = 'Cancelled' | lookup account_list, mkt_id AS mkt_code replace amount, account_name as name | stats count(mkt_code), avg(amount) by name`

PPL-Befehl	Beschreibung	CloudWatch Logs	Amazon S3	Security Lake	-Beispielbefehl
the section called “subquery”	Führt komplexe, verschachtelte Abfragen innerhalb Ihrer PPL-Anweisungen (Piped Processing Language) durch.	U zt	U zt	U zt	`where id in [ subquery source=users | where user in [ subquery source=actions | where action="login" | fields user ] | fields uid ]`
the section called “selten”	Findet die seltensten Werte aller Felder in der Feldliste.	U zt	U zt	U zt	`rare Field1 by Field2`
the section called “Trendlinie”	Berechnet die gleitenden Durchschnitte von Feldern.	U zt	U zt	U zt	`trendline sma(2, field1) as field1Alias`

PPL-Befehl	Beschreibung	CloudWatch Logs	Amazon S3	Security Lake	-Beispielbefehl
the section called “eventstats”	Reichert Ihre Eventdaten mit berechneten zusammenfassenden Statistiken an. Es analysiert bestimmte Felder innerhalb Ihrer Ereignisse, berechnet verschiedene statistische Kennzahlen und fügt diese Ergebnisse dann als neue Felder an jedes ursprüngliche Ereignis an.	U zt (außer) `count()`	U zt	U zt	`eventstats sum(field1) by field2`
the section called “flatten”	Macht ein Feld flach. Das Feld muss diesen Typ haben: `struct<?,?> or array<struct<?,?>>`	U zt	U zt	U zt	`source=table | flatten field1`

PPL-Befehl	Beschreibung	CloudWatch Logs	Amazon S3	Security Lake	-Beispielbefehl
the section called “Zusammenfassung des Feldes”	Berechnet grundlegende Statistiken für jedes Feld (Anzahl, eindeutige Anzahl, Min., Max, Durchschnitt, Standardwert und Mittelwert).	U zt (ein Feld pro Abfrage)	U zt	U zt	`where field1 != 200 | fieldsummary includefields=field1 nulls=true`
the section called “fillnull”	Füllt Nullfelder mit dem von Ihnen angegebenen Wert. Es kann in einem oder mehreren Feldern verwendet werden.	U zt	U zt	U zt	`fields field1 | eval field2=field1 | fillnull value=0 field1`
the section called “Erweitern”	Zerlegt ein Feld, das mehrere Werte enthält, in separate Zeilen und erstellt für jeden Wert im angegebenen Feld eine neue Zeile.	U zt	U zt	U zt	`expand employee | stats max(salary) as max by state, company`

PPL-Befehl	Beschreibung	CloudWatch Logs	Amazon S3	Security Lake	-Beispielbefehl
the section called “Beschreiben”	Ruft detaillierte Informationen zur Struktur und zu den Metadaten von Tabellen, Schemas und Katalogen ab	W nicht unterstützt	U zt	U zt	`describe schema.table`

Funktionen

PPL-Funktion	Beschreibung	CloudWatch Logs	Amazon S3	Security Lake	-Beispielbefehl
the section called “String” (`CONCAT`, `CONCAT_WS` , `LENGTH`, `LOWER`, `LTRIM`, `POSITION`, `REVERSE`, `RIGHT`, `RTRIM`, `SUBSTRING` , `TRIM`, `UPPER`)	Integrierte Funktionen in PPL, die Zeichenketten- und Textdaten in PPL-Abfragen manipulieren und transformieren können. Zum Beispiel das Konvertieren von	U zt	U zt	U zt	`eval col1Len = LENGTH(col1) | fields col1Len`

PPL-Funktion	Beschreibung	CloudWatch Logs	Amazon S3	Security Lake	-Beispielbefehl
	Groß- und Kleinschreibung, das Kombinieren von Zeichenketten, das Extrahieren von Teilen und das Bereinigen von Text.				

PPL-Funktion	Beschreibung	CloudWatch Logs	Amazon S3	Security Lake	-Beispielbefehl
the section called “Datum und Uhrzeit” (DAY, DAYOFMONTH , DAY_OF_MONTH ,DAYOFWEEK , DAY_OF_WEEK , DAYOFYEAR , DAY_OF_YEAR , DAYNAME, FROM_UNIXTIME , HOUR, HOUR_OF_DAY , LAST_DAY, LOCALTIMESTAMP , LOCALTIME , MAKE_DATE , MINUTE, MINUTE_OF_HOUR , MONTH, MONTHNAME , MONTH_OF_YEAR , NOW, QUARTER, SECOND, SECOND_OF_MINUTE , SUBDATE, SYSDATE, TIMESTAMP , UNIX_TIMESTAMP , WEEK, WEEKDAY, WEEK_OF_Y	Integrierte Funktionen für die Verarbeitung und Transformation von Datums- und Zeitstempeldaten in PPL-Abfragen. Zum Beispiel date_add, date_format, datediff und current_date.	U zt	U zt	U zt	`eval newDate = ADDDATE(DATE('2020-08-26'), 1) | fields newDate`

PPL-Funktion	Beschreibung	CloudWatch Logs	Amazon S3	Security Lake	-Beispielbefehl
EAR , DATE_ADD, DATE_SUB, TIMESTAMP ADD , TIMESTAMP DIFF , UTC_TIMESTAMP , CURRENT_TIMEZONE)					
the section called “Bedingung” (EXISTS, IF, IFNULL, ISNOTNULL , ISNULL, NULLIF)	Integrierte Funktionen, die Berechnungen für mehrere Zeilen durchführen, um einen einzigen zusammengefassten Wert zu erzeugen. Zum Beispiel Summe, Anzahl, Durchschnitt, Maximum und Min.	U zt	U zt	U zt	`eval field2 = isnull(col1) | fields field2, col1, field3`

PPL-Funktion	Beschreibung	CloudWatch Logs	Amazon S3	Security Lake	-Beispielbefehl
the section called “Math-Knoten” (ABS, ACOS, ASIN, ATAN, ATAN2, CEIL, CEILING, CONV, COS, COT, CRC32, DEGREES, E, EXP, FLOOR, LN, LOG, LOG2, LOG10, MOD, PI. POW, POWER, RADIANS, RAND, ROUND, SIGN, SIN, SQRT, CBRT)	Integrierte Funktionen zur Durchführung mathematischer Berechnungen und Transformationen in PPL-Abfragen. Zum Beispiel: abs (absoluter Wert), round (rundet Zahlen), sqrt (Quadratwurzel), pow (Potenzberechnung) und ceil (rundet auf die nächste Ganzzahl auf).	U zt	U zt	U zt	`eval field2 = ACOS(col1) | fields col1`

PPL-Funktion	Beschreibung	CloudWatch Logs	Amazon S3	Security Lake	-Beispielbefehl
the section called “Ausdrücke” (Arithmetische Operatoren (+,*)-, Prädikatoperatoren (,) >. < IN)	Integrierte Funktionen für Ausdrücke, insbesondere Wertausdrücke, geben einen Skalarwert zurück. Ausdrücke haben unterschiedliche Typen und Formen.	U zt	U zt	U zt	`where age > (25 + 5) | fields age`
the section called “IP-Adresse” (CIDRMATCH)	Integrierte Funktionen für den Umgang mit IP-Adressen wie CIDR.	U zt	U zt	U zt	`where cidrmatch (ip, '******** ***/24') | fields ip`

PPL-Funktion	Beschreibung	CloudWatch Logs	Amazon S3	Security Lake	-Beispielbefehl
the section called “JSON” (ARRAY_LENGTH , ARRAY_LENGTH , JSON, JSON_ARRAY , JSON_EXTRACT , JSON_KEYS , JSON_OBJECT , JSON_VALID , TO_JSON_STRING)	Integrierte Funktionen für den Umgang mit JSON, einschließlich Arrays, Extrahieren und Validieren.	U zt	U zt	U zt	`eval `json_extract('{"a":"b"}', '$.a')` = json_extract('{"a":"b"}', '$a')`
the section called “Lambda” (EXISTS, FILTER, REDUCE, TRANSFORM)	Integrierte Funktionen für den Umgang mit JSON, einschließlich Arrays, Extrahieren und Validieren.	W nicht unterstützt	U zt	U zt	`eval array = json_array(1, -1, 2), result = filter(array, x -> x > 0) | fields result`

PPL-Funktion	Beschreibung	CloudWatch Logs	Amazon S3	Security Lake	-Beispielbefehl
the section called “Kryptografisch” (MD5, SHA1, SHA2)	Integrierte Funktionen, mit denen Sie eindeutige Fingerabdrücke von Daten generieren können, die zur Überprüfung, zum Vergleich oder als Teil komplexerer Sicherheitsprotokolle verwendet werden können.	U zt	U zt	U zt	`eval `MD5('hello')` = MD5('hello') | fields `MD5('hello')``

Zusätzliche Informationen für CloudWatch Logs Insights-Benutzer, die OpenSearch PPL verwenden

CloudWatch Logs Insights unterstützt zwar die meisten OpenSearch PPL-Befehle und -Funktionen, einige Befehle und Funktionen werden jedoch derzeit nicht unterstützt. Beispielsweise unterstützt es derzeit keine Lookup-Befehle in PPL. Seit dem 2. Juni 2025 unterstützt CloudWatch Logs Insights jetzt die Funktionen JOIN, Unterabfragen, Flatten, Fillnull, Expand, Cidrmatch und JSON in PPL.

Eine vollständige Liste der unterstützten Abfragebefehle und -funktionen finden Sie in den Amazon CloudWatch Logs-Spalten in den obigen Tabellen.

Beispielabfragen und Kontingente

Das Folgende gilt sowohl für CloudWatch Logs Insights-Benutzer als auch für OpenSearch Benutzer, die CloudWatch Daten abfragen.

Informationen zu den Beschränkungen, die bei der Abfrage von CloudWatch Logs from OpenSearch Service gelten, finden Sie unter CloudWatch Log-Kontingente im Amazon CloudWatch Logs-Benutzerhandbuch. Die Beschränkungen betreffen die Anzahl der CloudWatch Protokollgruppen, die Sie abfragen können, die maximale Anzahl gleichzeitiger Abfragen, die Sie ausführen können, die maximale Ausführungszeit von Abfragen und die maximale Anzahl von Zeilen, die in Ergebnissen zurückgegeben werden. Die Grenzwerte sind dieselben, unabhängig davon, in welcher Sprache Sie CloudWatch Logs abfragen (nämlich OpenSearch PPL, SQL und Logs Insights QL).

PPL-Befehle

Themen

- Kommentar
- Korrelationsbefehl
- Befehl dedup
- Befehl beschreiben
- Befehl eval
- Befehl eventstats
- Befehl expandieren
- Befehl erläutern
- Befehl fillnull
- Befehl „Felder“
- Befehl flatten
- Befehl grok
- Befehl head
- Befehl join
- Lookup-Befehl
- Befehl parse

- Befehl „Muster“
- seltener Befehl
- Befehl umbenennen
- Suchbefehl
- Befehl sort
- Befehl stats
- Befehl subquery
- oberster Befehl
- Befehl trendline
- wo (Befehl)
- Zusammenfassung der Felder
- Befehl expandieren
- PPL-Funktionen

Kommentar

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen PPL-Befehl unterstützen, finden Sie unter. the section called “Befehle”

PPL unterstützt sowohl Zeilenkommentare als auch Blockkommentare. Das System wertet den Kommentartext nicht aus.

Zeilenkommentare

Zeilenkommentare beginnen mit zwei Schrägstrichen//und enden mit einer neuen Zeile.

Beispiel:

```
os> source=accounts | top gender // finds most common gender of all the accounts
fetched rows / total rows = 2/2
+----------+
| gender   |
|----------|
```

```
| M        |
| F        |
+----------+
```

Kommentare blockieren

Blockkommentare beginnen mit einem Schrägstrich, gefolgt von einem Sternchen\ *, und enden mit einem Sternchen, gefolgt von einem Schrägstrich */.

Beispiel:

```
os> source=accounts | dedup 2 gender /* dedup the document with gender field keep 2
 duplication */ | fields account_number, gender
fetched rows / total rows = 3/3
+------------------+----------+
| account_number   | gender   |
|------------------+----------|
| 1                | M        |
| 6                | M        |
| 13               | F        |
+------------------+----------+
```

Korrelationsbefehl

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen PPL-Befehl unterstützen, finden Sie unter. the section called “Befehle”

Sie können verschiedene Datenquellen anhand gemeinsamer Dimensionen und Zeitrahmen korrelieren.

Diese Korrelation ist entscheidend, wenn Sie es mit großen Datenmengen aus verschiedenen Branchen zu tun haben, die dieselben Zeiträume haben, aber nicht formal synchronisiert sind.

Indem Sie diese verschiedenen Datenquellen auf der Grundlage von Zeitrahmen und ähnlichen Dimensionen korrelieren, können Sie Ihre Daten anreichern und wertvolle Erkenntnisse gewinnen.

Beispiel

Der Bereich Observability besteht aus drei unterschiedlichen Datenquellen:

- Logs (Protokolle)
- Metriken
- Ablaufverfolgungen

Diese Datenquellen haben möglicherweise gemeinsame Dimensionen. Um von einer Datenquelle zur anderen zu wechseln, müssen Sie sie korrekt korrelieren. Mithilfe semantischer Namenskonventionen können Sie gemeinsam genutzte Elemente in Logs, Traces und Metriken identifizieren.

Beispiel:

```
{
  "@timestamp": "2018-07-02T22:23:00.186Z",
  "aws": {
    "elb": {
      "backend": {
        "http": {
          "response": {
            "status_code": 500
          }
        },
        "ip": "********",
        "port": "80"
      },
      ...
     "target_port": [
        "10.0.0.1:80"
      ],
      "target_status_code": [
        "500"
      ],
      "traceId": "Root=1-58337262-36d228ad5d99923122bbe354",
      "type": "http"
    }
  },
  "cloud": {
    "provider": "aws"
  },
  "http": {
    "request": {
    ...
  },
  "communication": {
```

```
    "source": {
      "address": "**************",
      "ip": "**************",
      "port": 2817
    }
  },
  "traceId": "Root=1-58337262-36d228ad5d99923122bbe354"
}
```

Dieses Beispiel zeigt ein AWS ELB-Protokoll, das von einem Dienst empfangen wird, der sich auf befindet. AWS Es zeigt eine Backend-HTTP-Antwort mit dem Statuscode 500, was auf einen Fehler hinweist. Dies könnte eine Warnung auslösen oder Teil Ihres regulären Überwachungsprozesses sein. Ihr nächster Schritt besteht darin, relevante Daten zu diesem Ereignis für eine gründliche Untersuchung zu sammeln.

Auch wenn Sie versucht sein könnten, alle Daten im Zusammenhang mit dem Zeitrahmen abzufragen, kann dieser Ansatz überwältigend sein. Sie könnten am Ende zu viele Informationen haben und mehr Zeit damit verbringen, irrelevante Daten herauszufiltern, als die Ursache zu ermitteln.

Stattdessen können Sie einen gezielteren Ansatz verfolgen, indem Sie Daten aus verschiedenen Quellen korrelieren. Sie können diese Dimensionen für die Korrelation verwenden:

- IP - `"ip": "10.0.0.1" | "ip": "**************"`
- Anschluss - `"port": 2817 | "target_port": "10.0.0.1:80"`

Vorausgesetzt, Sie haben Zugriff auf zusätzliche Traces und Metrikindizes und sind mit Ihrer Schemastruktur vertraut, können Sie eine genauere Korrelationsabfrage erstellen.

Hier ist ein Beispiel für ein Trace-Indexdokument, das HTTP-Informationen enthält, die Sie möglicherweise korrelieren möchten:

```
{
  "traceId": "c1d985bd02e1dbb85b444011f19a1ecc",
  "spanId": "55a698828fe06a42",
  "traceState": [],
  "parentSpanId": "",
  "name": "mysql",
  "kind": "CLIENT",
  "@timestamp": "2021-11-13T20:20:39+00:00",
  "events": [
```

```
    {
      "@timestamp": "2021-03-25T17:21:03+00:00",
       ...
    }
  ],
  "links": [
    {
      "traceId": "c1d985bd02e1dbb85b444011f19a1ecc",
      "spanId": "55a698828fe06a42w2",
      },
      "droppedAttributesCount": 0
    }
  ],
  "resource": {
    "service@name": "database",
    "telemetry@sdk@name": "opentelemetry",
    "host@hostname": "ip-172-31-10-8.us-west-2.compute.internal"
  },
  "status": {
    ...
  },
  "attributes": {
    "http": {
      "user_agent": {
        "original": "Mozilla/5.0"
      },
      "network": {
         ...
        }
      },
      "request": {
         ...
        }
      },
      "response": {
        "status_code": "200",
        "body": {
          "size": 500
        }
      },
      "client": {
        "server": {
          "socket": {
            "address": "***********",
```

```
            "domain": "example.com",
            "port": 80
          },
          "address": "***********",
          "port": 80
        },
        "resend_count": 0,
        "url": {
          "full": "http://example.com"
        }
      },
      "server": {
        "route": "/index",
        "address": "***********",
        "port": 8080,
        "socket": {
         ...
        },
        "client": {
         ...
         }
        },
        "url": {
         ...
        }
      }
    }
  }
}
```

Bei diesem Ansatz können Sie die `traceId` und die HTTPs sehen client/server `ip`, die mit den Elb-Protokollen korreliert werden können, um das Verhalten und den Zustand des Systems besser zu verstehen.

Neuer Befehl zur Korrelationsabfrage

Hier ist der neue Befehl, der diese Art von Untersuchung ermöglichen würde:

```
source alb_logs, traces | where alb_logs.ip="10.0.0.1" AND
 alb_logs.cloud.provider="aws"|
correlate exact fields(traceId, ip) scope(@timestamp, 1D) mapping(alb_logs.ip =
 traces.attributes.http.server.address, alb_logs.traceId = traces.traceId )
```

Jeder Teil des Befehls macht Folgendes:

1. `source alb_logs, traces`- Dadurch werden die Datenquellen ausgewählt, die Sie korrelieren möchten.
2. `where ip="10.0.0.1" AND cloud.provider="aws"`- Dadurch wird der Umfang Ihrer Suche eingegrenzt.
3. `correlate exact fields(traceId, ip)`- Dadurch wird das System angewiesen, Daten auf der Grundlage exakter Übereinstimmungen der folgenden Felder zu korrelieren:
   - Das `ip` Feld hat eine explizite Filterbedingung, sodass es bei der Korrelation für alle Datenquellen verwendet wird.
   - Das `traceId` Feld hat keinen expliziten Filter, sodass es in allen Datenquellen mit denselben TraceIDs übereinstimmt.

Die Feldnamen geben die logische Bedeutung der Funktion innerhalb des Korrelationsbefehls an. Die tatsächliche Verbindungsbedingung hängt von der von Ihnen angegebenen Zuordnungsanweisung ab.

Der Begriff `exact` bedeutet, dass bei den Korrelationsanweisungen alle Felder übereinstimmen müssen, um die Abfrageanweisung zu erfüllen.

Der Begriff `approximate` wird versuchen, im besten Fall eine Übereinstimmung herzustellen, und Zeilen mit teilweisen Übereinstimmungen werden nicht zurückgewiesen.

Adressierung unterschiedlicher Feldzuordnungen

In Fällen, in denen dasselbe logische Feld (z. B.`ip`) in Ihren Datenquellen unterschiedliche Namen hat, müssen Sie die explizite Zuordnung von Pfadfeldern bereitstellen. Um dieses Problem zu lösen, können Sie Ihre Korrelationsbedingungen so erweitern, dass sie unterschiedlichen Feldnamen mit ähnlicher logischer Bedeutung entsprechen. So könnten Sie das tun:

```
alb_logs.ip = traces.attributes.http.server.address, alb_logs.traceId = traces.traceId
```

Für jedes Feld, das an der Korrelationsverknüpfung beteiligt ist, sollten Sie eine entsprechende Zuordnungsanweisung angeben, die alle Tabellen enthält, die mit diesem Korrelationsbefehl verknüpft werden sollen.

Beispiel

In diesem Beispiel gibt es zwei Quellen: `alb_logs, traces`

Es gibt 2 Felder: `traceId, ip`

Es gibt 2 Zuordnungsanweisungen: `alb_logs.ip = traces.attributes.http.server.address, alb_logs.traceId = traces.traceId`

Festlegung des Zeitrahmens für die Korrelation

Um die Arbeit der Ausführungs-Engine (Treiber) zu vereinfachen, können Sie die Scope-Anweisung hinzufügen. Dadurch wird die Verbindungsabfrage explizit auf den Zeitpunkt geleitet, zu dem sie für diese Suche gelten soll.

`scope(@timestamp, 1D)i`

In diesem Beispiel konzentriert sich der Suchbereich auf Tagesbasis, sodass Korrelationen, die am selben Tag auftreten, gruppiert werden. Dieser Scoping-Mechanismus vereinfacht und ermöglicht eine bessere Kontrolle der Ergebnisse und ermöglicht eine schrittweise Auflösung der Suche, die Ihren Anforderungen entspricht.

Unterstützung von Treibern

Der neue Korrelationsbefehl ist eigentlich ein „versteckter“ Join-Befehl. Daher unterstützen nur die folgenden PPL-Treiber diesen Befehl. In diesen Treibern wird der Korrelationsbefehl direkt in den entsprechenden logischen Catalyst Join-Plan übersetzt.

Beispiel

```
source alb_logs, traces, metrics | where ip="10.0.0.1" AND
cloud.provider="aws"| correlate exact on (ip, port) scope(@timestamp,
2018-07-02T22:23:00, 1 D)
```

Logischer Plan:

```
'Project [*]
+- 'Join Inner, ('ip && 'port)
   :- 'Filter (('ip === "10.0.0.1" & 'cloud.provider === "aws") &
 inTimeScope('@timestamp, "2018-07-02T22:23:00", "1 D"))
      +- 'UnresolvedRelation [alb_logs]
   +- 'Join Inner, ('ip & 'port)
      :- 'Filter (('ip === "10.0.0.1" & 'cloud.provider === "aws") &
 inTimeScope('@timestamp, "2018-07-02T22:23:00", "1 D"))
```

```
        +- 'UnresolvedRelation [traces]
     +- 'Filter (('ip === "10.0.0.1" & 'cloud.provider === "aws") &
inTimeScope('@timestamp, "2018-07-02T22:23:00", "1 D"))
        +- 'UnresolvedRelation [metrics]
```

Die Catalyst-Engine optimiert diese Abfrage entsprechend der effizientesten Join-Reihenfolge.

Befehl dedup

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen PPL-Befehl unterstützen, finden Sie unter. the section called “Befehle”

Verwenden Sie den `dedup` Befehl, um identische Dokumente basierend auf bestimmten Feldern aus Ihren Suchergebnissen zu entfernen.

Syntax

Verwenden Sie die folgende Syntax:

```
dedup [int] <field-list> [keepempty=<bool>] [consecutive=<bool>]
```

`int`

- Optional.
- Der `dedup` Befehl behält mehrere Ereignisse für jede Kombination bei, wenn Sie dies angeben<int>. Die Zahl für <int>muss größer als 0 sein. Wenn Sie keine Zahl angeben, wird nur das erste Ereignis beibehalten. Alle anderen Duplikate werden aus den Ergebnissen entfernt.
- Standard: 1

`keepempty`

- Optional.
- Falls wahr, werden Dokumente beibehalten, in denen ein Feld in der Feldliste einen NULL-Wert hat oder FEHLT.
- Standard: false

`consecutive`

- Optional.
- Wenn der Wert wahr ist, werden nur Ereignisse mit aufeinanderfolgenden doppelten Wertekombinationen entfernt.
- Standard: false

`field-list`

- Zwingend erforderlich.
- Eine durch Kommas getrennte Liste von Feldern. Es ist mindestens ein Feld erforderlich.

Beispiel 1: Deduplizierung nach einem Feld

Dieses Beispiel zeigt, wie Dokumente mithilfe des Felds „Geschlecht“ dedupliziert werden.

PPL-Abfrage:

```
os> source=accounts | dedup gender | fields account_number, gender;
fetched rows / total rows = 2/2
+------------------+----------+
| account_number   | gender   |
|------------------+----------|
| 1                | M        |
| 13               | F        |
+------------------+----------+
```

Beispiel 2: Behalte 2 doppelte Dokumente

Das Beispiel zeigt, wie Dokumente mit dem Feld Geschlecht dedupliziert werden, wobei zwei Duplikate beibehalten werden.

PPL-Abfrage:

```
os> source=accounts | dedup 2 gender | fields account_number, gender;
fetched rows / total rows = 3/3
+------------------+----------+
| account_number   | gender   |
|------------------+----------|
| 1                | M        |
```

```
| 6                | M        |
| 13               | F        |
+------------------+----------+
```

Beispiel 3: Behalten oder ignorieren Sie das leere Feld standardmäßig

Das Beispiel zeigt, wie das Dokument dedupliziert wird, indem das Nullwertfeld beibehalten wird.

PPL-Abfrage:

```
os> source=accounts | dedup email keepempty=true | fields account_number, email;
fetched rows / total rows = 4/4
+------------------+-----------------------+
| account_number   | email                 |
+------------------+-----------------------+
| 1                | john_doe@example.com  |
| 6                | jane_doe@example.com  |
| 13               | null                  |
| 18               | juan_li@example.com   |
+------------------+-----------------------+
```

Das Beispiel zeigt, wie das Dokument dedupliziert wird, indem das leere Wertfeld ignoriert wird.

PPL-Abfrage:

```
os> source=accounts | dedup email | fields account_number, email;
fetched rows / total rows = 3/3
+------------------+-----------------------+
| account_number   | email                 |
+------------------+-----------------------+
| 1                | john_doe@example.com  |
| 6                | jane_doe@example.com  |
| 18               | juan_li@example.com   |
+------------------+-----------------------+
```

Beispiel 4: Dedup in aufeinanderfolgenden Dokumenten

Das Beispiel zeigt, wie man in aufeinanderfolgenden Dokumenten dedupliziert.

PPL-Abfrage:

```
os> source=accounts | dedup gender consecutive=true | fields account_number, gender;
```

```
fetched rows / total rows = 3/3
+------------------+----------+
| account_number   | gender   |
+------------------+----------+
| 1                | M        |
| 13               | F        |
| 18               | M        |
+------------------+----------+
```

Weitere Beispiele

- `source = table | dedup a | fields a,b,c`
- `source = table | dedup a,b | fields a,b,c`
- `source = table | dedup a keepempty=true | fields a,b,c`
- `source = table | dedup a,b keepempty=true | fields a,b,c`
- `source = table | dedup 1 a | fields a,b,c`
- `source = table | dedup 1 a,b | fields a,b,c`
- `source = table | dedup 1 a keepempty=true | fields a,b,c`
- `source = table | dedup 1 a,b keepempty=true | fields a,b,c`
- `source = table | dedup 2 a | fields a,b,c`
- `source = table | dedup 2 a,b | fields a,b,c`
- `source = table | dedup 2 a keepempty=true | fields a,b,c`
- `source = table | dedup 2 a,b keepempty=true | fields a,b,c`
- `source = table | dedup 1 a consecutive=true| fields a,b,c`(Konsekutive Deduplizierung wird nicht unterstützt)

Einschränkung

- Für `| dedup 2 a, b keepempty=false`

```
DataFrameDropColumns('_row_number_)
+- Filter ('_row_number_ <= 2) // allowed duplication = 2
   +- Window [row_number() windowspecdefinition('a, 'b, 'a ASC NULLS FIRST, 'b ASC
 NULLS FIRST, specifiedwindowframe(RowFrame, unboundedpreceding$(), currentrow$()))
 AS _row_number_], ['a, 'b], ['a ASC NULLS FIRST, 'b ASC NULLS FIRST]
       +- Filter (isnotnull('a) AND isnotnull('b)) // keepempty=false
```

```
          +- Project
             +- UnresolvedRelation
```

- Für `| dedup 2 a, b keepempty=true`

```
Union
:- DataFrameDropColumns('_row_number_)
:  +- Filter ('_row_number_ <= 2)
:     +- Window [row_number() windowspecdefinition('a, 'b, 'a ASC NULLS FIRST, 'b ASC
 NULLS FIRST, specifiedwindowframe(RowFrame, unboundedpreceding$(), currentrow$()))
 AS _row_number_], ['a, 'b], ['a ASC NULLS FIRST, 'b ASC NULLS FIRST]
:        +- Filter (isnotnull('a) AND isnotnull('b))
:           +- Project
:              +- UnresolvedRelation
+- Filter (isnull('a) OR isnull('b))
   +- Project
      +- UnresolvedRelation
```

Befehl beschreiben

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen PPL-Befehl unterstützen, finden Sie unter. the section called “Befehle”

Verwenden Sie den `describe` Befehl, um detaillierte Informationen zur Struktur und zu den Metadaten von Tabellen, Schemas und Katalogen abzurufen. Im Folgenden finden Sie verschiedene Beispiele und Anwendungsfälle für den `describe` Befehl.

Describe

- `describe table`Dieser Befehl entspricht dem `DESCRIBE EXTENDED table` SQL-Befehl
- `describe schema.table`
- `describe schema.\`table\``
- `describe catalog.schema.table`
- `describe catalog.schema.\`table\``
- `describe \`catalog\`.\`schema\`.\`table\``

Befehl eval

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen PPL-Befehl unterstützen, finden Sie unter. the section called “Befehle”

Der `eval` Befehl wertet den Ausdruck aus und fügt das Ergebnis an das Suchergebnis an.

Syntax

Verwenden Sie die folgende Syntax:

```
eval <field>=<expression> ["," <field>=<expression> ]...
```

- `field`: Obligatorisch. Wenn der Feldname nicht existiert, wird ein neues Feld hinzugefügt. Wenn der Feldname bereits existiert, wird er überschrieben.
- `expression`: Obligatorisch. Jeder Ausdruck, der vom System unterstützt wird.

Beispiel 1: Erstellen Sie das neue Feld

Dieses Beispiel zeigt, wie Sie für jedes Dokument ein neues `doubleAge` Feld erstellen. Neu `doubleAge` ist das Bewertungsergebnis des Alters multipliziert mit 2.

PPL-Abfrage:

```
os> source=accounts | eval doubleAge = age * 2 | fields age, doubleAge ;
fetched rows / total rows = 4/4
+-------+-------------+
| age   | doubleAge   |
|-------+-------------|
| 32    | 64          |
| 36    | 72          |
| 28    | 56          |
| 33    | 66          |
+-------+-------------+
```

Beispiel 2: Überschreiben Sie das bestehende Feld

Dieses Beispiel zeigt, wie das bestehende Altersfeld mit Alter plus 1 überschrieben wird.

PPL-Abfrage:

```
os> source=accounts | eval age = age + 1 | fields age ;
fetched rows / total rows = 4/4
+-------+
| age   |
|-------|
| 33    |
| 37    |
| 29    |
| 34    |
+-------+
```

Beispiel 3: Erstellen Sie das neue Feld mit dem in Eval definierten Feld

Dieses Beispiel zeigt, wie ein neues `ddAge` Feld mit einem im Befehl eval definierten Feld erstellt wird. Das neue Feld `ddAge` ist das Auswertungsergebnis `doubleAge` multipliziert mit 2, wobei `doubleAge` es im Befehl eval definiert ist.

PPL-Abfrage:

```
os> source=accounts | eval doubleAge = age * 2, ddAge = doubleAge * 2 | fields age,
 doubleAge, ddAge ;
fetched rows / total rows = 4/4
+-------+-------------+---------+
| age   | doubleAge   | ddAge   |
|-------+-------------+---------|
| 32    | 64          | 128     |
| 36    | 72          | 144     |
| 28    | 56          | 112     |
| 33    | 66          | 132     |
+-------+-------------+---------+
```

Annahmen:`a`,`b`, `c` sind vorhandene Felder in `table`

Weitere Beispiele

- `source = table | eval f = 1 | fields a,b,c,f`
- `source = table | eval f = 1`(gibt A-, B-, C- und F-Felder aus)
- `source = table | eval n = now() | eval t = unix_timestamp(a) | fields n,t`

- `source = table | eval f = a | where f > 1 | sort f | fields a,b,c | head 5`
- `source = table | eval f = a * 2 | eval h = f * 2 | fields a,f,h`
- `source = table | eval f = a * 2, h = f * 2 | fields a,f,h`
- `source = table | eval f = a * 2, h = b | stats avg(f) by h`
- `source = table | eval f = ispresent(a)`
- `source = table | eval r = coalesce(a, b, c) | fields r`
- `source = table | eval e = isempty(a) | fields e`
- `source = table | eval e = isblank(a) | fields e`
- `source = table | eval f = case(a = 0, 'zero', a = 1, 'one', a = 2, 'two', a = 3, 'three', a = 4, 'four', a = 5, 'five', a = 6, 'six', a = 7, 'se7en', a = 8, 'eight', a = 9, 'nine')`
- `source = table | eval f = case(a = 0, 'zero', a = 1, 'one' else 'unknown')`
- `source = table | eval f = case(a = 0, 'zero', a = 1, 'one' else concat(a, ' is an incorrect binary digit'))`
- `source = table | eval f = a in ('foo', 'bar') | fields f`
- `source = table | eval f = a not in ('foo', 'bar') | fields f`

Bewertung mit Fallbeispiel:

```
source = table | eval e = eval status_category =
case(a >= 200 AND a < 300, 'Success',
a >= 300 AND a < 400, 'Redirection',
a >= 400 AND a < 500, 'Client Error',
a >= 500, 'Server Error'
else 'Unknown')
```

Eval mit einem anderen Fallbeispiel:

Annahmen:a,b, c sind existierende Felder in `table`

Weitere Beispiele

- `source = table | eval f = 1 | fields a,b,c,f`

- `source = table | eval f = 1`(gibt A-, B-, C- und F-Felder aus)
- `source = table | eval n = now() | eval t = unix_timestamp(a) | fields n,t`
- `source = table | eval f = a | where f > 1 | sort f | fields a,b,c | head 5`
- `source = table | eval f = a * 2 | eval h = f * 2 | fields a,f,h`
- `source = table | eval f = a * 2, h = f * 2 | fields a,f,h`
- `source = table | eval f = a * 2, h = b | stats avg(f) by h`
- `source = table | eval f = ispresent(a)`
- `source = table | eval r = coalesce(a, b, c) | fields r`
- `source = table | eval e = isempty(a) | fields e`
- `source = table | eval e = isblank(a) | fields e`
- `source = table | eval f = case(a = 0, 'zero', a = 1, 'one', a = 2, 'two', a = 3, 'three', a = 4, 'four', a = 5, 'five', a = 6, 'six', a = 7, 'se7en', a = 8, 'eight', a = 9, 'nine')`
- `source = table | eval f = case(a = 0, 'zero', a = 1, 'one' else 'unknown')`
- `source = table | eval f = case(a = 0, 'zero', a = 1, 'one' else concat(a, ' is an incorrect binary digit'))`
- `source = table | eval f = a in ('foo', 'bar') | fields f`
- `source = table | eval f = a not in ('foo', 'bar') | fields f`

Bewertung mit Fallbeispiel:

```
source = table | eval e = eval status_category =
case(a >= 200 AND a < 300, 'Success',
a >= 300 AND a < 400, 'Redirection',
a >= 400 AND a < 500, 'Client Error',
a >= 500, 'Server Error'
else 'Unknown')
```

Eval mit einem anderen Fallbeispiel:

```
source = table |  where ispresent(a) |
```

```
eval status_category =
 case(a >= 200 AND a < 300, 'Success',
  a >= 300 AND a < 400, 'Redirection',
  a >= 400 AND a < 500, 'Client Error',
  a >= 500, 'Server Error'
  else 'Incorrect HTTP status code'
 )
 | stats count() by status_category
```

Einschränkungen

- Das Überschreiben vorhandener Felder wird nicht unterstützt. Abfragen, die dies versuchen, lösen Ausnahmen mit der Meldung „Die Referenz 'a' ist mehrdeutig“ aus.

```
- `source = table | eval a = 10 | fields a,b,c`
- `source = table | eval a = a * 2 | stats avg(a)`
- `source = table | eval a = abs(a) | where a > 0`
- `source = table | eval a = signum(a) | where a < 0`
```

Befehl eventstats

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen PPL-Befehl unterstützen, finden Sie unter. the section called “Befehle”

Verwenden Sie den `eventstats` Befehl, um Ihre Ereignisdaten mit berechneten Übersichtsstatistiken anzureichern. Dabei werden bestimmte Felder innerhalb Ihrer Ereignisse analysiert, verschiedene statistische Kennzahlen berechnet und diese Ergebnisse dann als neue Felder an jedes ursprüngliche Ereignis angehängt.

Die wichtigsten Aspekte von Eventstats

1. Es führt Berechnungen für den gesamten Ergebnissatz oder innerhalb definierter Gruppen durch.
2. Die ursprünglichen Ereignisse bleiben erhalten, und es werden neue Felder hinzugefügt, um die statistischen Ergebnisse zu enthalten.
3. Der Befehl ist besonders nützlich für vergleichende Analysen, die Identifizierung von Ausreißern oder die Bereitstellung von zusätzlichem Kontext für einzelne Ereignisse.

Unterschied zwischen Stats und Eventstats

Die `eventstats` Befehle `stats` und werden beide zur Berechnung von Statistiken verwendet, weisen jedoch einige wesentliche Unterschiede in ihrer Funktionsweise und ihrem Ergebnis auf.

Ausgabeformat

- `stats`: Erzeugt eine Übersichtstabelle, die nur die berechneten Statistiken enthält.
- `eventstats`: Fügt die berechneten Statistiken als neue Felder zu den vorhandenen Ereignissen hinzu, wobei die Originaldaten erhalten bleiben.

Aufbewahrung von Ereignissen

- `stats`: Reduziert die Ergebnismenge auf die statistische Zusammenfassung, wobei einzelne Ereignisse verworfen werden.
- `eventstats`: Behält alle ursprünglichen Ereignisse bei und fügt neue Felder mit den berechneten Statistiken hinzu.

Anwendungsfälle

- `stats`: Am besten für die Erstellung von Übersichtsberichten oder Dashboards geeignet. Wird oft als letzter Befehl verwendet, um Ergebnisse zusammenzufassen.
- `eventstats`: Nützlich, wenn Sie Ereignisse zur weiteren Analyse oder Filterung mit statistischem Kontext anreichern müssen. Kann während der Suche verwendet werden, um Statistiken hinzuzufügen, die in nachfolgenden Befehlen verwendet werden können.

Syntax

Verwenden Sie die folgende Syntax:

```
eventstats <aggregation>... [by-clause]
```

Aggregation

- Zwingend erforderlich.
- Eine Aggregationsfunktion.
- Das Argument der Aggregation muss ein Feld sein.

Nebenklausel

- Optional.
- Syntax: `by [span-expression,] [field,]...`
- Die by-Klausel kann Felder und Ausdrücke wie Skalarfunktionen und Aggregationsfunktionen enthalten. Sie können die Span-Klausel auch verwenden, um ein bestimmtes Feld in Gruppen mit gleichen Intervallen aufzuteilen. Der Befehl eventstats führt dann eine Aggregation auf der Grundlage dieser Span-Buckets durch.
- Standard: Wenn Sie keine by-Klausel angeben, aggregiert der Befehl eventstats die gesamte Ergebnismenge.

Span-Ausdruck

- Fakultativ, höchstens einer.
- Syntax: `span(field_expr, interval_expr)`
- Die Einheit des Intervallausdrucks ist standardmäßig die natürliche Einheit. Für Felder vom Typ Datum und Uhrzeit müssen Sie jedoch die Einheit im Intervallausdruck angeben, wenn Sie Datums-/Uhrzeiteinheiten verwenden.

  Um das Feld beispielsweise nach 10 Jahren `age` in Gruppen aufzuteilen, verwenden Sie. `span(age, 10)` Bei zeitbasierten Feldern können Sie ein `timestamp` Feld mithilfe von in stündliche Intervalle unterteilen. `span(timestamp, 1h)`

Verfügbare Zeiteinheiten

Einheiten für das Spanenintervall
Millisekunde (ms)
Sekunde (n)
Minute (m, Groß- und Kleinschreibung beachten)
Stunde (h)
Tag (d)
Woche (w)

Einheiten für das Spanenintervall
Monat (M, Groß- und Kleinschreibung beachten)
Quartal (q)
Jahr (y)

Aggregationsfunktionen

COUNT

`COUNT`gibt die Anzahl der Ausdrücke in den Zeilen zurück, die mit einer SELECT-Anweisung abgerufen wurden.

Verwenden Sie Abfragen für CloudWatch Logs, `COUNT` wird nicht unterstützt.

Beispiel:

```
os> source=accounts | eventstats count();
fetched rows / total rows = 4/4
+----------------+----------+-----------+----------+-----+--------+--------------------
+------------+--------------------------+--------+-------+---------+
| account_number | balance  | firstname | lastname | age | gender | address
 | employer   | email                    | city   | state | count() |
+----------------+----------+-----------+----------+-----+--------+--------------------
+------------+--------------------------+--------+-------+---------+
| 1              | 39225    | Jane      | Doe      | 32  | M      | *** Any Lane
 | AnyCorp    | janedoe@anycorp.com      | Brogan | IL    | 4       |
| 6              | 5686     | Mary      | Major    | 36  | M      | 671 Example Street
 | AnyCompany | marymajor@anycompany.com | Dante  | TN    | 4       |
| 13             | 32838    | Nikki     | Wolf     | 28  | F      | 789 Any Street
 | AnyOrg     |                          | Nogal  | VA    | 4       |
| 18             | 4180     | Juan      | Li       | 33  | M      | *** Example Court
 |            | juanli@exampleorg.com    | Orick  | MD    | 4       |
+----------------+----------+-----------+----------+-----+--------+--------------------
+------------+--------------------------+--------+-------+---------+
```

SUM

`SUM(expr)`gibt die Summe von expr zurück.

Beispiel:

```
os> source=accounts | eventstats sum(age) by gender;
fetched rows / total rows = 4/4
+----------------+----------+-----------+----------+-----+--------
+-----------------------+------------+--------------------------+--------+-------
+--------------------+
| account_number | balance  | firstname | lastname | age | gender | address
   | employer   | email                    | city   | state | sum(age) by gender |
+----------------+----------+-----------+----------+-----+--------
+-----------------------+------------+--------------------------+--------+-------
+--------------------+
| 1              | 39225    | Jane      | Doe      | 32  | M      | 880 Any Lane
   | AnyCorp    | janedoe@anycorp.com      | Brogan | IL    | 101                |
| 6              | 5686     | Mary      | Major    | 36  | M      | 671 Example Street
   | AnyCompany | marymajor@anycompany.com | Dante  | TN    | 101                |
| 13             | 32838    | Nikki     | Wolf     | 28  | F      | 789 Any Street
   | AnyOrg     |                          | Nogal  | VA    | 28                 |
| 18             | 4180     | Juan      | Li       | 33  | M      | 467 Example Court
   |            | juanli@exampleorg.com    | Orick  | MD    | 101                |
+----------------+----------+-----------+----------+-----+--------
+-----------------------+------------+--------------------------+--------+-------
+--------------------+
```

AVG

`AVG(expr)`gibt den Durchschnittswert von expr zurück.

Beispiel:

```
os> source=accounts | eventstats avg(age) by gender;
fetched rows / total rows = 4/4
+----------------+----------+-----------+----------+-----+--------
+-----------------------+------------+--------------------------+--------+-------
+--------------------+
| account_number | balance  | firstname | lastname | age | gender | address
   | employer    | email                    | city   | state | avg(age) by gender |
+----------------+----------+-----------+----------+-----+--------
+-----------------------+------------+--------------------------+--------+-------
+--------------------+
| 1              | 39225    | Jane      | Doe      | 32  | M      | 880 Any Lane
   | AnyCorp     | janedoe@anycorp.com      | Brogan | IL    | 33.67              |
```

```
| 6              | 5686     | Mary      | Major    | 36  | M      | 671 Example Street
   | Any Company | marymajor@anycompany.com | Dante  | TN    | 33.67             |
| 13             | 32838    | Nikki     | Wolf     | 28  | F      | 789 Any Street
   | AnyOrg      |                          | Nogal  | VA    | 28.00             |
| 18             | 4180     | Juan      | Li       | 33  | M      | 467 Example Court
   |             | juanli@exampleorg.com    | Orick  | MD    | 33.67             |
+----------------+----------+-----------+----------+-----+--------
+----------------------+-------------+--------------------------+--------+-------
+--------------------+
```

MAX

`MAX(expr)`Gibt den Maximalwert von expr zurück.

Beispiel

```
os> source=accounts | eventstats max(age);
fetched rows / total rows = 4/4
+----------------+----------+-----------+----------+-----+--------
+----------------------+-------------+--------------------------+--------+-------
+-----------+
| account_number | balance  | firstname | lastname | age | gender | address
   | employer    | email                    | city   | state | max(age)  |
+----------------+----------+-----------+----------+-----+--------
+----------------------+-------------+--------------------------+--------+-------
+-----------+
| 1              | 39225    | Jane      | Doe      | 32  | M      | 880 Any Lane
   | AnyCorp     | janedoe@anycorp.com      | Brogan | IL    | 36        |
| 6              | 5686     | Mary      | Major    | 36  | M      | 671 Example Street
   | Any Company | marymajor@anycompany.com | Dante  | TN    | 36        |
| 13             | 32838    | Nikki     | Wolf     | 28  | F      | 789 Any Street
   | AnyOrg      |                          | Nogal  | VA    | 36        |
| 18             | 4180     | Juan      | Li       | 33  | M      | *** Example Court
   |             | juanli@exampleorg.com    | Orick  | MD    | 36        |
+----------------+----------+-----------+----------+-----+--------
+----------------------+-------------+--------------------------+--------+-------
+-----------+
```

MIN

`MIN(expr)`Gibt den Minimalwert von expr zurück.

Beispiel

```
os> source=accounts | eventstats min(age);
fetched rows / total rows = 4/4
+----------------+----------+-----------+----------+-----+--------
+----------------------+-------------+--------------------------+--------+-------
+-----------+
| account_number | balance  | firstname | lastname | age | gender | address
   | employer    | email                    | city   | state | min(age)  |
+----------------+----------+-----------+----------+-----+--------
+----------------------+-------------+--------------------------+--------+-------
+-----------+
| 1              | 39225    | Jane      | Doe      | 32  | M      | 880 Any Lane
   | AnyCorp     | janedoe@anycorp.com      | Brogan | IL    | 28        |
| 6              | 5686     | Mary      | Major    | 36  | M      | 671 Example Street
   | Any Company | marymajor@anycompany.com | Dante  | TN    | 28        |
| 13             | 32838    | Nikki     | Wolf     | 28  | F      | *** Any Street
   | AnyOrg      |                          | Nogal  | VA    | 28        |
| 18             | 4180     | Juan      | Li       | 33  | M      | *** Example Court
   |             | juanli@exampleorg.com    | Orick  | MD    | 28        |
+----------------+----------+-----------+----------+-----+--------
+----------------------+-------------+--------------------------+--------+-------
+-----------+
```

STDDEV_SAMP

`STDDEV_SAMP(expr)`Gibt die Standardabweichung der Stichprobe von expr zurück.

Beispiel

```
os> source=accounts | eventstats stddev_samp(age);
fetched rows / total rows = 4/4
+----------------+----------+-----------+----------+-----+--------
+----------------------+-------------+--------------------------+--------+-------
+------------------------+
| account_number | balance  | firstname | lastname | age | gender | address
   | employer    | email                    | city   | state | stddev_samp(age)       |
+----------------+----------+-----------+----------+-----+--------
+----------------------+-------------+--------------------------+--------+-------
+------------------------+
| 1              | 39225    | Jane      | Doe      | 32  | M      | *** Any Lane
   | AnyCorp     | janedoe@anycorp.com      | Brogan | IL    | 3.304037933599835      |
| 6              | 5686     | Mary      | Major    | 36  | M      | 671 Example Street
   | Any Company | marymajor@anycompany.com | Dante  | TN    | 3.304037933599835      |
```

```
| 13             | 32838    | Nikki     | Wolf     | 28  | F      | 789 Any Street
   | AnyOrg      |                          | Nogal  | VA    | 3.304037933599835      |
| 18             | 4180     | Juan      | Li       | 33  | M      | 467 Example Court
   |             | juanli@exampleorg.com    | Orick  | MD    | 3.304037933599835      |
+----------------+----------+-----------+----------+-----+--------
+----------------------+-------------+--------------------------+--------+-------
+------------------------+
```

STDDEV_POP

`STDDEV_POP(expr)`Gibt die Standardabweichung der Grundgesamtheit von expr zurück.

Beispiel

```
os> source=accounts | eventstats stddev_pop(age);
fetched rows / total rows = 4/4
+----------------+----------+-----------+----------+-----+--------
+----------------------+-------------+--------------------------+--------+-------
+------------------------+
| account_number | balance  | firstname | lastname | age | gender | address
   | employer    | email                    | city   | state | stddev_pop(age)        |
+----------------+----------+-----------+----------+-----+--------
+----------------------+-------------+--------------------------+--------+-------
+------------------------+
| 1              | 39225    | Jane      | Doe      | 32  | M      | 880 Any Lane
   | AnyCorp     | janedoe@anycorp.com      | Brogan | IL    | 2.****************     |
| 6              | 5686     | Mary      | Major    | 36  | M      | *** Example Street
   | Any Company | marymajor@anycompany.com | Dante  | TN    | 2.****************     |
| 13             | 32838    | Nikki     | Wolf     | 28  | F      | *** Any Street
   | AnyOrg      |                          | Nogal  | VA    | 2.****************     |
| 18             | 4180     | Juan      | Li       | 33  | M      | *** Example Court
   |             | juanli@exampleorg.com    | Orick  | MD    | 2.****************     |
+----------------+----------+-----------+----------+-----+--------
+----------------------+-------------+--------------------------+--------+-------
+------------------------+
```

PERCENTILE oder PERCENTILE_APPROX

`PERCENTILE(expr, percent)`oder `PERCENTILE_APPROX(expr, percent)` Gibt den ungefähren Perzentilwert von expr zum angegebenen Prozentsatz zurück.

Prozent

- Die Zahl muss eine Konstante zwischen 0 und 100 sein.

Beispiel

```
os> source=accounts | eventstats percentile(age, 90) by gender;
fetched rows / total rows = 4/4
+----------------+----------+-----------+----------+-----+--------
+----------------------+-------------+--------------------------+--------+-------
+--------------------------------+
| account_number | balance  | firstname | lastname | age | gender | address
    | employer    | email                    | city   | state | percentile(age, 90) by
 gender  |
+----------------+----------+-----------+----------+-----+--------
+----------------------+-------------+--------------------------+--------+-------
+--------------------------------+
| 1              | 39225    | Jane      | Doe      | 32  | M      | *** Any Lane
   | AnyCorp     | janedoe@anycorp.com      | Brogan | IL    | 36
       |
| 6              | 5686     | Mary      | Major    | 36  | M      | 671 Example Street
   | Any Company | marymajor@anycompany.com | Dante  | TN    | 36
       |
| 13             | 32838    | Nikki     | Wolf     | 28  | F      | 789 Any Street
   | AnyOrg      |                          | Nogal  | VA    | 28
       |
| 18             | 4180     | Juan      | Li       | 33  | M      | *** Example Court
   |             | juanli@exampleorg.com    | Orick  | MD    | 36
       |
+----------------+----------+-----------+----------+-----+--------
+----------------------+-------------+--------------------------+--------+-------
+--------------------------------+
```

Beispiel 1: Berechnet den Durchschnitt, die Summe und die Anzahl eines Felds nach Gruppen

Das Beispiel zeigt die Berechnung des Durchschnittsalters, der Summe des Alters und der Anzahl der Ereignisse aller Konten, gruppiert nach Geschlecht.

```
os> source=accounts | eventstats avg(age) as avg_age, sum(age) as sum_age, count() as
 count by gender;
fetched rows / total rows = 4/4
```

```
+---------------+----------+-----------+----------+-----+--------
+----------------------+-------------+--------------------------+--------+-------
+-----------+-----------+--------+
| account_number | balance  | firstname | lastname | age | gender | address
    | employer    | email                    | city   | state | avg_age   | sum_age   |
 count |
+---------------+----------+-----------+----------+-----+--------
+----------------------+-------------+--------------------------+--------+-------
+-----------+-----------+--------+
| 1              | 39225    | Jane      | Doe      | 32  | M      | *** Any Lane
    | AnyCorp     | janedoe@anycorp.com      | Brogan | IL    | 33.666667 | 101       |
 3     |
| 6              | 5686     | Mary      | Major    | 36  | M      | 671 Example Street
    | Any Company | marymajor@anycompany.com | Dante  | TN    | 33.666667 | 101       |
 3     |
| 13             | 32838    | Nikki     | Wolf     | 28  | F      | 789 Any Street
    | AnyOrg      |                          | Nogal  | VA    | 28.000000 | 28        |
 1     |
| 18             | 4180     | Juan      | Li       | 33  | M      | *** Example Court
    |             | juanli@exampleorg.com    | Orick  | MD    | 33.666667 | 101       |
 3     |
+---------------+----------+-----------+----------+-----+--------
+----------------------+-------------+--------------------------+--------+-------
+-----------+-----------+--------+
```

Beispiel 2: Berechne die Anzahl anhand einer Spanne

Im Beispiel wird die Anzahl der Altersstufen im Intervall von 10 Jahren berechnet.

```
os> source=accounts | eventstats count(age) by span(age, 10) as age_span
fetched rows / total rows = 4/4
+---------------+----------+-----------+----------+-----+--------
+----------------------+-------------+--------------------------+--------+-------
+-----------+
| account_number | balance  | firstname | lastname | age | gender | address
   | employer    | email                    | city   | state | age_span |
+---------------+----------+-----------+----------+-----+--------
+----------------------+-------------+--------------------------+--------+-------
+-----------+
| 1              | 39225    | Jane      | Doe      | 32  | M      | *** Any Lane
   | AnyCorp     | janedoe@anycorp.com      | Brogan | IL    | 3        |
| 6              | 5686     | Mary      | Major    | 36  | M      | 671 Example Street
   | Any Company | marymajor@anycompany.com | Dante  | TN    | 3        |
```

```
| 13             | 32838    | Nikki     | Wolf     | 28  | F      | 789 Any Street
   | AnyOrg      |                          | Nogal  | VA    | 1        |
| 18             | 4180     | Juan      | Li       | 33  | M      | *** Example Court
   |             | juanli@exampleorg.com    | Orick  | MD    | 3        |
+----------------+----------+-----------+----------+-----+--------
+----------------------+-------------+--------------------------+--------+-------
+----------+
```

Beispiel 3: Berechnet die Anzahl anhand eines Geschlechts und einer Spanne

Im Beispiel wird die Anzahl der Altersgruppen im Intervall von 5 Jahren berechnet und nach Geschlecht gruppiert.

```
os> source=accounts | eventstats count() as cnt by span(age, 5) as age_span, gender
fetched rows / total rows = 4/4
+----------------+----------+-----------+----------+-----+--------
+----------------------+-------------+--------------------------+--------+-------
+-----+
| account_number | balance  | firstname | lastname | age | gender | address
   | employer    | email                    | city   | state | cnt |
+----------------+----------+-----------+----------+-----+--------
+----------------------+-------------+--------------------------+--------+-------
+-----+
| 1              | 39225    | Jane      | Doe      | 32  | M      | *** Any Lane
   | AnyCorp     | janedoe@anycorp.com      | Brogan | IL    | 2   |
| 6              | 5686     | Mary      | Majo     | 36  | M      | 671 Example Street
   | Any Company | hattiebond@anycompany.com | Dante  | TN    | 1   |
| 13             | 32838    | Nikki     | Wolf     | 28  | F      | *** Any Street
   | AnyOrg      |                          | Nogal  | VA    | 1   |
| 18             | 4180     | Juan      | Li       | 33  | M      | *** Example Court
   |             | juanli@exampleorg.com    | Orick  | MD    | 2   |
+----------------+----------+-----------+----------+-----+--------
+----------------------+-------------+--------------------------+--------+-------
+-----+
```

Verwendung

- `source = table | eventstats avg(a)`
- `source = table | where a < 50 | eventstats avg(c)`
- `source = table | eventstats max(c) by b`
- `source = table | eventstats count(c) by b | head 5`

- `source = table | eventstats distinct_count(c)`
- `source = table | eventstats stddev_samp(c)`
- `source = table | eventstats stddev_pop(c)`
- `source = table | eventstats percentile(c, 90)`
- `source = table | eventstats percentile_approx(c, 99)`

Aggregationen mit Span

- `source = table | eventstats count(a) by span(a, 10) as a_span`
- `source = table | eventstats sum(age) by span(age, 5) as age_span | head 2`
- `source = table | eventstats avg(age) by span(age, 20) as age_span, country | sort - age_span | head 2`

Aggregationen mit Zeitfensterspanne (Tumble-Windowing-Funktion)

- `source = table | eventstats sum(productsAmount) by span(transactionDate, 1d) as age_date | sort age_date`
- `source = table | eventstats sum(productsAmount) by span(transactionDate, 1w) as age_date, productId`

Aggregationen gruppieren nach mehreren Ebenen

- `source = table | eventstats avg(age) as avg_state_age by country, state | eventstats avg(avg_state_age) as avg_country_age by country`
- `source = table | eventstats avg(age) as avg_city_age by country, state, city | eval new_avg_city_age = avg_city_age - 1 | eventstats avg(new_avg_city_age) as avg_state_age by country, state | where avg_state_age > 18 | eventstats avg(avg_state_age) as avg_adult_country_age by country`

Befehl expandieren

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen PPL-Befehl unterstützen, finden Sie unter. the section called “Befehle”

Verwenden Sie den `expand` Befehl, um ein Feld des folgenden Typs zu reduzieren:

- `Array<Any>`
- `Map<Any>`

Syntax

Verwenden Sie die folgende Syntax:

```
expand <field> [As alias]
```

field

- Das Feld, das erweitert (aufgelöst) werden soll. Muss von einem unterstützten Typ sein.

alias

- Optional. Der Name, der anstelle des ursprünglichen Feldnamens verwendet werden soll.

Verwendung

Der `expand` Befehl erzeugt eine Zeile für jedes Element im angegebenen Array- oder Zuordnungsfeld, wobei:

- Array-Elemente werden zu einzelnen Zeilen.
- Map-Schlüssel-Wert-Paare werden in separate Zeilen aufgeteilt, wobei jeder Schlüsselwert als Zeile dargestellt wird.

- Wenn ein Alias angegeben wird, werden die explodierten Werte unter dem Alias statt unter dem ursprünglichen Feldnamen dargestellt.

- Dies kann in Kombination mit anderen Befehlen wie, und verwendet werden `statseval`, um Daten nach der `parse` Erweiterung zu bearbeiten oder zu extrahieren.

Beispiele

- `source = table | expand employee | stats max(salary) as max by state, company`
- `source = table | expand employee as worker | stats max(salary) as max by state, company`
- `source = table | expand employee as worker | eval bonus = salary * 3 | fields worker, bonus`
- `source = table | expand employee | parse description '(?<email>.+@.+)' | fields employee, email`
- `source = table | eval array=json_array(1, 2, 3) | expand array as uid | fields name, occupation, uid`
- `source = table | expand multi_valueA as multiA | expand multi_valueB as multiB`

Befehl erläutern

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen PPL-Befehl unterstützen, finden Sie unter. the section called “Befehle”

Der `explain` Befehl hilft Ihnen dabei, die Ausführungspläne für Abfragen zu verstehen, sodass Sie Ihre Abfragen analysieren und optimieren können, um eine bessere Leistung zu erzielen. Diese Einführung bietet einen kurzen Überblick über den Zweck des Befehls explain und seine Bedeutung für die Abfrageoptimierung.

Kommentar

- `source=accounts | top gender // finds most common gender of all the accounts`(Kommentar zur Zeile)

- `source=accounts | dedup 2 gender /* dedup the document with gender field keep 2 duplication */ | fields account_number, gender`(Kommentar blockieren)

Describe

- `describe table`Dieser Befehl entspricht dem `DESCRIBE EXTENDED table` SQL-Befehl
- `describe schema.table`
- `describe schema.\`table\``
- `describe catalog.schema.table`
- `describe catalog.schema.\`table\``
- `describe \`catalog\`.\`schema\`.\`table\``

Explain

- `explain simple | source = table | where a = 1 | fields a,b,c`
- `explain extended | source = table`
- `explain codegen | source = table | dedup a | fields a,b,c`
- `explain cost | source = table | sort a | fields a,b,c`
- `explain formatted | source = table | fields - a`
- `explain simple | describe table`

Felder

- `source = table`
- `source = table | fields a,b,c`
- `source = table | fields + a,b,c`
- `source = table | fields - b,c`
- `source = table | eval b1 = b | fields - b1,c`

Zusammenfassung der Felder

- `source = t | fieldsummary includefields=status_code nulls=false`

- `source = t | fieldsummary includefields= id, status_code, request_path nulls=true`
- `source = t | where status_code != 200 | fieldsummary includefields= status_code nulls=true`

Verschachteltes Feld

- `source = catalog.schema.table1, catalog.schema.table2 | fields A.nested1, B.nested1`
- `source = catalog.table | where struct_col2.field1.subfield > 'valueA' | sort int_col | fields int_col, struct_col.field1.subfield, struct_col2.field1.subfield`
- `source = catalog.schema.table | where struct_col2.field1.subfield > 'valueA' | sort int_col | fields int_col, struct_col.field1.subfield, struct_col2.field1.subfield`

Filter

- `source = table | where a = 1 | fields a,b,c`
- `source = table | where a >= 1 | fields a,b,c`
- `source = table | where a < 1 | fields a,b,c`
- `source = table | where b != 'test' | fields a,b,c`
- `source = table | where c = 'test' | fields a,b,c | head 3`
- `source = table | where ispresent(b)`
- `source = table | where isnull(coalesce(a, b)) | fields a,b,c | head 3`
- `source = table | where isempty(a)`
- `source = table | where isblank(a)`
- `source = table | where case(length(a) > 6, 'True' else 'False') = 'True'`
- `source = table | where a not in (1, 2, 3) | fields a,b,c`
- `source = table | where a between 1 and 4`- Hinweis: Dies gibt a >= 1 und a <= 4 zurück, d. h. [1, 4]
- `source = table | where b not between '2024-09-10' and '2025-09-10'`- Hinweis: Dies gibt b >= '**********' und b <= '2025-09-10' zurück

- `source = table | where cidrmatch(ip, '***********/24')`
- `source = table | where cidrmatch(ipv6, '2003:db8::/32')`
- `source = table | trendline sma(2, temperature) as temp_trend`

IP-bezogene Abfragen

- `source = table | where cidrmatch(ip, '**************')`
- `source = table | where isV6 = false and isValid = true and cidrmatch(ipAddress, '**************')`
- `source = table | where isV6 = true | eval inRange = case(cidrmatch(ipAddress, '2003:***::/32'), 'in' else 'out') | fields ip, inRange`

Komplexe Filter

```
source = table | eval status_category =
case(a >= 200 AND a < 300, 'Success',
    a >= 300 AND a < 400, 'Redirection',
    a >= 400 AND a < 500, 'Client Error',
    a >= 500, 'Server Error'
else 'Incorrect HTTP status code')
| where case(a >= 200 AND a < 300, 'Success',
    a >= 300 AND a < 400, 'Redirection',
    a >= 400 AND a < 500, 'Client Error',
    a >= 500, 'Server Error'
else 'Incorrect HTTP status code'
) = 'Incorrect HTTP status code'
```

```
source = table
| eval factor = case(a > 15, a - 14, isnull(b), a - 7, a < 3, a + 1 else 1)
| where case(factor = 2, 'even', factor = 4, 'even', factor = 6, 'even', factor = 8,
 'even' else 'odd') = 'even'
| stats count() by factor
```

Filter mit logischen Bedingungen

- `source = table | where c = 'test' AND a = 1 | fields a,b,c`

- `source = table | where c != 'test' OR a > 1 | fields a,b,c | head 1`
- `source = table | where c = 'test' NOT a > 1 | fields a,b,c`

Eval

Annahmen:a,b, c sind bestehende Felder in `table`

- `source = table | eval f = 1 | fields a,b,c,f`
- `source = table | eval f = 1`(gibt A-, B-, C- und F-Felder aus)
- `source = table | eval n = now() | eval t = unix_timestamp(a) | fields n,t`
- `source = table | eval f = a | where f > 1 | sort f | fields a,b,c | head 5`
- `source = table | eval f = a * 2 | eval h = f * 2 | fields a,f,h`
- `source = table | eval f = a * 2, h = f * 2 | fields a,f,h`
- `source = table | eval f = a * 2, h = b | stats avg(f) by h`
- `source = table | eval f = ispresent(a)`
- `source = table | eval r = coalesce(a, b, c) | fields r`
- `source = table | eval e = isempty(a) | fields e`
- `source = table | eval e = isblank(a) | fields e`
- `source = table | eval f = case(a = 0, 'zero', a = 1, 'one', a = 2, 'two', a = 3, 'three', a = 4, 'four', a = 5, 'five', a = 6, 'six', a = 7, 'se7en', a = 8, 'eight', a = 9, 'nine')`
- `source = table | eval f = case(a = 0, 'zero', a = 1, 'one' else 'unknown')`
- `source = table | eval f = case(a = 0, 'zero', a = 1, 'one' else concat(a, ' is an incorrect binary digit'))`
- `source = table | eval digest = md5(fieldName) | fields digest`
- `source = table | eval digest = sha1(fieldName) | fields digest`
- `source = table | eval digest = sha2(fieldName,256) | fields digest`
- `source = table | eval digest = sha2(fieldName,512) | fields digest`

Befehl fillnull

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen PPL-Befehl unterstützen, finden Sie unter. the section called “Befehle”

Beschreibung

Verwenden Sie den `fillnull` Befehl, um Nullwerte in einem oder mehreren Feldern Ihrer Suchergebnisse durch einen bestimmten Wert zu ersetzen.

Syntax

Verwenden Sie die folgende Syntax:

```
fillnull [with <null-replacement> in <nullable-field>["," <nullable-field>]] | [using
 <source-field> = <null-replacement> ["," <source-field> = <null-replacement>]]
```

- Null-Replacement: Obligatorisch. Der Wert, der verwendet wird, um Nullwerte zu ersetzen.
- nullable-field: Obligatorisch. Feldreferenz. Die Nullwerte in diesem Feld werden durch den unter Null-Replacement angegebenen Wert ersetzt.

Beispiel 1: Füllen Sie ein Feld mit Null

Das Beispiel zeigt, wie fillnull für ein einzelnes Feld verwendet wird:

```
os> source=logs | fields status_code | eval input=status_code | fillnull with 0 in
 status_code;
| input | status_code |
|-------|-------------|
| 403   | 403         |
| 403   | 403         |
| NULL  | 0           |
| NULL  | 0           |
| 200   | 200         |
| 404   | 404         |
| 500   | 500         |
| NULL  | 0           |
| 500   | 500         |
```

```
| 404   | 404         |
| 200   | 200         |
| 500   | 500         |
| NULL  | 0           |
| NULL  | 0           |
| 404   | 404         |
```

Beispiel 2: Fillnull wurde auf mehrere Felder angewendet

Das Beispiel zeigt, dass Fillnull auf mehrere Felder angewendet wurde.

```
os> source=logs | fields request_path, timestamp | eval
 input_request_path=request_path, input_timestamp = timestamp | fillnull with '???' in
 request_path, timestamp;
| input_request_path | input_timestamp       | request_path | timestamp              |
|-------------------------------------------------------------------------------------|
| /contact           | NULL                  | /contact     | ???                    |
| /home              | NULL                  | /home        | ???                    |
| /about             | 2023-10-01 10:30:00   | /about       | 2023-10-01 10:30:00    |
| /home              | 2023-10-01 10:15:00   | /home        | 2023-10-01 10:15:00    |
| NULL               | 2023-10-01 10:20:00   | ???          | 2023-10-01 10:20:00    |
| NULL               | 2023-10-01 11:05:00   | ???          | 2023-10-01 11:05:00    |
| /about             | NULL                  | /about       | ???                    |
| /home              | 2023-10-01 10:00:00   | /home        | 2023-10-01 10:00:00    |
| /contact           | NULL                  | /contact     | ???                    |
| NULL               | 2023-10-01 10:05:00   | ???          | 2023-10-01 10:05:00    |
| NULL               | 2023-10-01 10:50:00   | ???          | 2023-10-01 10:50:00    |
| /services          | NULL                  | /services    | ???                    |
| /home              | 2023-10-01 10:45:00   | /home        | 2023-10-01 10:45:00    |
| /services          | 2023-10-01 11:00:00   | /services    | 2023-10-01 11:00:00    |
| NULL               | 2023-10-01 10:35:00   | ???          | 2023-10-01 10:35:00    |
```

Beispiel 3: Fillnull wurde auf mehrere Felder mit verschiedenen Null-Ersatzwerten angewendet.

Das Beispiel zeigt Fillnull mit verschiedenen Werten, die verwendet werden, um Nullen zu ersetzen.

- `/error`im `request_path` Feld
- `1970-01-01 00:00:00`im `timestamp` Feld

```
os> source=logs | fields request_path, timestamp | eval
 input_request_path=request_path, input_timestamp = timestamp | fillnull using
 request_path = '/error', timestamp='1970-01-01 00:00:00';
```

```
| input_request_path | input_timestamp       | request_path | timestamp             |
|-------------------------------------------------------------------------------|
| /contact           | NULL                  | /contact     | 1970-01-01 00:00:00   |
| /home              | NULL                  | /home        | 1970-01-01 00:00:00   |
| /about             | 2023-10-01 10:30:00   | /about       | 2023-10-01 10:30:00   |
| /home              | 2023-10-01 10:15:00   | /home        | 2023-10-01 10:15:00   |
| NULL               | 2023-10-01 10:20:00   | /error       | 2023-10-01 10:20:00   |
| NULL               | 2023-10-01 11:05:00   | /error       | 2023-10-01 11:05:00   |
| /about             | NULL                  | /about       | 1970-01-01 00:00:00   |
| /home              | 2023-10-01 10:00:00   | /home        | 2023-10-01 10:00:00   |
| /contact           | NULL                  | /contact     | 1970-01-01 00:00:00   |
| NULL               | 2023-10-01 10:05:00   | /error       | 2023-10-01 10:05:00   |
| NULL               | 2023-10-01 10:50:00   | /error       | 2023-10-01 10:50:00   |
| /services          | NULL                  | /services    | 1970-01-01 00:00:00   |
| /home              | 2023-10-01 10:45:00   | /home        | 2023-10-01 10:45:00   |
| /services          | 2023-10-01 11:00:00   | /services    | 2023-10-01 11:00:00   |
| NULL               | 2023-10-01 10:35:00   | /error       | 2023-10-01 10:35:00   |
```

Befehl „Felder“

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen PPL-Befehl unterstützen, finden Sie unter. the section called “Befehle”

Verwenden Sie den `fields` Befehl, um Felder im Suchergebnis beizubehalten oder zu entfernen.

Syntax

Verwenden Sie die folgende Syntax:

```
field [+|-] <field-list>
```

- `index`: Optional.

  Wenn das Plus (+) verwendet wird, werden nur die in der Feldliste angegebenen Felder beibehalten.

  Wenn das Minuszeichen (-) verwendet wird, werden alle in der Feldliste angegebenen Felder entfernt.

Standard: +

- `field list`: Obligatorisch. Eine durch Kommas getrennte Liste von Feldern, die beibehalten oder entfernt werden sollen.

Beispiel 1: Wählen Sie bestimmte Felder aus dem Ergebnis aus

Dieses Beispiel zeigt, wie `lastname` Felder `account_numberfirstname`, und aus Suchergebnissen abgerufen werden.

PPL-Abfrage:

```
os> source=accounts | fields account_number, firstname, lastname;
fetched rows / total rows = 4/4
+------------------+-------------+------------+
| account_number   | firstname   | lastname   |
|------------------+-------------+------------|
| 1                | Jane        | Doe        |
| 6                | John        | Doe        |
| 13               | Jorge       | Souza      |
| 18               | Juan        | Li         |
+------------------+-------------+------------+
```

Beispiel 2: Entfernen Sie die angegebenen Felder aus dem Ergebnis

Dieses Beispiel zeigt, wie das `account_number` Feld aus den Suchergebnissen entfernt wird.

PPL-Abfrage:

```
os> source=accounts | fields account_number, firstname, lastname | fields -
 account_number ;
fetched rows / total rows = 4/4
+-------------+------------+
| firstname   | lastname   |
|-------------+------------|
| Jane        | Doe        |
| John        | Doe        |
| Jorge       | Souza      |
| Juan        | Li         |
+-------------+------------+
```

Weitere Beispiele

- `source = table`
- `source = table | fields a,b,c`
- `source = table | fields + a,b,c`
- `source = table | fields - b,c`
- `source = table | eval b1 = b | fields - b1,c`

Beispiel für verschachtelte Felder:

```
`source = catalog.schema.table1, catalog.schema.table2 | fields A.nested1, B.nested1`
`source = catalog.table | where struct_col2.field1.subfield > 'valueA' | sort int_col |
 fields  int_col, struct_col.field1.subfield, struct_col2.field1.subfield`
`source = catalog.schema.table | where struct_col2.field1.subfield > 'valueA' | sort
 int_col | fields  int_col, struct_col.field1.subfield, struct_col2.field1.subfield`
```

Befehl flatten

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen PPL-Befehl unterstützen, finden Sie unter. the section called “Befehle”

Verwenden Sie den Befehl flatten, um Felder der folgenden Typen zu erweitern:

- `struct<?,?>`
- `array<struct<?,?>>`

Syntax

Verwenden Sie die folgende Syntax:

```
flatten <field>
```

- Feld: Das Feld, das reduziert werden soll. Das Feld muss einen unterstützten Typ haben.

Schema

col_name	data_type
_Zeit	Zeichenfolge
Brücken	<length:bigint, name:string>array <struct>
city	Zeichenfolge
Farbe	Struktur<alt:bigint, lat:double, long:doub le>
country	Zeichenfolge

Daten

_Zeit	Brücken	city	Tür	country
2024-09-13T 12:00:00	[{801, Tower Bridge}, {928, London Bridge}]	London	{35, 51,5074, -0,1278}	England
2024-09-13T 12:00:00	[{232, Pont Neuf}, {160, Pont Alexandre III}]	Paris	{35, 48,8566, 2,3522}	Frankreich
2024-09-13T 12:00:00	[{48, Rialtobrü cke}, {11,	Venedig	{2, 45.4408, 12.3155}	Italien

_Zeit	Brücken	city	Tür	country
	Seufzerbrücke}]			
2024-09-13T 12:00:00	[{***, Karlsbrücke}, {343, Legionsbrücke}]	Prag	{200, 50,0755, 14,4378}	Tschechische Republik
2024-09-13T 12:00:00	[{375, Kettenbrücke}, {333, Liberty Bridge}]	Budapest	{96, 47,4979, 19,0402}	Ungarn
1990-09-13T 12:00:00	NULL	Warschau	NULL	Polen

Beispiel 1: Struktur abflachen

Dieses Beispiel zeigt, wie ein Strukturfeld geglättet wird.

PPL-Abfrage:

```
source=table | flatten coor
```

_Zeit	Brücken	city	country	alt	lat	long
2024-09-13T 12:00:00	[{801, Tower Bridge}, {928, London Bridge}]	London	England	35	51,5074	-0,1278

_Zeit	Brücken	city	country	alt	lat	long
2024-09-13T 12:00:00	[{232, Pont Neuf}, {160, Pont Alexandre III}]	Paris	Frankreich	35	48,8566	2,3522
2024-09-13T 12:00:00	[{48, Rialtobrücke}, {11, Seufzerbrücke}]	Venedig	Italien	2	45.4408	12,3155
2024-09-13T 12:00:00	[{516, Karlsbrücke}, {343, Legionsbrücke}]	Prag	Tschechische Republik	200	50,0755	14,4378
2024-09-13T 12:00:00	[{375, Kettenbrücke}, {333, Liberty Bridge}]	Budapest	Ungarn	96	47,4979	19,0402
1990-09-13T 12:00:00	NULL	Warschau	Polen	NULL	NULL	NULL

Beispiel 2: Array abflachen

Das Beispiel zeigt, wie ein Array von Strukturfeldern reduziert wird.

PPL-Abfrage:

```
source=table | flatten bridges
```

_Zeit	city	Farbe	country	length	Name
2024-09-13T 12:00:00	London	{35, 51,5074, -0,1278}	England	801	Turmbrücke
2024-09-13T 12:00:00	London	{35, 51,5074, -0,1278}	England	928	Londoner Brücke
2024-09-13T 12:00:00	Paris	{35, 48,8566, 2,3522}	Frankreich	232	Brücke Neuf
2024-09-13T 12:00:00	Paris	{35, 48,8566, 2,3522}	Frankreich	160	Pont Alexandre III
2024-09-13T 12:00:00	Venedig	{2, 45.4408, 12.3155}	Italien	48	Rialto-Brücke
2024-09-13T 12:00:00	Venedig	{2, 45.4408, 12.3155}	Italien	11	Seufzerbrücke
2024-09-13T 12:00:00	Prag	{200, 50,0755, 14,4378}	Tschechische Republik	516	Karlsbrücke
2024-09-13T 12:00:00	Prag	{200, 50,0755, 14,4378}	Tschechische Republik	343	Legion-Brücke
2024-09-13T 12:00:00	Budapest	{96, 47,4979, 19,0402}	Ungarn	375	Kettenbrücke
2024-09-13T 12:00:00	Budapest	{96, 47,4979, 19,0402}	Ungarn	333	Freiheitsbrücke
1990-09-13T 12:00:00	Warschau	NULL	Polen	NULL	NULL

Beispiel 3: Array und Struktur reduzieren

Dieses Beispiel zeigt, wie mehrere Felder geglättet werden.

PPL-Abfrage:

```
source=table | flatten bridges | flatten coor
```

_Zeit	city	country	length	Name	alt	lat	long
2024-09-13T 12:00:00	London	England	801	Turmbrücke	35	51.5074	-0,1278
2024-09-13T 12:00:00	London	England	928	Londoner Brücke	35	51,5074	-0,1278
2024-09-13T 12:00:00	Paris	Frankreich	232	Pont Neuf	35	48,8566	2,3522
2024-09-13T 12:00:00	Paris	Frankreich	160	Brücke Alexandre III	35	48,8566	2,3522
2024-09-13T 12:00:00	Venedig	Italien	48	Rialto-Brücke	2	45.4408	12,3155
2024-09-13T 12:00:00	Venedig	Italien	11	Brücke der Seufzer	2	45.4408	12,3155
2024-09-13T 12:00:00	Prag	Tschechische Republik	516	Karlsbrücke	200	50.0755	14,4378

_Zeit	city	country	length	Name	alt	lat	long
2024-09-13T 12:00:00	Prag	Tschechische Republik	343	Legion-Brücke	200	50.0755	14,4378
2024-09-13T 12:00:00	Budape	Ungarn	375	Kettenbrücke	96	47.4979	19,0402
2024-09-13T 12:00:00	Budape	Ungarn	333	Freiheitsbrücke	96	47.4979	19,0402
1990-09-13T 12:00:00	Warsch	Polen	NULL	NULL	NULL	NULL	NULL

Befehl grok

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen PPL-Befehl unterstützen, finden Sie unter. the section called “Befehle”

Der `grok` Befehl analysiert ein Textfeld mit einem Grok-Muster und hängt die Ergebnisse an das Suchergebnis an.

Syntax

Verwenden Sie die folgende Syntax:

```
grok <field> <pattern>
```

field

- Zwingend erforderlich.

- Das Feld muss ein Textfeld sein.

pattern

- Zwingend erforderlich.
- Das Grok-Muster, das verwendet wird, um neue Felder aus dem angegebenen Textfeld zu extrahieren.
- Wenn bereits ein neuer Feldname existiert, ersetzt er das ursprüngliche Feld.

Grok-Muster

Das Grok-Muster wird verwendet, um das Textfeld jedes Dokuments abzugleichen und neue Felder zu extrahieren.

Beispiel 1: Erstellen Sie das neue Feld

Dieses Beispiel zeigt, wie Sie `host` für jedes Dokument ein neues Feld erstellen. `host`wird der Hostname danach `@` in dem `email` Feld sein. Die Analyse eines Nullfeldes gibt eine leere Zeichenfolge zurück.

```
os> source=accounts | grok email '.+@%{HOSTNAME:host}' | fields email, host ;
fetched rows / total rows = 4/4
+-------------------------+-------------+
| email                   | host        |
|-------------------------+-------------|
| jane_doe@example.com    | example.com |
| arnav_desai@example.net | example.net |
| null                    |             |
| juan_li@example.org     | example.org |
+-------------------------+-------------+
```

Beispiel 2: Überschreiben Sie das bestehende Feld

Dieses Beispiel zeigt, wie das vorhandene `address` Feld überschrieben wird, wobei die Hausnummer entfernt wird.

```
os> source=accounts | grok address '%{NUMBER} %{GREEDYDATA:address}' | fields address ;
fetched rows / total rows = 4/4
+------------------+
```

```
| address          |
|------------------|
| Example Lane     |
| Any Street       |
| Main Street      |
| Example Court    |
+------------------+
```

Beispiel 3: Verwendung von Grok zum Analysieren von Protokollen

Dieses Beispiel zeigt, wie man Grok verwendet, um Rohprotokolle zu analysieren.

```
os> source=apache | grok message '%{COMMONAPACHELOG}' | fields COMMONAPACHELOG,
 timestamp, response, bytes ;
fetched rows / total rows = 4/4
+-----------------------------------------------------------------------------------------------------------
+----------------------------+------------+---------+
| COMMONAPACHELOG
                                          | timestamp                  | response   |
 bytes   |
|-----------------------------------------------------------------------------------------------------------
+----------------------------+------------+---------|
| 177.95.8.74 - upton5450 [28/Sep/2022:10:15:57 -0700] "HEAD /e-business/mindshare
 HTTP/1.0" 404 19927                        | 28/Sep/2022:10:15:57 -0700 | 404        |
 19927   |
| 127.45.152.6 - pouros8756 [28/Sep/2022:10:15:57 -0700] "GET /architectures/
convergence/niches/mindshare HTTP/1.0" 100 28722 | 28/Sep/2022:10:15:57 -0700 | 100
    | 28722   |
| *************** - - [28/Sep/2022:10:15:57 -0700] "PATCH /strategize/out-of-the-box
 HTTP/1.0" 401 27439                       | 28/Sep/2022:10:15:57 -0700 | 401        |
 27439   |
| ************** - - [28/Sep/2022:10:15:57 -0700] "POST /users HTTP/1.1" 301 9481
                                       | 28/Sep/2022:10:15:57 -0700 | 301        | 9481
    |
+-----------------------------------------------------------------------------------------------------------
+----------------------------+------------+---------+
```

Einschränkungen

Der Befehl grok hat dieselben Einschränkungen wie der Befehl parse.

Befehl head

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen PPL-Befehl unterstützen, finden Sie unter. the section called “Befehle”

Verwenden Sie den `head` Befehl, um die ersten N der angegebenen Ergebnisse nach einem optionalen Offset in der Suchreihenfolge zurückzugeben.

Syntax

Verwenden Sie die folgende Syntax:

```
head [<size>] [from <offset>]
```

<size>

- Optionale Ganzzahl.
- Die Anzahl der zurückzugebenden Ergebnisse.
- Standard: 10

<offset>

- Ganzzahl nach optional`from`.
- Die Anzahl der Ergebnisse, die übersprungen werden sollen.
- Standard: 0

Beispiel 1: Holen Sie sich die ersten 10 Ergebnisse

Dieses Beispiel zeigt, wie maximal 10 Ergebnisse aus dem Kontenindex abgerufen werden können.

PPL-Abfrage:

```
os> source=accounts | fields firstname, age | head;
fetched rows / total rows = 4/4
```

```
+-------------+-------+
| firstname   | age   |
|-------------+-------|
| Jane        | 32    |
| John        | 36    |
| Jorge       | 28    |
| Juan        | 33    |
+-------------+-------+
```

Beispiel 2: Holen Sie sich die ersten N Ergebnisse

Das Beispiel zeigt die ersten N Ergebnisse aus dem Kontenindex.

PPL-Abfrage:

```
os> source=accounts | fields firstname, age | head 3;
fetched rows / total rows = 3/3
+-------------+-------+
| firstname   | age   |
|-------------+-------|
| Jane        | 32    |
| John        | 36    |
| Jorge       | 28    |
+-------------+-------+
```

Beispiel 3: Holen Sie sich die ersten N Ergebnisse nach Offset M

Dieses Beispiel zeigt, wie die ersten N Ergebnisse abgerufen werden, nachdem M Ergebnisse aus dem Kontenindex übersprungen wurden.

PPL-Abfrage:

```
os> source=accounts | fields firstname, age | head 3 from 1;
fetched rows / total rows = 3/3
+-------------+-------+
| firstname   | age   |
|-------------+-------|
| John        | 36    |
| Jorge       | 28    |
| Juan        | 33    |
+-------------+-------+
```

Befehl join

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen PPL-Befehl unterstützen, finden Sie unter. the section called “Befehle”

Mit dem Befehl join können Sie Daten aus mehreren Quellen auf der Grundlage gemeinsamer Felder kombinieren, sodass Sie komplexe Analysen durchführen und tiefere Einblicke aus Ihren verteilten Datensätzen gewinnen können

Schema

Es gibt mindestens zwei Indizes, `otel-v1-apm-span-*` (groß) und `otel-v1-apm-service-map` (klein).

Relevante Felder aus Indizes:

`otel-v1-apm-span-*`

- traceId — Ein eindeutiger Bezeichner für einen Trace. Alle Spans aus derselben Trace haben dieselbe traceId.
- spanID — Ein eindeutiger Bezeichner für einen Bereich innerhalb eines Traces, der bei der Erstellung des Spans zugewiesen wird.
- parentSpanId - Die SpanID des übergeordneten Bereichs dieser Spanne. Wenn es sich um einen Wurzelbereich handelt, muss dieses Feld leer sein.
- durationInNanos - Der Unterschied in Nanosekunden zwischen StartTime und EndTime. (Das ist `latency` in der Benutzeroberfläche)
- serviceName — Die Ressource, aus der der Span stammt.
- traceGroup — Der Name des Root-Spans des Traces.

`otel-v1-apm-service-map`

- serviceName — Der Name des Dienstes, der den Span ausgegeben hat.
- destination.domain — Der ServiceName des Dienstes, der von diesem Client aufgerufen wird.
- destination.resource — Der Span-Name (API, Operation usw.), der von diesem Client aufgerufen wird.

- target.domain — Der ServiceName des Dienstes, der von einem Client aufgerufen wird.
- target.resource — Der Span-Name (API, Operation usw.), der von einem Client aufgerufen wird.
- traceGroupName — Der Span-Name der obersten Ebene, mit dem die Anforderungskette gestartet wurde.

Anforderung

Support join bei der Berechnung der folgenden Werte:

Kombinieren Sie für jeden Service den Span-Index mit dem Service Map-Index, um Metriken unter verschiedenen Filtertypen zu berechnen.

Diese Beispielabfrage berechnet die Latenz, wenn sie nach der Trace-Gruppe `client_cancel_order` für den `order` Service gefiltert wird.

```
SELECT avg(durationInNanos)
FROM `otel-v1-apm-span-000001` t1
WHERE t1.serviceName = `order`
  AND ((t1.name in
          (SELECT target.resource
           FROM `otel-v1-apm-service-map`
           WHERE serviceName = `order`
             AND traceGroupName = `client_cancel_order`)
        AND t1.parentSpanId != NULL)
       OR (t1.parentSpanId = NULL
           AND t1.name = `client_cancel_order`))
  AND t1.traceId in
    (SELECT traceId
     FROM `otel-v1-apm-span-000001`
     WHERE serviceName = `order`)
```

Migrieren Sie zu PPL

Syntax des Join-Befehls

```
SEARCH source=<left-table>
| <other piped command>
| [joinType] JOIN
    [leftAlias]
    ON joinCriteria
    <right-table>
```

```
| <other piped command>
```

Umschreiben

```
SEARCH source=otel-v1-apm-span-000001
| WHERE serviceName = 'order'
| JOIN left=t1 right=t2
    ON t1.traceId = t2.traceId AND t2.serviceName = 'order'
    otel-v1-apm-span-000001 -- self inner join
| EVAL s_name = t1.name -- rename to avoid ambiguous
| EVAL s_parentSpanId = t1.parentSpanId -- RENAME command would be better when it is
 supported
| EVAL s_durationInNanos = t1.durationInNanos
| FIELDS s_name, s_parentSpanId, s_durationInNanos -- reduce colunms in join
| LEFT JOIN left=s1 right=t3
    ON s_name = t3.target.resource AND t3.serviceName = 'order' AND t3.traceGroupName =
 'client_cancel_order'
    otel-v1-apm-service-map
| WHERE (s_parentSpanId IS NOT NULL OR (s_parentSpanId IS NULL AND s_name =
 'client_cancel_order'))
| STATS avg(s_durationInNanos) -- no need to add alias if there is no ambiguous
```

Verbindungstyp

- Syntax: `INNER | LEFT OUTER | CROSS`
- Optional
- Der Typ der auszuführenden Verknüpfung. Die Standardeinstellung ist `INNER` wenn nicht angegeben.

Linker Alias

- Syntax: `left = <leftAlias>`
- Optional
- Der Alias der Unterabfrage, der mit der linken Join-Seite verwendet werden soll, um mehrdeutige Benennungen zu vermeiden.

Verbindungskriterien

- Syntax: `<expression>`

- Erforderlich
- Die Syntax beginnt mit. `ON` Es könnte ein beliebiger Vergleichsausdruck sein. Im Allgemeinen sehen die Verbindungskriterien wie folgt aus`<leftAlias>.<leftField>=<rightAlias>.<rightField>`.

  Beispiel: `l.id = r.id`. Wenn das Join-Kriterium mehrere Bedingungen enthält, können Sie zwischen jedem Vergleichsausdruck einen `OR` Operator angeben`AND`. Beispiel, `l.id = r.id AND l.email = r.email AND (r.age > 65 OR r.age < 18)`.

Weitere Beispiele

Migration von einer SQL-Abfrage (TPC-H Q13):

```
SELECT c_count, COUNT(*) AS custdist
FROM
  ( SELECT c_custkey, COUNT(o_orderkey) c_count
    FROM customer LEFT OUTER JOIN orders ON c_custkey = o_custkey
        AND o_comment NOT LIKE '%unusual%packages%'
    GROUP BY c_custkey
  ) AS c_orders
GROUP BY c_count
ORDER BY custdist DESC, c_count DESC;
```

Mit der PPL-Join-Abfrage neu geschrieben:

```
SEARCH source=customer
| FIELDS c_custkey
| LEFT OUTER JOIN
    ON c_custkey = o_custkey AND o_comment NOT LIKE '%unusual%packages%'
    orders
| STATS count(o_orderkey) AS c_count BY c_custkey
| STATS count() AS custdist BY c_count
| SORT - custdist, - c_count
```

Einschränkung: Untersuchen werden in Join Right Side nicht unterstützt.

Wenn Teilsuchen unterstützt werden, können Sie die obige PPL-Abfrage wie folgt umschreiben:

```
SEARCH source=customer
| FIELDS c_custkey
```

```
| LEFT OUTER JOIN
   ON c_custkey = o_custkey
   [
      SEARCH source=orders
      | WHERE o_comment NOT LIKE '%unusual%packages%'
      | FIELDS o_orderkey, o_custkey
   ]
| STATS count(o_orderkey) AS c_count BY c_custkey
| STATS count() AS custdist BY c_count
| SORT - custdist, - c_count
```

Lookup-Befehl

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen PPL-Befehl unterstützen, finden Sie unter. the section called “Befehle”

Verwenden Sie den `lookup` Befehl, um Ihre Suchdaten anzureichern, indem Sie Daten aus einem Nachschlageindex (Dimensionstabelle) hinzufügen oder ersetzen. Mit diesem Befehl können Sie Felder eines Index mit Werten aus einer Dimensionstabelle erweitern. Sie können ihn auch verwenden, um Werte anzuhängen oder zu ersetzen, wenn die Suchbedingungen erfüllt sind. Der `lookup` Befehl eignet sich besser als der `Join` Befehl, um Quelldaten mit einem statischen Datensatz anzureichern.

Syntax

Verwenden Sie die folgende Syntax:

```
SEARCH source=<sourceIndex>
| <other piped command>
| LOOKUP <lookupIndex> (<lookupMappingField> [AS <sourceMappingField>])...
    [(REPLACE | APPEND) (<inputField> [AS <outputField>])...]
| <other piped command>
```

LookupIndex

- Erforderlich
- Der Name des Nachschlageindex (Dimensionstabelle).

lookupMappingField

- Erforderlich
- Ein Zuordnungsschlüssel im Lookup-Index, analog zu einem Join-Schlüssel aus der rechten Tabelle. Sie können mehrere Felder angeben, die durch Kommas getrennt sind.

sourceMappingField

- Optional.
- Standard: < lookupMappingField >.
- Ein Zuordnungsschlüssel aus der Quellabfrage, analog zu einem Join-Schlüssel von der linken Seite.

Eingabefeld

- Optional.
- Standard: Alle Felder des Lookup-Index, in denen übereinstimmende Werte gefunden wurden.
- Ein Feld im Nachschlageindex, in dem übereinstimmende Werte auf die Ergebnisausgabe angewendet werden. Sie können mehrere Felder angeben, die durch Kommas getrennt sind.

Ausgabefeld

- Optional.
- Standard: <inputField>.
- Ein Feld in der Ausgabe. Sie können mehrere Ausgabefelder angeben. Wenn Sie einen vorhandenen Feldnamen aus der Quellabfrage angeben, werden seine Werte durch übereinstimmende Werte aus InputField ersetzt oder angefügt. Wenn Sie einen neuen Feldnamen angeben, wird dieser den Ergebnissen hinzugefügt.

ERSETZEN | ANHÄNGEN

- Optional.
- Standard: REPLACE
- Gibt an, wie mit übereinstimmenden Werten umgegangen werden soll. Wenn Sie REPLACE angeben, <lookupIndex>überschreiben übereinstimmende Werte im Feld die Werte im Ergebnis.

Wenn Sie angebenAPPEND, werden übereinstimmende Werte im <lookupIndex>Feld nur an die fehlenden Werte im Ergebnis angehängt.

Verwendung

- <lookupIndex>ID ALS CID NACHSCHLAGEN, E-Mail ALS E-Mail ERSETZEN
- <lookupIndex>NAME NACHSCHLAGEN E-Mail ALS E-Mail ERSETZEN
- <lookupIndex>LOOKUP-ID ALS CID, Name, Adresse ANFÜGEN, E-Mail ALS E-Mail
- <lookupIndex>LOOKUP-ID

Beispiel

Sehen Sie sich die folgenden Beispiele an.

```
SEARCH source=<sourceIndex>
| WHERE orderType = 'Cancelled'
| LOOKUP account_list, mkt_id AS mkt_code REPLACE amount, account_name AS name
| STATS count(mkt_code), avg(amount) BY name
```

```
SEARCH source=<sourceIndex>
| DEDUP market_id
| EVAL category=replace(category, "-", ".")
| EVAL category=ltrim(category, "dvp.")
| LOOKUP bounce_category category AS category APPEND classification
```

```
SEARCH source=<sourceIndex>
| LOOKUP bounce_category category
```

Befehl parse

Der `parse` Befehl analysiert ein Textfeld mit einem regulären Ausdruck und hängt das Ergebnis an das Suchergebnis an.

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen PPL-Befehl unterstützen, finden Sie unter. the section called “Befehle”

Syntax

Verwenden Sie die folgende Syntax:

```
parse <field> <pattern>
```

`field`

- Zwingend erforderlich.
- Das Feld muss ein Textfeld sein.

`pattern`

- Obligatorische Zeichenfolge.
- Dies ist das Muster für reguläre Ausdrücke, das verwendet wird, um neue Felder aus dem angegebenen Textfeld zu extrahieren.
- Wenn bereits ein neuer Feldname vorhanden ist, ersetzt er das ursprüngliche Feld.

Regulärer Ausdruck

Das Muster für reguläre Ausdrücke wird verwendet, um das gesamte Textfeld jedes Dokuments mit der Java-Regex-Engine abzugleichen. Jede benannte Capture-Gruppe im Ausdruck wird zu einem neuen `STRING` Feld.

Beispiel 1: Erstellen Sie ein neues Feld

Das Beispiel zeigt, wie `host` für jedes Dokument ein neues Feld erstellt wird. `host`wird der Hostname danach `@` im `email` Feld sein. Die Analyse eines Nullfeldes gibt eine leere Zeichenfolge zurück.

PPL-Abfrage:

```
os> source=accounts | parse email '.+@(?<host>.+)' | fields email, host ;
fetched rows / total rows = 4/4
+----------------------+-------------+
| email                | host        |
|----------------------+-------------|
| jane_doe@example.com  | example.com |
| john_doe@example.net  | example.net |
| null                 |             |
```

```
| juan_li@example.org   | example.org |
+-----------------------+-------------+
```

Beispiel 2: Überschreiben Sie ein vorhandenes Feld

Das Beispiel zeigt, wie das vorhandene `address` Feld überschrieben wird, wobei die Hausnummer entfernt wird.

PPL-Abfrage:

```
os> source=accounts | parse address '\d+ (?<address>.+)' | fields address ;
fetched rows / total rows = 4/4
+------------------+
| address          |
|------------------|
| Example Lane     |
| Example Street   |
| Example Avenue   |
| Example Court    |
+------------------+
```

Beispiel 3: Filtern und sortieren Sie nach einem gecasteten, analysierten Feld

Das Beispiel zeigt, wie Straßennummern sortiert werden, die in dem `address` Feld höher als 500 sind.

PPL-Abfrage:

```
os> source=accounts | parse address '(?<streetNumber>\d+) (?<street>.+)' | where
 cast(streetNumber as int) > 500 | sort num(streetNumber) | fields streetNumber,
 street ;
fetched rows / total rows = 3/3
+----------------+----------------+
| streetNumber   | street         |
|----------------+----------------|
| ***            | Example Street |
| ***            | Example Avenue |
| 880            | Example Lane   |
+----------------+----------------+
```

Einschränkungen

Der Parse-Befehl weist einige Einschränkungen auf:

- Durch Parse definierte Felder können nicht erneut analysiert werden.

  Der folgende Befehl funktioniert nicht:

  ```
  source=accounts | parse address '\d+ (?<street>.+)' | parse street '\w+ (?<road>\w+)'
  ```

- Durch Parse definierte Felder können nicht mit anderen Befehlen überschrieben werden.

  `where`passt zu keinem Dokument, da es nicht überschrieben `street` werden kann:

  ```
  source=accounts | parse address '\d+ (?<street>.+)' | eval street='1' | where
   street='1' ;
  ```

- Das von parse verwendete Textfeld kann nicht überschrieben werden.

  `street`wird nicht erfolgreich analysiert, da es überschrieben wird: `address`

  ```
  source=accounts | parse address '\d+ (?<street>.+)' | eval address='1' ;
  ```

- Durch Parse definierte Felder können nicht gefiltert oder sortiert werden, nachdem sie im Befehl verwendet wurden. `stats`

  `where`im folgenden Befehl funktioniert nicht:

  ```
  source=accounts | parse email '.+@(?<host>.+)' | stats avg(age) by host | where
   host=pyrami.com ;
  ```

Befehl „Muster“

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen PPL-Befehl unterstützen, finden Sie unter. the section called “Befehle”

Der `patterns` Befehl extrahiert Protokollmuster aus einem Textfeld und fügt die Ergebnisse an das Suchergebnis an. Durch die Gruppierung von Protokollen nach ihren Mustern ist es einfacher, Statistiken aus großen Mengen von Protokolldaten zur Analyse und Fehlerbehebung zu aggregieren.

Syntax

Verwenden Sie die folgende Syntax:

```
patterns [new_field=<new-field-name>] [pattern=<pattern>] <field>
```

new-field-name

- Optionale Zeichenfolge.
- Dies ist der Name des neuen Felds für extrahierte Muster.
- Der Standardwert ist `patterns_field`.
- Wenn der Name bereits existiert, ersetzt er das ursprüngliche Feld.

pattern

- Optionale Zeichenfolge.
- Dies ist das Regex-Muster von Zeichen, die aus dem Textfeld herausgefiltert werden sollen.
- Falls nicht, besteht das Standardmuster aus alphanumerischen Zeichen (). `[a-zA-Z\d]`

field

- Zwingend erforderlich.
- Das Feld muss ein Textfeld sein.

Beispiel 1: Erstellen Sie das neue Feld

Das Beispiel zeigt, wie in `email` jedem Dokument extraktierte Satzzeichen verwendet werden. Beim Analysieren eines Nullfeldes wird eine leere Zeichenfolge zurückgegeben.

PPL-Abfrage:

```
os> source=accounts | patterns email | fields email, patterns_field ;
fetched rows / total rows = 4/4
+----------------------+------------------+
| email                | patterns_field   |
|----------------------+------------------|
| jane_doe@example.com  | @.               |
| john_doe@example.net  | @.               |
| null                 |                  |
| juan_li@example.org   | @.               |
```

```
+----------------------+-----------------+
```

Beispiel 2: Extrahieren von Protokollmustern

Das Beispiel zeigt, wie Interpunktionen mithilfe der Standardmuster aus einem unformatierten Protokollfeld extrahiert werden.

PPL-Abfrage:

```
os> source=apache | patterns message | fields message, patterns_field ;
fetched rows / total rows = 4/4
+-----------------------------------------------------------------------------------------------------
+---------------------------------+
| message
                                       | patterns_field                 |
|-----------------------------------------------------------------------------------------------------
+---------------------------------|
| 177.95.8.74 - upton5450 [28/Sep/2022:10:15:57 -0700] "HEAD /e-business/mindshare
 HTTP/1.0" 404 19927                         | ... -  [//::: -] " /-/ /."      |
| ************ - pouros8756 [28/Sep/2022:10:15:57 -0700] "GET /architectures/
convergence/niches/mindshare HTTP/1.0" 100 28722 | ... -  [//::: -] " //// /."     |
| *************** - - [28/Sep/2022:10:15:57 -0700] "PATCH /strategize/out-of-the-box
 HTTP/1.0" 401 27439                        | ... - - [//::: -] " //--- /."   |
| ************** - - [28/Sep/2022:10:15:57 -0700] "POST /users HTTP/1.1" 301 9481
                                       | ... - - [//::: -] " / /."       |
+-----------------------------------------------------------------------------------------------------
+---------------------------------+
```

Beispiel 3: Extrahieren Sie Protokollmuster mit einem benutzerdefinierten Regex-Muster

Das Beispiel zeigt, wie Interpunktionen mithilfe benutzerdefinierter Muster aus einem unformatierten Protokollfeld extrahiert werden.

PPL-Abfrage:

```
os> source=apache | patterns new_field='no_numbers' pattern='[0-9]' message | fields
 message, no_numbers ;
fetched rows / total rows = 4/4
+-----------------------------------------------------------------------------------------------------
+-------------------------------------------------------------------------------
+
```

```
| message
                                    | no_numbers
                                    |
|-----------------------------------------------------------------------------------------------
+-------------------------------------------------------------------------------|
| 177.95.8.74 - upton5450 [28/Sep/2022:10:15:57 -0700] "HEAD /e-business/mindshare
 HTTP/1.0" 404 19927                       | ... - upton [/Sep/::: -] "HEAD /e-
business/mindshare HTTP/."                          |
| 127.45.152.6 - pouros8756 [28/Sep/2022:10:15:57 -0700] "GET /architectures/
convergence/niches/mindshare HTTP/1.0" 100 28722 | ... - pouros [/Sep/::: -] "GET /
architectures/convergence/niches/mindshare HTTP/."   |
| *************** - - [28/Sep/2022:10:15:57 -0700] "PATCH /strategize/out-of-the-box
 HTTP/1.0" 401 27439                      | ... - - [/Sep/::: -] "PATCH /strategize/
out-of-the-box HTTP/."                         |
| ************** - - [28/Sep/2022:10:15:57 -0700] "POST /users HTTP/1.1" 301 9481
                                    | ... - - [/Sep/::: -] "POST /users HTTP/."
                                    |
+-----------------------------------------------------------------------------------------------
+-------------------------------------------------------------------------------
+
```

Einschränkung

Der Befehl patterns hat dieselben Einschränkungen wie der Befehl parse.

seltener Befehl

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen PPL-Befehl unterstützen, finden Sie unter. the section called “Befehle”

Verwenden Sie den `rare` Befehl, um das am wenigsten gemeinsame Wertetupel aller Felder in der Feldliste zu finden.

> **Note**
>
> Für jedes einzelne Wertetupel der Gruppierungsfelder werden maximal 10 Ergebnisse zurückgegeben.

Syntax

Verwenden Sie die folgende Syntax:

```
rare [N] <field-list> [by-clause] rare_approx [N] <field-list> [by-clause]
```

Feldliste

- Zwingend erforderlich.
- Eine kommagetrennte Liste von Feldnamen.

Nebenklausel

- Optional.
- Ein oder mehrere Felder, nach denen die Ergebnisse gruppiert werden sollen.

N

- Die Anzahl der zurückzugebenden Ergebnisse.
- Standard: 10

selten_ca

- Die ungefähre Anzahl der seltenen (n) Felder unter Verwendung des Algorithmus „Geschätzte Kardinalität nach ++“. HyperLogLog

Beispiel 1: Finden Sie die am wenigsten gemeinsamen Werte in einem Feld

In diesem Beispiel wird das am wenigsten gemeinsame Geschlecht aller Konten ermittelt.

PPL-Abfrage:

```
os> source=accounts | rare gender;
os> source=accounts | rare_approx 10 gender;
os> source=accounts | rare_approx gender;
fetched rows / total rows = 2/2
+----------+
| gender   |
```

```
|----------|
| F        |
| M        |
+----------+
```

Beispiel 2: Finden Sie die am wenigsten gemeinsamen Werte, geordnet nach Geschlecht

In diesem Beispiel wird das Alter aller nach Geschlecht gruppierten Konten ermittelt, das am seltensten vorkommt.

PPL-Abfrage:

```
os> source=accounts | rare 5 age by gender;
os> source=accounts | rare_approx 5 age by gender;
fetched rows / total rows = 4/4
+----------+-------+
| gender   | age   |
|----------+-------|
| F        | 28    |
| M        | 32    |
| M        | 33    |
| M        | 36    |
+----------+-------+
```

Befehl umbenennen

Verwenden Sie den `rename` Befehl, um die Namen eines oder mehrerer Felder im Suchergebnis zu ändern.

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen PPL-Befehl unterstützen, finden Sie unter. the section called “Befehle”

Syntax

Verwenden Sie die folgende Syntax:

```
rename <source-field> AS <target-field>["," <source-field> AS <target-field>]...
```

Quellfeld

- Zwingend erforderlich.
- Dies ist der Name des Feldes, das Sie umbenennen möchten.

Zielfeld

- Zwingend erforderlich.
- Dies ist der Name, in den Sie umbenennen möchten.

Beispiel 1: Benennen Sie ein Feld um

Dieses Beispiel zeigt, wie ein einzelnes Feld umbenannt wird.

PPL-Abfrage:

```
os> source=accounts | rename account_number as an | fields an;
fetched rows / total rows = 4/4
+------+
| an   |
|------|
| 1    |
| 6    |
| 13   |
| 18   |
+------+
```

Beispiel 2: Benennen Sie mehrere Felder um

Dieses Beispiel zeigt, wie mehrere Felder umbenannt werden.

PPL-Abfrage:

```
os> source=accounts | rename account_number as an, employer as emp | fields an, emp;
fetched rows / total rows = 4/4
+------+---------+
| an   | emp     |
|------+---------|
| 1    | Pyrami  |
| 6    | Netagy  |
| 13   | Quility |
```

```
| 18   | null    |
+------+---------+
```

Einschränkungen

- Das Überschreiben eines vorhandenen Felds wird nicht unterstützt:

```
source=accounts | grok address '%{NUMBER} %{GREEDYDATA:address}' | fields address
```

Suchbefehl

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen PPL-Befehl unterstützen, finden Sie unter. the section called “Befehle”

Verwenden Sie den `search` Befehl, um Dokumente aus einem Index abzurufen. Der `search` Befehl kann nur als erster Befehl in einer PPL-Abfrage verwendet werden.

Syntax

Verwenden Sie die folgende Syntax:

```
search source=[<remote-cluster>:]<index> [boolean-expression]
```

search

- Optional.
- Suchschlüsselwörter, die weggelassen werden können.

index

- Zwingend erforderlich.
- Der Suchbefehl muss angeben, aus welchem Index abgefragt werden soll.
- Bei clusterübergreifenden Suchen kann dem Indexnamen ein Präfix `<cluster name>:` vorangestellt werden.

boolischer Ausdruck

- Optional.
- Jeder Ausdruck, der einen booleschen Wert ergibt.

Beispiel 1: Alle Daten abrufen

Das Beispiel zeigt, wie das gesamte Dokument aus dem Kontoindex abgerufen werden kann.

PPL-Abfrage:

```
os> source=accounts;
+------------------+-------------+----------------------+-----------+----------
+--------+----------------+---------+-------+-----------------------+------------+
| account_number   | firstname   | address              | balance   | gender   | city
 | employer       | state   | age   | email                 | lastname   |
|------------------+-------------+----------------------+-----------+----------
+--------+----------------+---------+-------+-----------------------+------------|
| 1                | Jorge       | *** Any Lane         | 39225     | M        | Brogan
 | ExampleCorp    | IL      | 32    | jane_doe@example.com  | Souza      |
| 6                | John        | *** Example Street   | 5686      | M        | Dante
 | AnyCorp        | TN      | 36    | john_doe@example.com  | Doe        |
| 13               | Jane        | *** Any Street       | *****     | F        | Nogal
 | ExampleCompany | VA      | 28    | null                  | Doe        |
| 18               | Juan        | *** Example Court    | 4180      | M        | Orick
 | null           | MD      | 33    | juan_li@example.org   | Li         |
+------------------+-------------+----------------------+-----------+----------
+--------+----------------+---------+-------+-----------------------+------------+
```

Beispiel 2: Daten mit Bedingung abrufen

Das Beispiel zeigt das Abrufen des gesamten Dokuments aus dem Kontoindex mit.

PPL-Abfrage:

```
os> SEARCH source=accounts account_number=1 or gender="F";
+------------------+-------------+--------------------+-----------+----------+--------
+----------------+---------+-------+-----------------------+------------+
| account_number   | firstname   | address            | balance   | gender   | city   |
 employer       | state   | age   | email                 -  | lastname   |
```

```
|-----------------+-------------+--------------------+-----------+----------+--------
+----------------+---------+-------+-----------------------+------------|
| 1                | Jorge       | *** Any Lane       | *****     | M        | Brogan |
 ExampleCorp    | IL      | 32    | jorge_souza@example.com | Souza      |
| 13               | Jane        | *** Any Street     | *****     | F        | Nogal  |
 ExampleCompany | VA      | 28    | null                    | Doe        |
+-----------------+-------------+--------------------+-----------+----------+--------
+-----------------+---------+-------+-----------------------+------------+
```

Befehl sort

Verwenden Sie den `sort` Befehl, um das Suchergebnis nach bestimmten Feldern zu sortieren.

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen PPL-Befehl unterstützen, finden Sie unter. the section called “Befehle”

Syntax

Verwenden Sie die folgende Syntax:

```
sort <[+|-] sort-field>...
```

[+|-]

- Optional.
- Das Plus [+] steht für eine aufsteigende Reihenfolge, bei NULL/MISSING der die Werte an erster Stelle stehen.
- Das Minus [-] steht für absteigende Reihenfolge, wobei die NULL/MISSING Werte zuletzt stehen.
- Standard: Aufsteigende Reihenfolge, wobei die NULL/MISSING Werte an erster Stelle stehen.

Sortierfeld

- Zwingend erforderlich.
- Das für die Sortierung verwendete Feld.

Beispiel 1: Sortiert nach einem Feld

Das Beispiel zeigt, wie das Dokument mit dem Altersfeld in aufsteigender Reihenfolge sortiert wird.

PPL-Abfrage:

```
os> source=accounts | sort age | fields account_number, age;
fetched rows / total rows = 4/4
+------------------+-------+
| account_number   | age   |
|------------------+-------|
| 13               | 28    |
| 1                | 32    |
| 18               | 33    |
| 6                | 36    |
+------------------+-------+
```

Beispiel 2: Sortiere nach einem Feld und gib alle Ergebnisse zurück

Das Beispiel zeigt, wie das Dokument mit dem Altersfeld in aufsteigender Reihenfolge sortiert wird.

PPL-Abfrage:

```
os> source=accounts | sort age | fields account_number, age;
fetched rows / total rows = 4/4
+------------------+-------+
| account_number   | age   |
|------------------+-------|
| 13               | 28    |
| 1                | 32    |
| 18               | 33    |
| 6                | 36    |
+------------------+-------+
```

Beispiel 3: Sortiert nach einem Feld in absteigender Reihenfolge

Das Beispiel zeigt, wie das Dokument mit dem Altersfeld in absteigender Reihenfolge sortiert wird.

PPL-Abfrage:

```
os> source=accounts | sort - age | fields account_number, age;
fetched rows / total rows = 4/4
+------------------+-------+
```

```
| account_number   | age   |
|------------------+-------|
| 6                | 36    |
| 18               | 33    |
| 1                | 32    |
| 13               | 28    |
+------------------+-------+
```

Beispiel 4: Nach mehreren Feldern sortieren

Das Beispiel zeigt, wie das Dokument mit dem Geschlechtsfeld in aufsteigender Reihenfolge und dem Altersfeld in absteigender Reihenfolge sortiert wird.

PPL-Abfrage:

```
os> source=accounts | sort + gender, - age | fields account_number, gender, age;
fetched rows / total rows = 4/4
+------------------+----------+-------+
| account_number   | gender   | age   |
|------------------+----------+-------|
| 13               | F        | 28    |
| 6                | M        | 36    |
| 18               | M        | 33    |
| 1                | M        | 32    |
+------------------+----------+-------+
```

Beispiel 5: Nach Feld sortieren, Nullwert enthalten

Das Beispiel zeigt, wie das Arbeitgeberfeld nach der Standardoption sortiert wird (aufsteigende Reihenfolge und Null zuerst). Das Ergebnis zeigt, dass der Nullwert in der ersten Zeile steht.

PPL-Abfrage:

```
os> source=accounts | sort employer | fields employer;
fetched rows / total rows = 4/4
+------------+
| employer   |
|------------|
| null       |
| AnyCompany |
| AnyCorp    |
| AnyOrgty   |
```

```
+------------+
```

Befehl stats

Verwenden Sie den `stats` Befehl, um die Aggregation anhand des Suchergebnisses zu berechnen.

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen PPL-Befehl unterstützen, finden Sie unter. the section called “Befehle”

Behandlung von NULL-/FEHLENDEN Werten

Behandlung von NULL-/FEHLENDEN Werten

Funktion	NULL	MISSING
COUNT	Nicht gezählt	Nicht gezählt
SUM	Ignore	Ignore
AVG	Ignore	Ignore
MAX	Ignore	Ignore
MIN	Ignore	Ignore

Syntax

Verwenden Sie die folgende Syntax:

```
stats <aggregation>... [by-clause]
```

Aggregation

- Zwingend erforderlich.
- Eine Aggregationsfunktion, die auf ein Feld angewendet wird.

Nebenklausel

- Optional.
- Syntax: `by [span-expression,] [field,]...`
- Gibt Felder und Ausdrücke für die Gruppierung der Aggregationsergebnisse an. Die Nebenklausel ermöglicht es Ihnen, Ihre Aggregationsergebnisse mithilfe von Feldern und Ausdrücken zu gruppieren. Sie können Skalarfunktionen, Aggregationsfunktionen und sogar Span-Ausdrücke verwenden, um bestimmte Felder in Gruppen mit gleichen Intervallen aufzuteilen.
- Standard: Wenn kein Wert angegeben `<by-clause>` ist, gibt der Befehl stats eine einzelne Zeile zurück, die die Aggregation über die gesamte Ergebnismenge darstellt.

Span-Ausdruck

- Fakultativ, höchstens einer.
- Syntax: `span(field_expr, interval_expr)`
- Die Einheit des Intervallausdrucks ist standardmäßig die natürliche Einheit. Wenn es sich bei dem Feld um ein Feld vom Typ Datum und Uhrzeit handelt und das Intervall in date/time Einheiten angegeben ist, geben Sie die Einheit im Intervallausdruck an.
- Wenn Sie das `age` Feld beispielsweise nach 10 Jahren in Bereiche aufteilen, sieht das so aus. `span(age, 10)` Um ein Zeitstempelfeld in stündliche Intervalle aufzuteilen, verwenden Sie. `span(timestamp, 1h)`

Verfügbare Zeiteinheiten

Einheiten für das Spanenintervall
Millisekunde (ms)
Sekunde (n)
Minute (m, Groß- und Kleinschreibung beachten)
Stunde (h)
Tag (d)
Woche (w)

Einheiten für das Spanenintervall
Monat (M, Groß- und Kleinschreibung beachten)
Quartal (q)
Jahr (y)

Aggregationsfunktionen

COUNT

Gibt die Anzahl der Ausdrücke in den Zeilen zurück, die mit einer SELECT-Anweisung abgerufen wurden.

Beispiel:

```
os> source=accounts | stats count();
fetched rows / total rows = 1/1
+-----------+
| count()   |
|-----------|
| 4         |
+-----------+
```

SUM

Wird verwendet`SUM(expr)`, um die Summe der Ausdrücke zurückzugeben.

Beispiel

```
os> source=accounts | stats sum(age) by gender;
fetched rows / total rows = 2/2
+------------+----------+
| sum(age)   | gender   |
|------------+----------|
| 28         | F        |
| 101        | M        |
+------------+----------+
```

AVG

Wird verwendet`AVG(expr)`, um den Durchschnittswert von expr zurückzugeben.

Beispiel

```
os> source=accounts | stats avg(age) by gender;
fetched rows / total rows = 2/2
+--------------------+----------+
| avg(age)           | gender   |
|--------------------+----------|
| 28.0               | F        |
| 33.666666666666664 | M        |
+--------------------+----------+
```

MAX

Wird verwendet`MAX(expr)`, um den Maximalwert von expr zurückzugeben.

Beispiel

```
os> source=accounts | stats max(age);
fetched rows / total rows = 1/1
+------------+
| max(age)   |
|------------|
| 36         |
+------------+
```

MIN

Wird verwendet`MIN(expr)`, um den Minimalwert von expr zurückzugeben.

Beispiel

```
os> source=accounts | stats min(age);
fetched rows / total rows = 1/1
+------------+
| min(age)   |
|------------|
| 28         |
+------------+
```

STDDEV_SAMP

Wird verwendet`STDDEV_SAMP(expr)`, um die Standardabweichung der Stichprobe von expr zurückzugeben.

Beispiel:

```
os> source=accounts | stats stddev_samp(age);
fetched rows / total rows = 1/1
+--------------------+
| stddev_samp(age)   |
|--------------------|
| 3.304037933599835  |
+--------------------+
```

STDDEV_POP

Wird verwendet`STDDEV_POP(expr)`, um die Standardabweichung der Grundgesamtheit von Expr zurückzugeben.

Beispiel:

```
os> source=accounts | stats stddev_pop(age);
fetched rows / total rows = 1/1
+--------------------+
| stddev_pop(age)    |
|--------------------|
| 2.***************** |
+--------------------+
```

DAUERN

Wird verwendet`TAKE(field [, size])`, um die ursprünglichen Werte eines Felds zurückzugeben. Es garantiert nicht die Reihenfolge der Werte.

field

- Zwingend erforderlich.
- Das Feld muss ein Textfeld sein.

size

- Optionale Ganzzahl.

- Die Anzahl der Werte sollte zurückgegeben werden.
- Die Standardeinstellung ist 10.

Beispiel

```
os> source=accounts | stats take(firstname);
fetched rows / total rows = 1/1
+-----------------------------+
| take(firstname)             |
|-----------------------------|
| [Jane, Mary, Nikki, Juan    |
+-----------------------------+
```

PERCENTILE oder PERCENTILE_APPROX

Verwenden Sie `PERCENTILE(expr, percent)` oder`PERCENTILE_APPROX(expr, percent)`, um den ungefähren Perzentilwert von expr zum angegebenen Prozentsatz zurückzugeben.

Prozent

- Die Zahl muss eine Konstante zwischen 0 und 100 sein.

Beispiel

```
os> source=accounts | stats percentile(age, 90) by gender;
fetched rows / total rows = 2/2
+-----------------------+----------+
| percentile(age, 90)   | gender   |
|-----------------------+----------|
| 28                    | F        |
| 36                    | M        |
+-----------------------+----------+
```

Beispiel 1: Berechne die Anzahl der Ereignisse

Das Beispiel zeigt, wie die Anzahl der Ereignisse in den Konten berechnet wird.

```
os> source=accounts | stats count();
fetched rows / total rows = 1/1
```

```
+-----------+
| count()   |
|-----------|
| 4         |
+-----------+
```

Beispiel 2: Den Durchschnitt eines Felds berechnen

Das Beispiel zeigt, wie das Durchschnittsalter für alle Konten berechnet wird.

```
os> source=accounts | stats avg(age);
fetched rows / total rows = 1/1
+------------+
| avg(age)   |
|------------|
| 32.25      |
+------------+
```

Beispiel 3: Berechnet den Durchschnitt eines Felds nach Gruppen

Das Beispiel zeigt, wie das Durchschnittsalter für alle Konten, gruppiert nach Geschlecht, berechnet wird.

```
os> source=accounts | stats avg(age) by gender;
fetched rows / total rows = 2/2
+--------------------+----------+
| avg(age)           | gender   |
|--------------------+----------|
| 28.0               | F        |
| 33.666666666666664 | M        |
+--------------------+----------+
```

Beispiel 4: Berechnet den Durchschnitt, die Summe und die Anzahl eines Felds nach Gruppen

Das Beispiel zeigt, wie das Durchschnittsalter, das Gesamtalter und die Anzahl der Ereignisse für alle Konten, gruppiert nach Geschlecht, berechnet werden.

```
os> source=accounts | stats avg(age), sum(age), count() by gender;
fetched rows / total rows = 2/2
+--------------------+------------+-----------+----------+
| avg(age)           | sum(age)   | count()   | gender   |
|--------------------+------------+-----------+----------|
```

```
| 28.0               | 28         | 1          | F        |
| 33.666666666666664 | 101        | 3          | M        |
+--------------------+------------+------------+----------+
```

Beispiel 5: Berechnet das Maximum eines Felds

Das Beispiel berechnet das Höchstalter für alle Konten.

```
os> source=accounts | stats max(age);
fetched rows / total rows = 1/1
+------------+
| max(age)   |
|------------|
| 36         |
+------------+
```

Beispiel 6: Berechnet das Maximum und das Minimum eines Felds nach Gruppen

Das Beispiel berechnet die Werte für das Höchst- und Mindestalter für alle Konten, gruppiert nach Geschlecht.

```
os> source=accounts | stats max(age), min(age) by gender;
fetched rows / total rows = 2/2
+------------+------------+----------+
| max(age)   | min(age)   | gender   |
|------------+------------+----------|
| 28         | 28         | F        |
| 36         | 32         | M        |
+------------+------------+----------+
```

Beispiel 7: Berechnet die eindeutige Anzahl eines Felds

Um die Anzahl der unterschiedlichen Werte eines Felds zu ermitteln, können Sie stattdessen die Funktion `DISTINCT_COUNT` (oder`DC`) verwenden`COUNT`. In diesem Beispiel werden sowohl die Anzahl als auch die eindeutige Anzahl der Geschlechter aller Konten berechnet.

```
os> source=accounts | stats count(gender), distinct_count(gender);
fetched rows / total rows = 1/1
+-----------------+--------------------------+
| count(gender)   | distinct_count(gender)   |
|-----------------+--------------------------|
| 4               | 2                        |
```

```
+-----------------+--------------------------+
```

Beispiel 8: Berechnet die Anzahl anhand einer Spanne

Im Beispiel wird die Anzahl der Altersstufen im Intervall von 10 Jahren berechnet.

```
os> source=accounts | stats count(age) by span(age, 10) as age_span
fetched rows / total rows = 2/2
+--------------+------------+
| count(age)   | age_span   |
|--------------+------------|
| 1            | 20         |
| 3            | 30         |
+--------------+------------+
```

Beispiel 9: Berechnet die Anzahl anhand eines Geschlechts und einer Spanne

In diesem Beispiel werden Datensätze gezählt, die nach Geschlecht und Alter gruppiert sind, und zwar über einen Zeitraum von 5 Jahren.

```
os> source=accounts | stats count() as cnt by span(age, 5) as age_span, gender
fetched rows / total rows = 3/3
+-------+------------+----------+
| cnt   | age_span   | gender   |
|-------+------------+----------|
| 1     | 25         | F        |
| 2     | 30         | M        |
| 1     | 35         | M        |
+-------+------------+----------+
```

Der Span-Ausdruck wird immer als erster Gruppierungsschlüssel angezeigt, unabhängig von der im Befehl angegebenen Reihenfolge.

```
os> source=accounts | stats count() as cnt by gender, span(age, 5) as age_span
fetched rows / total rows = 3/3
+-------+------------+----------+
| cnt   | age_span   | gender   |
|-------+------------+----------|
| 1     | 25         | F        |
| 2     | 30         | M        |
| 1     | 35         | M        |
+-------+------------+----------+
```

Beispiel 10: Berechnet die Anzahl und ruft die E-Mail-Liste nach Geschlecht und Spanne ab

Im Beispiel wird die Anzahl der Altersgruppen im Intervall von 10 Jahren ermittelt und nach Geschlecht gruppiert. Zusätzlich wird für jede Zeile eine Liste mit maximal 5 E-Mails abgerufen.

```
os> source=accounts | stats count() as cnt, take(email, 5) by span(age, 5) as age_span,
 gender
fetched rows / total rows = 3/3
+-------+-----------------------------------------------------+------------+----------+
| cnt   | take(email, 5)                                      | age_span   | gender   |
|-------+-----------------------------------------------------+------------+----------|
| 1     | []                                                  | 25         | F        |
| 2     | [janedoe@anycompany.com,juanli@examplecompany.org] | 30         | M        |
| 1     | [marymajor@examplecorp.com]                         | 35         | M        |
+-------+-----------------------------------------------------+------------+----------+
```

Beispiel 11: Berechnet das Perzentil eines Feldes

Das Beispiel zeigt, wie das Perzentil des 90. Alters aller Konten berechnet wird.

```
os> source=accounts | stats percentile(age, 90);
fetched rows / total rows = 1/1
+-----------------------+
| percentile(age, 90)   |
|-----------------------|
| 36                    |
+-----------------------+
```

Beispiel 12: Berechnet das Perzentil eines Felds nach Gruppen

Das Beispiel zeigt, wie der Perzentil für das 90. Lebensjahr aller nach Geschlecht gruppierten Konten berechnet wird.

```
os> source=accounts | stats percentile(age, 90) by gender;
fetched rows / total rows = 2/2
+-----------------------+----------+
| percentile(age, 90)   | gender   |
|-----------------------+----------|
| 28                    | F        |
| 36                    | M        |
+-----------------------+----------+
```

Beispiel 13: Berechnet das Perzentil anhand eines Geschlechts und einer Spanne

Im Beispiel wird das Perzentil für das 90. Lebensjahr im Abstand von 10 Jahren berechnet und nach Geschlecht gruppiert.

```
os> source=accounts | stats percentile(age, 90) as p90 by span(age, 10) as age_span,
 gender
fetched rows / total rows = 2/2
+-------+------------+----------+
| p90   | age_span   | gender   |
|-------+------------+----------|
| 28    | 20         | F        |
| 36    | 30         | M        |
+-------+------------+----------+
```

```
- `source = table | stats avg(a) `
- `source = table | where a < 50 | stats avg(c) `
- `source = table | stats max(c) by b`
- `source = table | stats count(c) by b | head 5`
- `source = table | stats distinct_count(c)`
- `source = table | stats stddev_samp(c)`
- `source = table | stats stddev_pop(c)`
- `source = table | stats percentile(c, 90)`
- `source = table | stats percentile_approx(c, 99)`
```

Aggregationen mit Spanne

```
- `source = table  | stats count(a) by span(a, 10) as a_span`
- `source = table  | stats sum(age) by span(age, 5) as age_span | head 2`
- `source = table  | stats avg(age) by span(age, 20) as age_span, country  | sort -
 age_span |  head 2`
```

Aggregationen mit Timewindow Span (Tumble-Windowing-Funktion)

```
- `source = table | stats sum(productsAmount) by span(transactionDate, 1d) as age_date
 | sort age_date`
- `source = table | stats sum(productsAmount) by span(transactionDate, 1w) as age_date,
 productId`
```

Aggregationen gruppieren nach mehreren Ebenen

```
- `source = table | stats avg(age) as avg_state_age by country, state | stats
 avg(avg_state_age) as avg_country_age by country`
- `source = table | stats avg(age) as avg_city_age by country, state, city | eval
 new_avg_city_age = avg_city_age - 1 | stats avg(new_avg_city_age) as avg_state_age
 by country, state | where avg_state_age > 18 | stats avg(avg_state_age) as
 avg_adult_country_age by country`
```

Befehl subquery

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen PPL-Befehl unterstützen, finden Sie unter. the section called “Befehle”

Verwenden Sie den `subquery` Befehl, um komplexe, verschachtelte Abfragen innerhalb Ihrer PPL-Anweisungen (Piped Processing Language) auszuführen.

```
source=logs | where field in [ subquery source=events | where condition | fields
 field ]
```

In diesem Beispiel wird die primäre Suche (`source=logs`) nach Ergebnissen der Unterabfrage () gefiltert. `source=events`

Der Befehl subquery unterstützt mehrere Verschachtelungsebenen für komplexe Datenanalysen.

Beispiel für eine verschachtelte Unterabfrage

```
source=logs | where id in [ subquery source=users | where user in [ subquery
 source=actions | where action="login" | fields user] | fields uid ]
```

InSubquery Verwendung

- `source = outer | where a in [ source = inner | fields b ]`
- `source = outer | where (a) in [ source = inner | fields b ]`
- `source = outer | where (a,b,c) in [ source = inner | fields d,e,f ]`
- `source = outer | where a not in [ source = inner | fields b ]`

- `source = outer | where (a) not in [ source = inner | fields b ]`
- `source = outer | where (a,b,c) not in [ source = inner | fields d,e,f ]`
- `source = outer a in [ source = inner | fields b ]`(Suchfilterung mit Unterabfrage)
- `source = outer a not in [ source = inner | fields b ]`(Suchfilterung mit Unterabfrage)
- `source = outer | where a in [ source = inner1 | where b not in [ source = inner2 | fields c ] | fields b ]`(verschachtelt)
- `source = table1 | inner join left = l right = r on l.a = r.a AND r.a in [ source = inner | fields d ] | fields l.a, r.a, b, c`(als Verbindungsfilter)

Beispiele für die SQL-Migration mit PPL in Subquery

TPC-H Q4 (in der Unterabfrage mit Aggregation)

```
select
  o_orderpriority,
  count(*) as order_count
from
  orders
where
  o_orderdate >= date '1993-07-01'
  and o_orderdate < date '1993-07-01' + interval '3' month
  and o_orderkey in (
    select
      l_orderkey
    from
      lineitem
    where l_commitdate < l_receiptdate
  )
group by
  o_orderpriority
order by
  o_orderpriority
```

Durch InSubquery PPL-Abfrage neu geschrieben:

```
source = orders
| where o_orderdate >= "1993-07-01" and o_orderdate < "1993-10-01" and o_orderkey IN
  [ source = lineitem
```

```
    | where l_commitdate < l_receiptdate
    | fields l_orderkey
  ]
| stats count(1) as order_count by o_orderpriority
| sort o_orderpriority
| fields o_orderpriority, order_count
```

TPC-H Q20 (verschachtelt in einer Unterabfrage)

```
select
  s_name,
  s_address
from
  supplier,
  nation
where
  s_suppkey in (
    select
      ps_suppkey
    from
      partsupp
    where
      ps_partkey in (
        select
          p_partkey
        from
          part
        where
          p_name like 'forest%'
      )
  )
  and s_nationkey = n_nationkey
  and n_name = 'CANADA'
order by
  s_name
```

Durch InSubquery PPL-Abfrage neu geschrieben:

```
source = supplier
| where s_suppkey IN [
    source = partsupp
    | where ps_partkey IN [
        source = part
```

```
        | where like(p_name, "forest%")
        | fields p_partkey
      ]
    | fields ps_suppkey
  ]
| inner join left=l right=r on s_nationkey = n_nationkey and n_name = 'CANADA'
  nation
| sort s_name
```

ExistsSubquery Verwendung

Annahmen:a, b sind Felder der äußeren Tabelle,c, d sind Felder der inneren Tabelle,e, f sind Felder der inneren Tabelle 2.

- `source = outer | where exists [ source = inner | where a = c ]`
- `source = outer | where not exists [ source = inner | where a = c ]`
- `source = outer | where exists [ source = inner | where a = c and b = d ]`
- `source = outer | where not exists [ source = inner | where a = c and b = d ]`
- `source = outer exists [ source = inner | where a = c ]`(Suchfilterung mit Unterabfrage)
- `source = outer not exists [ source = inner | where a = c ]`(Suchfilterung mit Unterabfrage)
- `source = table as t1 exists [ source = table as t2 | where t1.a = t2.a ]`(Der Tabellenalias ist in der vorhandenen Unterabfrage nützlich)
- `source = outer | where exists [ source = inner1 | where a = c and exists [ source = inner2 | where c = e ] ]`(verschachtelt)
- `source = outer | where exists [ source = inner1 | where a = c | where exists [ source = inner2 | where c = e ] ]`(verschachtelt)
- `source = outer | where exists [ source = inner | where c > 10 ]`(unkorreliert existiert)
- `source = outer | where not exists [ source = inner | where c > 10 ]`(unkorreliert existiert)
- `source = outer | where exists [ source = inner ] | eval l = "nonEmpty" | fields l`(es gibt ein spezielles unkorreliertes Objekt)

ScalarSubquery Verwendung

Annahmen:a, b sind Felder der äußeren Tabelle,c, d sind Felder der inneren Tabelle,e, f sind Felder der Tabelle verschachtelt

Unkorrelierte skalare Unterabfrage

In Auswahl:

- `source = outer | eval m = [ source = inner | stats max(c) ] | fields m, a`
- `source = outer | eval m = [ source = inner | stats max(c) ] + b | fields m, a`

Wo:

- `source = outer | where a > [ source = inner | stats min(c) ] | fields a`

Im Suchfilter:

- `source = outer a > [ source = inner | stats min(c) ] | fields a`

Korrelierte skalare Unterabfrage

In der Auswahl:

- `source = outer | eval m = [ source = inner | where outer.b = inner.d | stats max(c) ] | fields m, a`
- `source = outer | eval m = [ source = inner | where b = d | stats max(c) ] | fields m, a`
- `source = outer | eval m = [ source = inner | where outer.b > inner.d | stats max(c) ] | fields m, a`

Wo:

- `source = outer | where a = [ source = inner | where outer.b = inner.d | stats max(c) ]`
- `source = outer | where a = [ source = inner | where b = d | stats max(c) ]`

- `source = outer | where [ source = inner | where outer.b = inner.d OR inner.d = 1 | stats count() ] > 0 | fields a`

Im Suchfilter:

- `source = outer a = [ source = inner | where b = d | stats max(c) ]`
- `source = outer [ source = inner | where outer.b = inner.d OR inner.d = 1 | stats count() ] > 0 | fields a`

Verschachtelte skalare Unterabfrage

- `source = outer | where a = [ source = inner | stats max(c) | sort c ] OR b = [ source = inner | where c = 1 | stats min(d) | sort d ]`
- `source = outer | where a = [ source = inner | where c = [ source = nested | stats max(e) by f | sort f ] | stats max(d) by c | sort c | head 1 ]`

(Beziehung) Unterabfrage

`InSubquery`, `ExistsSubquery` und `ScalarSubquery` sind alles Unterabfrageausdrücke. Es `RelationSubquery` handelt sich jedoch nicht um einen Unterabfrageausdruck, sondern um einen Unterabfrageplan, der häufig in der Join- oder From-Klausel verwendet wird.

- `source = table1 | join left = l right = r [ source = table2 | where d > 10 | head 5 ]`(Unterabfrage in Join auf der rechten Seite)
- `source = [ source = table1 | join left = l right = r [ source = table2 | where d > 10 | head 5 ] | stats count(a) by b ] as outer | head 1`

Zusätzlicher Kontext

`InSubqueryExistsSubquery`, und `ScalarSubquery` sind Unterabfrageausdrücke, die häufig in `where` Klauseln und Suchfiltern verwendet werden.

Wo Befehl:

```
| where <boolean expression> | ...
```

Suchfilter:

```
search source=* <boolean expression> | ...
```

Ein Unterabfrageausdruck könnte in einem booleschen Ausdruck verwendet werden:

```
| where orders.order_id in [ source=returns | where return_reason="damaged" | field
 order_id ]
```

Das `orders.order_id in [ source=... ]` ist ein. `<boolean expression>`

Im Allgemeinen nennen wir diese Art von Unterabfrageklausel den `InSubquery` Ausdruck. Es ist ein`<boolean expression>`.

Unterabfrage mit unterschiedlichen Join-Typen

Beispiel für die Verwendung eines `ScalarSubquery`:

```
source=employees
| join source=sales on employees.employee_id = sales.employee_id
| where sales.sale_amount > [ source=targets | where target_met="true" | fields
 target_value ]
```

Im Gegensatz zu InSubquery ExistsSubquery ScalarSubquery, und RelationSubquery ist a kein Unterabfrageausdruck. Stattdessen handelt es sich um einen Unterabfrageplan.

```
SEARCH source=customer
| FIELDS c_custkey
| LEFT OUTER JOIN left = c, right = o ON c.c_custkey = o.o_custkey
   [
      SEARCH source=orders
      | WHERE o_comment NOT LIKE '%unusual%packages%'
      | FIELDS o_orderkey, o_custkey
   ]
| STATS ...
```

oberster Befehl

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen PPL-Befehl unterstützen, finden Sie unter. the section called “Befehle”

Verwenden Sie den `top` Befehl, um das häufigste Wertetupel aller Felder in der Feldliste zu finden.

Syntax

Verwenden Sie die folgende Syntax:

```
top [N] <field-list> [by-clause] top_approx [N] <field-list> [by-clause]
```

N

- Die Anzahl der zurückzugebenden Ergebnisse.
- Standard: 10

Feldliste

- Zwingend erforderlich.
- Eine kommagetrennte Liste von Feldnamen.

Nebenklausel

- Optional.
- Ein oder mehrere Felder, nach denen die Ergebnisse gruppiert werden sollen.

top_approx

- Eine ungefähre Anzahl der (n) obersten Felder unter Verwendung des Algorithmus „Geschätzte Kardinalität nach ++“. HyperLogLog

Beispiel 1: Finden Sie die häufigsten Werte in einem Feld

In diesem Beispiel wird das häufigste Geschlecht für alle Konten ermittelt.

PPL-Abfrage:

```
os> source=accounts | top gender;
os> source=accounts | top_approx gender;
fetched rows / total rows = 2/2
+----------+
| gender   |
```

```
|----------|
| M        |
| F        |
+----------+
```

Beispiel 2: Finden Sie die häufigsten Werte in einem Feld (begrenzt auf 1)

In diesem Beispiel wird für alle Konten das am häufigsten vorkommende Geschlecht ermittelt.

PPL-Abfrage:

```
os> source=accounts | top_approx 1 gender;
fetched rows / total rows = 1/1
+----------+
| gender   |
|----------|
| M        |
+----------+
```

Beispiel 3: Finden Sie die gängigsten Werte, gruppiert nach Geschlecht

In diesem Beispiel wird das häufigste Alter für alle Konten ermittelt, gruppiert nach Geschlecht.

PPL-Abfrage:

```
os> source=accounts | top 1 age by gender;
os> source=accounts | top_approx 1 age by gender;
fetched rows / total rows = 2/2
+----------+-------+
| gender   | age   |
|----------+-------|
| F        | 28    |
| M        | 32    |
+----------+-------+
```

Befehl trendline

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen PPL-Befehl unterstützen, finden Sie unter. the section called “Befehle”

Verwenden Sie den `trendline` Befehl, um gleitende Durchschnitte von Feldern zu berechnen.

Syntax

Verwenden Sie die folgende Syntax

```
TRENDLINE [sort <[+|-] sort-field>] SMA(number-of-datapoints, field) [AS alias]
 [SMA(number-of-datapoints, field) [AS alias]]...
```

[+|-]

- Optional.
- Das Plus [+] steht für aufsteigende Reihenfolge, wobei die NULL/MISSING Werte an erster Stelle stehen.
- Das Minus [-] steht für absteigende Reihenfolge, wobei die NULL/MISSING Werte zuletzt stehen.
- Standard: Aufsteigende Reihenfolge, wobei die NULL/MISSING Werte an erster Stelle stehen.

Sortierfeld

- Obligatorisch, wenn die Sortierung verwendet wird.
- Das für die Sortierung verwendete Feld.

number-of-datapoints

- Zwingend erforderlich.
- Die Anzahl der Datenpunkte, die den gleitenden Durchschnitt berechnen.
- Muss größer als Null sein.

field

- Zwingend erforderlich.
- Der Name des Feldes, für das der gleitende Durchschnitt berechnet werden soll.

alias

- Optional.

- Der Name der resultierenden Spalte, die den gleitenden Durchschnitt enthält.

Nur der Typ Simple Moving Average (SMA) wird unterstützt. Er wird wie folgt berechnet:

```
f[i]: The value of field 'f' in the i-th data-point
n: The number of data-points in the moving window (period)
t: The current time index

SMA(t) = (1/n) * Σ(f[i]), where i = t-n+1 to t
```

Beispiel 1: Berechne den einfachen gleitenden Durchschnitt für eine Zeitreihe von Temperaturen

Das Beispiel berechnet den einfachen gleitenden Durchschnitt über Temperaturen anhand von zwei Datenpunkten.

PPL-Abfrage:

```
os> source=t | trendline sma(2, temperature) as temp_trend;
fetched rows / total rows = 5/5
+-----------+---------+--------------------+----------+
|temperature|device-id|           timestamp|temp_trend|
+-----------+---------+--------------------+----------+
|         12|     1492|2023-04-06 17:07:...|      NULL|
|         12|     1492|2023-04-06 17:07:...|      12.0|
|         13|      256|2023-04-06 17:07:...|      12.5|
|         14|      257|2023-04-06 17:07:...|      13.5|
|         15|      258|2023-04-06 17:07:...|      14.5|
+-----------+---------+--------------------+----------+
```

Beispiel 2: Berechnung einfacher gleitender Durchschnitte für eine Zeitreihe von Temperaturen mit Sortierung

Das Beispiel berechnet zwei einfache gleitende Durchschnittswerte über Temperaturen anhand von zwei und drei Datenpunkten, die absteigend nach der Geräte-ID sortiert sind.

PPL-Abfrage:

```
os> source=t | trendline sort - device-id sma(2, temperature) as temp_trend_2 sma(3,
 temperature) as temp_trend_3;
fetched rows / total rows = 5/5
+-----------+---------+--------------------+------------+------------------+
```

```
|temperature|device-id|           timestamp|temp_trend_2|      temp_trend_3|
+-----------+---------+--------------------+------------+------------------+
|         15|      258|2023-04-06 17:07:...|        NULL|              NULL|
|         14|      257|2023-04-06 17:07:...|        14.5|              NULL|
|         13|      256|2023-04-06 17:07:...|        13.5|              14.0|
|         12|     1492|2023-04-06 17:07:...|        12.5|              13.0|
|         12|     1492|2023-04-06 17:07:...|        12.0|12.333333333333334|
+-----------+---------+--------------------+------------+------------------+
```

wo (Befehl)

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen PPL-Befehl unterstützen, finden Sie unter. the section called “Befehle”

Der `where` Befehl verwendet einen Bool-Ausdruck, um das Suchergebnis zu filtern. Das Ergebnis wird nur zurückgegeben, wenn der bool-Ausdruck den Wert true ergibt.

Syntax

Verwenden Sie die folgende Syntax:

```
where <boolean-expression>
```

boolischer Ausdruck

- Optional.
- Jeder Ausdruck, der zu einem booleschen Wert ausgewertet werden könnte.

Beispiel 1: Filtert den Ergebnissatz mit einer Bedingung

Das Beispiel zeigt, wie Dokumente aus dem Kontenindex abgerufen werden, die bestimmte Bedingungen erfüllen.

PPL-Abfrage:

```
os> source=accounts | where account_number=1 or gender="F" | fields account_number,
 gender;
fetched rows / total rows = 2/2
```

```
+------------------+----------+
| account_number   | gender   |
|------------------+----------|
| 1                | M        |
| 13               | F        |
+------------------+----------+
```

Weitere Beispiele

Filter mit logischen Bedingungen

- `source = table | where c = 'test' AND a = 1 | fields a,b,c`
- `source = table | where c != 'test' OR a > 1 | fields a,b,c | head 1`
- `source = table | where c = 'test' NOT a > 1 | fields a,b,c`
- `source = table | where a = 1 | fields a,b,c`
- `source = table | where a >= 1 | fields a,b,c`
- `source = table | where a < 1 | fields a,b,c`
- `source = table | where b != 'test' | fields a,b,c`
- `source = table | where c = 'test' | fields a,b,c | head 3`
- `source = table | where ispresent(b)`
- `source = table | where isnull(coalesce(a, b)) | fields a,b,c | head 3`
- `source = table | where isempty(a)`
- `source = table | where isblank(a)`
- `source = table | where case(length(a) > 6, 'True' else 'False') = 'True'`
- `source = table | where a between 1 and 4`- Hinweis: Dies gibt a >= 1 und a <= 4 zurück, also [1, 4]
- `source = table | where b not between '2024-09-10' and '2025-09-10'`- Hinweis: Dies gibt b >= '**********' und b <= '2025-09-10' zurück
- `source = table | where cidrmatch(ip, '***********/24')`
- `source = table | where cidrmatch(ipv6, '2003:db8::/32')`

```
source = table | eval status_category =
    case(a >= 200 AND a < 300, 'Success',
    a >= 300 AND a < 400, 'Redirection',
```

```
    a >= 400 AND a < 500, 'Client Error',
    a >= 500, 'Server Error'
    else 'Incorrect HTTP status code')
    | where case(a >= 200 AND a < 300, 'Success',
    a >= 300 AND a < 400, 'Redirection',
    a >= 400 AND a < 500, 'Client Error',
    a >= 500, 'Server Error'
    else 'Incorrect HTTP status code'
    ) = 'Incorrect HTTP status code'
```

```
source = table
    | eval factor = case(a > 15, a - 14, isnull(b), a - 7, a < 3, a + 1 else 1)
    | where case(factor = 2, 'even', factor = 4, 'even', factor = 6, 'even', factor =
 8, 'even' else 'odd') = 'even'
    |  stats count() by factor
```

Zusammenfassung der Felder

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diesen PPL-Befehl unterstützen, finden Sie unter. the section called “Befehle”

Verwenden Sie den `fieldsummary` Befehl, um grundlegende Statistiken für jedes Feld (Anzahl, eindeutige Anzahl, Min., Max, Avg, Stddev, Mittelwert) zu berechnen und den Datentyp für jedes Feld zu bestimmen. Dieser Befehl kann mit jeder vorhergehenden Pipe verwendet werden und berücksichtigt sie.

Syntax

Verwenden Sie die folgende Syntax: Für CloudWatch Logs-Anwendungsfälle wird nur ein Feld in einer Abfrage unterstützt.

```
... | fieldsummary <field-list> (nulls=true/false)
```

Felder einschließen

- Liste aller Spalten, die zusammen mit Statistiken in einer einheitlichen Ergebnismenge gesammelt werden sollen.

Null-Werte

- Optional.
- Wenn der Wert auf „true“ gesetzt ist, werden Nullwerte in die Aggregationsberechnungen einbezogen (ersetzen Sie Null durch Null für numerische Werte).

Beispiel 1

PPL-Abfrage:

```
os> source = t | where status_code != 200 | fieldsummary includefields= status_code
 nulls=true
+------------------+-------------+-----------+-----------+-----------+-----------
+-----------+-----------+----------------|
| Fields           | COUNT       | COUNT_DISTINCT    |  MIN  |  MAX   |  AVG   |  MEAN
  |        STDDEV       | NUlls | TYPEOF |
|------------------+-------------+-----------+-----------+-----------+-----------
+-----------+-----------+----------------|
| "status_code"    |      2      |         2         | 301   |   403  |  352.0 |  352.0
  |  72.12489168102785  |  0    | "int"  |
+------------------+-------------+-----------+-----------+-----------+-----------
+-----------+-----------+----------------|
```

Beispiel 2

PPL-Abfrage:

```
os> source = t | fieldsummary includefields= id, status_code, request_path nulls=true
+------------------+-------------+-----------+-----------+-----------+-----------
+-----------+-----------+----------------|
| Fields           | COUNT       | COUNT_DISTINCT    |  MIN  |  MAX   |  AVG   |  MEAN
  |        STDDEV       | NUlls | TYPEOF |
|------------------+-------------+-----------+-----------+-----------+-----------
+-----------+-----------+----------------|
|       "id"       |      6      |         6         | 1     |   6    |  3.5   |   3.5
 |  1.8708286933869707  |  0    | "int"  |
+------------------+-------------+-----------+-----------+-----------+-----------
+-----------+-----------+----------------|
| "status_code"    |      4      |         3         | 200   |   403  |  184.0 |  184.0
  |  161.16699413961905 |  2    | "int"  |
+------------------+-------------+-----------+-----------+-----------+-----------
+-----------+-----------+----------------|
```

```
| "request_path"   |      2      |         2         | /about| /home   |  0.0    |  0.0
    |      0            |  2    |"string"|
+------------------+-------------+-----------+-----------+-----------+-----------
+-----------+-----------+---------------|
```

Befehl expandieren

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diese PPL-Funktion unterstützen, finden Sie unter. the section called “Funktionen”

Verwenden Sie den `expand` Befehl, um ein Feld vom Typ Array <Any>oder Map zu reduzieren<Any>, sodass für jedes Element oder jedes Schlüssel-Wert-Paar einzelne Zeilen erzeugt werden.

Syntax

Verwenden Sie die folgende Syntax:

```
expand <field> [As alias]
```

field

- Das Feld, das erweitert (aufgelöst) werden soll.
- Das Feld muss einen unterstützten Typ haben.

alias

- Optional.
- Der Name, der anstelle des ursprünglichen Feldnamens verwendet werden soll.

Richtlinien für die Verwendung

Der Befehl expand erzeugt eine Zeile für jedes Element im angegebenen Array- oder Zuordnungsfeld, wobei:

- Array-Elemente werden zu einzelnen Zeilen.

- Map-Schlüssel-Wert-Paare werden in separate Zeilen aufgeteilt, wobei jeder Schlüsselwert als Zeile dargestellt wird.
- Wenn ein Alias angegeben wird, werden die explodierten Werte unter dem Alias statt unter dem ursprünglichen Feldnamen dargestellt.

Sie können diesen Befehl in Kombination mit anderen Befehlen wie stats, eval und parse verwenden, um Daten nach der Erweiterung zu bearbeiten oder zu extrahieren.

Beispiele

- `source = table | expand employee | stats max(salary) as max by state, company`
- `source = table | expand employee as worker | stats max(salary) as max by state, company`
- `source = table | expand employee as worker | eval bonus = salary * 3 | fields worker, bonus`
- `source = table | expand employee | parse description '(?<email>.+@.+)' | fields employee, email`
- `source = table | eval array=json_array(1, 2, 3) | expand array as uid | fields name, occupation, uid`
- `source = table | expand multi_valueA as multiA | expand multi_valueB as multiB`

Sie können den Befehl expand in Kombination mit anderen Befehlen wie eval, stats und anderen verwenden. Durch die Verwendung mehrerer Erweiterungsbefehle wird ein kartesisches Produkt aller internen Elemente in jeder zusammengesetzten Anordnung oder Map erstellt.

Effektive SQL-Pushdown-Abfrage

Der Befehl expand wird mithilfe von LATERAL VIEW explode in eine äquivalente SQL-Operation übersetzt, was eine effiziente Auflösung von Arrays oder Maps auf SQL-Abfrageebene ermöglicht.

```
SELECT customer exploded_productId
FROM table
LATERAL VIEW explode(productId) AS exploded_productId
```

Der Befehl explode bietet die folgenden Funktionen:

- Es handelt sich um eine Spaltenoperation, die eine neue Spalte zurückgibt.
- Es erstellt eine neue Zeile für jedes Element in der aufgelösten Spalte.
- Interne Nullen werden als Teil des explodierten Felds ignoriert (keine Zeile steht created/exploded für Null).

PPL-Funktionen

Themen

- Funktionen für PPL-Bedingungen
- Kryptografische PPL-Hash-Funktionen
- PPL-Funktionen für Datum und Uhrzeit
- PPL-Ausdrücke
- PPL-IP-Adressfunktionen
- PPL JSON-Funktionen
- PPL Lambda-Funktionen
- Mathematische Funktionen von PPL
- PPL-String-Funktionen
- Funktionen zur Konvertierung des PPL-Typs

Funktionen für PPL-Bedingungen

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diese PPL-Funktion unterstützen, finden Sie unter. the section called “Funktionen”

ISNULL

Beschreibung: `isnull(field)` gibt true zurück, wenn das Feld Null ist.

Typ des Arguments:

- Alle unterstützten Datentypen.

Rückgabetyp:

- BOOLEAN

Beispiel:

```
os> source=accounts | eval result = isnull(employer) | fields result, employer,
 firstname
fetched rows / total rows = 4/4
+----------+-------------+-------------+
| result   | employer    | firstname   |
|----------+-------------+-------------|
| False    | AnyCompany  | Mary        |
| False    | ExampleCorp | Jane        |
| False    | ExampleOrg  | Nikki       |
| True     | null        | Juan        |
+----------+-------------+-------------+
```

IST NICHT NULL

Beschreibung: `isnotnull(field)` gibt true zurück, wenn das Feld nicht Null ist.

Typ des Arguments:

- Alle unterstützten Datentypen.

Rückgabetyp:

- BOOLEAN

Beispiel:

```
os> source=accounts | where not isnotnull(employer) | fields account_number, employer
fetched rows / total rows = 1/1
+------------------+------------+
| account_number   | employer   |
|------------------+------------|
| 18               | null       |
+------------------+------------+
```

EXISTS

Beispiel:

```
os> source=accounts | where exists(email) | fields account_number, email
fetched rows / total rows = 1/1
```

WENN NULL

Beschreibung: `ifnull(field1, field2)` gibt zurück, `field2` ob `field1` es Null ist.

Typ des Arguments:

- Alle unterstützten Datentypen.
- Wenn die beiden Parameter unterschiedliche Typen haben, schlägt die Funktion die Semantikprüfung fehl.

Rückgabetyp:

- Any

Beispiel:

```
os> source=accounts | eval result = ifnull(employer, 'default') | fields result,
 employer, firstname
fetched rows / total rows = 4/4
+------------+------------+-------------+
| result     | employer   | firstname   |
|------------+------------+-------------|
| AnyCompany | AnyCompany | Mary        |
| ExampleCorp| ExampleCorp| Jane        |
| ExampleOrg | ExampleOrg | Nikki       |
| default    | null       | Juan        |
+------------+------------+-------------+
```

NULLIF

Beschreibung: Geben Sie Null `nullif(field1, field2)` zurück, wenn zwei Parameter identisch sind, andernfalls geben Sie Feld1 zurück.

Typ des Arguments:

- Alle unterstützten Datentypen.
- Wenn die beiden Parameter unterschiedliche Typen haben, schlägt die Funktion die Semantikprüfung fehl.

Rückgabetyp:

- Any

Beispiel:

```
os> source=accounts | eval result = nullif(employer, 'AnyCompany') | fields result,
 employer, firstname
fetched rows / total rows = 4/4
+----------------+----------------+-------------+
| result         | employer       | firstname   |
|----------------+----------------+-------------|
| null           | AnyCompany     | Mary        |
| ExampleCorp    | ExampleCorp    | Jane        |
| ExampleOrg     | ExampleOrg     | Nikki       |
| null           | null           | Juan        |
+----------------+----------------+-------------+
```

IF

Beschreibung: `if(condition, expr1, expr2)` gibt zurück`expr1`, ob die Bedingung wahr ist, andernfalls kehrt sie zurück`expr2`.

Typ des Arguments:

- Alle unterstützten Datentypen.
- Wenn die beiden Parameter unterschiedliche Typen haben, schlägt die Funktion die Semantikprüfung fehl.

Rückgabetyp:

- Any

Beispiel:

```
os> source=accounts | eval result = if(true, firstname, lastname) | fields result,
 firstname, lastname
fetched rows / total rows = 4/4
+----------+-------------+----------+
| result   | firstname | lastname   |
|----------+-------------+----------|
| Jane     | Jane      | Doe        |
| Mary     | Mary      | Major      |
| Pat      | Pat       | Candella   |
| Dale     | Jorge     | Souza      |
+----------+-----------+------------+

os> source=accounts | eval result = if(false, firstname, lastname) | fields result,
 firstname, lastname
fetched rows / total rows = 4/4
+----------+-------------+------------+
| result   | firstname   | lastname   |
|----------+-------------+------------|
| Doe      | Jane        | Doe        |
| Major    | Mary        | Major      |
| Candella | Pat         | Candella   |
| Souza    | Jorge       | Souza      |
+----------+-------------+------------+

os> source=accounts | eval is_vip = if(age > 30 AND isnotnull(employer), true, false) |
 fields is_vip, firstname, lastname
fetched rows / total rows = 4/4
+----------+-------------+------------+
| is_vip   | firstname   | lastname   |
|----------+-------------+------------|
| True     | Jane        | Doe        |
| True     | Mary        | Major      |
| False    | Pat         | Candella   |
| False    | Jorge       | Souza      |
+----------+-------------+------------+
```

Kryptografische PPL-Hash-Funktionen

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diese PPL-Funktion unterstützen, finden Sie unter. the section called “Funktionen”

MD5

MD5 berechnet den MD5 Digest und gibt den Wert als 32-stellige Hexadezimalzeichenfolge zurück.

Verwendung: `md5('hello')`

Art des Arguments:

- STRING

Rückgabetyp:

- STRING

Beispiel:

```
os> source=people | eval `MD5('hello')` = MD5('hello') | fields `MD5('hello')`
fetched rows / total rows = 1/1
+----------------------------------+
| MD5('hello')                     |
|----------------------------------|
| <32 character hex string>        |
+----------------------------------+
```

SHA1

SHA1 gibt das Hex-String-Ergebnis von SHA-1 zurück.

Verwendung: `sha1('hello')`

Art des Arguments:

- STRING

Rückgabetyp:

- STRING

Beispiel:

```
os> source=people | eval `SHA1('hello')` = SHA1('hello') | fields `SHA1('hello')`
fetched rows / total rows = 1/1
+------------------------------------------+
| SHA1('hello')                            |
|------------------------------------------|
| <40-character SHA-1 hash result>         |
+------------------------------------------+
```

SHA2

SHA2 gibt das Hex-String-Ergebnis der SHA-2-Familie von Hashfunktionen (SHA-224, SHA-256, SHA-384 und SHA-512) zurück. NumBits gibt die gewünschte Bitlänge des Ergebnisses an, das einen Wert von 224, 256, 384, 512 haben muss

Verwendung:

- `sha2('hello',256)`
- `sha2('hello',512)`

Typ des Arguments:

- ZEICHENFOLGE, GANZZAHL

Rückgabetyp:

- STRING

Beispiel:

```
os> source=people | eval `SHA2('hello',256)` = SHA2('hello',256) | fields
 `SHA2('hello',256)`
fetched rows / total rows = 1/1
+------------------------------------------------------------------+
```

```
| SHA2('hello',256)                                                  |
|--------------------------------------------------------------------|
| <64-character SHA-256 hash result>                                 |
+--------------------------------------------------------------------+

os> source=people | eval `SHA2('hello',512)` = SHA2('hello',512) | fields
 `SHA2('hello',512)`
fetched rows / total rows = 1/1
+--------------------------------------------------------------------+
| SHA2('hello',512)                                                  |
                                          |
|--------------------------------------------------------------------|
| <128-character SHA-512 hash result>                                |
+--------------------------------------------------------------------+
```

PPL-Funktionen für Datum und Uhrzeit

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diese PPL-Funktion unterstützen, finden Sie unter. the section called “Funktionen”

DAY

Verwendung: `DAY(date)` Extrahiert den Tag des Monats für ein Datum im Bereich von 1 bis 31.

Argumenttyp: STRING/DATE/TIMESTAMP

Rückgabetyp: INTEGER

Synonyme:`DAYOFMONTH`, `DAY_OF_MONTH`

Beispiel:

```
os> source=people | eval `DAY(DATE('2020-08-26'))` = DAY(DATE('2020-08-26')) | fields
 `DAY(DATE('2020-08-26'))`
fetched rows / total rows = 1/1
+--------------------------+
| DAY(DATE('2020-08-26'))  |
|--------------------------|
| 26                       |
```

```
+--------------------------+
```

DAYOFMONTH

Verwendung: `DAYOFMONTH(date)` Extrahiert den Tag des Monats für ein Datum im Bereich von 1 bis 31.

Argumenttyp: STRING/DATE/TIMESTAMP

Rückgabetyp: INTEGER

Synonyme:`DAY`, `DAY_OF_MONTH`

Beispiel:

```
os> source=people | eval `DAYOFMONTH(DATE('2020-08-26'))` =
 DAYOFMONTH(DATE('2020-08-26')) | fields `DAYOFMONTH(DATE('2020-08-26'))`
fetched rows / total rows = 1/1
+----------------------------------+
| DAYOFMONTH(DATE('2020-08-26'))   |
|----------------------------------|
| 26                               |
+----------------------------------+
```

DAY_OF_MONTH

Verwendung: `DAY_OF_MONTH(DATE)` Extrahiert den Tag des Monats für ein Datum im Bereich von 1 bis 31.

Argumenttyp: STRING/DATE/TIMESTAMP

Rückgabetyp: INTEGER

Synonyme:`DAY`, `DAYOFMONTH`

Beispiel:

```
os> source=people | eval `DAY_OF_MONTH(DATE('2020-08-26'))` =
 DAY_OF_MONTH(DATE('2020-08-26')) | fields `DAY_OF_MONTH(DATE('2020-08-26'))`
fetched rows / total rows = 1/1
+----------------------------------+
| DAY_OF_MONTH(DATE('2020-08-26'))   |
```

```
|-------------------------------------|
| 26                                  |
+-------------------------------------+
```

DAYOFWEEK

Verwendung: `DAYOFWEEK(DATE)` Gibt den Wochentagsindex für ein Datum zurück (1 = Sonntag, 2 = Montag,..., 7 = Samstag).

Typ des Arguments: STRING/DATE/TIMESTAMP

Rückgabetyp: INTEGER

Synonyme: `DAY_OF_WEEK`

Beispiel:

```
os> source=people | eval `DAYOFWEEK(DATE('2020-08-26'))` =
 DAYOFWEEK(DATE('2020-08-26')) | fields `DAYOFWEEK(DATE('2020-08-26'))`
fetched rows / total rows = 1/1
+---------------------------------+
| DAYOFWEEK(DATE('2020-08-26'))   |
|---------------------------------|
| 4                               |
+---------------------------------+
```

DAY_OF_WEEK

Verwendung: `DAY_OF_WEEK(DATE)` Gibt den Wochentagsindex für ein Datum zurück (1 = Sonntag, 2 = Montag,..., 7 = Samstag).

Typ des Arguments: STRING/DATE/TIMESTAMP

Rückgabetyp: INTEGER

Synonyme: `DAYOFWEEK`

Beispiel:

```
os> source=people | eval `DAY_OF_WEEK(DATE('2020-08-26'))` =
 DAY_OF_WEEK(DATE('2020-08-26')) | fields `DAY_OF_WEEK(DATE('2020-08-26'))`
fetched rows / total rows = 1/1
```

```
+-----------------------------------+
| DAY_OF_WEEK(DATE('2020-08-26'))   |
|-----------------------------------|
| 4                                 |
+-----------------------------------+
```

DAYOFYEAR

Verwendung: DAYOFYEAR(DATE) Gibt den Tag des Jahres für ein Datum im Bereich von 1 bis 366 zurück.

Typ des Arguments: STRING/DATE/TIMESTAMP

Rückgabetyp: INTEGER

Synonyme: DAY_OF_YEAR

Beispiel:

```
os> source=people | eval `DAYOFYEAR(DATE('2020-08-26'))` =
 DAYOFYEAR(DATE('2020-08-26')) | fields `DAYOFYEAR(DATE('2020-08-26'))`
fetched rows / total rows = 1/1
+-----------------------------------+
| DAYOFYEAR(DATE('2020-08-26'))   |
|-----------------------------------|
| 239                               |
+-----------------------------------+
```

DAY_OF_YEAR

Verwendung: DAY_OF_YEAR(DATE) Gibt den Tag des Jahres für ein Datum im Bereich von 1 bis 366 zurück.

Typ des Arguments: STRING/DATE/TIMESTAMP

Rückgabetyp: INTEGER

Synonyme: DAYOFYEAR

Beispiel:

```
os> source=people | eval `DAY_OF_YEAR(DATE('2020-08-26'))` =
 DAY_OF_YEAR(DATE('2020-08-26')) | fields `DAY_OF_YEAR(DATE('2020-08-26'))`
```

```
fetched rows / total rows = 1/1
+----------------------------------+
| DAY_OF_YEAR(DATE('2020-08-26'))   |
|----------------------------------|
| 239                              |
+----------------------------------+
```

DAYNAME

Verwendung: DAYNAME(DATE) Gibt den Namen des Wochentags für ein Datum zurück, einschließlich Montag, Dienstag, Mittwoch, Donnerstag, Freitag, Samstag und Sonntag.

Typ des Arguments: STRING/DATE/TIMESTAMP

Rückgabetyp: STRING

Beispiel:

```
os> source=people | eval `DAYNAME(DATE('2020-08-26'))` = DAYNAME(DATE('2020-08-26')) |
 fields `DAYNAME(DATE('2020-08-26'))`
fetched rows / total rows = 1/1
+------------------------------+
| DAYNAME(DATE('2020-08-26'))   |
|------------------------------|
| Wednesday                    |
+------------------------------+
```

FROM_UNIXTIME

Verwendung: FROM_UNIXTIME Gibt eine Darstellung des angegebenen Arguments als Zeitstempel oder Zeichenkettenwert zurück. Diese Funktion führt eine umgekehrte Konvertierung der UNIX_TIMESTAMP Funktion durch.

Wenn Sie ein zweites Argument angeben, FROM_UNIXTIME verwendet es, um das Ergebnis ähnlich der DATE_FORMAT Funktion zu formatieren.

Wenn der Zeitstempel außerhalb des Bereichs 1970-01-01 00:00:00 bis 3001-01-18 23:59:59.999 999 (0 bis 32536771199.999999 Epochenzeit) liegt, gibt die Funktion zurück. NULL

Argumenttyp: DOUBLE, STRING

Rückgabetyp Map:

DOPPELT -> ZEITSTEMPEL

DOPPELT, ZEICHENFOLGE -> ZEICHENFOLGE

Beispiele:

```
os> source=people | eval `FROM_UNIXTIME(1220249547)` = FROM_UNIXTIME(1220249547) |
 fields `FROM_UNIXTIME(1220249547)`
fetched rows / total rows = 1/1
+-----------------------------+
| FROM_UNIXTIME(1220249547)   |
|-----------------------------|
| 2008-09-01 06:12:27         |
+-----------------------------+

os> source=people | eval `FROM_UNIXTIME(1220249547, 'HH:mm:ss')` =
 FROM_UNIXTIME(1220249547, 'HH:mm:ss') | fields `FROM_UNIXTIME(1220249547, 'HH:mm:ss')`
fetched rows / total rows = 1/1
+---------------------------------------+
| FROM_UNIXTIME(1220249547, 'HH:mm:ss')   |
|---------------------------------------|
| 06:12:27                              |
+---------------------------------------+
```

HOUR

Verwendung: `HOUR(TIME)` Extrahiert den Stundenwert für die Zeit.

Im Gegensatz zu einer Standardzeit kann der Zeitwert in dieser Funktion einen Bereich von mehr als 23 haben. Daher `HOUR(TIME)` kann der Rückgabewert von größer als 23 sein.

Typ des Arguments: STRING/TIME/TIMESTAMP

Rückgabetyp: INTEGER

Synonyme: `HOUR_OF_DAY`

Beispiel:

```
os> source=people | eval `HOUR(TIME('01:02:03'))` = HOUR(TIME('01:02:03')) | fields
 `HOUR(TIME('01:02:03'))`
fetched rows / total rows = 1/1
+-------------------------+
```

```
| HOUR(TIME('01:02:03'))   |
|--------------------------|
| 1                        |
+--------------------------+
```

HOUR_OF_DAY

Verwendung: `HOUR_OF_DAY(TIME)` Extrahiert den Stundenwert aus der angegebenen Zeit.

Im Gegensatz zu einer Standardzeit kann der Zeitwert in dieser Funktion einen Bereich von mehr als 23 haben. Daher `HOUR_OF_DAY(TIME)` kann der Rückgabewert von größer als 23 sein.

Typ des Arguments: STRING/TIME/TIMESTAMP

Rückgabetyp: INTEGER

Synonyme: `HOUR`

Beispiel:

```
os> source=people | eval `HOUR_OF_DAY(TIME('01:02:03'))` =
 HOUR_OF_DAY(TIME('01:02:03')) | fields `HOUR_OF_DAY(TIME('01:02:03'))`
fetched rows / total rows = 1/1
+--------------------------------+
| HOUR_OF_DAY(TIME('01:02:03'))   |
|--------------------------------|
| 1                              |
+--------------------------------+
```

LAST_DAY

Verwendung: `LAST_DAY` Gibt den letzten Tag des Monats als DATE-Wert für das angegebene Datumsargument zurück.

Typ des Arguments: DATE/STRING/TIMESTAMP/TIME

Rückgabetyp: DATUM

Beispiel:

```
os> source=people | eval `last_day('2023-02-06')` = last_day('2023-02-06') | fields
 `last_day('2023-02-06')`
```

```
fetched rows / total rows = 1/1
+-------------------------+
| last_day('2023-02-06')  |
|-------------------------|
| 2023-02-28              |
+-------------------------+
```

LOCALTIMESTAMP

Verwendung: `LOCALTIMESTAMP()` ist ein Synonym für`NOW()`.

Beispiel:

```
> source=people | eval `LOCALTIMESTAMP()` = LOCALTIMESTAMP() | fields
 `LOCALTIMESTAMP()`
fetched rows / total rows = 1/1
+---------------------+
| LOCALTIMESTAMP()    |
|---------------------|
| 2022-08-02 15:54:19 |
+---------------------+
```

LOCALTIME

Verwendung: `LOCALTIME()` ist ein Synonym für. `NOW()`

Beispiel:

```
> source=people | eval `LOCALTIME()` = LOCALTIME() | fields `LOCALTIME()`
fetched rows / total rows = 1/1
+---------------------+
| LOCALTIME()         |
|---------------------|
| 2022-08-02 15:54:19 |
+---------------------+
```

MAKE_DATE

Verwendung: `MAKE_DATE` Gibt einen Datumswert zurück, der auf den angegebenen Jahres-, Monats- und Tageswerten basiert. Alle Argumente werden auf ganze Zahlen gerundet.

Spezifikationen: 1. MAKE_DATE (GANZZAHL, GANZZAHL, GANZZAHL) -> DATUM

Argumenttyp: INTEGER, INTEGER, INTEGER

Rückgabetyp: DATE

Beispiel:

```
os> source=people | eval `MAKE_DATE(1945, 5, 9)` = MAKEDATE(1945, 5, 9) | fields
 `MAKEDATE(1945, 5, 9)`
fetched rows / total rows = 1/1
+------------------------+
| MAKEDATE(1945, 5, 9)   |
|------------------------|
| 1945-05-09             |
+------------------------+
```

MINUTE

Verwendung: `MINUTE(TIME)` Gibt die Minutenkomponente der angegebenen Zeit als Ganzzahl im Bereich 0 bis 59 zurück.

Typ des Arguments: STRING/TIME/TIMESTAMP

Rückgabetyp: INTEGER

Synonyme: `MINUTE_OF_HOUR`

Beispiel:

```
os> source=people | eval `MINUTE(TIME('01:02:03'))` =  MINUTE(TIME('01:02:03')) |
 fields `MINUTE(TIME('01:02:03'))`
fetched rows / total rows = 1/1
+----------------------------+
| MINUTE(TIME('01:02:03'))   |
|----------------------------|
| 2                          |
+----------------------------+
```

MINUTE_OF_HOUR

Verwendung: `MINUTE_OF_HOUR(TIME)` Gibt die Minutenkomponente der angegebenen Zeit als Ganzzahl im Bereich von 0 bis 59 zurück.

Typ des Arguments: STRING/TIME/TIMESTAMP

Rückgabetyp: INTEGER

Synonyme: `MINUTE`

Beispiel:

```
os> source=people | eval `MINUTE_OF_HOUR(TIME('01:02:03'))` =
 MINUTE_OF_HOUR(TIME('01:02:03')) | fields `MINUTE_OF_HOUR(TIME('01:02:03'))`
fetched rows / total rows = 1/1
+-----------------------------------+
| MINUTE_OF_HOUR(TIME('01:02:03'))   |
|-----------------------------------|
| 2                                 |
+-----------------------------------+
```

MONTH

Verwendung: `MONTH(DATE)` Gibt den Monat des angegebenen Datums als Ganzzahl im Bereich 1 bis 12 zurück (wobei 1 für Januar und 12 für Dezember steht).

Typ des Arguments: STRING/DATE/TIMESTAMP

Rückgabetyp: INTEGER

Synonyme: `MONTH_OF_YEAR`

Beispiel:

```
os> source=people | eval `MONTH(DATE('2020-08-26'))` =  MONTH(DATE('2020-08-26')) |
 fields `MONTH(DATE('2020-08-26'))`
fetched rows / total rows = 1/1
+----------------------------+
| MONTH(DATE('2020-08-26'))   |
|----------------------------|
| 8                          |
+----------------------------+
```

MONTHNAME

Verwendung: `MONTHNAME(DATE)` Gibt den Monat des angegebenen Datums als Ganzzahl im Bereich 1 bis 12 zurück (wobei 1 für Januar und 12 für Dezember steht).

Typ des Arguments: STRING/DATE/TIMESTAMP

Rückgabetyp: INTEGER

Synonyme: `MONTH_OF_YEAR`

Beispiel:

```
os> source=people | eval `MONTHNAME(DATE('2020-08-26'))` =
 MONTHNAME(DATE('2020-08-26')) | fields `MONTHNAME(DATE('2020-08-26'))`
fetched rows / total rows = 1/1
+---------------------------------+
| MONTHNAME(DATE('2020-08-26'))   |
|---------------------------------|
| August                          |
+---------------------------------+
```

MONTH_OF_YEAR

Verwendung: `MONTH_OF_YEAR(DATE)` Gibt den Monat des angegebenen Datums als Ganzzahl im Bereich 1 bis 12 zurück (wobei 1 für Januar und 12 für Dezember steht).

Typ des Arguments: STRING/DATE/TIMESTAMP

Rückgabetyp: INTEGER

Synonyme: `MONTH`

Beispiel:

```
os> source=people | eval `MONTH_OF_YEAR(DATE('2020-08-26'))` =
 MONTH_OF_YEAR(DATE('2020-08-26')) | fields `MONTH_OF_YEAR(DATE('2020-08-26'))`
fetched rows / total rows = 1/1
+-----------------------------------+
| MONTH_OF_YEAR(DATE('2020-08-26'))   |
|-----------------------------------|
| 8                                 |
+-----------------------------------+
```

NOW

Verwendung: `NOW` Gibt das aktuelle Datum und die aktuelle Uhrzeit als `TIMESTAMP` Wert im YYYY-MM-DD Format 'hh:mm:ss' zurück. Der Wert wird in der Cluster-Zeitzone ausgedrückt.

> **Note**
>
> `NOW()` gibt eine konstante Zeit zurück, die angibt, wann die Anweisung ausgeführt wurde. Dies unterscheidet sich von `SYSDATE()`, welche den genauen Zeitpunkt der Ausführung zurückgibt.

Rückgabetyp: TIMESTAMP

Spezifikation: NOW () -> TIMESTAMP

Beispiel:

```
os> source=people | eval `value_1` = NOW(), `value_2` = NOW() | fields `value_1`,
 `value_2`
fetched rows / total rows = 1/1
+---------------------+---------------------+
| value_1             | value_2             |
|---------------------+---------------------|
| 2022-08-02 15:39:05 | 2022-08-02 15:39:05 |
+---------------------+---------------------+
```

QUARTER

Verwendung: `QUARTER(DATE)` Gibt das Quartal des Jahres für das angegebene Datum als Ganzzahl im Bereich 1 bis 4 zurück.

Typ des Arguments: STRING/DATE/TIMESTAMP

Rückgabetyp: INTEGER

Beispiel:

```
os> source=people | eval `QUARTER(DATE('2020-08-26'))` = QUARTER(DATE('2020-08-26')) |
 fields `QUARTER(DATE('2020-08-26'))`
fetched rows / total rows = 1/1
+------------------------------+
| QUARTER(DATE('2020-08-26'))  |
|------------------------------|
| 3                            |
+------------------------------+
```

SECOND

Verwendung: `SECOND(TIME)` Gibt die zweite Komponente der angegebenen Zeit als Ganzzahl im Bereich 0 bis 59 zurück.

Typ des Arguments: STRING/TIME/TIMESTAMP

Rückgabetyp: INTEGER

Synonyme: `SECOND_OF_MINUTE`

Beispiel:

```
os> source=people | eval `SECOND(TIME('01:02:03'))` = SECOND(TIME('01:02:03')) | fields
 `SECOND(TIME('01:02:03'))`
fetched rows / total rows = 1/1
+----------------------------+
| SECOND(TIME('01:02:03'))   |
|----------------------------|
| 3                          |
+----------------------------+
```

SECOND_OF_MINUTE

Verwendung: `SECOND_OF_MINUTE(TIME)` Gibt die zweite Komponente der angegebenen Zeit als Ganzzahl im Bereich 0 bis 59 zurück.

Typ des Arguments: STRING/TIME/TIMESTAMP

Rückgabetyp: INTEGER

Synonyme: `SECOND`

Beispiel:

```
os> source=people | eval `SECOND_OF_MINUTE(TIME('01:02:03'))` =
 SECOND_OF_MINUTE(TIME('01:02:03')) | fields `SECOND_OF_MINUTE(TIME('01:02:03'))`
fetched rows / total rows = 1/1
+------------------------------------+
| SECOND_OF_MINUTE(TIME('01:02:03'))   |
|------------------------------------|
| 3                                  |
+------------------------------------+
```

SUBDATE

Verwendung: `SUBDATE(DATE, DAYS)` subtrahiert das zweite Argument (wie `DATE` oder`DAYS`) vom angegebenen Datum.

Argumenttyp: DATE/TIMESTAMP, LONG

Rückgabetypzuordnung: (DATE, LONG) -> DATE

Antonymen: `ADDDATE`

Beispiel:

```
os> source=people | eval `'2008-01-02' - 31d` = SUBDATE(DATE('2008-01-02'), 31),
 `'2020-08-26' - 1` = SUBDATE(DATE('2020-08-26'), 1), `ts '2020-08-26 01:01:01' -
 1` = SUBDATE(TIMESTAMP('2020-08-26 01:01:01'), 1) | fields `'2008-01-02' - 31d`,
 `'2020-08-26' - 1`, `ts '2020-08-26 01:01:01' - 1`
fetched rows / total rows = 1/1
+----------------------+--------------------+--------------------------------+
| '2008-01-02' - 31d   | '2020-08-26' - 1   | ts '2020-08-26 01:01:01' - 1   |
|----------------------+--------------------+--------------------------------|
| 2007-12-02 00:00:00  | 2020-08-25         | 2020-08-25 01:01:01            |
+----------------------+--------------------+--------------------------------+
```

SYSDATE

Verwendung: `SYSDATE()` Gibt das aktuelle Datum und die aktuelle Uhrzeit als `TIMESTAMP` Wert im YYYY-MM-DD Format 'hh:mm:ss.nnnnnn' zurück.

`SYSDATE()`gibt die genaue Uhrzeit zurück, zu der es ausgeführt wird. Dies unterscheidet sich von NOW (), das eine konstante Zeit zurückgibt, die angibt, wann die Anweisung ausgeführt wurde.

Optionaler Argumenttyp: INTEGER (0 bis 6) — Gibt die Anzahl der Ziffern für Sekundenbruchteile im Rückgabewert an.

Rückgabetyp: TIMESTAMP

Beispiel:

```
os> source=people | eval `SYSDATE()` = SYSDATE() | fields `SYSDATE()`
fetched rows / total rows = 1/1
+----------------------------+
| SYSDATE()                  |
```

```
|----------------------------|
| 2022-08-02 15:39:05.123456 |
+----------------------------+
```

TIMESTAMP

Verwendung: `TIMESTAMP(EXPR)` Konstruiert einen Zeitstempeltyp mit der Eingabezeichenfolge `expr` als Zeitstempel.

`TIMESTAMP(expr)`Konstruiert mit einem einzigen Argument einen Zeitstempel aus der Eingabe. Wenn es `expr` sich um eine Zeichenfolge handelt, wird sie als Zeitstempel interpretiert. Bei Argumenten, die keine Zeichenfolge sind, wandelt die Funktion mithilfe der UTC-Zeitzone in einen Zeitstempel `expr` um. Wenn ein `TIME` Wert `expr` ist, wendet die Funktion vor der Umwandlung das heutige Datum an.

Bei Verwendung mit zwei Argumenten wird der Zeitausdruck (`expr2`) zum Datums- oder Zeitstempelausdruck (`expr1`) `TIMESTAMP(expr1, expr2)` hinzugefügt und das Ergebnis als Zeitstempelwert zurückgegeben.

Typ des Arguments: STRING/DATE/TIME/TIMESTAMP

Rückgabetyp Map:

(STRING/DATE/TIME/TIMESTAMP) -> ZEITSTEMPEL

(STRING/DATE/TIME/TIMESTAMP, STRING/DATE/TIME/TIMESTAMP) -> ZEITSTEMPEL

Beispiel:

```
os> source=people | eval `TIMESTAMP('2020-08-26 13:49:00')` = TIMESTAMP('2020-08-26
 13:49:00'), `TIMESTAMP('2020-08-26 13:49:00', TIME('12:15:42'))` =
 TIMESTAMP('2020-08-26 13:49:00', TIME('12:15:42')) | fields `TIMESTAMP('2020-08-26
 13:49:00')`, `TIMESTAMP('2020-08-26 13:49:00', TIME('12:15:42'))`
fetched rows / total rows = 1/1
+-----------------------------------
+-----------------------------------------------------+
| TIMESTAMP('2020-08-26 13:49:00')   | TIMESTAMP('2020-08-26 13:49:00',
 TIME('12:15:42'))   |
|-----------------------------------
+-----------------------------------------------------|
| 2020-08-26 13:49:00                | 2020-08-27 02:04:42
     |
```

```
+-----------------------------------
+-----------------------------------------------------+
```

UNIX_TIMESTAMP

Verwendung: `UNIX_TIMESTAMP` Konvertiert ein gegebenes Datumsargument in Unix-Zeit (Sekunden seit der Epoche, die Anfang 1970 begann). Wenn kein Argument angegeben wird, gibt es die aktuelle Unix-Zeit zurück.

Das Datumsargument kann eine`DATE`, eine `TIMESTAMP` Zeichenfolge oder eine Zahl in einem der folgenden Formate sein: `YYMMDDYYMMDDhhmmss`,`YYYYMMDD`, oder`YYYYMMDDhhmmss`. Wenn das Argument eine Zeitkomponente enthält, kann es optional Sekundenbruchteile enthalten.

Wenn das Argument ein ungültiges Format hat oder außerhalb des Bereichs von 1970-01-01 00:00:00 bis 3001-01-18 23:59:59.999 999 (0 bis 32536771199.999999 in Epochenzeit) liegt, gibt die Funktion zurück. `NULL`

Die Funktion akzeptiert, oder als `DATE` Argumenttypen oder `DOUBLE` kein Argument. `TIMESTAMP` Sie gibt immer einen `DOUBLE` Wert zurück, der den Unix-Zeitstempel darstellt.

Für die umgekehrte Konvertierung können Sie die Funktion FROM_UNIXTIME verwenden.

Argumenttyp:/DOUBLE/DATE/TIMESTAMP<NONE>

Rückgabetyp: DOUBLE

Beispiel:

```
os> source=people | eval `UNIX_TIMESTAMP(double)` = UNIX_TIMESTAMP(20771122143845),
 `UNIX_TIMESTAMP(timestamp)` = UNIX_TIMESTAMP(TIMESTAMP('1996-11-15 17:05:42')) |
 fields `UNIX_TIMESTAMP(double)`, `UNIX_TIMESTAMP(timestamp)`
fetched rows / total rows = 1/1
+-------------------------+----------------------------+
| UNIX_TIMESTAMP(double)   | UNIX_TIMESTAMP(timestamp)   |
|-------------------------+----------------------------|
| 3404817525.0             | 848077542.0                |
+-------------------------+----------------------------+
```

WEEK

Verwendung: `WEEK(DATE)` Gibt die Wochennummer für ein bestimmtes Datum zurück.

Typ des Arguments: DATE/TIMESTAMP/STRING

Rückgabetyp: INTEGER

Synonyme: `WEEK_OF_YEAR`

Beispiel:

```
os> source=people | eval `WEEK(DATE('2008-02-20'))` = WEEK(DATE('2008-02-20')) | fields
 `WEEK(DATE('2008-02-20'))`
fetched rows / total rows = 1/1
+----------------------------+
| WEEK(DATE('2008-02-20'))   |
|----------------------------|
| 8                          |
+----------------------------+
```

`WEEKDAY`

Verwendung: `WEEKDAY(DATE)` Gibt den Wochentagsindex für das Datum zurück (0 = Montag, 1 = Dienstag,..., 6 = Sonntag).

Sie ähnelt der `dayofweek` Funktion, gibt jedoch für jeden Tag unterschiedliche Indizes zurück.

Typ des Arguments: STRING/DATE/TIME/TIMESTAMP

Rückgabetyp: INTEGER

Beispiel:

```
os> source=people | eval `weekday(DATE('2020-08-26'))` = weekday(DATE('2020-08-26'))
 | eval `weekday(DATE('2020-08-27'))` = weekday(DATE('2020-08-27')) | fields
 `weekday(DATE('2020-08-26'))`, `weekday(DATE('2020-08-27'))`
fetched rows / total rows = 1/1
+------------------------------+------------------------------+
| weekday(DATE('2020-08-26'))  | weekday(DATE('2020-08-27'))  |
|------------------------------+------------------------------|
| 2                            | 3                            |
+------------------------------+------------------------------+
```

`WEEK_OF_YEAR`

Verwendung: `WEEK_OF_YEAR(DATE)` Gibt die Wochennummer für das angegebene Datum zurück.

Typ des Arguments: DATE/TIMESTAMP/STRING

Rückgabetyp: INTEGER

Synonyme: `WEEK`

Beispiel:

```
os> source=people | eval `WEEK_OF_YEAR(DATE('2008-02-20'))` = WEEK(DATE('2008-02-20'))|
 fields `WEEK_OF_YEAR(DATE('2008-02-20'))`
fetched rows / total rows = 1/1
+-----------------------------------+
| WEEK_OF_YEAR(DATE('2008-02-20'))   |
|-----------------------------------|
| 8                                 |
+-----------------------------------+
```

`YEAR`

Verwendung: `YEAR(DATE)` Gibt das Jahr für das Datum im Bereich 1000 bis 9999 oder 0 für das Datum „Null“ zurück.

Typ des Arguments: STRING/DATE/TIMESTAMP

Rückgabetyp: INTEGER

Beispiel:

```
os> source=people | eval `YEAR(DATE('2020-08-26'))` = YEAR(DATE('2020-08-26')) | fields
 `YEAR(DATE('2020-08-26'))`
fetched rows / total rows = 1/1
+---------------------------+
| YEAR(DATE('2020-08-26'))   |
|---------------------------|
| 2020                      |
+---------------------------+
```

`DATE_ADD`

Verwendung: `DATE_ADD(date, INTERVAL expr unit)` Fügt dem angegebenen Datum das angegebene Intervall hinzu.

Argumenttyp: DATE, INTERVAL

Rückgabetyp: DATE

Antonymen: DATE_SUB

Beispiel:

```
os> source=people | eval `'2020-08-26' + 1d` = DATE_ADD(DATE('2020-08-26'), INTERVAL 1
 DAY) | fields `'2020-08-26' + 1d`
fetched rows / total rows = 1/1
+---------------------+
| '2020-08-26' + 1d   |
|---------------------|
| 2020-08-27          |
+---------------------+
```

DATE_SUB

Verwendung: DATE_SUB(date, INTERVAL expr unit) subtrahiert das Intervall expr vom Datum.

Argumenttyp: DATE, INTERVAL

Rückgabetyp: DATE

Antonymen: DATE_ADD

Beispiel:

```
os> source=people | eval `'2008-01-02' - 31d` = DATE_SUB(DATE('2008-01-02'), INTERVAL
 31 DAY) | fields `'2008-01-02' - 31d`
fetched rows / total rows = 1/1
+---------------------+
| '2008-01-02' - 31d  |
|---------------------|
| 2007-12-02          |
+---------------------+
```

TIMESTAMPADD

Verwendung: Gibt einen TIMESTAMP Wert zurück, nachdem ein bestimmtes Zeitintervall zu einem bestimmten Datum hinzugefügt wurde.

Argumente:

- Intervall: INTERVALL (SEKUNDE, MINUTE, STUNDE, TAG, WOCHE, MONAT, QUARTAL, JAHR)
- Ganzzahl: GANZZAHL
- Datum: DATE, TIMESTAMP oder STRING

Wenn Sie a `STRING` als Datumsargument angeben, formatieren Sie es als `TIMESTAMP` gültiges Argument. Die Funktion konvertiert ein `DATE` Argument automatisch in ein`TIMESTAMP`.

Beispiele:

```
os> source=people | eval `TIMESTAMPADD(DAY, 17, '2000-01-01 00:00:00')` =
 TIMESTAMPADD(DAY, 17, '2000-01-01 00:00:00') | eval `TIMESTAMPADD(QUARTER, -1,
 '2000-01-01 00:00:00')` = TIMESTAMPADD(QUARTER, -1, '2000-01-01 00:00:00') | fields
 `TIMESTAMPADD(DAY, 17, '2000-01-01 00:00:00')`, `TIMESTAMPADD(QUARTER, -1, '2000-01-01
 00:00:00')`
fetched rows / total rows = 1/1
+-----------------------------------------------
+-------------------------------------------------+
| TIMESTAMPADD(DAY, 17, '2000-01-01 00:00:00') | TIMESTAMPADD(QUARTER, -1, '2000-01-01
 00:00:00') |
|-----------------------------------------------
+-------------------------------------------------|
| 2000-01-18 00:00:00                           | 1999-10-01 00:00:00
           |
+-----------------------------------------------
+-------------------------------------------------+
```

`TIMESTAMPDIFF`

Verwendung: `TIMESTAMPDIFF(interval, start, end)` Gibt die Differenz zwischen Start und Ende date/times in angegebenen Intervalleinheiten zurück.

Argumente:

- Intervall: INTERVALL (SEKUNDE, MINUTE, STUNDE, TAG, WOCHE, MONAT, QUARTAL, JAHR)
- Start: DATUM, ZEITSTEMPEL oder ZEICHENFOLGE
- Ende: DATE, TIMESTAMP oder STRING

Die Funktion konvertiert Argumente TIMESTAMP bei Bedarf automatisch in. Formatieren Sie STRING Argumente als gültiges TIMESTAMP s.

Beispiele:

```
os> source=people | eval `TIMESTAMPDIFF(YEAR, '1997-01-01 00:00:00', '2001-03-06
 00:00:00')` = TIMESTAMPDIFF(YEAR, '1997-01-01 00:00:00', '2001-03-06 00:00:00') |
 eval `TIMESTAMPDIFF(SECOND, timestamp('1997-01-01 00:00:23'), timestamp('1997-01-01
 00:00:00'))` = TIMESTAMPDIFF(SECOND, timestamp('1997-01-01 00:00:23'),
 timestamp('1997-01-01 00:00:00')) | fields `TIMESTAMPDIFF(YEAR, '1997-01-01 00:00:00',
 '2001-03-06 00:00:00')`, `TIMESTAMPDIFF(SECOND, timestamp('1997-01-01 00:00:23'),
 timestamp('1997-01-01 00:00:00'))`
fetched rows / total rows = 1/1
+-----------------------------------------------------------------
+-----------------------------------------------------------------------------------
+
| TIMESTAMPDIFF(YEAR, '1997-01-01 00:00:00', '2001-03-06 00:00:00') |
 TIMESTAMPDIFF(SECOND, timestamp('1997-01-01 00:00:23'), timestamp('1997-01-01
 00:00:00')) |
|-----------------------------------------------------------------
+-----------------------------------------------------------------------------------|
| 4                                                               | -23
                                                                       |
+-----------------------------------------------------------------
+-----------------------------------------------------------------------------------
+
```

UTC_TIMESTAMP

Verwendung: UTC_TIMESTAMP Gibt den aktuellen UTC-Zeitstempel als Wert in 'YYYY-MM-DD hh:mm:ss' zurück.

Rückgabetyp: TIMESTAMP

Spezifikation: UTC_TIMESTAMP () -> TIMESTAMP

Beispiel:

```
> source=people | eval `UTC_TIMESTAMP()` = UTC_TIMESTAMP() | fields `UTC_TIMESTAMP()`
fetched rows / total rows = 1/1
+---------------------+
| UTC_TIMESTAMP()     |
|---------------------|
```

```
| 2022-10-03 17:54:28 |
+---------------------+
```

CURRENT_TIMEZONE

Syntax: `CURRENT_TIMEZONE` gibt die aktuelle lokale Zeitzone zurück.

Rückgabetyp: STRING

Beispiel:

```
> source=people | eval `CURRENT_TIMEZONE()` = CURRENT_TIMEZONE() | fields
 `CURRENT_TIMEZONE()`
fetched rows / total rows = 1/1
+------------------------+
| CURRENT_TIMEZONE()     |
|------------------------|
| America/Chicago        |
+------------------------+
```

PPL-Ausdrücke

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diese PPL-Funktion unterstützen, finden Sie unter. the section called “Funktionen”

Ausdrücke, insbesondere Wertausdrücke, geben einen Skalarwert zurück. Ausdrücke haben unterschiedliche Typen und Formen. Beispielsweise gibt es Literalwerte als Atomausdrücke und darauf aufbauende Arithmetik-, Prädikat- und Funktionsausdrücke. Sie können Ausdrücke in verschiedenen Klauseln verwenden, z. B. mithilfe von arithmetischen Ausdrücken in Befehlen und. `Filter` `Stats`

Operatoren

Ein arithmetischer Ausdruck ist ein Ausdruck, der aus numerischen Literalen und binären arithmetischen Operatoren wie folgt besteht:

1. +: Hinzufügen.

2. -: Subtrahieren.
3. *: Multiplizieren.
4. /: Dividieren (Bei ganzen Zahlen ist das Ergebnis eine ganze Zahl, wobei der Bruchteil verworfen wird)
5. %: Modulo (Nur für ganze Zahlen verwenden; das Ergebnis ist der Rest der Division)

Vorrang

Verwenden Sie Klammern, um die Rangfolge arithmetischer Operatoren zu steuern. Andernfalls werden Operatoren mit höherer Priorität zuerst ausgeführt.

Typkonvertierung

Die implizite Typkonvertierung wird beim Nachschlagen von Operatorsignaturen durchgeführt. Beispielsweise entspricht eine Ganzzahl und + eine reelle Zahl einer Signatur`+(double,double)`, was zu einer reellen Zahl führt. Diese Regel gilt auch für Funktionsaufrufen.

Beispiel für verschiedene Arten von arithmetischen Ausdrücken:

```
os> source=accounts | where age > (25 + 5) | fields age ;
fetched rows / total rows = 3/3
+-------+
| age   |
|-------|
| 32    |
| 36    |
| 33    |
+-------+
```

Prädikatoperatoren

Ein Prädikatoperator ist ein Ausdruck, der als wahr ausgewertet wird. Der Vergleich von `NULL` Werten `MISSING` und Werten folgt den folgenden Regeln:

- Ein `MISSING` Wert entspricht nur einem `MISSING` Wert und ist kleiner als andere Werte.
- Ein `NULL` Wert entspricht einem `NULL` Wert, ist größer als ein `MISSING` Wert, aber kleiner als alle anderen Werte.

Operatoren

Prädikat-Operatoren

Name	Beschreibung
>	Größer als Operator
>=	Operator größer als oder gleich
<	Kleiner als Operator
!=	Nicht gleicher Operator
<=	Operator „Kleiner als“ oder „gleich“
=	Gleicher Operator
LIKE	Einfacher Musterabgleich
IN	NULL-Wert-Test
AND	AND-Operator
OR	OR-Operator
XOR	XOR-Operator
NOT	NICHT NULL-Werttest

Sie können Datums- und Uhrzeitangaben vergleichen. Beim Vergleich verschiedener Datetime-Typen (z. B. `DATE` und`TIME`) werden beide in umgewandelt. `DATETIME` Für die Konvertierung gelten die folgenden Regeln:

- `TIME`gilt für das heutige Datum.
- `DATE`wird um Mitternacht gedolmetscht.

Grundlegender Prädikatoperator

Beispiel für Vergleichsoperatoren:

```
os> source=accounts | where age > 33 | fields age ;
```

```
fetched rows / total rows = 1/1
+-------+
| age   |
|-------|
| 36    |
+-------+
```

IN

Beispiel für das `IN` Operator-Testfeld in Wertelisten:

```
os> source=accounts | where age in (32, 33) | fields age ;
fetched rows / total rows = 2/2
+-------+
| age   |
|-------|
| 32    |
| 33    |
+-------+
```

OR

Beispiel für den `OR` Operator:

```
os> source=accounts | where age = 32 OR age = 33 | fields age ;
fetched rows / total rows = 2/2
+-------+
| age   |
|-------|
| 32    |
| 33    |
+-------+
```

NOT

Beispiel für den `NOT` Operator:

```
os> source=accounts | where age not in (32, 33) | fields age ;
fetched rows / total rows = 2/2
+-------+
| age   |
```

```
|-------|
| 36    |
| 28    |
+-------+
```

PPL-IP-Adressfunktionen

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diese PPL-Funktion unterstützen, finden Sie unter. the section called “Funktionen”

`CIDRMATCH`

Verwendung: `CIDRMATCH(ip, cidr)` Überprüft, ob die angegebene IP-Adresse innerhalb des angegebenen CIDR-Bereichs liegt.

Typ des Arguments:

- ZEICHENFOLGE, ZEICHENFOLGE
- Rückgabetyp: BOOLEAN

Beispiel:

```
os> source=ips | where cidrmatch(ip, '***********/24') | fields ip
fetched rows / total rows = 1/1
+--------------+
| ip           |
|--------------|
| ***********  |
+--------------+

os> source=ipsv6 | where cidrmatch(ip, '2003:db8::/32') | fields ip
fetched rows / total rows = 1/1
+-----------------------------------------+
| ip                                      |
|-----------------------------------------|
| 2003:0db8:****:****:****:****:****:0000 |
+-----------------------------------------+
```

> **Note**
>
> - `ip`kann eine IPv4 oder eine IPv6 Adresse sein.
> - `cidr`kann ein IPv4 oder ein IPv6 Block sein.
> - `ip`und `cidr` muss entweder beides IPv4 oder beides sein IPv6.
> - `ip`und `cidr` müssen sowohl gültig als auch nicht leer/nicht null sein.

PPL JSON-Funktionen

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diese PPL-Funktion unterstützen, finden Sie unter. the section called “Funktionen”

`JSON`

Verwendung: `json(value)` Prüft, ob eine Zeichenfolge im JSON-Format analysiert werden kann. Die Funktion gibt die ursprüngliche Zeichenfolge zurück, wenn sie gültiges JSON ist, oder null, wenn sie ungültig ist.

Argumenttyp: STRING

Rückgabetyp: STRING/NULL. Ein STRING-Ausdruck eines gültigen JSON-Objektformats.

Beispiele:

```
os> source=people | eval `valid_json()` = json('[1,2,3,{"f1":1,"f2":[5,6]},4]') |
 fields valid_json
fetched rows / total rows = 1/1
+-----------------------------------+
| valid_json                        |
+-----------------------------------+
| [1,2,3,{"f1":1,"f2":[5,6]},4]   |
+-----------------------------------+

os> source=people | eval `invalid_json()` = json('{"invalid": "json"') | fields
 invalid_json
```

```
fetched rows / total rows = 1/1
+----------------+
| invalid_json   |
+----------------+
| null           |
+----------------+
```

JSON_OBJECT

Verwendung: `json_object(<key>, <value>[, <key>, <value>]...)` Gibt ein JSON-Objekt von Mitgliedern von Schlüssel-Wert-Paaren zurück.

Typ des Arguments:

- A <key>muss STRING sein.
- A <value>kann ein beliebiger Datentyp sein.

Rückgabetyp: JSON_OBJECT. Ein StructType Ausdruck eines gültigen JSON-Objekts.

Beispiele:

```
os> source=people | eval result = json_object('key', 123.45) | fields result
fetched rows / total rows = 1/1
+------------------+
| result           |
+------------------+
| {"key":123.45}   |
+------------------+

os> source=people | eval result = json_object('outer', json_object('inner', 123.45)) |
 fields result
fetched rows / total rows = 1/1
+-----------------------------+
| result                      |
+-----------------------------+
| {"outer":{"inner":123.45}}  |
+-----------------------------+
```

JSON_ARRAY

Verwendung: `json_array(<value>...)` erstellt ein JSON-ARRAY anhand einer Werteliste.

Argumenttyp: A <value> kann ein beliebiger Wert sein, z. B. eine Zeichenfolge, eine Zahl oder ein boolescher Wert.

Rückgabetyp: ARRAY. Ein Array mit einem beliebigen unterstützten Datentyp für ein gültiges JSON-Array.

Beispiele:

```
os> source=people | eval `json_array` = json_array(1, 2, 0, -1, 1.1, -0.11)
fetched rows / total rows = 1/1
+-----------------------------+
| json_array                  |
+-----------------------------+
| [1.0,2.0,0.0,-1.0,1.1,-0.11] |
+-----------------------------+

os> source=people | eval `json_array_object` = json_object("array", json_array(1, 2, 0,
 -1, 1.1, -0.11))
fetched rows / total rows = 1/1
+---------------------------------------+
| json_array_object                     |
+---------------------------------------+
| {"array":[1.0,2.0,0.0,-1.0,1.1,-0.11]} |
+---------------------------------------+
```

TO_JSON_STRING

Verwendung: to_json_string(json0bject) Gibt eine JSON-Zeichenfolge mit einem bestimmten JSON-Objektwert zurück.

Argumenttyp: JSON_OBJECT

Rückgabetyp: STRING

Beispiele:

```
os> source=people | eval `json_string` = to_json_string(json_array(1, 2, 0, -1, 1.1,
 -0.11)) | fields json_string
fetched rows / total rows = 1/1
+-------------------------------+
| json_string                   |
+-------------------------------+
| [1.0,2.0,0.0,-1.0,1.1,-0.11]   |
```

```
+--------------------------------+

os> source=people | eval `json_string` = to_json_string(json_object('key', 123.45)) |
 fields json_string
fetched rows / total rows = 1/1
+-----------------+
| json_string     |
+-----------------+
| {'key', 123.45} |
+-----------------+
```

ARRAY_LENGTH

Verwendung: `array_length(jsonArray)` Gibt die Anzahl der Elemente im äußersten Array zurück.

Argumenttyp: ARRAY. Ein ARRAY- oder JSON_ARRAY-Objekt.

Rückgabetyp: INTEGER

Beispiel:

```
os> source=people | eval `json_array` = json_array_length(json_array(1,2,3,4)),
 `empty_array` = json_array_length(json_array())
fetched rows / total rows = 1/1
+--------------+---------------+
| json_array   | empty_array   |
+--------------+---------------+
| 4            | 0             |
+--------------+---------------+
```

JSON_EXTRACT

Verwendung: `json_extract(jsonStr, path)` Extrahiert ein JSON-Objekt aus einer JSON-Zeichenfolge, die auf dem angegebenen JSON-Pfad basiert. Die Funktion gibt Null zurück, wenn die eingegebene JSON-Zeichenfolge ungültig ist.

Argumenttyp: STRING, STRING

Rückgabetyp: STRING

- Ein STRING-Ausdruck eines gültigen JSON-Objektformats.
- `NULL`wird im Falle eines ungültigen JSON-Codes zurückgegeben.

Beispiele:

```
os> source=people | eval `json_extract('{"a":"b"}', '$.a')` = json_extract('{"a":"b"}',
 '$a')
fetched rows / total rows = 1/1
+----------------------------------+
| json_extract('{"a":"b"}', 'a')   |
+----------------------------------+
| b                                |
+----------------------------------+

os> source=people | eval `json_extract('{"a":[{"b":1},{"b":2}]}', '$.a[1].b')` =
 json_extract('{"a":[{"b":1},{"b":2}]}', '$.a[1].b')
fetched rows / total rows = 1/1
+------------------------------------------------------------+
| json_extract('{"a":[{"b":1.0},{"b":2.0}]}', '$.a[1].b')   |
+------------------------------------------------------------+
| 2.0                                                        |
+------------------------------------------------------------+

os> source=people | eval `json_extract('{"a":[{"b":1},{"b":2}]}', '$.a[*].b')` =
 json_extract('{"a":[{"b":1},{"b":2}]}', '$.a[*].b')
fetched rows / total rows = 1/1
+------------------------------------------------------------+
| json_extract('{"a":[{"b":1.0},{"b":2.0}]}', '$.a[*].b')   |
+------------------------------------------------------------+
| [1.0,2.0]                                                  |
+------------------------------------------------------------+

os> source=people | eval `invalid_json` = json_extract('{"invalid": "json"')
fetched rows / total rows = 1/1
+----------------+
| invalid_json   |
+----------------+
| null           |
+----------------+
```

JSON_KEYS

Verwendung: `json_keys(jsonStr)` gibt alle Schlüssel des äußersten JSON-Objekts als Array zurück.

Argumenttyp: STRING. Ein STRING-Ausdruck in einem gültigen JSON-Objektformat.

Rückgabetyp: ARRAY [STRING]. Die Funktion gibt NULL für jede andere gültige JSON-Zeichenfolge eine leere Zeichenfolge oder eine ungültige JSON-Zeichenfolge zurück.

Beispiele:

```
os> source=people | eval `keys` = json_keys('{"f1":"abc","f2":{"f3":"a","f4":"b"}}')
fetched rows / total rows = 1/1
+------------+
| keus       |
+------------+
| [f1, f2]   |
+------------+

os> source=people | eval `keys` = json_keys('[1,2,3,{"f1":1,"f2":[5,6]},4]')
fetched rows / total rows = 1/1
+--------+
| keys   |
+--------+
| null   |
+--------+
```

JSON_VALID

Verwendung: `json_valid(jsonStr)` wertet aus, ob eine JSON-Zeichenfolge eine gültige JSON-Syntax verwendet, und gibt TRUE oder FALSE zurück.

Argumenttyp: STRING

Rückgabetyp: BOOLEAN

Beispiele:

```
os> source=people | eval `valid_json` = json_valid('[1,2,3,4]'), `invalid_json` =
 json_valid('{"invalid": "json"') | feilds `valid_json`, `invalid_json`
fetched rows / total rows = 1/1
+--------------+----------------+
| valid_json   | invalid_json   |
+--------------+----------------+
| True         | False          |
+--------------+----------------+

os> source=accounts | where json_valid('[1,2,3,4]') and isnull(email) | fields
 account_number, email
```

```
fetched rows / total rows = 1/1
+------------------+---------+
| account_number   | email   |
|------------------+---------|
| 13               | null    |
+------------------+---------+
```

PPL Lambda-Funktionen

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diese PPL-Funktion unterstützen, finden Sie unter. the section called “Funktionen”

`EXISTS`

Verwendung: `exists(array, lambda)` bewertet, ob ein Lambda-Prädikat für ein oder mehrere Elemente im Array gilt.

Argumenttyp: ARRAY, LAMBDA

Rückgabetyp: BOOLEAN. Gibt zurück`TRUE`, ob mindestens ein Element im Array das Lambda-Prädikat erfüllt, andernfalls. `FALSE`

Beispiele:

```
 os> source=people | eval array = json_array(1, -1, 2), result = exists(array, x -> x >
 0) | fields result
fetched rows / total rows = 1/1
+-----------+
| result    |
+-----------+
| true      |
+-----------+

os> source=people | eval array = json_array(-1, -3, -2), result = exists(array, x -> x
 > 0) | fields result
fetched rows / total rows = 1/1
+-----------+
| result    |
```

```
+-----------+
| false     |
+-----------+
```

FILTER

Verwendung: `filter(array, lambda)` Filtert das Eingabearray mit der angegebenen Lambda-Funktion.

Argumenttyp: ARRAY, LAMBDA

Rückgabetyp: ARRAY. Ein ARRAY, das alle Elemente im Eingabearray enthält, die das Lambda-Prädikat erfüllen.

Beispiele:

```
 os> source=people | eval array = json_array(1, -1, 2), result = filter(array, x -> x >
 0) | fields result
fetched rows / total rows = 1/1
+-----------+
| result    |
+-----------+
| [1, 2]    |
+-----------+

os> source=people | eval array = json_array(-1, -3, -2), result = filter(array, x -> x
 > 0) | fields result
fetched rows / total rows = 1/1
+-----------+
| result    |
+-----------+
| []        |
+-----------+
```

TRANSFORM

Verwendung: `transform(array, lambda)` transformiert Elemente in einem Array mithilfe der Lambda-Transformationsfunktion. Das zweite Argument impliziert den Index des Elements, wenn die binäre Lambda-Funktion verwendet wird. Dies ähnelt a `map` in der funktionalen Programmierung.

Argumenttyp: ARRAY, LAMBDA

Rückgabetyp: ARRAY. Ein ARRAY, das das Ergebnis der Anwendung der Lambda-Transformationsfunktion auf jedes Element im Eingabearray enthält.

Beispiele:

```
os> source=people | eval array = json_array(1, 2, 3), result = transform(array, x -> x
 + 1) | fields result
fetched rows / total rows = 1/1
+--------------+
| result       |
+--------------+
| [2, 3, 4]    |
+--------------+

os> source=people | eval array = json_array(1, 2, 3), result = transform(array, (x, i)
 -> x + i) | fields result
fetched rows / total rows = 1/1
+--------------+
| result       |
+--------------+
| [1, 3, 5]    |
+--------------+
```

REDUCE

Verwendung: `reduce(array, start, merge_lambda, finish_lambda)` reduziert ein Array auf einen einzigen Wert, indem Lambda-Funktionen angewendet werden. Die Funktion wendet merge_lambda auf den Startwert und alle Array-Elemente an und wendet das dann auf das Ergebnis an. `finish_lambda`

Argumenttyp: ARRAY, ANY, LAMBDA, LAMBDA

Rückgabetyp: ANY. Das Endergebnis der Anwendung der Lambda-Funktionen auf den Startwert und das Eingabearray.

Beispiele:

```
 os> source=people | eval array = json_array(1, 2, 3), result = reduce(array, 0, (acc,
 x) -> acc + x) | fields result
fetched rows / total rows = 1/1
+-----------+
| result    |
```

```
+-----------+
| 6         |
+-----------+

os> source=people | eval array = json_array(1, 2, 3), result = reduce(array, 10, (acc,
 x) -> acc + x) | fields result
fetched rows / total rows = 1/1
+-----------+
| result    |
+-----------+
| 16        |
+-----------+

os> source=people | eval array = json_array(1, 2, 3), result = reduce(array, 0, (acc,
 x) -> acc + x, acc -> acc * 10) | fields result
fetched rows / total rows = 1/1
+-----------+
| result    |
+-----------+
| 60        |
+-----------+
```

Mathematische Funktionen von PPL

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diese PPL-Funktion unterstützen, finden Sie unter. the section called “Funktionen”

ABS

Verwendung: `ABS(x)` Berechnet den absoluten Wert von x.

Typ des Arguments: INTEGER/LONG/FLOAT/DOUBLE

Rückgabetyp: INTEGER/LONG/FLOAT/DOUBLE

Beispiel:

```
os> source=people | eval `ABS(-1)` = ABS(-1) | fields `ABS(-1)`
fetched rows / total rows = 1/1
```

```
+-----------+
| ABS(-1)   |
|-----------|
| 1         |
+-----------+
```

ACOS

Verwendung: `ACOS(x)` berechnet den Arkuskosinus von x. Es wird zurückgegeben`NULL`, wenn x nicht im Bereich von -1 bis 1 liegt.

Typ des Arguments: INTEGER/LONG/FLOAT/DOUBLE

Rückgabetyp: DOUBLE

Beispiel:

```
os> source=people | eval `ACOS(0)` = ACOS(0) | fields `ACOS(0)`
fetched rows / total rows = 1/1
+--------------------+
| ACOS(0)            |
|--------------------|
| 1.5707963267948966 |
+--------------------+
```

ASIN

Verwendung: `asin(x)` berechnet den Arkussinus von x. Es wird zurückgegeben`NULL`, wenn x nicht im Bereich von -1 bis 1 liegt.

Typ des Arguments: INTEGER/LONG/FLOAT/DOUBLE

Rückgabetyp: DOUBLE

Beispiel:

```
os> source=people | eval `ASIN(0)` = ASIN(0) | fields `ASIN(0)`
fetched rows / total rows = 1/1
+-----------+
| ASIN(0)   |
|-----------|
```

```
| 0.0       |
+-----------+
```

ATAN

Syntax: `ATAN(x)` berechnet den Arkustangens von x. `atan(y, x)` Berechnet den Arkustangens von y/x, mit der Ausnahme, dass die Vorzeichen beider Argumente den Quadranten des Ergebnisses bestimmen.

Argumenttyp: INTEGER/LONG/FLOAT/DOUBLE

Rückgabetyp: DOUBLE

Beispiel:

```
os> source=people | eval `ATAN(2)` = ATAN(2), `ATAN(2, 3)` = ATAN(2, 3) | fields
 `ATAN(2)`, `ATAN(2, 3)`
fetched rows / total rows = 1/1
+--------------------+--------------------+
| ATAN(2)            | ATAN(2, 3)         |
|--------------------+--------------------|
| 1.1071487177940904 | 0.5880026035475675 |
+--------------------+--------------------+
```

ATAN2

Verwendung: `ATAN2(y, x)` Berechnet den Arkustangens von y/x, mit der Ausnahme, dass die Vorzeichen beider Argumente den Quadranten des Ergebnisses bestimmen.

Typ des Arguments: INTEGER/LONG/FLOAT/DOUBLE

Rückgabetyp: DOUBLE

Beispiel:

```
os> source=people | eval `ATAN2(2, 3)` = ATAN2(2, 3) | fields `ATAN2(2, 3)`
fetched rows / total rows = 1/1
+--------------------+
| ATAN2(2, 3)        |
|--------------------|
| 0.5880026035475675 |
```

```
+--------------------+
```

CBRT

Verwendung: CBRT berechnet die Kubikwurzel einer Zahl.

Typ des Arguments: INTEGER/LONG/FLOAT/DOUBLE

Rückgabetyp: DOUBLE:

INTEGER/LONG/FLOAT/DOUBLE-> DOPPELT

Beispiel:

```
opensearchsql> source=location | eval `CBRT(8)` = CBRT(8), `CBRT(9.261)` = CBRT(9.261),
 `CBRT(-27)` = CBRT(-27) | fields `CBRT(8)`, `CBRT(9.261)`, `CBRT(-27)`;
fetched rows / total rows = 2/2
+-----------+---------------+-------------+
| CBRT(8)   | CBRT(9.261)   | CBRT(-27)   |
|-----------+---------------+-------------|
| 2.0       | 2.1           | -3.0        |
| 2.0       | 2.1           | -3.0        |
+-----------+---------------+-------------+
```

CEIL

Verwendung: Ein Alias für die `CEILING` Funktion. `CEILING(T)`nimmt die Obergrenze des Wertes T an.

Einschränkung: funktioniert `CEILING` nur erwartungsgemäß, wenn der Typ IEEE 754 Double beim Speichern eine Dezimalzahl anzeigt.

Argumenttyp: INTEGER/LONG/FLOAT/DOUBLE

Rückgabetyp: LONG

Beispiel:

```
os> source=people | eval `CEILING(0)` = CEILING(0), `CEILING(50.00005)` =
 CEILING(50.00005), `CEILING(-50.00005)` = CEILING(-50.00005) | fields `CEILING(0)`,
 `CEILING(50.00005)`, `CEILING(-50.00005)`
fetched rows / total rows = 1/1
```

```
+--------------+---------------------+----------------------+
| CEILING(0)   | CEILING(50.00005)   | CEILING(-50.00005)   |
|--------------+---------------------+----------------------|
| 0            | 51                  | -50                  |
+--------------+---------------------+----------------------+

os> source=people | eval `CEILING(3147483647.12345)` = CEILING(3147483647.12345),
 `CEILING(113147483647.12345)` = CEILING(113147483647.12345),
 `CEILING(3147483647.00001)` = CEILING(3147483647.00001) | fields
 `CEILING(3147483647.12345)`, `CEILING(113147483647.12345)`,
 `CEILING(3147483647.00001)`
fetched rows / total rows = 1/1
+-----------------------------+------------------------------
+-----------------------------+
| CEILING(3147483647.12345)   | CEILING(113147483647.12345)   |
 CEILING(3147483647.00001)   |
|-----------------------------+------------------------------
+-----------------------------|
| 3147483648                  | 113147483648                 | 3147483648
     |
+-----------------------------+------------------------------
+-----------------------------+
```

CONV

Verwendung: `CONV(x, a, b)` Konvertiert die Zahl x von einer Basis in eine B-Basis.

Argumenttyp: x: STRING, a: INTEGER, b: INTEGER

Rückgabetyp: STRING

Beispiel:

```
os> source=people | eval `CONV('12', 10, 16)` = CONV('12', 10, 16), `CONV('2C', 16,
 10)` = CONV('2C', 16, 10), `CONV(12, 10, 2)` = CONV(12, 10, 2), `CONV(1111, 2, 10)` =
 CONV(1111, 2, 10) | fields `CONV('12', 10, 16)`, `CONV('2C', 16, 10)`, `CONV(12, 10,
 2)`, `CONV(1111, 2, 10)`
fetched rows / total rows = 1/1
+---------------------+---------------------+------------------
+---------------------+
| CONV('12', 10, 16)   | CONV('2C', 16, 10)   | CONV(12, 10, 2)   | CONV(1111, 2, 10)
 |
|---------------------+---------------------+------------------
+---------------------|
```

```
| c                    | 44                   | 1100              | 15
 |
+----------------------+----------------------+-------------------
+---------------------+
```

COS

Verwendung: `COS(x)` Berechnet den Kosinus von x, wobei x im Bogenmaß angegeben wird.

Typ des Arguments: INTEGER/LONG/FLOAT/DOUBLE

Rückgabetyp: DOUBLE

Beispiel:

```
os> source=people | eval `COS(0)` = COS(0) | fields `COS(0)`
fetched rows / total rows = 1/1
+----------+
| COS(0)   |
|----------|
| 1.0      |
+----------+
```

COT

Verwendung: `COT(x)` berechnet den Kotangens von x. Es gibt einen out-of-range Fehler zurück, wenn x gleich 0 ist.

Typ des Arguments: INTEGER/LONG/FLOAT/DOUBLE

Rückgabetyp: DOUBLE

Beispiel:

```
os> source=people | eval `COT(1)` = COT(1) | fields `COT(1)`
fetched rows / total rows = 1/1
+--------------------+
| COT(1)             |
|--------------------|
| 0.6420926159343306 |
+--------------------+
```

CRC32

Verwendung: CRC32 Berechnet einen Wert für die zyklische Redundanzprüfung und gibt einen 32-Bit-Wert ohne Vorzeichen zurück.

Argumenttyp: STRING

Rückgabetyp: LONG

Beispiel:

```
os> source=people | eval `CRC32('MySQL')` = CRC32('MySQL') | fields `CRC32('MySQL')`
fetched rows / total rows = 1/1
+------------------+
| CRC32('MySQL')   |
|------------------|
| 3259397556       |
+------------------+
```

DEGREES

Verwendung: DEGREES(x) wandelt X von Radiant in Grad um.

Argumenttyp: INTEGER/LONG/FLOAT/DOUBLE

Rückgabetyp: DOUBLE

Beispiel:

```
os> source=people | eval `DEGREES(1.57)` = DEGREES(1.57) | fields `DEGREES(1.57)`
fetched rows / total rows  = 1/1
+-------------------+
| DEGREES(1.57)     |
|-------------------|
| 89.95437383553924 |
+-------------------+
```

E

Verwendung: E() gibt die Euler-Zahl zurück.

Rückgabetyp: DOUBLE

Beispiel:

```
os> source=people | eval `E()` = E() | fields `E()`
fetched rows / total rows = 1/1
+-------------------+
| E()               |
|-------------------|
| 2.718281828459045 |
+-------------------+
```

EXP

Verwendungszweck: EXP(x) gibt e potenziert mit x zurück.

Typ des Arguments: INTEGER/LONG/FLOAT/DOUBLE

Rückgabetyp: DOUBLE

Beispiel:

```
os> source=people | eval `EXP(2)` = EXP(2) | fields `EXP(2)`
fetched rows / total rows = 1/1
+------------------+
| EXP(2)           |
|------------------|
| 7.38905609893065 |
+------------------+
```

FLOOR

Verwendungszweck: FLOOR(T) Nimmt den unteren Teil des Werts T ein.

Einschränkung: funktioniert FLOOR nur erwartungsgemäß, wenn der IEEE 754-Double-Typ beim Speichern eine Dezimalzahl anzeigt.

Argumenttyp: INTEGER/LONG/FLOAT/DOUBLE

Rückgabetyp: LONG

Beispiel:

```
os> source=people | eval `FLOOR(0)` = FLOOR(0), `FLOOR(50.00005)` = FLOOR(50.00005),
 `FLOOR(-50.00005)` = FLOOR(-50.00005) | fields `FLOOR(0)`, `FLOOR(50.00005)`,
 `FLOOR(-50.00005)`
```

```
fetched rows / total rows = 1/1
+------------+------------------+--------------------+
| FLOOR(0)   | FLOOR(50.00005)   | FLOOR(-50.00005)   |
|------------+------------------+--------------------|
| 0          | 50                | -51                |
+------------+------------------+--------------------+

os> source=people | eval `FLOOR(3147483647.12345)` = FLOOR(3147483647.12345),
 `FLOOR(113147483647.12345)` = FLOOR(113147483647.12345), `FLOOR(3147483647.00001)`
 = FLOOR(3147483647.00001) | fields `FLOOR(3147483647.12345)`,
 `FLOOR(113147483647.12345)`, `FLOOR(3147483647.00001)`
fetched rows / total rows = 1/1
+--------------------------+----------------------------+--------------------------+
| FLOOR(3147483647.12345)   | FLOOR(113147483647.12345)   | FLOOR(3147483647.00001)   |
|--------------------------+----------------------------+--------------------------|
| 3147483647                | 113147483647                | 3147483647                |
+--------------------------+----------------------------+--------------------------+

os> source=people | eval `FLOOR(282474973688888.022)` = FLOOR(282474973688888.022),
 `FLOOR(9223372036854775807.022)` = FLOOR(9223372036854775807.022),
 `FLOOR(9223372036854775807.0000001)` = FLOOR(9223372036854775807.0000001)
 | fields `FLOOR(282474973688888.022)`, `FLOOR(9223372036854775807.022)`,
 `FLOOR(9223372036854775807.0000001)`
fetched rows / total rows = 1/1
+-----------------------------+-----------------------------------
+--------------------------------------+
| FLOOR(282474973688888.022)   | FLOOR(9223372036854775807.022)   |
 FLOOR(9223372036854775807.0000001)   |
|-----------------------------+-----------------------------------
+--------------------------------------|
| 282474973688888              | 9223372036854775807             | 9223372036854775807
                  |
+-----------------------------+-----------------------------------
+--------------------------------------+
```

LN

Verwendung: `LN(x)` Gibt den natürlichen Logarithmus von x zurück.

Typ des Arguments: INTEGER/LONG/FLOAT/DOUBLE

Rückgabetyp: DOUBLE

Beispiel:

```
os> source=people | eval `LN(2)` = LN(2) | fields `LN(2)`
fetched rows / total rows = 1/1
+--------------------+
| LN(2)              |
|--------------------|
| 0.6931471805599453 |
+--------------------+
```

LOG

Verwendung: `LOG(x)` Gibt den natürlichen Logarithmus von x zurück, der dem Logarithmus zur Basis e von X entspricht. log (B, x) entspricht log (x) /log (B).

Typ des Arguments: INTEGER/LONG/FLOAT/DOUBLE

Rückgabetyp: DOUBLE

Beispiel:

```
os> source=people | eval `LOG(2)` = LOG(2), `LOG(2, 8)` = LOG(2, 8) | fields `LOG(2)`,
 `LOG(2, 8)`
fetched rows / total rows = 1/1
+--------------------+-------------+
| LOG(2)             | LOG(2, 8)   |
|--------------------+-------------|
| 0.6931471805599453 | 3.0         |
+--------------------+-------------+
```

LOG2

Verwendung: `LOG2(x)` entspricht`log(x)/log(2)`.

Typ des Arguments: INTEGER/LONG/FLOAT/DOUBLE

Rückgabetyp: DOUBLE

Beispiel:

```
os> source=people | eval `LOG2(8)` = LOG2(8) | fields `LOG2(8)`
fetched rows / total rows = 1/1
+-----------+
```

```
| LOG2(8)   |
|-----------|
| 3.0       |
+-----------+
```

LOG10

Verwendung: `LOG10(x)` entspricht`log(x)/log(10)`.

Typ des Arguments: INTEGER/LONG/FLOAT/DOUBLE

Rückgabetyp: DOUBLE

Beispiel:

```
os> source=people | eval `LOG10(100)` = LOG10(100) | fields `LOG10(100)`
fetched rows / total rows = 1/1
+--------------+
| LOG10(100)   |
|--------------|
| 2.0          |
+--------------+
```

MOD

Verwendung: `MOD(n, m)` berechnet den Rest der Zahl n geteilt durch m.

Typ des Arguments: INTEGER/LONG/FLOAT/DOUBLE

Rückgabetyp: Breiterer Typ zwischen den Typen von n und m, wenn m ein Wert ungleich Null ist. Wenn m gleich 0 ist, wird NULL zurückgegeben.

Beispiel:

```
os> source=people | eval `MOD(3, 2)` = MOD(3, 2), `MOD(3.1, 2)` = MOD(3.1, 2) | fields
 `MOD(3, 2)`, `MOD(3.1, 2)`
fetched rows / total rows = 1/1
+-------------+---------------+
| MOD(3, 2)   | MOD(3.1, 2)   |
|-------------+---------------|
| 1           | 1.1           |
+-------------+---------------+
```

PI

Syntax: `PI()` gibt die Konstante Pi zurück.

Rückgabetyp: DOUBLE

Beispiel:

```
os> source=people | eval `PI()` = PI() | fields `PI()`
fetched rows / total rows = 1/1
+-------------------+
| PI()              |
|-------------------|
| 3.141592653589793 |
+-------------------+
```

POW

Verwendung: `POW(x, y)` Berechnet den Wert von x potenziert mit y. Schlechte Eingaben geben ein `NULL` Ergebnis zurück.

Typ des Arguments: INTEGER/LONG/FLOAT/DOUBLE

Rückgabetyp: DOUBLE

Synonyme: `POWER(_, _)`

Beispiel:

```
os> source=people | eval `POW(3, 2)` = POW(3, 2), `POW(-3, 2)` = POW(-3, 2), `POW(3,
 -2)` = POW(3, -2) | fields `POW(3, 2)`, `POW(-3, 2)`, `POW(3, -2)`
fetched rows / total rows = 1/1
+-------------+--------------+--------------------+
| POW(3, 2)   | POW(-3, 2)   | POW(3, -2)         |
|-------------+--------------+--------------------|
| 9.0         | 9.0          | 0.1111111111111111 |
+-------------+--------------+--------------------+
```

POWER

Verwendung: `POWER(x, y)` berechnet den Wert von x potenziert mit y. Schlechte Eingaben geben ein `NULL` Ergebnis zurück.

Typ des Arguments: INTEGER/LONG/FLOAT/DOUBLE

Rückgabetyp: DOUBLE

Synonyme: `POW(_, _)`

Beispiel:

```
os> source=people | eval `POWER(3, 2)` = POWER(3, 2), `POWER(-3, 2)` = POWER(-3, 2),
 `POWER(3, -2)` = POWER(3, -2) | fields `POWER(3, 2)`, `POWER(-3, 2)`, `POWER(3, -2)`
fetched rows / total rows = 1/1
+---------------+----------------+--------------------+
| POWER(3, 2)   | POWER(-3, 2)   | POWER(3, -2)       |
|---------------+----------------+--------------------|
| 9.0           | 9.0            | 0.1111111111111111 |
+---------------+----------------+--------------------+
```

RADIANS

Verwendung: `RADIANS(x)` wandelt X von Grad in Radiant um.

Argumenttyp: INTEGER/LONG/FLOAT/DOUBLE

Rückgabetyp: DOUBLE

Beispiel:

```
os> source=people | eval `RADIANS(90)` = RADIANS(90) | fields `RADIANS(90)`
fetched rows / total rows  = 1/1
+--------------------+
| RADIANS(90)        |
|--------------------|
| 1.5707963267948966 |
+--------------------+
```

RAND

Verwendung:`RAND()`/`RAND(N)`gibt einen zufälligen Gleitkommawert im Bereich 0 <= Wert < 1,0 zurück. Wenn Sie die Ganzzahl N angeben, initialisiert die Funktion den Startwert vor der Ausführung. Eine Folge dieses Verhaltens ist, dass bei einem identischen Argument N jedes Mal derselbe Wert `rand(N)` zurückgegeben wird, wodurch eine wiederholbare Folge von Spaltenwerten entsteht.

Argumenttyp: INTEGER

Rückgabetyp: FLOAT

Beispiel:

```
os> source=people | eval `RAND(3)` = RAND(3) | fields `RAND(3)`
fetched rows / total rows = 1/1
+------------+
| RAND(3)    |
|------------|
| 0.73105735 |
+------------+
```

ROUND

Verwendung: `ROUND(x, d)` rundet das Argument x auf d Dezimalstellen ab. Wenn Sie d nicht angeben, wird standardmäßig 0 verwendet.

Typ des Arguments: INTEGER/LONG/FLOAT/DOUBLE

Rückgabetyp Map:

- (GANZZAHL/LANG [, GANZZAHL]) -> LANG
- (GLEITKOMMAZAHL/DOPPELT [, GANZZAHL]) -> LANG

Beispiel:

```
os> source=people | eval `ROUND(12.34)` = ROUND(12.34), `ROUND(12.34, 1)` =
 ROUND(12.34, 1), `ROUND(12.34, -1)` = ROUND(12.34, -1), `ROUND(12, 1)` = ROUND(12, 1)
 | fields `ROUND(12.34)`, `ROUND(12.34, 1)`, `ROUND(12.34, -1)`, `ROUND(12, 1)`
fetched rows / total rows = 1/1
+---------------+------------------+--------------------+----------------+
| ROUND(12.34)  | ROUND(12.34, 1)  | ROUND(12.34, -1)   | ROUND(12, 1)   |
|---------------+------------------+--------------------+----------------|
| 12.0          | 12.3             | 10.0               | 12             |
+---------------+------------------+--------------------+----------------+
```

SIGN

Verwendung: `SIGN` Gibt das Vorzeichen des Arguments als -1, 0 oder 1 zurück, je nachdem, ob die Zahl negativ, Null oder positiv ist.

Typ des Arguments: INTEGER/LONG/FLOAT/DOUBLE

Rückgabetyp: INTEGER

Beispiel:

```
os> source=people | eval `SIGN(1)` = SIGN(1), `SIGN(0)` = SIGN(0), `SIGN(-1.1)` =
 SIGN(-1.1) | fields `SIGN(1)`, `SIGN(0)`, `SIGN(-1.1)`
fetched rows / total rows = 1/1
+-----------+-----------+--------------+
| SIGN(1)   | SIGN(0)   | SIGN(-1.1)   |
|-----------+-----------+--------------|
| 1         | 0         | -1           |
+-----------+-----------+--------------+
```

SIN

Verwendung: `sin(x)` Berechnet den Sinus von x, wobei x im Bogenmaß angegeben wird.

Typ des Arguments: INTEGER/LONG/FLOAT/DOUBLE

Rückgabetyp: DOUBLE

Beispiel:

```
os> source=people | eval `SIN(0)` = SIN(0) | fields `SIN(0)`
fetched rows / total rows = 1/1
+----------+
| SIN(0)   |
|----------|
| 0.0      |
+----------+
```

SQRT

Verwendung: SQRT berechnet die Quadratwurzel einer nicht negativen Zahl.

Typ des Arguments: INTEGER/LONG/FLOAT/DOUBLE

Rückgabetyp Map:

- (Nicht negativ) INTEGER/LONG/FLOAT/DOUBLE -> DOPPELT

- (Negativ) INTEGER/LONG/FLOAT/DOUBLE -> NULL

Beispiel:

```
os> source=people | eval `SQRT(4)` = SQRT(4), `SQRT(4.41)` = SQRT(4.41) | fields
 `SQRT(4)`, `SQRT(4.41)`
fetched rows / total rows = 1/1
+-----------+--------------+
| SQRT(4)   | SQRT(4.41)   |
|-----------+--------------|
| 2.0       | 2.1          |
+-----------+--------------+
```

PPL-String-Funktionen

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diese PPL-Funktion unterstützen, finden Sie unter. the section called “Funktionen”

`CONCAT`

Verwendung: `CONCAT(str1, str2, ...., str_9)` Addiert bis zu 9 Zeichenketten zusammen.

Typ des Arguments:

- ZEICHENFOLGE, ZEICHENFOLGE,..., ZEICHENFOLGE
- Rückgabetyp: STRING

Beispiel:

```
os> source=people | eval `CONCAT('hello', 'world')` = CONCAT('hello', 'world'),
 `CONCAT('hello ', 'whole ', 'world', '!')` = CONCAT('hello ', 'whole ', 'world', '!')
 | fields `CONCAT('hello', 'world')`, `CONCAT('hello ', 'whole ', 'world', '!')`
fetched rows / total rows = 1/1
+---------------------------+-------------------------------------------+
| CONCAT('hello', 'world')  | CONCAT('hello ', 'whole ', 'world', '!')  |
|---------------------------+-------------------------------------------|
| helloworld                | hello whole world!                        |
```

```
+---------------------------+-------------------------------------------+
```

CONCAT_WS

Verwendung: `CONCAT_WS(sep, str1, str2)` verkettet zwei oder mehr Zeichenketten unter Verwendung eines angegebenen Trennzeichens zwischen ihnen.

Typ des Arguments:

- ZEICHENFOLGE, ZEICHENFOLGE,..., ZEICHENFOLGE
- Rückgabetyp: STRING

Beispiel:

```
os> source=people | eval `CONCAT_WS(',', 'hello', 'world')` = CONCAT_WS(',', 'hello',
 'world') | fields `CONCAT_WS(',', 'hello', 'world')`
fetched rows / total rows = 1/1
+-----------------------------------+
| CONCAT_WS(',', 'hello', 'world')   |
|-----------------------------------|
| hello,world                       |
+-----------------------------------+
```

LENGTH

Verwendung: `length(str)` Gibt die Länge der Eingabezeichenfolge in Byte zurück.

Typ des Arguments:

- STRING
- Rückgabetyp: INTEGER

Beispiel:

```
os> source=people | eval `LENGTH('helloworld')` = LENGTH('helloworld') | fields
 `LENGTH('helloworld')`
fetched rows / total rows = 1/1
+------------------------+
| LENGTH('helloworld')   |
|------------------------|
```

```
| 10                    |
+-----------------------+
```

LOWER

Verwendung: `lower(string)` Konvertiert die Eingabezeichenfolge in Kleinbuchstaben.

Typ des Arguments:

- STRING
- Rückgabetyp: STRING

Beispiel:

```
os> source=people | eval `LOWER('helloworld')` = LOWER('helloworld'),
 `LOWER('HELLOWORLD')` = LOWER('HELLOWORLD') | fields `LOWER('helloworld')`,
 `LOWER('HELLOWORLD')`
fetched rows / total rows = 1/1
+----------------------+-----------------------+
| LOWER('helloworld')   | LOWER('HELLOWORLD')   |
|----------------------+-----------------------|
| helloworld            | helloworld            |
+----------------------+-----------------------+
```

LTRIM

Verwendung: `ltrim(str)` entfernt führende Leerzeichen aus der Eingabezeichenfolge.

Typ des Arguments:

- STRING
- Rückgabetyp: STRING

Beispiel:

```
os> source=people | eval `LTRIM('   hello')` = LTRIM('   hello'), `LTRIM('hello   ')` =
 LTRIM('hello   ') | fields `LTRIM('   hello')`, `LTRIM('hello   ')`
fetched rows / total rows = 1/1
+---------------------+---------------------+
| LTRIM('   hello')   | LTRIM('hello   ')   |
|---------------------+---------------------|
```

```
| hello               | hello               |
+---------------------+---------------------+
```

POSITION

Syntax: `POSITION(substr IN str)` Gibt die Position des ersten Vorkommens einer Teilzeichenfolge in einer Zeichenfolge zurück. Es gibt 0 zurück, wenn die Teilzeichenfolge nicht in der Zeichenfolge enthalten ist. Sie gibt NULL zurück, wenn ein Argument NULL ist.

Typ des Arguments:

- ZEICHENFOLGE, ZEICHENFOLGE
- Rückgabetyp INTEGER

Beispiel:

```
os> source=people | eval `POSITION('world' IN 'helloworld')` = POSITION('world'
 IN 'helloworld'), `POSITION('invalid' IN 'helloworld')`= POSITION('invalid' IN
 'helloworld')  | fields `POSITION('world' IN 'helloworld')`, `POSITION('invalid' IN
 'helloworld')`
fetched rows / total rows = 1/1
+-------------------------------------+---------------------------------------+
| POSITION('world' IN 'helloworld')   | POSITION('invalid' IN 'helloworld')   |
|-------------------------------------+---------------------------------------|
| 6                                   | 0                                     |
+-------------------------------------+---------------------------------------+
```

REVERSE

Verwendung: `REVERSE(str)` Gibt die umgekehrte Zeichenfolge der Eingabezeichenfolge zurück.

Typ des Arguments:

- STRING
- Rückgabetyp: STRING

Beispiel:

```
os> source=people | eval `REVERSE('abcde')` = REVERSE('abcde') | fields
 `REVERSE('abcde')`
```

```
fetched rows / total rows = 1/1
+--------------------+
| REVERSE('abcde')   |
|--------------------|
| edcba              |
+--------------------+
```

RIGHT

Verwendung: `right(str, len)` Gibt die am weitesten rechts stehenden Zeichen der Eingabezeichenfolge zurück. Es gibt 0 zurück, wenn die Teilzeichenfolge nicht in der Zeichenfolge enthalten ist. Sie gibt NULL zurück, wenn ein Argument NULL ist.

Typ des Arguments:

- ZEICHENFOLGE, GANZZAHL
- Rückgabetyp: STRING

Beispiel:

```
os> source=people | eval `RIGHT('helloworld', 5)` = RIGHT('helloworld', 5),
 `RIGHT('HELLOWORLD', 0)` = RIGHT('HELLOWORLD', 0) | fields `RIGHT('helloworld', 5)`,
 `RIGHT('HELLOWORLD', 0)`
fetched rows / total rows = 1/1
+--------------------------+--------------------------+
| RIGHT('helloworld', 5)   | RIGHT('HELLOWORLD', 0)   |
|--------------------------+--------------------------|
| world                    |                          |
+--------------------------+--------------------------+
```

RTRIM

Verwendung: `rtrim(str)` schneidet nachfolgende Leerzeichen aus der Eingabezeichenfolge ab.

Typ des Arguments:

- STRING
- Rückgabetyp: STRING

Beispiel:

```
os> source=people | eval `RTRIM('   hello')` = RTRIM('   hello'), `RTRIM('hello   ')` =
 RTRIM('hello   ') | fields `RTRIM('   hello')`, `RTRIM('hello   ')`
fetched rows / total rows = 1/1
+---------------------+---------------------+
| RTRIM('   hello')   | RTRIM('hello   ')   |
|---------------------+---------------------|
|    hello            | hello               |
+---------------------+---------------------+
```

SUBSTRING

Verwendungszweck: `substring(str, start)` oder `substring(str, start, length)` gibt eine Teilzeichenfolge der Eingabezeichenfolge zurück. Ohne Angabe einer Länge wird die gesamte Zeichenfolge von der Startposition zurückgegeben.

Typ des Arguments:

- ZEICHENFOLGE, GANZZAHL, GANZZAHL
- Rückgabetyp: STRING

Beispiel:

```
os> source=people | eval `SUBSTRING('helloworld', 5)` = SUBSTRING('helloworld',
 5), `SUBSTRING('helloworld', 5, 3)` = SUBSTRING('helloworld', 5, 3) | fields
 `SUBSTRING('helloworld', 5)`, `SUBSTRING('helloworld', 5, 3)`
fetched rows / total rows = 1/1
+------------------------------+---------------------------------+
| SUBSTRING('helloworld', 5)   | SUBSTRING('helloworld', 5, 3)   |
|------------------------------+---------------------------------|
| oworld                       | owo                             |
+------------------------------+---------------------------------+
```

TRIM

Verwendung: `trim(string)` entfernt führende und nachfolgende Leerzeichen aus der Eingabezeichenfolge.

Typ des Arguments:

- STRING

- Rückgabetyp: STRING

Beispiel:

```
os> source=people | eval `TRIM('   hello')` = TRIM('   hello'), `TRIM('hello   ')` =
 TRIM('hello   ') | fields `TRIM('   hello')`, `TRIM('hello   ')`
fetched rows / total rows = 1/1
+--------------------+--------------------+
| TRIM('   hello')   | TRIM('hello   ')   |
|--------------------+--------------------|
| hello              | hello              |
+--------------------+--------------------+
```

UPPER

Verwendung: `upper(string)` Konvertiert die Eingabezeichenfolge in Großbuchstaben.

Typ des Arguments:

- STRING
- Rückgabetyp: STRING

Beispiel:

```
os> source=people | eval `UPPER('helloworld')` = UPPER('helloworld'),
 `UPPER('HELLOWORLD')` = UPPER('HELLOWORLD') | fields `UPPER('helloworld')`,
 `UPPER('HELLOWORLD')`
fetched rows / total rows = 1/1
+----------------------+----------------------+
| UPPER('helloworld')   | UPPER('HELLOWORLD')   |
|----------------------+----------------------|
| HELLOWORLD            | HELLOWORLD            |
+----------------------+----------------------+
```

Funktionen zur Konvertierung des PPL-Typs

> **Note**
>
> Informationen darüber, welche AWS Datenquellenintegrationen diese PPL-Funktion unterstützen, finden Sie unter. the section called “Funktionen”

`TRIM`

Verwendung: wandelt `cast(expr as dateType)` den `expr` in den um `dataType` und gibt den Wert von zurück. `dataType`

Es gelten die folgenden Konvertierungsregeln:

Geben Sie Konvertierungsregeln ein

Src/Target	STRING	NUMBER	BOOLEAN	TIMESTAMP (ZEITSTEMPEL)	DATUM	TIME
STRING		Hinweis 1	Anmerkung 1	TIMESTAMP()	DATUM()	TIME()
NUMBER	Anmerkung 1		v! =0	N/A	–	N/A
BOOLEAN	Hinweis 1	v? 1:0		N/A	–	N/A
TIMESTAMP (ZEITSTEMPEL)	Anmerkung 1	N/A	N/A		DATUM()	TIME()
DATUM	Anmerkung 1	N/A	–	–		N/A
TIME	Anmerkung 1	N/A	–	–	N/A	

Beispiel für die Umwandlung in eine Zeichenfolge:

```
os> source=people | eval `cbool` = CAST(true as string), `cint` = CAST(1 as string),
 `cdate` = CAST(CAST('2012-08-07' as date) as string) | fields `cbool`, `cint`, `cdate`
fetched rows / total rows = 1/1
+---------+--------+------------+
| cbool   | cint   | cdate      |
|---------+--------+------------|
| true    | 1      | 2012-08-07 |
```

```
+---------+--------+------------+
```

Beispiel für die Umwandlung in eine Zahl:

```
os> source=people | eval `cbool` = CAST(true as int), `cstring` = CAST('1' as int) |
 fields `cbool`, `cstring`
fetched rows / total rows = 1/1
+---------+-----------+
| cbool   | cstring   |
|---------+-----------|
| 1       | 1         |
+---------+-----------+
```

Beispiel für die aktuelle Besetzung:

```
os> source=people | eval `cdate` = CAST('2012-08-07' as date), `ctime` =
 CAST('01:01:01' as time), `ctimestamp` = CAST('2012-08-07 01:01:01' as timestamp) |
 fields `cdate`, `ctime`, `ctimestamp`
fetched rows / total rows = 1/1
+------------+----------+---------------------+
| cdate      | ctime    | ctimestamp          |
|------------+----------+---------------------|
| 2012-08-07 | 01:01:01 | 2012-08-07 01:01:01 |
+------------+----------+---------------------+
```

Beispiel für eine verkettete Besetzung:

```
os> source=people | eval `cbool` = CAST(CAST(true as string) as boolean) | fields
 `cbool`
fetched rows / total rows = 1/1
+---------+
| cbool   |
|---------|
| True    |
+---------+
```

Überwachung von Amazon OpenSearch Service-Domains

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung von Amazon OpenSearch Service und Ihren anderen AWS Lösungen. AWS bietet die folgenden Tools, um Ihre OpenSearch Serviceressourcen zu überwachen, Probleme zu melden und gegebenenfalls automatische Maßnahmen zu ergreifen:

Amazon CloudWatch

Amazon CloudWatch überwacht Ihre OpenSearch Serviceressourcen in Echtzeit. Sie können Metriken erfassen und verfolgen, benutzerdefinierte Dashboards erstellen und Alarme festlegen, die Sie benachrichtigen oder Maßnahmen ergreifen, wenn eine Metrik einen bestimmten Schwellenwert erreicht. Weitere Informationen finden Sie im CloudWatch Amazon-Benutzerhandbuch.

CloudWatch Amazon-Protokolle

Mit Amazon CloudWatch Logs können Sie Ihre OpenSearch Protokolldateien überwachen, speichern und darauf zugreifen. CloudWatch Logs überwacht die Informationen in Protokolldateien und kann Sie benachrichtigen, wenn bestimmte Schwellenwerte erreicht werden. Weitere Informationen finden Sie im Amazon CloudWatch Logs-Benutzerhandbuch.

Amazon EventBridge

Amazon EventBridge liefert nahezu in Echtzeit einen Stream von Systemereignissen, die Änderungen in Ihren OpenSearch Service-Domains beschreiben. Sie können Regeln erstellen, die auf bestimmte Ereignisse achten und automatisierte Aktionen in anderen AWS Diensten auslösen, wenn diese Ereignisse eintreten. Weitere Informationen finden Sie im EventBridge Amazon-Benutzerhandbuch.

AWS CloudTrail

AWS CloudTrail erfasst Konfigurations-API-Aufrufe an OpenSearch Service als Ereignisse. Es kann diese Ereignisse an einen von Ihnen angegebenen Amazon-S3-Bucket übermitteln. Anhand dieser Informationen können Sie feststellen, welche Benutzer und Konten Anfragen gestellt haben, die Quell-IP-Adresse, von der die Anfragen gestellt wurden und wann die Anfragen aufgetreten sind. Weitere Informationen finden Sie im AWS CloudTrail Benutzerhandbuch.

Themen

- Überwachung von OpenSearch Cluster-Metriken mit Amazon CloudWatch
- OpenSearch Protokolle mit Amazon CloudWatch Logs überwachen
- Überwachung von Auditprotokollen in Amazon OpenSearch Service
- Überwachung von OpenSearch Service-Ereignissen mit Amazon EventBridge
- Überwachung von Amazon OpenSearch Service API-Aufrufen mit AWS CloudTrail

Überwachung von OpenSearch Cluster-Metriken mit Amazon CloudWatch

Amazon OpenSearch Service veröffentlicht Daten aus Ihren Domains bei Amazon CloudWatch. CloudWatch ermöglicht Ihnen, Statistiken zu diesen Datenpunkten als geordneten Satz von Zeitreihendaten, als Metriken bezeichnet, abzurufen. OpenSearch Der Service sendet die meisten Metriken CloudWatch in 60-Sekunden-Intervallen an. Wenn Sie universelle oder magnetische EBS-Volumes verwenden, werden die EBS-Volume-Metriken nur alle fünf Minuten aktualisiert. Alle kumulativen Metriken (z. `ThreadpoolWriteRejected` B.`ThreadpoolSearchRejected`) befinden sich im Arbeitsspeicher und verlieren ihren Status. Metriken werden bei einem Node-Drop, einem Node-Bounce, einem Node-Austausch und einer Blau/Grün-Implementierung zurückgesetzt. Weitere Informationen über Amazon CloudWatch finden Sie im CloudWatch Amazon-Benutzerhandbuch.

Die OpenSearch Service-Konsole zeigt eine Reihe von Diagrammen an, die auf den unformatierten Daten aus basieren CloudWatch. Abhängig von Ihren Anforderungen möchten Sie möglicherweise Clusterdaten in CloudWatch den Diagrammen in der Konsole anzeigen. Der Service archiviert die Metriken für zwei Wochen, bevor sie verworfen werden. Die Metriken werden ohne Zusatzkosten bereitgestellt, aber es fallen CloudWatch weiterhin Gebühren für das Erstellen von Dashboards und Alarmen an. Weitere Informationen finden Sie unter CloudWatchAmazon-Preise.

OpenSearch Service veröffentlicht die folgenden Kennzahlen für CloudWatch:

- the section called “Cluster-Metriken”
- the section called “Dedizierte Hauptknoten-Metriken”
- the section called “EBS-Volume-Metriken”
- the section called “Instance-Metriken”
- the section called “UltraWarm Metriken”
- the section called “Dedizierte Statistiken für Koordinator-Knoten”

- the section called “Cold-Storage-Metriken”
- the section called “Warnungsmetriken”
- the section called “Metriken zur Anomalieerkennung”
- the section called “Asynchrone Suchmetriken”
- the section called “SQL-Metriken”
- the section called “k-NN-Metriken”
- the section called “Metriken für Cluster-übergreifende Suchen”
- the section called “Cluster-übergreifende Replikationsmetriken”
- the section called “Learning-to-Rank-Metriken”
- the section called “Metriken für Piped Processing Language”

Metriken anzeigen in CloudWatch

CloudWatch Metriken werden zunächst nach dem Service-Namespace und anschließend nach den verschiedenen Dimensionskombinationen in den einzelnen Namespaces gruppiert.

Zeigen Sie -Metriken mithilfe der CloudWatch -Konsole wie folgt an:

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Suchen Sie im linken Navigationsbereich nach Metrics (Metriken) und wählen Sie All metrics (Alle Metriken) aus. Wählen Sie den ES/ OpenSearchService Namespace aus.
3. Wählen Sie eine Dimension aus, um die entsprechenden Metriken anzuzeigen. Metriken für einzelne Knoten befinden sich in der `ClientId, DomainName, NodeId`-Dimension. Cluster-Metriken befinden sich in der `Per-Domain, Per-Client Metrics`-Dimension. Einige Knotenmetriken werden auf Clusterebene aggregiert und somit in beide Dimensionen eingeschlossen. Shard-Metriken befinden sich in der `ClientId, DomainName, NodeId, ShardRole`-Dimension.

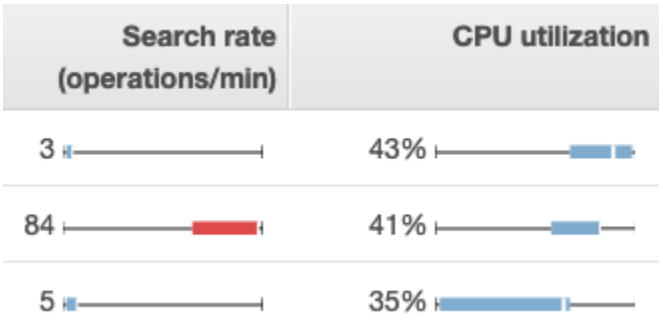
Um eine Liste von Metriken anzuzeigen, verwenden Sie AWS CLI

Führen Sie den folgenden Befehl aus:

```
aws cloudwatch list-metrics --namespace "AWS/ES"
```

OpenSearch Integritäts-Interpretations-Diagrammen

Verwenden Sie die Registerkarten Clusterstatus und Instanzstatus, um Metriken in OpenSearch Service anzuzeigen. Die Registerkarte Instance-Status macht mithilfe von Box-Diagrammen den Status eines jeden OpenSearch Knotens at-a-glance sichtbar:



- Jedes farbige Feld zeigt den Wertebereich für den Knoten im angegebenen Zeitraum.
- Blaue Felder stehen für Werte, die mit anderen Knoten konsistent sind. Rote Felder stellen Ausreißer dar.
- Die weiße Linie innerhalb der einzelnen Felder zeigt den aktuellen Wert des Knotens.
- Die "Whisker" auf beiden Seiten jedes Feldes zeigen die minimalen und maximalen Werte für alle Knoten über den Zeitraum.

Wenn Sie Änderungen an der Konfiguration Ihrer Domain vornehmen, verdoppelt sich häufig die Größe der Liste mit den einzelnen Instances auf den Registerkarten Cluster health (Cluster-Zustand) und Instance health (Instance-Zustand) für einen kurzen Zeitraum, bevor wieder die richtige Zahl angezeigt wird. Eine Erklärung dieser Verhaltensweise finden Sie unter the section called “Konfigurationsänderungen”.

Cluster-Metriken

Amazon OpenSearch Service bietet die folgenden Metriken für Cluster.

Metrik	Beschreibung
`ClusterStatus.green`	Ein Wert von 1 gibt an, dass alle Index-Shards zu Knoten im Cluster zugeordnet sind. Relevante Statistiken: Maximum

Metrik	Beschreibung
`ClusterStatus.yellow`	Ein Wert von 1 bedeutet, dass die primären Shards für alle Indizes den Knoten im Cluster zugewiesen sind, die Replikat-Shards für mindestens einen Index jedoch nicht. Weitere Informationen finden Sie unter the section called “Gelber Cluster-Status”. Relevante Statistiken: Maximum
`ClusterStatus.red`	Ein Wert von 1 gibt an, dass die Primär- und Replikat-Shards für mindestens einen Index keinen Knoten im Cluster zugeordnet sind. Weitere Informationen finden Sie unter the section called “Roter Cluster-Status”. Relevante Statistiken: Maximum
`Shards.active`	Die Gesamtzahl der aktiven primären und Replikat-Shards. Relevante Statistiken: Maximum, Summe
`Shards.unassigned`	Die Anzahl der Shards, die Knoten im Cluster nicht zugeordnet sind. Relevante Statistiken: Maximum, Summe
`Shards.delayedUnassigned`	Die Anzahl der Shards, deren Knotenzuordnung durch die Timeout-Einstellungen verzögert wurde. Relevante Statistiken: Maximum, Summe
`Shards.activePrimary`	Die Anzahl der aktiven primären Shards. Relevante Statistiken: Maximum, Summe
`Shards.initializing`	Die Anzahl der Shards, die derzeit initialisiert werden. Relevante Statistiken: Summe
`Shards.relocating`	Die Anzahl der Shards, die derzeit verschoben werden. Relevante Statistiken: Summe

Metrik	Beschreibung
`Nodes`	Die Anzahl der Knoten im OpenSearch Service-Cluster, einschließlich dedizierte Hauptknoten und UltraWarm Knoten. Weitere Informationen finden Sie unter the section called “Konfigurationsänderungen”. Relevante Statistiken: Maximum
`SearchableDocuments`	Die Gesamtzahl der durchsuchbaren Dokumente in allen Datenknoten im Cluster. Relevante Statistiken: Minimum, Maximum, Durchschnitt
`DeletedDocuments`	Die Gesamtzahl der zum Löschen markierten Dokumente in allen Datenknoten im Cluster. Diese Dokumente erscheinen nicht mehr in den Suchergebnissen. Sie entfernen OpenSearch gelöschte Dokumente während Segmentzusammenführungen vom Datenträger. Diese Metrik steigt nach Löschanfragen und sinkt nach Segmentzusammenführungen. Relevante Statistiken: Minimum, Maximum, Durchschnitt
`CPUUtilization`	Der Prozentsatz der CPU-Nutzung für Datenknoten im Cluster. „Maximum“ zeigt den Knoten mit der höchsten CPU-Nutzung an. „Average“ (Durchschnitt) stellt alle Knoten im Cluster dar. Diese Metrik ist auch für einzelne Knoten verfügbar. Relevante Statistiken: Maximum, Durchschnitt

Metrik	Beschreibung
`FreeStorageSpace`	Der freie Platz für Datenknoten im Cluster. `Sum` zeigt den gesamten freien Speicherplatz für den Cluster an, Sie müssen jedoch den Zeitraum bei einer Minute belassen, um einen genauen Wert zu erhalten. `Minimum` und `Maximum` zeigen die Knoten mit dem wenigsten bzw. dem meisten freien Speicherplatz an. Diese Metrik ist auch für individuelle Knoten verfügbar. OpenSearch Der Service gibt eine aus`ClusterBlockException` , wenn diese Metrik erreicht `0` ist. Zum Wiederherstellen müssen Sie entweder Indizes löschen, größere Instances hinzufügen oder EBS-basierten Speicher zu vorhandenen Instances hinzufügen. Weitere Informationen hierzu finden Sie unter the section called “Zu wenig verfügbarer Speicherplatz”. Dieser Wert wird in der OpenSearch Servicekonsole in GiB angezeigt. In der CloudWatch Amazon-Konsole wird dieser Wert in MiB angezeigt. **Note** `FreeStorageSpace` wird immer niedriger sein als die Werte, die von OpenSearch `_cluster/stats` und zur `_cat/allocation` APIs Verfügung gestellt werden. OpenSearch Der Service reserviert einen Prozentsatz des Speicherplatzes auf jeder Instance für interne Operationen. Weitere Informationen finden Sie unter Berechnen von Speicheranforderungen. Relevante Statistiken: Minimum, Maximum, Durchschnitt, Summe

Metrik	Beschreibung
`ClusterUsedSpace`	Der insgesamt für den Cluster verwendete Speicherplatz. Sie müssen den Zeitraum bei einer Minute belassen, um einen korrekten Wert zu erhalten. Dieser Wert wird in der OpenSearch Servicekonsole in GiB angezeigt. In der CloudWatch Amazon-Konsole wird dieser Wert in MiB angezeigt. Relevante Statistiken: Minimum, Maximum
`ClusterIndexWritesBlocked`	Gibt an, ob Ihr Cluster eingehende Schreibanforderungen akzeptiert oder blockiert. Ein Wert von 0 bedeutet, dass der Cluster Anforderungen akzeptiert. Ein Wert von 1 bedeutet, dass Anforderungen blockiert werden. Einige der häufigsten Faktoren sind folgende: `FreeStorageSpace` ist zu gering, oder `JVMMemoryPressure` ist zu hoch. Um dieses Problem zu lösen, sollten Sie erwägen, mehr Speicherplatz hinzuzufügen oder Ihren Cluster zu skalieren. Relevante Statistiken: Maximum

Metrik	Beschreibung
`JVMMemoryPressure`	Der maximale Prozentsatz des Java-Heaps, der für alle Datenknoten im Cluster verwendet wird. OpenSearch Der Service 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 horizontale Skalierung durchführen, indem Sie Instances hinzufügen. Siehe the section called “Empfohlene CloudWatch Alarme”. Relevante Statistiken: Maximum **Note** Die Logik für diese Metrik wurde in der Service-Software R20220323 geändert. Weitere Informationen finden Sie in den Versionshinweisen.
`OldGenJVMMemoryPressure`	Der maximale Prozentsatz des Java-Heaps, der für die „alte Generation“ auf allen Datenknoten im Cluster verwendet wird. Diese Metrik ist auch auf Knotenebene verfügbar. Relevante Statistiken: Maximum
`AutomatedSnapshotFailure`	Die Anzahl fehlgeschlagener automatischer Snapshots für den Cluster. Der Wert 1 gibt an, dass keine automatischen Snapshots für die Domain in den vorherigen 36 Stunden erstellt wurden. Relevante Statistiken: Minimum, Maximum
`CPUCreditBalance`	Das verbleibende CPU-Guthaben für die Datenknoten im Cluster. Ein CPU-Guthaben stellt die Leistung eines gesamten CPU-Kerns für eine Minute zur Verfügung. Weitere Informationen finden Sie unter CPU-Guthaben im Amazon EC2 Developer Guide. Diese Metrik ist nur für die T2-Instance-Typen verfügbar. Relevante Statistiken: Minimum

Metrik	Beschreibung
OpenSearchDashboardsHealthyNodes	Eine Zustandsprüfung für OpenSearch Dashboards. Wenn Minimum, Maximum und Durchschnitt alle gleich 1 sind, verhalten sich Dashboards normal. Wenn Sie 10 Knoten mit einem Maximum von 1, Minimum von 0 und Durchschnitt von 0,7 haben, bedeutet dies, dass 7 Knoten (70 %) gesund und 3 Knoten (30 %) ungesund sind. Relevante Statistiken: Minimum, Maximum, Durchschnitt
OpensearchDashboardsReportingFailedRequestSysErrCount	Die Anzahl der Anfragen zum Generieren von OpenSearch Dashboards-Berichten, die aufgrund von Serverproblemen oder Funktionseinschränkungen fehlgeschlagen sind. Relevante Statistiken: Summe
OpensearchDashboardsReportingFailedRequestUserErrCount	Die Anzahl der Anfragen zum Generieren von OpenSearch Dashboards-Berichten, die aufgrund von Clientproblemen fehlgeschlagen sind. Relevante Statistiken: Summe
OpensearchDashboardsReportingRequestCount	Die Gesamtzahl der Anfragen zum Generieren von OpenSearch Dashboards-Berichten. Relevante Statistiken: Summe
OpensearchDashboardsReportingSuccessCount	Die Anzahl der erfolgreichen Anfragen zum Generieren von OpenSearch Dashboards-Berichten. Relevante Statistiken: Summe

Metrik	Beschreibung
KMSKeyError	Der Wert 1 gibt an, dass der AWS KMS -Schlüssel zum Verschlüsseln von Data-at-Rest deaktiviert wurde. Aktivieren Sie den Schlüssel wieder, um den normalen Betrieb für die Domain wiederherzustellen. In der Konsole wird diese Metrik nur für Domains angezeigt, in denen Daten im Ruhezustand verschlüsselt werden. Relevante Statistiken: Minimum, Maximum
KMSKeyInaccessible	Der Wert 1 gibt an, dass der AWS KMS -Schlüssel zum Verschlüsseln von Data-at-Rest gelöscht wurde oder dass die gewährten Berechtigungen für Service widerrufen wurden. OpenSearch Für Domains, die sich in diesem Zustand befinden, ist die Wiederherstellung nicht möglich. Aber wenn Sie über einen manuellen Snapshot verfügen, können Sie diesen verwenden, um die Daten der Domain zu einer neuen Domain zu migrieren. In der Konsole wird diese Metrik nur für Domains angezeigt, in denen Daten im Ruhezustand verschlüsselt werden. Relevante Statistiken: Minimum, Maximum
InvalidHostHeaderRequests	Die Anzahl der HTTP-Anfragen an den OpenSearch Cluster mit einem ungültigen (oder fehlenden) Host-Header. Gültige Anforderungen umfassen den Domains-Hostnamen als Host-Headerwert. OpenSearch Der Service weist ungültige Anfragen für Domains mit öffentlichem Zugriff zurück, die nicht über restriktive Zugriffsrichtlinien verfügen. Wir empfehlen, auf alle Domains eine restriktive Zugriffsrichtlinie anzuwenden. Wenn für diese Metrik hohe Werte angezeigt werden, stellen Sie sicher, dass Ihre OpenSearch -Clients den Hostnamen der Domäne (und nicht z. B. die IP-Adresse) in ihren Anfragen beinhalten. Relevante Statistiken: Summe

Metrik	Beschreibung
`OpenSearchRequests (previously ElasticsearchRequests)`	Die Anzahl der Anfragen an den OpenSearch Cluster Relevante Statistiken: Summe
`2xx, 3xx, 4xx, 5xx`	Die Anzahl der Anforderungen an die Domain, die zum jeweiligen HTTP-Antwortcode (2xx, 3xx, 4xx, 5xx) geführt haben. Relevante Statistiken: Summe
`ThroughputThrottle`	Gibt an, ob Festplatten gedrosselt wurden oder nicht. Eine Drosselung tritt auf, wenn der kombinierte Durchsatz von `ReadThroughputMicroBursting` und höher als der maximale Durchsatz, `WriteThroughputMicroBursting` ist. `MaxProvisionedThroughput` `MaxProvisionedThroughput` ist der niedrigere Wert des Instanzdurchsatzes oder des bereitgestellten Volumendurchsatzes. Ein Wert von 1 gibt an, dass Festplatten gedrosselt wurden. Ein Wert von 0 zeigt ein normales Verhalten an. Informationen zum Instance-Durchsatz finden Sie unter Amazon EBS-optimierte Instances. Informationen zum Volumendurchsatz finden Sie unter Amazon EBS-Volumetypen. Relevante Statistiken: Minimum, Maximum
`IopsThrottle`	Gibt an, ob die Anzahl der Ein-/Ausgabevorgänge pro Sekunde (IOPS) in der Domäne gedrosselt wurde. Eine Drosselung erfolgt, wenn die IOPS des Datenknotens die maximal zulässige Grenze des EBS-Volumes oder der Instanz des Datenknotens überschre iten. EC2 Informationen zu Instance-IOPS finden Sie unter Amazon EBS-optimierte Instances. Informationen zu Volume-IOPS finden Sie unter Amazon EBS-Volumetypen. Relevante Statistiken: Minimum, Maximum

Metrik	Beschreibung
`HighSwapUsage`	Ein Wert von 1 gibt an, dass das Auslagern aufgrund von Seitenfehlern möglicherweise zu Spitzenwerten bei der zugrunde liegenden Festplattennutzung während eines bestimmten Zeitraums geführt hat. Relevante Statistiken: Maximum

Dedizierte Hauptknoten-Metriken

Amazon OpenSearch Service bietet die folgenden Metriken für dedizierte Hauptknoten.

Metrik	Beschreibung
`MasterCPUUtilization`	Der maximale Prozentsatz der CPU-Ressourcen, die von den dedizierten Hauptknoten verwendet werden. Wir empfehlen, die Größe des Instance-Typs zu erhöhen, wenn diese Metrik 60 Prozent erreicht. Relevante Statistiken: Maximum
`MasterFreeStorageSpace`	Diese Metrik ist nicht relevant und kann ignoriert werden. Der Service verwendet keine Hauptknoten als Datenknoten.
`MasterJVMMemoryPressure`	Der maximale Prozentsatz des Java-Heap, der für alle dedizierten Hauptknoten im Cluster verwendet wird. Wir empfehlen die Verlagerung auf einen größeren Instance-Typen, wenn diese Metrik 85 Prozent erreicht. Relevante Statistiken: Maximum **Note** Die Logik für diese Metrik wurde in der Service-Software R20220323 geändert. Weitere Informationen finden Sie in den Versionshinweisen.

Metrik	Beschreibung
`MasterOldGenJVMMemoryPressure`	Der maximale Prozentsatz des Java-Heap pro Hauptknoten, der für die „alte Generation“ verwendet wird. Relevante Statistiken: Maximum
`MasterCPUCreditBalance`	Das verbleibende CPU-Guthaben für die dedizierte Hauptknoten im Cluster. Ein CPU-Guthaben stellt die Leistung eines gesamten CPU-Kerns für eine Minute zur Verfügung. Weitere Informationen finden Sie unter CPU-Guthaben im Amazon EC2 Developer Guide. Diese Metrik ist nur für die T2-Instance-Typen verfügbar. Relevante Statistiken: Minimum
`MasterReachableFromNode`	Eine Zustandsprüfung für `MasterNotDiscovered` -Ausnahmen. Ein Wert von 1 zeigt ein normales Verhalten an. Ein Wert von 0 zeigt an, dass `/_cluster/health/` fehlschlägt. Wenn beispielsweise der Hauptknoten vom Quellknoten aus nicht erreichbar ist, wird von Fehlschlägen gesprochen. Sie sind üblicherweise das Ergebnis eines Problems mit der Netzwerkkonnektivität oder eines AWS -Abhängigkeitsproblems. Relevante Statistiken: Maximum
`MasterSysMemoryUtilization`	Der Prozentsatz des Arbeitsspeichers des Hauptknotens, der verwendet wird. Relevante Statistiken: Maximum

Dedizierte Statistiken für Koordinator-Knoten

Amazon OpenSearch Service bietet die folgenden Metriken für dedizierte Koordinatorknoten.

Metrik	Beschreibung
`CoordinatorCPUUtilization`	Der maximale Prozentsatz der CPU-Ressourcen, die von den dedizierten Koordinatorknoten verwendet werden. Wir empfehlen

Metrik	Beschreibung
	, die Größe des Instance-Typs zu erhöhen, wenn diese Metrik 80 Prozent erreicht. Relevante Statistiken: Maximum
`CoordinatorJVMMemoryPressure`	Der maximale Prozentsatz des Java-Heaps, der für alle dedizierten Koordinatorknoten im Cluster verwendet wird. Wir empfehlen die Verlagerung auf einen größeren Instance-Typen, wenn diese Metrik 85 Prozent erreicht. Relevante Statistiken: Maximum
`CoordinatorOldGenJVMMemoryPressure`	Der maximale Prozentsatz des Java-Heap pro Hauptknoten, der für die „alte Generation“ verwendet wird. Relevante Statistiken: Maximum
`CoordinatorSysMemoryUtilization`	Der Prozentsatz des Arbeitsspeichers des Koordinator-Knotens, der verwendet wird. Relevante Statistiken: Maximum
`CoordinatorFreeStorageSpace`	Diese Metrik gibt an, dass der Service keine Koordinatorknoten als Datenknoten verwendet.

EBS-Volume-Metriken

Amazon OpenSearch Service bietet die folgenden Metriken für EBS-Volumes.

Metrik	Beschreibung
`ReadLatency`	Die Latenz für Lesevorgänge auf EBS-Volumes in Sekunden. Diese Metrik ist auch für einzelne Knoten verfügbar. Relevante Statistiken: Minimum, Maximum, Durchschnitt
`WriteLatency`	Die Latenz für Schreibvorgänge auf EBS-Volumes in Sekunden. Diese Metrik ist auch für einzelne Knoten verfügbar.

Metrik	Beschreibung
	Relevante Statistiken: Minimum, Maximum, Durchschnitt
`ReadThroughput`	Der Durchsatz für Lesevorgänge auf EBS-Volumes in Byte pro Sekunde. Diese Metrik ist auch für einzelne Knoten verfügbar. Relevante Statistiken: Minimum, Maximum, Durchschnitt
`ReadThroughputMicroBursting`	Der Durchsatz in Byte pro Sekunde für Lesevorgänge auf EBS-Volumes, wenn Micro-Bursting berücksichtigt wird. Diese Metrik ist auch für einzelne Knoten verfügbar. Micro-Bursting tritt auf, wenn ein EBS-Volume hohe IOPS- oder Durchsatzraten für deutlich kürzere Zeiträume (weniger als eine Minute) aufweist. Relevante Statistiken: Minimum, Maximum, Durchschnitt
`WriteThroughput`	Der Durchsatz für Schreibvorgänge auf EBS-Volumes in Byte pro Sekunde. Diese Metrik ist auch für einzelne Knoten verfügbar. Relevante Statistiken: Minimum, Maximum, Durchschnitt
`WriteThroughputMicroBursting`	Der Durchsatz in Byte pro Sekunde für Schreibvorgänge auf EBS-Volumes, wenn Micro-Bursting berücksichtigt wird. Diese Metrik ist auch für einzelne Knoten verfügbar. Micro-Bursting tritt auf, wenn ein EBS-Volume hohe IOPS- oder Durchsatzraten für deutlich kürzere Zeiträume (weniger als eine Minute) aufweist. Relevante Statistiken: Minimum, Maximum, Durchschnitt
`DiskQueueDepth`	Die Anzahl der ausstehenden Eingabe- und Ausgabe(I/O)-Anforderungen für ein EBS-Volume. Relevante Statistiken: Minimum, Maximum, Durchschnitt
`ReadIOPS`	Die Anzahl der Eingabe- und Ausgabe(I/O)-Vorgänge pro Sekunde für Lesevorgänge in EBS-Volumes. Diese Metrik ist auch für einzelne Knoten verfügbar. Relevante Statistiken: Minimum, Maximum, Durchschnitt

Metrik	Beschreibung
`ReadIOPSMicroBursting`	Die Anzahl der Eingabe- und Ausgabe (I/O) -Vorgänge pro Sekunde für Lesevorgänge in EBS-Volumes, wenn Microbursting berücksichtigt wird. Diese Metrik ist auch für einzelne Knoten verfügbar. Micro-Bursting tritt auf, wenn ein EBS-Volume hohe IOPS- oder Durchsatzraten für deutlich kürzere Zeiträume (weniger als eine Minute) überbrückt. Relevante Statistiken: Minimum, Maximum, Durchschnitt
`WriteIOPS`	Die Anzahl der Eingabe- und Ausgabe(I/O)-Vorgänge pro Sekunde für Schreibvorgänge in EBS-Volumes. Diese Metrik ist auch für einzelne Knoten verfügbar. Relevante Statistiken: Minimum, Maximum, Durchschnitt
`WriteIOPSMicroBursting`	Die Anzahl der Eingabe- und Ausgabe (I/O) -Vorgänge pro Sekunde für Schreibvorgänge in EBS-Volumes, wenn Microbursting berücksichtigt wird. Diese Metrik ist auch für einzelne Knoten verfügbar. Micro-Bursting tritt auf, wenn ein EBS-Volume hohe IOPS- oder Durchsatzraten für deutlich kürzere Zeiträume (weniger als eine Minute) übertrifft. Relevante Statistiken: Minimum, Maximum, Durchschnitt
`BurstBalance`	Der Prozentsatz der Ein- und Ausgabe (E/A)-Guthaben, die im Burst-Bucket für ein EBS-Volume verbleiben. Ein Wert von 100 bedeutet, dass das Volumen die maximale Anzahl von Credits erreicht hat. Wenn dieser Prozentsatz unter 70 % fällt, lesen Sie the section called “Niedrige EBS-Burst-Balance”. Das Burst-Balance bleibt für Domains mit GP3-Volume-Typen und Domains mit GP2-Volumes mit einer Volume-Größe von über 1.000 GiB bei 0. Relevante Statistiken: Minimum, Maximum, Durchschnitt

Metrik	Beschreibung
`VolumeStalledIOcheck`	Der Status Ihrer EBS-Volumes, um festzustellen, wenn sie beeinträchtigt sind. Bei der Metrik handelt es sich um einen binären Wert, der je nachdem, ob das EBS-Volume Eingabe- und Ausgabe abschließen kann, den Status 0 1 (bestanden) oder (nicht bestanden) zurückgibt. `VolumeStalledIOcheck` ist auch für einzelne Knoten verfügbar. Relevante Statistiken: Minimum, Maximum, Durchschnitt

Instance-Metriken

Amazon OpenSearch Service bietet die folgenden Metriken für jede Instance in einer Domain. OpenSearch Service fasst diese Instance-Metriken ebenfalls zusammen, um Informationen über den allgemeinen Cluster-Zustand bereitzustellen. Sie können dieses Verhalten mithilfe der Statistik über Beispielzähler in der Konsole überprüfen. Beachten Sie, dass jede Metrik in der folgenden Tabelle relevante Statistiken für den Knoten und den Cluster enthält.

> **Important**
>
> Verschiedene Versionen von Elasticsearch nutzen unterschiedliche Threadpools für die Verarbeitung von Aufrufen der `_index`-API. Elasticsearch 1.5 und 2.3 nutzen den Index-Threadpool. Elasticsearch 5. x, 6.0 und 6.2 nutzen den Massen-Threadpool. OpenSearch und Elasticsearch 6.3 und höher nutzen den Schreib-Threadpool. Derzeit enthält die OpenSearch Service-Konsole kein Diagramm für den Massen-Threadpool.
> Verwenden Sie `GET _cluster/settings?include_defaults=true`, um die Thread-Pool- und Warteschlangengrößen für Ihren Cluster zu überprüfen.

Metrik	Beschreibung
`FetchLatency`	Der Unterschied in Millisekunden in der Gesamtzeit aller Shard-Abruf-Operationen in einem Knoten zwischen Minute N und Minute (N — 1). Relevante Statistiken für Knoten: Durchschnitt

Metrik	Beschreibung
	Relevante Statistiken für Cluster: Durchschnitt, Maximum
FetchRate	Die Gesamtzahl der Shard-Abrufvorgänge pro Minute für alle Shards auf einem Datenknoten. Relevante Statistiken für Knoten: Durchschnitt Relevante Statistiken für Cluster: Durchschnitt, Maximum, Summe
ScrollTotal	Die Gesamtzahl der Shard-Scroll-Operationen pro Minute für alle Shards auf einem Datenknoten. Relevante Statistiken für Knoten: Durchschnitt, Maximum Relevante Statistiken für Cluster: Durchschnitt, Maximum, Summe
ScrollCurrent	Die Anzahl der Shard-Scrolloperationen, die derzeit ausgeführt werden. Relevante Statistiken für Knoten: Durchschnitt, Maximum Relevante Statistiken für Cluster: Durchschnitt, Maximum, Summe
OpenContexts	Die Anzahl offener Suchkontexte. Relevante Statistiken für Knoten: Durchschnitt, Maximum Relevante Statistiken für Cluster: Durchschnitt, Maximum, Summe
ThreadCount	Die Gesamtzahl der Threads, die derzeit vom OpenSearch Prozess verwendet werden. Relevante Statistiken für Knoten: Durchschnitt, Maximum Relevante Statistiken für Cluster: Durchschnitt, Maximum, Summe

Metrik	Beschreibung
`ShardReactivateCount`	Gibt an, wie oft alle Shards aus einem Ruhezustand heraus aktiviert wurden. Relevante Statistiken für Knoten: Summe, Maximum Relevante Statistiken für Cluster: Summe, Maximum
`ConcurrentSearchRate`	Die Gesamtzahl der Suchanfragen mit gleichzeitiger Segmentsuche pro Minute für alle Shards auf einem Datenknoten. Eine einzelner Aufruf der `_search`-API gibt möglicherweise Ergebnisse von vielen unterschiedlichen Shards zurück. Befinden sich fünf dieser Shards in einem Knoten, meldet der Knoten für diese Metrik 5, auch wenn der Client nur eine Anfrage durchgeführt hat. Relevante Statistiken für Knoten: Durchschnitt Relevante Statistiken für Cluster: Durchschnitt, Maximum, Summe
`ConcurrentSearchLatency`	Der Unterschied in der Gesamtzeit in Millisekunden, die bei allen Suchen mit gleichzeitiger Segmentsuche in einem Knoten zwischen Minute N und Minute (N-1) benötigt wird. Relevante Statistiken für Knoten: Durchschnitt Relevante Statistiken für Cluster: Durchschnitt, Maximum
`IndexingLatency`	Die Differenz in Millisekunden in der Gesamtzeit aller Indizierungsvorgänge in einem Knoten zwischen Minute N und Minute (N-1). Relevante Statistiken für Knoten: Durchschnitt Relevante Statistiken für Cluster: Durchschnitt, Maximum

Metrik	Beschreibung
`IndexingRate`	Die Anzahl der Indizierungsvorgänge pro Minute. Ein einzelner Aufruf der `_bulk`-API, der zwei Dokumente und zwei Aktualisierungen hinzufügt, zählt als vier Vorgänge, die auf mehrere Knoten verteilt werden können. Wenn dieser Index über ein oder mehrere Replikate verfügt und sich auf einer OpenSearch Domain ohne optimierte Instances befindet, zeichnen andere Knoten im Cluster ebenfalls insgesamt vier Indizierungsvorgänge auf. Bei OpenSearch Domänen mit optimierten Instanzen zeichnen andere Knoten mit Replikaten keine Vorgänge auf. Löschungen von Dokumenten werden bei dieser Metrik nicht gezählt. Relevante Statistiken für Knoten: Durchschnitt Relevante Statistiken für Cluster: Durchschnitt, Maximum, Summe
`SearchLatency`	Der Unterschied in der Gesamtzeit in Millisekunden, die bei allen Suchen in einem Knoten zwischen Minute N und Minute (N-1) benötigt wird. Relevante Statistiken für Knoten: Durchschnitt Relevante Statistiken für Cluster: Durchschnitt, Maximum
`SearchRate`	Die Gesamtanzahl von Suchabfragen pro Minute für alle Shards in einem Datenknoten. Eine einzelner Aufruf der `_search`-API gibt möglicherweise Ergebnisse von vielen unterschiedlichen Shards zurück. Befinden sich fünf dieser Shards in einem Knoten, meldet der Knoten für diese Metrik 5, auch wenn der Client nur eine Anfrage durchgeführt hat. Relevante Statistiken für Knoten: Durchschnitt Relevante Statistiken für Cluster: Durchschnitt, Maximum, Summe

Metrik	Beschreibung
`SegmentCount`	Die Anzahl der Segmente auf einem Datenknoten. Je mehr Segmente Sie haben, desto länger dauert jede Suche. OpenSearch führt gelegentlich kleinere Segmente zu einem größeren zusammen. Relevante Statistiken für Knoten: Maximum, Durchschnitt Relevante Statistiken für Cluster: Summe, Maximum, Durchschnitt
`SysMemoryUtilization`	Der Prozentsatz des Arbeitsspeichers einer Instance, die in dem Cluster verwendet wird. Hohe Werte für diese Metrik sind normal und stellen normalerweise kein Problem mit Ihrem Cluster dar. Einen besseren Indikator für potenzielle Leistungs- und Stabilitätsprobleme finden Sie in der `JVMMemoryPressure` -Metrik. Relevante Statistiken für Knoten: Minimum, Maximum, Durchschnitt Relevante Statistiken für Cluster: Minimum, Maximum, Durchschnitt
`JVMGCYoungCollectionCount`	Die Anzahl der Ausführungen der automatischen Speicherbereinigung (Garbage Collection) "young generation". Eine stets zunehmende große Anzahl von Ausführungen ist ein normaler Aspekt bei Clustervorgängen. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe, Maximum, Durchschnitt
`JVMGCYoungCollectionTime`	Die Dauer in Millisekunden, die ein Cluster für die Ausführungen der automatischen Speicherbereinigung (Garbage Collection) „young generation“ aufgewendet hat. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe, Maximum, Durchschnitt

Metrik	Beschreibung
`JVMGCOldCollectionCount`	Die Anzahl der Ausführungen der automatischen Speicherbereinigung (Garbage Collection) "old generation". In einem Cluster mit genügend Ressourcen sollte diese Zahl relativ klein bleiben und selten zunehmen. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe, Maximum, Durchschnitt
`JVMGCOldCollectionTime`	Die Dauer in Millisekunden, die ein Cluster für die Ausführungen der automatischen Speicherbereinigung (Garbage Collection) „old generation“ aufgewendet hat. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe, Maximum, Durchschnitt
`OpenSearchDashboardsConcurrentConnections`	Die Anzahl der aktiven gleichzeitigen Verbindungen mit OpenSearch Dashboards. Wenn diese Zahl konstant hoch ist, sollten Sie Ihren Cluster skalieren. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe, Maximum, Durchschnitt
`OpenSearchDashboardsHealthyNode`	Eine Zustandsprüfung für individuelle OpenSearch Dashboards-Knoten. Ein Wert von 1 zeigt ein normales Verhalten an. Ein Wert von 0 zeigt an, dass auf Dashboards nicht zugegriffen werden kann. Relevante Statistiken für Knoten: Minimum Relevante Statistiken für Cluster: Minimum, Maximum, Durchschnitt

Metrik	Beschreibung
`OpenSearchDashboardsHeapTotal`	Die Menge des Heap-Speichers, der OpenSearch Dashboards in MiB zugewiesen ist. Verschiedene EC2 Instance-Typen können sich auf die genaue Speicherzuweisung auswirken. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe, Maximum, Durchschnitt
`OpenSearchDashboardsHeapUsed`	Die absolute Menge an Heap-Speicher, die von OpenSearch Dashboards in MiB verwendet wird. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe, Maximum, Durchschnitt
`OpenSearchDashboardsHeapUtilization`	Der maximale Prozentsatz des verfügbaren Heap-Speichers, der von OpenSearch Dashboards verwendet wird. Erhöht dieser Wert über 80 %, erwägen Sie eine Skalierung Ihres Clusters. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Minimum, Maximum, Durchschnitt
`OpenSearchDashboardsOS1MinuteLoad`	Der durchschnittliche CPU-Auslastungsdurchschnitt von einer Minute für OpenSearch Dashboards. Die CPU-Last sollte idealerweise unter 1,00 liegen. Während temporäre Spitzen in Ordnung sind, empfehlen wir, die Größe des Instance-Typs zu erhöhen, wenn diese Metrik konsistent über 1,00 liegt. Relevante Statistiken für Knoten: Durchschnitt Relevante Statistiken für Cluster: Durchschnitt, Maximum

Metrik	Beschreibung
`OpenSearchDashboardsRequestTotal`	Die Gesamtzahl der HTTP-Anforderungen, die an OpenSearch Dashboards gesendet werden. Wenn Ihr System langsam ist oder eine hohe Anzahl von Dashboards-Anforderungen angezeigt wird, sollten Sie die Größe des Instance-Typs erhöhen. Relevante Knoten-Statistiken: Summe Relevante Statistiken für Cluster: Summe
`OpenSearchDashboardsResponseTimesMaxInMillis`	Die maximale Dauer in Millisekunden, die für OpenSearch Dashboards benötigt wird, um auf eine Anfrage zu reagieren. Wenn Anforderungen konsistent lange brauchen, bis Ergebnisse zurückgegeben werden, sollten Sie die Größe des Instance-Typs erhöhen. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Maximum, Durchschnitt
`SearchTaskCancelled`	Die Anzahl der Stornierungen von Koordinatorknoten. Relevante Knoten-Statistiken: Summe Relevante Statistiken für Cluster: Summe
`SearchShardTaskCancelled`	Die Anzahl der Stornierungen von Datenknoten. Relevante Knoten-Statistiken: Summe Relevante Statistiken für Cluster: Summe,
`ThreadpoolForce_mergeQueue`	Die maximale Anzahl von Aufgaben in einer Warteschlange im Threadpool erzwungener Zusammenführungen. Wenn die Größe der Warteschlange gleichbleibend hoch ist, erwägen Sie eine Skalierung Ihres Clusters. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe, Maximum, Durchschnitt

Metrik	Beschreibung
ThreadpoolForce_mergeRejected	Die Anzahl abgewiesener Aufgaben im Threadpool erzwungener Zusammenführungen. Wenn die Anzahl stätig wächst, erwägen Sie eine Skalierung Ihres Clusters. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe
ThreadpoolForce_mergeThreads	Die Größe des Threadpools erzwungener Zusammenführungen. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Durchschnitt, Summe
ThreadpoolIndexQueue	Die Anzahl von Aufgaben in einer Warteschlange im Index-Threadpool. Wenn die Größe der Warteschlange gleichbleibend hoch ist, erwägen Sie eine Skalierung Ihres Clusters. Die maximale Größe der Index-Warteschlange beträgt 200. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe, Maximum, Durchschnitt
ThreadpoolIndexRejected	Die Anzahl abgewiesener Aufgaben im Index-Threadpool. Wenn die Anzahl stätig wächst, erwägen Sie eine Skalierung Ihres Clusters. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe
ThreadpoolIndexThreads	Die Größe des Index-Threadpools. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Durchschnitt, Summe

Metrik	Beschreibung
ThreadpoolSearchQueue	Die Anzahl von Aufgaben in einer Warteschlange im Such-Threadpool. Wenn die Größe der Warteschlange gleichbleibend hoch ist, erwägen Sie eine Skalierung Ihres Clusters. Die maximale Größe der Such-Warteschlange beträgt 1.000. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe, Maximum, Durchschnitt
ThreadpoolSearchRejected	Die Anzahl abgewiesener Aufgaben im Such-Threadpool. Wenn die Anzahl stätig wächst, erwägen Sie eine Skalierung Ihres Clusters. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe
ThreadpoolSearchThreads	Die Größe des Such-Threadpools. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Durchschnitt, Summe
Threadpoolsql-workerQueue	Die Anzahl von Aufgaben in einer Warteschlange im SQL-Such-Threadpool. Wenn die Größe der Warteschlange gleichbleibend hoch ist, erwägen Sie eine Skalierung Ihres Clusters. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe, Maximum, Durchschnitt
Threadpoolsql-workerRejected	Die Anzahl abgewiesener Aufgaben im SQL-Such-Threadpool. Wenn die Anzahl stätig wächst, erwägen Sie eine Skalierung Ihres Clusters. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe

Metrik	Beschreibung
`Threadpoolsql-workerThreads`	Die Größe des SQL-Such-Threadpools. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Durchschnitt, Summe
`ThreadpoolBulkQueue`	Die Anzahl von Aufgaben in einer Warteschlange im Massen-Threadpool. Wenn die Größe der Warteschlange gleichbleibend hoch ist, erwägen Sie eine Skalierung Ihres Clusters. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe, Maximum, Durchschnitt
`ThreadpoolBulkRejected`	Die Anzahl abgewiesener Aufgaben im Massen-Threadpool. Wenn die Anzahl stätig wächst, erwägen Sie eine Skalierung Ihres Clusters. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe
`ThreadpoolBulkThreads`	Die Größe des Massen-Threadpools. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Durchschnitt, Summe
`ThreadpoolIndexSearcherQueue`	Die Anzahl von Aufgaben in einer Warteschlange im Index-Such-Threadpool. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe, Maximum, Durchschnitt
`ThreadpoolIndexSearcherRejected`	Die Anzahl abgewiesener Aufgaben im Index-Such-Threadpool. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe

Metrik	Beschreibung
`ThreadpoolIndexSearcherThreads`	Die Größe des Index-Such-Threadpools. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Durchschnitt, Summe
`ThreadpoolWriteThreads`	Die Größe des Schreib-Threadpools. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Durchschnitt, Summe
`ThreadpoolWriteQueue`	Die Anzahl von Aufgaben in einer Warteschlange im Schreib-Threadpool. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Durchschnitt, Summe
`ThreadpoolWriteRejected`	Die Anzahl abgewiesener Aufgaben im Schreib-Threadpool. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Durchschnitt, Summe **Note** Da die Standard-Schreibwarteschlangengröße in Version 7.1 von 200 auf 10 000 erhöht wurde, ist diese Metrik nicht mehr der einzige Indikator für Ablehnungen von OpenSearch Service. Verwenden Sie die `CoordinatingWriteRejected` , `PrimaryWriteRejected` und `ReplicaWriteRejected` -Metriken, um Ablehnungen in Version 7.1 und höher zu überwachen.

Metrik	Beschreibung
`CoordinatingWriteRejected`	Die Gesamtzahl der Ablehnungen, die auf dem koordinierenden Knoten aufgrund des Indizierungsdrucks seit dem letzten Start des OpenSearch Serviceprozesses aufgetreten sind. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Durchschnitt, Summe Diese Metrik ist in Version 7.1 und höher verfügbar.
`PrimaryWriteRejected`	Die Gesamtzahl der Ablehnungen, die auf dem primären Shard aufgrund des Indizierungsdrucks seit dem letzten Start des OpenSearch Serviceprozesses aufgetreten sind. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Durchschnitt, Summe Diese Metrik ist in Version 7.1 und höher verfügbar.
`ReplicaWriteRejected`	Die Gesamtzahl der Ablehnungen, die auf dem Replikat-Shard aufgrund des Indizierungsdrucks seit dem letzten OpenSearch Start des Serviceprozesses aufgetreten sind. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Durchschnitt, Summe Diese Metrik ist in Version 7.1 und höher verfügbar.
`WorkloadManagementEnabled`	Gibt an, ob die Workload-Management-Funktion aktiviert ist. Ein Wert von 1 bedeutet, dass sie aktiviert ist, und ein Wert von 0 bedeutet, dass sie aktiviert `monitor_only` oder deaktiviert ist. Relevante Statistiken für Knoten: Maximum, Minimum Relevante Statistiken für Cluster: Durchschnitt, Summe Diese Metrik ist in Version 7.1 und höher verfügbar.

Metrik	Beschreibung
`SoftQueryGroupCount`	Anzahl der Abfragegruppen im Soft-Modus in der Domäne. Relevante Statistiken für Knoten: Durchschnitt, Maximum Relevante Statistiken für Cluster: Durchschnitt, Maximum, Summe Diese Metrik ist in Version 7.1 und höher verfügbar.
`EnforcedQueryGroupCount`	Anzahl der Abfragegruppen in der Domäne im erzwungenen Modus. Relevante Statistiken für Knoten: Durchschnitt, Maximum Relevante Statistiken für Cluster: Durchschnitt, Maximum, Summe Diese Metrik ist in Version 7.1 und höher verfügbar.

UltraWarm Metriken

Amazon OpenSearch Service bietet die folgenden Metriken für UltraWarmKnoten.

Metrik	Beschreibung
`WarmCPUUtilization`	Der Prozentsatz der CPU-Auslastung für UltraWarm Knoten im Cluster „Maximum“ zeigt den Knoten mit der höchsten CPU-Nutzung an. Durchschnitt steht für alle UltraWarm Knoten im Cluster Diese Metrik ist auch für individuelle UltraWarm Knoten verfügbar. Relevante Statistiken: Maximum, Durchschnitt
`WarmFreeStorageSpace`	Die Menge an Warm-Speicherplatz in MiB. Das ist die einzige relevante Statistik, weil Amazon S3 anstatt angeschlossener Festplatten UltraWarm verwendet `Sum` wird. Sie müssen den Zeitraum bei einer Minute belassen, um einen korrekten Wert zu erhalten. Relevante Statistiken: Summe

Metrik	Beschreibung
`WarmSearchableDocuments`	Die Gesamtzahl der durchsuchbaren Dokumente in allen Warm-Indizes im Cluster. Sie müssen den Zeitraum bei einer Minute belassen, um einen korrekten Wert zu erhalten. Relevante Statistiken: Summe
`WarmSearchLatency`	Der Unterschied in der Gesamtzeit in Millisekunden für alle Suchanfragen UltraWarm zwischen Minute N und Minute (N-1). Relevante Statistiken für Knoten: Durchschnitt Relevante Statistiken für Cluster: Durchschnitt, Maximum
`WarmSearchRate`	Die Gesamtzahl der Suchanfragen pro Minute für alle Shards auf einem UltraWarm Knoten. Eine einzelner Aufruf der `_search`-API gibt möglicherweise Ergebnisse von vielen unterschiedlichen Shards zurück. Befinden sich fünf dieser Shards in einem Knoten, meldet der Knoten für diese Metrik 5, auch wenn der Client nur eine Anfrage durchgeführt hat. Relevante Statistiken für Knoten: Durchschnitt Relevante Statistiken für Cluster: Durchschnitt, Maximum, Summe
`WarmStorageSpaceUtilization`	Die Gesamtmenge an Warm-Speicherplatz, in MiB, die vom Cluster belegt wird. Relevante Statistiken: Maximum
`HotStorageSpaceUtilization`	Die Gesamtmenge an „Hot Storage“-Speicherplatz, die vom Cluster belegt wird. Relevante Statistiken: Maximum
`WarmSysMemoryUtilization`	Der Prozentsatz des Arbeitsspeichers des Warm-Knotens, der verwendet wird. Relevante Statistiken: Maximum

Metrik	Beschreibung
`HotToWarm Migration QueueSize`	Die Anzahl der Indizes, die derzeit darauf warten, vom Hot- zum Warm-Speicher zu migrieren. Relevante Statistiken: Maximum
`WarmToHot Migration QueueSize`	Die Anzahl der Indizes, die derzeit darauf warten, vom Warm zum Hot Storage zu migrieren. Relevante Statistiken: Maximum
`HotToWarm Migration FailureCount`	Die Gesamtzahl der fehlgeschlagenen Hot-zu-Warm-Migrationen. Relevante Statistiken: Summe
`HotToWarm Migration ForceMerg eLatency`	Die durchschnittliche Latenz der erzwungenen Verschmelzungsphas e des Migrationsprozesses. Wenn diese Phase durchweg zu lange dauert, ziehen Sie in Betracht, `index.ultrawarm.migration.f orce_merge.max_num_segments` zu erhöhen. Relevante Statistiken: Durchschnitt
`HotToWarm Migration SnapshotL atency`	Die durchschnittliche Latenz der Snapshot-Phase des Migration sprozesses. Wenn dieser Schritt konsistent zu lange dauert, stellen Sie sicher, dass die Shards entsprechend dimensioniert und im gesamten Cluster verteilt sind. Relevante Statistiken: Durchschnitt
`HotToWarm Migration Processin gLatency`	Die durchschnittliche Latenz erfolgreicher Hot-to-Warm-Migrationen, ohne die in der Warteschlange verbrachte Zeit. Dieser Wert ist die Summe der Zeit, die benötigt wird, um die Phasen Zusammenführung zu erzwingen, Snapshot und Shard-Verlagerung des Migrationsprozesses abzuschließen. Relevante Statistiken: Durchschnitt

Metrik	Beschreibung
`HotToWarm Migration SuccessCount`	Die Gesamtzahl der erfolgreichen Hot-zu-Warm-Migrationen. Relevante Statistiken: Summe
`HotToWarm Migration SuccessLatency`	Die durchschnittliche Latenz erfolgreicher Hot-to-Warm-Migrationen, mit der in der Warteschlange verbrachten Zeit. Relevante Statistiken: Durchschnitt
`WarmThrea dpoolSear chThreads`	Die Größe des UltraWarm Such-Threadpools. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Durchschnitt, Summe
`WarmThrea dpoolSear chRejected`	Die Anzahl abgewiesener Aufgaben im UltraWarm Such-Threadpool. Wenn diese Anzahl ständig wächst, erwägen Sie das Hinzufügen weiterer UltraWarm Knoten. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe
`WarmThrea dpoolSear chQueue`	Die Anzahl von Aufgaben in einer Warteschlange im UltraWarm Such-Threadpool. Wenn die Größe der Warteschlange gleichbleibend hoch ist, erwägen Sie das Hinzufügen weiterer UltraWarm Knoten. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe, Maximum, Durchschnitt

Metrik	Beschreibung
`WarmJVMMemoryPressure`	Der maximale Prozentsatz des Java-Heaps, der für UltraWarm Knoten verwendet wird. Relevante Statistiken: Maximum **Note** Die Logik für diese Metrik wurde in der Service-Software R20220323 geändert. Weitere Informationen finden Sie in den Versionshinweisen.
`WarmOldGenJVMMemoryPressure`	Der maximale Prozentsatz des Java-Heaps pro UltraWarm Knoten, der für die „alte Generation“ verwendet wird. Relevante Statistiken: Maximum
`WarmJVMGCYoungCollectionCount`	Die Anzahl der Ausführungen der automatischen Speicherbereinigung (Garbage Collection) „young generation“ in UltraWarm Knoten. Eine stets zunehmende große Anzahl von Ausführungen ist ein normaler Aspekt bei Clustervorgängen. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe, Maximum, Durchschnitt
`WarmJVMGCYoungCollectionTime`	Die Dauer in Millisekunden, die ein Cluster für die Ausführungen der automatischen Speicherbereinigung (Garbage Collection) „young generation“ auf Knoten aufgewendet hat. UltraWarm Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe, Maximum, Durchschnitt

Metrik	Beschreibung
`WarmJVMGCOldCollectionCount`	Die Anzahl der Ausführungen der automatischen Speicherbereinigung (Garbage Collection) „old generation“ in UltraWarm Knoten. In einem Cluster mit genügend Ressourcen sollte diese Zahl relativ klein bleiben und selten zunehmen. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe, Maximum, Durchschnitt
`WarmConcurrentSearchRate`	Die Gesamtzahl der Suchanfragen mit gleichzeitiger Segmentsuche pro Minute für alle Shards auf einem UltraWarm Knoten. Eine einzelner Aufruf der `_search`-API gibt möglicherweise Ergebnisse von vielen unterschiedlichen Shards zurück. Befinden sich fünf dieser Shards in einem Knoten, meldet der Knoten für diese Metrik 5, auch wenn der Client nur eine Anfrage durchgeführt hat. Relevante Statistiken für Knoten: Durchschnitt Relevante Statistiken für Cluster: Summe, Maximum, Durchschnitt
`WarmConcurrentSearchLatency`	Der Unterschied in der Gesamtzeit in Millisekunden, die bei allen Suchen mit gleichzeitiger Segmentsuche in einem UltraWarm Knoten zwischen Minute N und Minute (N-1) benötigt wird. Relevante Statistiken für Knoten: Durchschnitt Relevante Statistiken für Cluster: Maximum, Durchschnitt
`WarmThreadpoolIndexSearcherQueue`	Die Anzahl von Aufgaben in einer Warteschlange im UltraWarm Index-Sucher-Threadpool. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe, Maximum, Durchschnitt

Metrik	Beschreibung
`WarmThreadpoolIndexSearcherRejected`	Die Anzahl abgewiesener Aufgaben im UltraWarm Index-Sucher-Threadpool. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe
`WarmThreadpoolIndexSearcherThreads`	Die Größe des UltraWarm Index-Such-Threadpools. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe, Durchschnitt

Cold-Storage-Metriken

Amazon OpenSearch Service bietet die folgenden Metriken für Cold Storage.

Metrik	Beschreibung
`ColdStorageSpaceUtilization`	Die Gesamtmenge an Cold-Storage-Platz, in MiB, die vom Cluster belegt wird. Relevante Statistiken: Maximum
`ColdToWarmMigrationFailureCount`	Die Gesamtzahl der fehlgeschlagenen Cold-zu-Warm-Migrationen. Relevante Statistiken: Summe
`ColdToWarmMigrationLatency`	Die Zeitspanne für erfolgreiche Cold-zu-Warm-Migrationen. Relevante Statistiken: Durchschnitt
`ColdToWarmMigrationQueueSize`	Die Anzahl der Indizes, die derzeit darauf warten, vom Cold- zum Warm-Speicher zu migrieren. Relevante Statistiken: Maximum

Metrik	Beschreibung
`ColdToWarmMigrationSuccessCount`	Die Gesamtzahl der erfolgreichen Cold-zu-Warm-Migrationen. Relevante Statistiken: Summe
`WarmToColdMigrationFailureCount`	Die Gesamtzahl der fehlgeschlagenen Warm-zu-Cold-Migrationen. Relevante Statistiken: Summe
`WarmToColdMigrationLatency`	Die Zeitspanne für erfolgreiche Warm-zu-Cold-Migrationen. Relevante Statistiken: Durchschnitt
`WarmToColdMigrationQueueSize`	Die Anzahl der Indizes, die derzeit darauf warten, vom Warm zum Cold Storage zu migrieren. Relevante Statistiken: Maximum
`WarmToColdMigrationSuccessCount`	Die Gesamtzahl der erfolgreichen Warm-zu-Cold-Migrationen. Relevante Statistiken: Summe

OR1 Metriken

Amazon OpenSearch Service bietet die folgenden Metriken für OR1Instances.

Metrik	Beschreibung
`RemoteStorageUsedSpace`	Die Gesamtmenge an Amazon S3 S3-Speicherplatz, in MiB, die vom Cluster belegt wird. Relevante Statistiken: Summe
`RemoteStorageWriteRejected`	Die Gesamtzahl der Anfragen, die aufgrund von Remote-Speicher- und Replikationsdruck auf primären Shards abgelehnt wurden. Dies wird ab dem letzten Start des OpenSearch Serviceprozesses berechnet.

Metrik	Beschreibung
	Relevante Statistiken: Summe
`ReplicationLagMaxTime`	Die Dauer in Millisekunden, die ein Replikat-Shard hinter den primären Shard zurückbleibt. Relevante Statistiken: Maximum

Warnungsmetriken

Amazon OpenSearch Service bietet die folgenden Metriken für Warnungen.

Metrik	Beschreibung
`AlertingDegraded`	Ein Wert von 1 bedeutet, dass entweder der Warnungsindex rot ist, oder ein oder mehrere Knoten nicht im Zeitplan sind. Ein Wert von 0 zeigt ein normales Verhalten an. Relevante Statistiken: Maximum
`AlertingIndexExists`	Ein Wert von 1 bedeutet, dass der `.opensearch-alerting-config` -Index existiert. Ein Wert von 0 bedeutet, dass dies nicht der Fall ist. Bis Sie die Warnfunktion zum ersten Mal verwenden, bleibt dieser Wert bei 0. Relevante Statistiken: Maximum
`AlertingIndexStatus.green`	Der Zustand des Index. Ein Wert von 1 bedeutet „grün“. Der Wert 0 bedeutet, dass der Index entweder nicht existiert oder nicht grün ist. Relevante Statistiken: Maximum
`AlertingIndexStatus.red`	Der Zustand des Index. Ein Wert von 1 bedeutet „rot“. Der Wert 0 bedeutet, dass der Index entweder nicht existiert oder nicht rot ist. Relevante Statistiken: Maximum

Metrik	Beschreibung
`AlertingIndexStatus.yellow`	Der Zustand des Index. Ein Wert von 1 bedeutet „gelb“. Der Wert 0 bedeutet, dass der Index entweder nicht vorhanden ist oder nicht gelb ist. Relevante Statistiken: Maximum
`AlertingNodesNotOnSchedule`	Ein Wert von 1 bedeutet, dass einige Aufgaben nicht termingerecht ausgeführt werden. Der Wert 0 bedeutet, dass alle Alarmaufgaben termingerecht ausgeführt werden (oder dass keine Alarmaufgaben vorhanden sind). Überprüfen Sie die OpenSearch Service-Konsole, oder stellen Sie eine `_nodes/stats` Anfrage, um festzustellen, ob Knoten eine hohe Ressourcennutzung aufweisen. Relevante Statistiken: Maximum
`AlertingNodesOnSchedule`	Ein Wert von 1 bedeutet, dass alle Alarmaufgaben termingerecht ausgeführt werden (oder dass keine Alarmaufgaben vorhanden sind). Der Wert 0 bedeutet, dass einige Aufgaben nicht termingerecht ausgeführt werden. Relevante Statistiken: Maximum
`AlertingScheduledJobEnabled`	Der Wert 1 bedeutet, dass die `opensearch.scheduled_jobs.enabled` -Clustereinstellung „true“ ist. Der Wert 0 bedeutet, dass diese „false“ ist und geplante Aufgaben deaktiviert sind. Relevante Statistiken: Maximum

Metriken zur Anomalieerkennung

Amazon OpenSearch Service bietet die folgenden Metriken für Anomalieerkennung.

Metrik	Beschreibung
`ADPluginUnhealthy`	Ein Wert von 1 bedeutet, dass das Plug-in zur Anomalieerkennung nicht ordnungsgemäß funktioniert, entweder wegen einer hohen Anzahl von

Metrik	Beschreibung
	Fehlern oder weil einer der Indizes, die es verwendet, rot ist. Ein Wert 0 gibt an, dass das Plug-in wie erwartet funktioniert. Relevante Statistiken: Maximum
`ADExecute RequestCount`	Die Anzahl der Anfragen zur Erkennung von Anomalien. Relevante Statistiken: Summe
`ADExecute FailureCount`	Die Anzahl der fehlgeschlagenen Anfragen zur Erkennung von Anomalien. Relevante Statistiken: Summe
`ADHCExecu teFailureCount`	Die Anzahl der fehlgeschlagenen Anforderungen zum Erkennen von Anomalien für Detektoren mit hoher Kardinalität. Relevante Statistiken: Summe
`ADHCExecu teRequestCount`	Die Anzahl der Anforderungen zum Erkennen von Anomalien für Detektoren mit hoher Kardinalität. Relevante Statistiken: Summe
`ADAnomaly ResultsIn dexStatus IndexExists`	Ein Wert 1 bedeutet, dass der Index, auf den der `.opensearch-anomaly-results` -Alias verweist, vorhanden ist. Bis Sie die Funktion zur Anomalieerkennung zum ersten Mal verwenden, bleibt dieser Wert 0. Relevante Statistiken: Maximum
`ADAnomaly ResultsIn dexStatus.red`	Ein Wert 1 bedeutet, dass der Index, auf den der `.opensearch-anomaly-results` -Alias zeigt, rot ist. Ein Wert von 0 bedeutet, dass dies nicht der Fall ist. Bis Sie die Funktion zur Anomalieerkennung zum ersten Mal verwenden, bleibt dieser Wert 0. Relevante Statistiken: Maximum

Metrik	Beschreibung
`ADAnomaly Detectors IndexStat usIndexExists`	Ein Wert von 1 bedeutet, dass der `.opensearch-anomaly-detectors` -Index existiert. Ein Wert von 0 bedeutet, dass dies nicht der Fall ist. Bis Sie die Funktion zur Anomalieerkennung zum ersten Mal verwenden, bleibt dieser Wert 0. Relevante Statistiken: Maximum
`ADAnomaly Detectors IndexStat us.red`	Ein Wert von 1 bedeutet, dass der `.opensearch-anomaly-detectors` -Index rot ist. Ein Wert von 0 bedeutet, dass dies nicht der Fall ist. Bis Sie die Funktion zur Anomalieerkennung zum ersten Mal verwenden, bleibt dieser Wert 0. Relevante Statistiken: Maximum
`ADModelsC heckpoint IndexStat usIndexExists`	Ein Wert von 1 bedeutet, dass der `.opensearch-anomaly-checkpoints` -Index existiert. Ein Wert von 0 bedeutet, dass dies nicht der Fall ist. Bis Sie die Funktion zur Anomalieerkennung zum ersten Mal verwenden, bleibt dieser Wert 0. Relevante Statistiken: Maximum
`ADModelsC heckpoint IndexStat us.red`	Ein Wert von 1 bedeutet, dass der `.opensearch-anomaly-checkpoints` -Index rot ist. Ein Wert von 0 bedeutet, dass dies nicht der Fall ist. Bis Sie die Funktion zur Anomalieerkennung zum ersten Mal verwenden, bleibt dieser Wert 0. Relevante Statistiken: Maximum

Asynchrone Suchmetriken

Amazon OpenSearch Service bietet die folgenden Metriken für asynchrone Suche.

Asynchrone Suchkoordinator-Knotenstatistik (pro Koordinator-Knoten)

Metrik	Beschreibung
`AsynchronousSearchSubmissionRate`	Die Anzahl der asynchronen Suchen, die in der letzten Minute gesendet wurden.
`AsynchronousSearchInitializedRate`	Die Anzahl der asynchronen Suchen, die in der letzten Minute initialisiert wurden.
`AsynchronousSearchRunningCurrent`	Die Anzahl der derzeit ausgeführten asynchronen Suchen.
`AsynchronousSearchCompletionRate`	Die Anzahl der asynchronen Suchen, die in der letzten Minute erfolgreich beendet wurden.
`AsynchronousSearchFailureRate`	Die Anzahl der asynchronen Suchen, die in der letzten Minute beendet wurden und fehlgeschlagen sind.
`AsynchronousSearchPersistRate`	Die Anzahl der asynchronen Suchen, die in der letzten Minute beibehalten wurden.
`AsynchronousSearchPersistFailedRate`	Die Anzahl der asynchronen Suchen, deren Beibehaltung in der letzten Minute fehlgeschlagen ist.
`AsynchronousSearchRejected`	Die Gesamtzahl der seit der Knotenbetriebszeit abgelehnten asynchronen Suchen.

Metrik	Beschreibung
`AsynchronousSearchCancelled`	Die Gesamtzahl der seit der Knotenbetriebszeit abgebrochenen asynchronen Suchen.
`AsynchronousSearchMaxRunningTime`	Die Dauer der längsten asynchronen Suche auf einem Knoten in der letzten Minute.

Asynchrone Suchcluster-Statistiken

Metrik	Beschreibung
`AsynchronousSearchStoreHealth`	Der Zustand des Speichers im anhaltenden Index (Rot/Nicht-Rot) in der letzten Minute.
`AsynchronousSearchStoreSize`	Die Größe des Systemindex über alle Shards in der letzten Minute.
`AsynchronousSearchStoredResponseCount`	Die Anzahl der gespeicherten Antworten im Systemindex in der letzten Minute.

Automatische Optimierung

Amazon OpenSearch Service bietet die folgenden Metriken für Auto-Tune.

Metrik	Beschreibung
`AutoTuneChangesHistoryHeapSize`	Die Änderungshistorie in MiB für Werte zur Optimierung der Heap-Größe.

Metrik	Beschreibung
`AutoTuneChangesHistoryJVMYoungGenArgs`	Die Änderungshistorie für JVM-Argumente YongGen .
`AutoTuneFailed`	Ein boolescher Wert, der angibt, ob die Auto-Tune-Änderung fehlgeschlagen ist.
`AutoTuneSucceeded`	Ein boolescher Wert, der angibt, ob die Auto-Tune-Änderung erfolgreich war.
`AutoTuneValue`	Der Änderungsverlauf der Warteschlange (Anzahl) und die Cache-Tunings ändern den Verlauf (in MiB) für unterbrechungsfreie Änderungen.

Multi-AZ mit Standby-Metriken

Amazon OpenSearch Service bietet die folgenden Metriken für Multi-AZ mit Standby.

Metriken auf Knotenebene für Datenknoten in aktiven Availability Zones

Metrik	Beschreibung
`CPUUtilization`	Der Prozentsatz der CPU-Nutzung für Datenknoten im Cluster. „Maximum“ zeigt den Knoten mit der höchsten CPU-Nutzung an. „Average“ (Durchschnitt) stellt alle Knoten im Cluster dar. Diese Metrik ist auch für einzelne Knoten verfügbar.
`FreeStorageSpace`	Der freie Platz für Datenknoten im Cluster. `Sum` zeigt den gesamten freien Speicherplatz für den Cluster an, Sie müssen jedoch den Zeitraum bei einer Minute belassen, um einen genauen Wert zu erhalten. `Minimum` und `Maximum` zeigen die Knoten mit dem wenigsten bzw. dem meisten freien Speicherplatz an. Diese Metrik ist auch für individuelle Knoten verfügbar. OpenSearch Der Service gibt eine aus`ClusterBlockException` , wenn diese Metrik erreicht `0` ist. Zum Wiederherstellen müssen Sie entweder Indizes löschen, größere Instances hinzufügen oder EBS-basierten Speicher zu vorhandenen Instances

Metrik	Beschreibung
	hinzufügen. Weitere Informationen hierzu finden Sie unter the section called “Zu wenig verfügbarer Speicherplatz”. Dieser Wert wird in der OpenSearch Servicekonsole in GiB angezeigt. In der CloudWatch Amazon-Konsole wird dieser Wert in MiB angezeigt.
`JVMMemory Pressure`	Der maximale Prozentsatz des Java-Heaps, der für alle Datenknoten im Cluster verwendet wird. OpenSearch Der Service 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 horizontale Skalierung durchführen, indem Sie Instances hinzufügen. Siehe the section called “Empfohlene CloudWatch Alarme”.
`SysMemory Utilization`	Der Prozentsatz des Arbeitsspeichers einer Instance, die in dem Cluster verwendet wird. Hohe Werte für diese Metrik sind normal und stellen normalerweise kein Problem mit Ihrem Cluster dar. Einen besseren Indikator für potenzielle Leistungs- und Stabilitätsprobleme finden Sie in der `JVMMemoryPressure` -Metrik.
`IndexingLatency`	Der Unterschied zwischen Minute N und Minute (N-1) in Millisekunden in der Gesamtzeit aller Indizierungsvorgänge in einem Knoten.
`IndexingRate`	Die Anzahl der Indizierungsvorgänge pro Minute.
`SearchLatency`	Der Unterschied in der Gesamtzeit in Millisekunden, die bei allen Suchvorgängen in einem Knoten zwischen Minute N und Minute (N-1) gemessen wird.
`SearchRate`	Die Gesamtanzahl von Suchabfragen pro Minute für alle Shards in einem Datenknoten.
`Threadpoo lSearchQueue`	Die Anzahl von Aufgaben in einer Warteschlange im Such-Threadpool. Wenn die Größe der Warteschlange gleichbleibend hoch ist, erwägen Sie eine Skalierung Ihres Clusters. Die maximale Größe der Such-Wart eschlange beträgt 1.000.

Metrik	Beschreibung
`ThreadpoolWriteQueue`	Die Anzahl von Aufgaben in einer Warteschlange im Schreib-Threadpool.
`ThreadpoolSearchRejected`	Die Anzahl abgewiesener Aufgaben im Such-Threadpool. Wenn die Anzahl stätig wächst, erwägen Sie eine Skalierung Ihres Clusters.
`ThreadpoolWriteRejected`	Die Anzahl abgewiesener Aufgaben im Schreib-Threadpool.

Metriken auf Clusterebene für Cluster in aktiven Availability Zones

Metrik	Beschreibung
`DataNodes`	Die Gesamtzahl der aktiven und Standby-Shards.
`DataNodesShards.active`	Die Gesamtzahl der aktiven primären und Replikat-Shards.
`DataNodesShards.unassigned`	Die Anzahl der Shards, die Knoten im Cluster nicht zugeordnet sind.
`DataNodesShards.initializing`	Die Anzahl der Shards, die derzeit initialisiert werden.
`DataNodesShards.relocating`	Die Anzahl der Shards, die derzeit verschoben werden.

Metriken zur Rotation der Verfügbarkeits

Wenn`ActiveReads.`*`Availability-Zone`* = `1`, dann ist die Zone aktiv.
Wenn`ActiveReads.`*`Availability-Zone`* = `0`, dann befindet sich die Zone im Standby-Modus.

Point-in-Time-Metriken

Amazon OpenSearch Service bietet die folgenden Metriken für Point-in-Time-Suchen (PIT).

PIT-Koordinator-Knotenstatistik (pro Koordinator-Knoten)

Metrik	Beschreibung
`CurrentPointInTime`	Die Anzahl der aktiven PIT-Suchkontexte im Knoten.
`TotalPointInTime`	Die Anzahl abgelaufener PIT-Suchkontexte seit der Knotenbetriebszeit.
`AvgPointInTimeAliveTime`	Der durchschnittliche Keep-Alive der PIT-Suchkontexte seit der Knotenbetriebszeit.
`HasActivePointInTime`	Ein Wert von 1 gibt an, dass es seit der Verfügbarkeit des Knotens aktive PIT-Kontexte auf Knoten gibt. Der Wert 0 bedeutet, dass es keine gegeben hat.
`HasUsedPointInTime`	Ein Wert von 1 gibt an, dass seit der Betriebszeit des Knotens abgelaufene PIT-Kontexte auf Knoten vorhanden sind. Der Wert 0 bedeutet, dass es keine gegeben hat.

SQL-Metriken

Amazon OpenSearch Service bietet die folgenden Metriken für SQL-Support.

Metrik	Beschreibung
`SQLFailedRequestCountByCusErr`	Die Anzahl der Anforderungen an die `_sql`-API, die aufgrund eines Clientproblems fehlgeschlagen sind. Beispielsweise kann eine Anforderung den HTTP-Statuscode 400 aufgrund eines `IndexNotFoundException` zurückgeben. Relevante Statistiken: Summe

Metrik	Beschreibung
SQLFailedRequestCountBySysErr	Die Anzahl der Anforderungen an die _sql-API, die aufgrund eines Serverproblems oder einer Funktionseinschränkung fehlgeschlagen sind. Beispielsweise kann eine Anforderung den HTTP-Statuscode 503 aufgrund eines VerificationException zurückgeben. Relevante Statistiken: Summe
SQLRequestCount	Die Anzahl der Anforderungen an die _sql-API. Relevante Statistiken: Summe
SQLDefaultCursorRequestCount	Ähnlich wieSQLRequestCount , zählt aber nur Paginierungsanfragen. Relevante Statistiken: Summe
SQLUnhealthy	Ein Wert von 1 gibt an, dass das SQL-Plugin als Reaktion auf bestimmte Anforderungen 5xx Antwortcodes zurückgibt oder ungültige Abfrage-DSL an OpenSearch übergibt. Andere Anfragen sollten weiterhin erfolgreich sein. Der Wert 0 zeigt an, dass keine aktuellen Fehler vorliegen. Wenn Sie einen dauerhaften Wert von 1 sehen, beheben Sie die Anforderungen, die Ihre Clients an das Plug-in stellen. Relevante Statistiken: Maximum

k-NN-Metriken

Amazon OpenSearch Service enthält die folgenden Metriken für das k-NN -Plug-In (k-nearest neighbor).

Metrik	Beschreibung
KNNCacheCapacityReached	Metrik pro Knoten, ob die Cache-Kapazität erreicht wurde. Diese Metrik ist nur für die ungefähre k-NN-Suche relevant. Relevante Statistiken: Maximum

Metrik	Beschreibung
KNNCircuitBreakerTriggered	Metrik pro Cluster, ob der Leistungsschalter ausgelöst wird. Wenn Knoten einen Wert von 1 für KNNCacheCapacityReached zurückgibt, wird dieser Wert auch 1 zurückgeben. Diese Metrik ist nur für die ungefähre k-NN-Suche relevant. Relevante Statistiken: Maximum
KNNEvictionCount	Metrik pro Knoten für die Anzahl der Diagramme, die aufgrund von Speichereinschränkungen oder Leerlaufzeit aus dem Cache entfernt wurden. Explizite Bereinigungen, die aufgrund des Indexlöschens auftreten, werden nicht gezählt. Diese Metrik ist nur für die ungefähre k-NN-Suche relevant. Relevante Statistiken: Summe
KNNGraphIndexErrors	Metrik pro Knoten für die Anzahl der Anforderungen, um das knn_vector -Feld eines Dokuments in ein Diagramm hinzufügen, das einen Fehler erzeugt hat. Relevante Statistiken: Summe
KNNGraphIndexRequests	Metrik pro Knoten für die Anzahl der Anforderungen, um das knn_vector -Feld eines Dokuments in ein Diagramm hinzufügen. Relevante Statistiken: Summe
KNNGraphMemoryUsage	Metrik pro Knoten für die aktuelle Cachegröße (Gesamtgröße aller Diagramme im Speicher) in Kilobyte. Diese Metrik ist nur für die ungefähre k-NN-Suche relevant. Relevante Statistiken: Durchschnitt
KNNGraphQueryErrors	Metrik pro Knoten für die Anzahl der Diagrammabfragen, die einen Fehler verursacht haben. Relevante Statistiken: Summe

Metrik	Beschreibung
KNNGraphQueryRequests	Metrik pro Knoten für die Anzahl der Diagrammabfragen. Relevante Statistiken: Summe
KNNHitCount	Metrik pro Knoten für die Anzahl der Cache-Treffer. Ein Cache-Treffer tritt auf, wenn ein Benutzer ein Diagramm abfragt, das bereits in den Speicher geladen ist. Diese Metrik ist nur für die ungefähre k-NN-Suche relevant. Relevante Statistiken: Summe
KNNLoadExceptionCount	Metrik pro Knoten für die Häufigkeit, mit der eine Ausnahme aufgetreten ist, während versucht wurde, ein Diagramm in den Cache zu laden. Diese Metrik ist nur für die ungefähre k-NN-Suche relevant. Relevante Statistiken: Summe
KNNLoadSuccessCount	Metrik pro Knoten, wie oft das Plug-In ein Diagramm erfolgreich in den Cache geladen hat. Diese Metrik ist nur für die ungefähre k-NN-Suche relevant. Relevante Statistiken: Summe
KNNMissCount	Metrik pro Knoten für die Anzahl der Cache-Fehlschläge. Ein Cache-Fehlschlag tritt auf, wenn ein Benutzer ein Diagramm abfragt, das noch nicht in den Speicher geladen ist. Diese Metrik ist nur für die ungefähre k-NN-Suche relevant. Relevante Statistiken: Summe
KNNQueryRequests	Metrik pro Knoten für die Anzahl der Abfrageanforderungen, die das k–NN-Plug-In empfangen hat. Relevante Statistiken: Summe

Metrik	Beschreibung
KNNScriptCompilationErrors	Metrik pro Knoten für die Anzahl der Fehler während der Skript-Kompilierung. Diese Statistik ist nur relevant für die Suche nach k-NN-Skripten. Relevante Statistiken: Summe
KNNScriptCompilations	Metrik pro Knoten für die Anzahl der Kompilierung des k-NN-Skripts. Dieser Wert sollte normalerweise 1 oder 0 sein, aber wenn der Cache mit den kompilierten Skripten gefüllt ist, wird das k-NN-Skript möglicherweise neu kompiliert. Diese Statistik ist nur relevant für die Suche nach k-NN-Skripten. Relevante Statistiken: Summe
KNNScriptQueryErrors	Metrik pro Knoten für die Anzahl der Fehler bei Skriptabfragen. Diese Statistik ist nur relevant für die Suche nach k-NN-Skripten. Relevante Statistiken: Summe
KNNScriptQueryRequests	Metrik pro Knoten für die Gesamtzahl der Skriptabfragen. Diese Statistik ist nur relevant für die Suche nach k-NN-Skripten. Relevante Statistiken: Summe
KNNTotalLoadTime	Die Zeit in Nanosekunden, die k-NN benötigt hat, um Diagramme in den Cache zu laden. Diese Metrik ist nur für die ungefähre k-NN-Suche relevant. Relevante Statistiken: Summe

Metriken für Cluster-übergreifende Suchen

Amazon OpenSearch Service bietet die folgenden Metriken für cluster-übergreifende Suche.

Metriken der Quell-Domain

Metrik	Dimension	Beschreibung
`CrossClusterOutboundConnections`	`ConnectionId`	Anzahl der verbundenen Knoten. Wenn Ihre Antwort eine oder mehrere übersprungene Domains enthält, verwenden Sie diese Metrik, um alle fehlerhaften Verbindungen nachzuverfolgen. Wenn diese Zahl auf 0 fällt, ist die Verbindung fehlerhaft.
`CrossClusterOutboundRequests`	`ConnectionId`	Anzahl der an die Ziel-Domain gesendeten Suchabfragen. Verwenden Sie dies, um zu überprüfen, ob die Last von Cluster-übergreifenden Suchabfragen Ihre Domain überfordert, korrelieren Sie jede Spitze in dieser Metrik mit jeder JVM/CPU-Spitze.

Metrik der Ziel-Domain

Metrik	Dimension	Beschreibung
`CrossClusterInboundRequests`	`ConnectionId`	Anzahl der eingehenden Verbindungsanforderungen, die von der Quell-Domain empfangen wurden.

Fügen Sie einen CloudWatch Alarm für den Fall hinzu, dass Sie unerwartet eine Verbindung verlieren. Schritte zum Erstellen eines Alarms finden Sie unter Erstellen eines CloudWatch Alarms auf der Grundlage eines statischen Schwellenwerts.

Cluster-übergreifende Replikationsmetriken

Amazon OpenSearch Service bietet die folgenden Metriken für cluster-übergreifende cluster-übergreifende Replikation.

Metrik	Beschreibung
`ReplicationRate`	Die durchschnittliche Rate der Replikationsvorgänge pro Sekunde. Diese Metrik ähnelt der `IndexingRate` -Metrik.

Metrik	Beschreibung
LeaderCheckPoint	Die Summe der Leader-Checkpoint-Werte für eine bestimmte Verbindung über alle replizierenden Indizes. Sie können diese Metrik verwenden, um die Latenz der Replikation zu messen.
FollowerCheckPoint	Die Summe der Follower-Checkpoint-Werte für eine bestimmte Verbindung über alle replizierenden Indizes. Sie können diese Metrik verwenden, um die Latenz der Replikation zu messen.
ReplicationNumSyncingIndices	Die Anzahl der Indizes, die den Replikationsstatus SYNCING haben.
ReplicationNumBootstrappingIndices	Die Anzahl der Indizes, die den Replikationsstatus BOOTSTRAPPING haben.
ReplicationNumPausedIndices	Die Anzahl der Indizes, die den Replikationsstatus PAUSED haben.
ReplicationNumFailedIndices	Die Anzahl der Indizes, die den Replikationsstatus FAILED haben.
CrossClusterOutboundReplicationRequests	Die Anzahl der Replikationstransportanfragen auf der Follower-Domain. Transportanfragen sind intern und treten bei jedem Aufruf eines Replikations-API-Vorgangs auf. Sie treten auch auf, wenn die Follower-Domain Änderungen gegenüber der Leader-Domain abfragt.
CrossClusterInboundReplicationRequests	Die Anzahl der Replikationstransportanfragen in der Leader-Domäne. Transportanfragen sind intern und treten bei jedem Aufruf eines Replikations-API-Vorgangs auf.

Metrik	Beschreibung
`AutoFollowNumSuccessStartReplication`	Die Anzahl der Follower-Indizes, die durch eine Replikationsregel für eine bestimmte Verbindung erfolgreich erstellt wurden.
`AutoFollowNumFailedStartReplication`	Die Anzahl der Follower-Indizes, die von einer Replikationsregel nicht erstellt werden konnten, wenn ein übereinstimmendes Muster vorhanden war. Dieses Problem kann aufgrund eines Netzwerkproblems auf dem Remote-Cluster oder eines Sicherheitsproblems auftreten (d. h. die zugeordnete Rolle hat keine Berechtigung zum Starten der Replikation).
`AutoFollowLeaderCallFailure`	Ob es fehlgeschlagene Abfragen vom Follower-Index zum Leader-Index gegeben hat, um neue Daten abzurufen. Ein Wert von 1 bedeutet, dass es in der letzten Minute 1 oder mehr fehlgeschlagene Anrufe gegeben hat.

Learning-to-Rank-Metriken

Amazon OpenSearch Service bietet die folgenden Metriken für Learning to Rank.

Metrik	Beschreibung
`LTRRequestTotalCount`	Gesamtzahl der Ranglistenanforderungen.
`LTRRequestErrorCount`	Gesamtzahl der fehlgeschlagenen Anforderungen.
`LTRStatus.red`	Verfolgt, ob einer der Indizes, die zum Ausführen des Plug-Ins benötigt werden, rot ist.
`LTRMemoryUsage`	Der Gesamtspeicher, der vom Plug-In verwendet wird.

Metrik	Beschreibung
`LTRFeatureMemoryUsageInBytes`	Die Menge an Arbeitsspeicher in Byte, die von den Learning-to-Rank-Funktionsfeldern verwendet wird.
`LTRFeaturesetMemoryUsageInBytes`	Die Menge an Arbeitsspeicher in Byte, die von allen Learning-to-Rank-Funktionssets verwendet wird.
`LTRModelMemoryUsageInBytes`	Die Menge an Arbeitsspeicher in Byte, die von allen Learning-to-Rank-Modellen verwendet wird.

Metriken für Piped Processing Language

Amazon OpenSearch Service bietet die folgenden Metriken für Piped Processing Language.

Metrik	Beschreibung
`PPLFailedRequestCountByCusErr`	Die Anzahl der Anforderungen an die `_ppl`-API, die aufgrund eines Clientproblems fehlgeschlagen sind. Beispielsweise kann eine Anforderung den HTTP-Statuscode 400 aufgrund eines `IndexNotFoundException` zurückgeben.
`PPLFailedRequestCountBySysErr`	Die Anzahl der Anforderungen an die `_ppl`-API, die aufgrund eines Serverproblems oder einer Funktionseinschränkung fehlgeschlagen sind. Beispielsweise kann eine Anforderung den HTTP-Statuscode 503 aufgrund eines `VerificationException` zurückgeben.
`PPLRequestCount`	Die Anzahl der Anforderungen an die `_ppl`-API.

OpenSearch Protokolle mit Amazon CloudWatch Logs überwachen

Amazon OpenSearch Service stellt die folgenden OpenSearch Protokolle über Amazon CloudWatch Logs zur Verfügung:

- Fehlerprotokolle
- Langsame Protokolle für Suchanfragen
- Langsame Protokolle teilen
- Prüfungsprotokolle

Search Shard Slow-Logs, Indexing Shard Slow-Logs und Fehlerprotokolle sind nützlich, um Leistungs- und Stabilitätsprobleme zu beheben. Prüfungsprotokolle verfolgen Benutzeraktivitäten zu Compliance-Zwecken. Alle Protokolle sind standardmäßig deaktiviert. Wenn diese Option aktiviert ist, gelten die Standardpreise CloudWatch .

> **Note**
>
> Fehlerprotokolle sind nur für OpenSearch Elasticsearch-Versionen 5.1 und höher verfügbar. Langsame Logs sind für alle Versionen OpenSearch und für Elasticsearch verfügbar.

OpenSearch Verwendet für seine Logs Apache Log4j 2 und die integrierten Log-Levels (vom geringsten bis zum schwersten) von`TRACE`,`DEBUG`, `INFO``WARN`, `ERROR` und. `FATAL`

Wenn Sie Fehlerprotokolle aktivieren, veröffentlicht OpenSearch Service die Protokollzeilen von `WARN``ERROR`, und `FATAL` bis. CloudWatch OpenSearch Service veröffentlicht auch mehrere Ausnahmen von der `DEBUG` Ebene, darunter die folgenden:

- `org.opensearch.index.mapper.MapperParsingException`
- `org.opensearch.index.query.QueryShardException`
- `org.opensearch.action.search.SearchPhaseExecutionException`
- `org.opensearch.common.util.concurrent.OpenSearchRejectedExecutionException`
- `java.lang.IllegalArgumentException`

Fehlerprotokolle können bei der Fehlerbehebung in zahlreichen Situationen helfen, unter anderem:

- Probleme bei der Kompilierung von Painless-Skripts
- Ungültige Abfragen
- Probleme bei der Indizierung
- Snapshot-Fehler

- Migrationsfehler beim Indexstatusmanagement

> **Note**
>
> Nicht alle Fehler werden in den Fehlerprotokollen gemeldet.

> **Note**
>
> OpenSearch Der Dienst protokolliert nicht alle auftretenden Fehler.

Themen

- Aktivieren der Veröffentlichung von Protokollen (Konsole)
- Aktivieren der Veröffentlichung von Protokollen (AWS CLI)
- Aktivieren der Protokollveröffentlichung ()AWS SDKs
- Aktivieren der Veröffentlichung von Protokollen (CloudFormation)
- Schwellenwerte für langsame Protokollierung von Suchanfragen festlegen
- Schwellenwerte für Shard Slow Log festlegen
- Langsame Protokolle testen
- Anzeigen von -Protokollen

Aktivieren der Veröffentlichung von Protokollen (Konsole)

Die OpenSearch Servicekonsole ist die einfachste Methode, um die Veröffentlichung von Protokollen zu ermöglichen CloudWatch.

Um die Veröffentlichung von Protokollen in CloudWatch (Konsole) zu aktivieren

1. Gehen Sie zu aws.amazon.com, wählen Sie dann Anmelden und geben Sie Ihre Anmeldeinformationen ein.
2. Wählen Sie unter Analytics Amazon OpenSearch Service aus.
3. Wählen Sie die Domain aus, die Sie aktualisieren möchten.
4. Wählen Sie auf der Registerkarte Protokolle einen Protokolltyp aus und wählen Sie Aktivieren aus.

5. Erstellen Sie eine neue CloudWatch Protokollgruppe oder wählen Sie eine bestehende aus.

> **Note**
>
> Wenn Sie die mehrere Protokolle aktivieren möchten, sollten Sie jedes Protokoll in einer eigenen Protokollgruppe veröffentlichen. Diese Trennung ermöglicht ein einfacheres Scannen der Protokolle.

6. Wählen Sie eine Zugriffsrichtlinie mit den entsprechenden Berechtigungen aus, oder erstellen Sie eine Richtlinie mit dem in der Konsole verfügbaren JSON:

   JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "es.amazonaws.com"
      },
      "Action": [
        "logs:PutLogEvents",
        "logs:CreateLogStream"
      ],
      "Resource": "cw_log_group_arn:*"
    }
  ]
}
```

   Wir empfehlen Ihnen, die `aws:SourceAccount`- und `aws:SourceArn`-Bedingungsschlüssel zur Richtlinie hinzuzufügen, um sich vor dem Problem des verwirrten Stellvertreters zu schützen. Das Quellkonto ist der Eigentümer der Domain und der Quell-ARN ist der ARN der Domain. Ihre Domain muss zum Hinzufügen dieser Bedingungsschlüssel über Service-Software R20211203 oder höher verfügen.

   Beispielsweise können Sie der Richtlinie den folgenden Bedingungsblock hinzufügen:

```
"Condition": {
```

```
    "StringEquals": {
        "aws:SourceAccount": "account-id"
    },
    "ArnLike": {
        "aws:SourceArn": "arn:aws:es:region:account-id:domain/domain-name"
    }
}
```

> **Important**
>
> CloudWatch Logs unterstützt 10 Ressourcenrichtlinien pro Region. Wenn Sie beabsichtigen, Protokolle für mehrere OpenSearch Dienstdomänen zu aktivieren, sollten Sie eine umfassendere Richtlinie erstellen und wiederverwenden, die mehrere Protokollgruppen umfasst, um zu verhindern, dass dieses Limit erreicht wird. Anweisungen zum Aktualisieren Ihrer Richtlinie finden Sie unter the section called “Aktivieren der Veröffentlichung von Protokollen (AWS CLI)”.

7. Wählen Sie Enable (Aktivieren) aus.

   Der Status Ihrer Domain ändert sich von Active (Aktiv) zu Processing (In Verarbeitung). Der Status muss auf Active (Aktiv) zurückgesetzt werden, bevor die Veröffentlichung von Protokollen aktiviert wird. Diese Änderung dauert in der Regel 30 Minuten, kann jedoch je nach Domain-Konfiguration auch länger dauern.

Wenn Sie eines der Shard Slow-Logs aktiviert haben, finden Sie weitere Informationen unterthe section called “Schwellenwerte für Shard Slow Log festlegen”. Wenn Sie Prüfungsprotokolle aktiviert haben, siehe the section called “Schritt 2: Aktivieren Sie Audit-Logs in OpenSearch Dashboards”. Wenn Sie nur Fehlerprotokolle aktiviert haben, müssen Sie keine weiteren Konfigurationsschritte ausführen.

Aktivieren der Veröffentlichung von Protokollen (AWS CLI)

Bevor Sie die Protokollveröffentlichung aktivieren können, benötigen Sie eine CloudWatch Protokollgruppe. Wenn Sie noch keine Gruppe vorliegen haben, können Sie mit dem folgenden Befehl eine Gruppe erstellen:

```
aws logs create-log-group --log-group-name my-log-group
```

Geben Sie den folgenden Befehl ein, um den ARN der Protokollgruppe zu ermitteln, und notieren Sie sich den ARN:

```
aws logs describe-log-groups --log-group-name my-log-group
```

Jetzt können Sie dem OpenSearch Dienst Schreibberechtigungen für die Protokollgruppe erteilen. Sie müssen die ARN der Protokollgruppe nahe am Ende des Befehls bereitstellen:

```
aws logs put-resource-policy \
  --policy-name my-policy \
  --policy-document '{ "Version": "2012-10-17", "Statement": [{ "Sid": "",
 "Effect": "Allow", "Principal": { "Service": "es.amazonaws.com"}, "Action":
[ "logs:PutLogEvents","logs:CreateLogStream"],"Resource": "cw_log_group_arn:*"}]}'
```

> **Important**
>
> CloudWatch Logs unterstützt 10 Ressourcenrichtlinien pro Region. Wenn Sie planen, Shard Slow Logs für mehrere OpenSearch Dienstdomänen zu aktivieren, sollten Sie eine umfassendere Richtlinie erstellen und wiederverwenden, die mehrere Protokollgruppen umfasst, um zu verhindern, dass dieses Limit erreicht wird.

Wenn Sie diese Richtlinie zu einem späteren Zeitpunkt überprüfen müssen, verwenden Sie den `aws logs describe-resource-policies`-Befehl. Um die Richtlinie zu aktualisieren, geben Sie denselben `aws logs put-resource-policy`-Befehl für ein neues Richtliniendokument aus.

Schließlich können Sie die Option `--log-publishing-options` zum Aktivieren der Veröffentlichung verwenden. Die Syntax für die Option ist identisch für die `create-domain`- und `update-domain-config`-Befehle.

Parameter	Zulässige Werte
`--log-publishing-options`	`SEARCH_SLOW_LOGS={CloudWatchLogsLogGroupArn= cw_log_group_arn ,Enabled=true|false}`
	`INDEX_SLOW_LOGS={CloudWatchLogsLogGroupArn= cw_log_group_arn ,Enabled=true|false}`

Parameter	Zulässige Werte
	`ES_APPLICATION_LOGS={CloudWatchLogsLogGroupAr n= cw_log_group_arn ,Enabled=true|false}`
	`AUDIT_LOGS={CloudWatchLogsLogGroupAr n= cw_log_group_arn ,Enabled=true|false}`

> **Note**
>
> Wenn Sie die mehrere Protokolle aktivieren möchten, sollten Sie jedes Protokoll in einer eigenen Protokollgruppe veröffentlichen. Diese Trennung ermöglicht ein einfacheres Scannen der Protokolle.

Beispiel

Das folgende Beispiel ermöglicht die Veröffentlichung von Shard Slow-Protokollen für die Suche und Indizierung von Shard Slow für die angegebene Domäne:

```
aws opensearch update-domain-config \
  --domain-name my-domain \
  --log-publishing-options
 "SEARCH_SLOW_LOGS={CloudWatchLogsLogGroupArn=arn:aws:logs:us-east-1:123456789012:log-
group:my-log-
group,Enabled=true},INDEX_SLOW_LOGS={CloudWatchLogsLogGroupArn=arn:aws:logs:us-
east-1:123456789012:log-group:my-other-log-group,Enabled=true}"
```

Um das Veröffentlichen in zu deaktivieren CloudWatch, führen Sie denselben Befehl mit aus. `Enabled=false`

Wenn Sie eines der Shard Slow-Logs aktiviert haben, finden Sie weitere Informationen unterthe section called “Schwellenwerte für Shard Slow Log festlegen”. Wenn Sie Prüfungsprotokolle aktiviert haben, siehe the section called “Schritt 2: Aktivieren Sie Audit-Logs in OpenSearch Dashboards”. Wenn Sie nur Fehlerprotokolle aktiviert haben, müssen Sie keine weiteren Konfigurationsschritte ausführen.

Aktivieren der Protokollveröffentlichung ()AWS SDKs

Bevor Sie die Protokollveröffentlichung aktivieren können, müssen Sie zunächst eine CloudWatch Protokollgruppe erstellen, ihren ARN abrufen und dem OpenSearch Dienst Schreibberechtigungen für diese Gruppe erteilen. Die entsprechenden Vorgänge sind in der Amazon CloudWatch Logs API-Referenz dokumentiert:

- `CreateLogGroup`
- `DescribeLogGroup`
- `PutResourcePolicy`

Sie können auf diese Operationen zugreifen, indem Sie AWS SDKs

Die AWS SDKs (außer Android und iOS SDKs) unterstützen alle Operationen, die in der Amazon OpenSearch Service API-Referenz definiert sind, einschließlich der `--log-publishing-options` Option für `CreateDomain` und`UpdateDomainConfig`.

Wenn Sie eines der Shard Slow-Logs aktiviert haben, finden Sie weitere Informationen unterthe section called “Schwellenwerte für Shard Slow Log festlegen”. Wenn Sie nur Fehlerprotokolle aktiviert haben, müssen Sie keine weiteren Konfigurationsschritte ausführen.

Aktivieren der Veröffentlichung von Protokollen (CloudFormation)

In diesem Beispiel erstellen wir eine Protokollgruppe mit dem Namen`opensearch-logs`, weisen ihnen die entsprechenden Berechtigungen CloudFormation zu und erstellen dann eine Domäne, in der die Protokollveröffentlichung für Anwendungsprotokolle, Shard-Slow-Logs für die Suche und Indexierung von Slow-Logs aktiviert ist.

Bevor Sie die Protokollveröffentlichung aktivieren können, müssen Sie eine CloudWatch Protokollgruppe erstellen:

```
Resources:
  OpenSearchLogGroup:
    Type: AWS::Logs::LogGroup
    Properties:
      LogGroupName: opensearch-logs
Outputs:
  Arn:
```

```
    Value:
      'Fn::GetAtt':
        - OpenSearchLogGroup
        - Arn
```

Die Vorlage gibt den ARN der Protokollgruppe aus. In diesem Fall ist der ARN `arn:aws:logs:us-east-1:123456789012:log-group:opensearch-logs`.

Erstellen Sie mithilfe des ARN eine Ressourcenrichtlinie, die dem OpenSearch Dienst Schreibberechtigungen für die Protokollgruppe erteilt:

```
Resources:
 OpenSearchLogPolicy:
   Type: AWS::Logs::ResourcePolicy
   Properties:
     PolicyName: my-policy
     PolicyDocument: "{ \"Version\": \"2012-10-17\", \"Statement\": [{ \"Sid\": \"\",
 \"Effect\": \"Allow\", \"Principal\": { \"Service\": \"es.amazonaws.com\"}, \"Action
\":[ \"logs:PutLogEvents\",\"logs:CreateLogStream\"],\"Resource\": \"arn:aws:logs:us-
east-1:123456789012:log-group:opensearch-logs:*\"}]}"
```

Erstellen Sie abschließend den folgenden CloudFormation Stack, der eine OpenSearch Dienstdomäne mit Protokollveröffentlichung generiert. Die Zugriffsrichtlinie ermöglicht es dem Benutzer AWS-Konto , alle HTTP-Anfragen an die Domain zu stellen.

```
Resources:
  OpenSearchServiceDomain:
    Type: "AWS::OpenSearchService::Domain"
    Properties:
      DomainName: my-domain
      EngineVersion: "OpenSearch_1.0"
      ClusterConfig:
        InstanceCount: 2
        InstanceType: "r6g.xlarge.search"
        DedicatedMasterEnabled: true
        DedicatedMasterCount: 3
        DedicatedMasterType: "r6g.xlarge.search"
      EBSOptions:
        EBSEnabled: true
        VolumeSize: 10
        VolumeType: "gp2"
      AccessPolicies:
```

```
        Version: "2012-10-17"
        Statement:
            Effect: "Allow"
            Principal:
                AWS: "arn:aws:iam::123456789012:user/es-user"
            Action: "es:*"
            Resource: "arn:aws:es:us-east-1:123456789012:domain/my-domain/*"
      LogPublishingOptions:
        ES_APPLICATION_LOGS:
          CloudWatchLogsLogGroupArn: "arn:aws:logs:us-east-1:123456789012:log-
group:opensearch-logs"
          Enabled: true
        SEARCH_SLOW_LOGS:
          CloudWatchLogsLogGroupArn: "arn:aws:logs:us-east-1:123456789012:log-
group:opensearch-logs"
          Enabled: true
        INDEX_SLOW_LOGS:
          CloudWatchLogsLogGroupArn: "arn:aws:logs:us-east-1:123456789012:log-
group:opensearch-logs"
          Enabled: true
```

Ausführliche Syntaxinformationen finden Sie unter Optionen für die Protokollveröffentlichung im AWS CloudFormation -Benutzerhandbuch.

Schwellenwerte für langsame Protokollierung von Suchanfragen festlegen

Protokolle für langsame Suchanfragen sind für die Suche in OpenSearch Dienstdomänen verfügbar, die auf Version 2.13 und höher ausgeführt werden. Die Protokollschwellenwerte für langsame Suchanfragen sind für die Gesamtdauer der Anfrage konfiguriert. Dies unterscheidet sich von langsamen Protokollen für Shard-Anfragen, die so konfiguriert sind, dass einzelne Shard Zeit in Anspruch nehmen.

Sie können Logs für langsame Suchanfragen mit Clustereinstellungen angeben. Dies unterscheidet sich von Shard Slow Logs, die Sie mit Indexeinstellungen aktivieren. Sie können beispielsweise die folgenden Einstellungen über die OpenSearch REST-API angeben:

```
PUT domain-endpoint/_cluster/settings
{
  "transient": {
    "cluster.search.request.slowlog.threshold.warn": "5s",
    "cluster.search.request.slowlog.threshold.info": "2s"
  }
```

```
}
```

Schwellenwerte für Shard Slow Log festlegen

OpenSearch deaktiviert standardmäßig Shard Slow Logs. Nachdem Sie die Veröffentlichung von Shard Slow-Logs auf aktiviert haben CloudWatch, müssen Sie immer noch Schwellenwerte für die Protokollierung für jeden Index angeben. OpenSearch Diese Schwellenwerte definieren genau, was auf welcher Protokollebene protokolliert werden soll.

Sie können diese Einstellungen beispielsweise über die OpenSearch REST-API angeben:

```
PUT domain-endpoint/index/_settings
{
  "index.search.slowlog.threshold.query.warn": "5s",
  "index.search.slowlog.threshold.query.info": "2s"
}
```

Langsame Protokolle testen

Um zu testen, ob sowohl die Protokolle für Suchanfragen als auch für Shard Slow erfolgreich veröffentlicht werden, sollten Sie mit sehr niedrigen Werten beginnen, um zu überprüfen, ob die Protokolle auch angezeigt werden CloudWatch, und dann die Schwellenwerte auf sinnvollere Werte erhöhen.

Wenn die Protokolle nicht angezeigt werden, überprüfen Sie Folgendes:

- Existiert die CloudWatch Protokollgruppe? Überprüfen Sie die CloudWatch Konsole.
- Hat OpenSearch Service die Rechte, in die Protokollgruppe zu schreiben? Überprüfen Sie die OpenSearch Servicekonsole.
- Ist die OpenSearch Dienstdomäne für die Veröffentlichung in der Protokollgruppe konfiguriert? Überprüfen Sie die OpenSearch Servicekonsole, verwenden Sie die AWS CLI `describe-domain-config` Option oder rufen Sie `DescribeDomainConfig` mit einer der folgenden Optionen an SDKs.
- Sind die Schwellenwerte für die OpenSearch Protokollierung so niedrig, dass Ihre Anfragen sie überschreiten?

  Verwenden Sie den folgenden Befehl, um die Schwellenwerte für die langsame Protokollierung Ihrer Suchanfrage für eine Domain zu überprüfen:

```
GET domain-endpoint/_cluster/settings?flat_settings
```

Verwenden Sie den folgenden Befehl, um die Schwellenwerte für das Shard Slow Log für einen Index zu überprüfen:

```
GET domain-endpoint/index/_settings?pretty
```

Wenn Sie Slow-Protokolle für einen Index deaktivieren möchten, setzen Sie alle geänderten Schwellenwerte wieder auf die Standardwerte von `-1` zurück.

Wenn Sie die Veröffentlichung CloudWatch über die OpenSearch Service Console deaktivieren oder AWS CLI nicht die Erstellung OpenSearch von Protokollen beenden, sondern nur die Veröffentlichung dieser Protokolle beenden. Überprüfen Sie unbedingt Ihre Indexeinstellungen, falls Sie die Shard Slow-Logs nicht mehr benötigen, und Ihre Domain-Einstellungen, falls Sie die Slow-Logs für Suchanfragen nicht mehr benötigen.

Anzeigen von -Protokollen

Das Anzeigen der Anwendung und die langsame Anmeldung CloudWatch sind wie die Anzeige jedes anderen CloudWatch Protokolls. Weitere Informationen finden Sie unter Protokolldaten anzeigen im Amazon CloudWatch Logs-Benutzerhandbuch.

Hier finden Sie einige Überlegungen zur Anzeige der Protokolle:

- OpenSearch Service veröffentlicht nur die ersten 255.000 Zeichen jeder Zeile an CloudWatch. Alle verbleibenden Inhalte werden abgeschnitten. Bei Prüfungsprotokollen sind es 10 000 Zeichen pro Nachricht.
- In CloudWatch haben die Namen der Protokolldatenströme die Suffixe`-index-slow-logs`,,, und `-search-slow-logs-application-logs`, `-audit-logs` um den Inhalt leichter zu identifizieren.

Überwachung von Auditprotokollen in Amazon OpenSearch Service

Wenn Ihre Amazon OpenSearch Service-Domain eine differenzierte Zugriffskontrolle verwendet, können Sie Audit-Logs für Ihre Daten aktivieren. Audit-Logs sind hochgradig anpassbar und ermöglichen es Ihnen, Benutzeraktivitäten in Ihren OpenSearch Clustern nachzuverfolgen,

einschließlich erfolgreicher und fehlgeschlagener Authentifizierungen OpenSearch, Anfragen an, Indexänderungen und eingehende Suchanfragen. Die Standardkonfiguration verfolgt einen beliebten Satz von Benutzeraktionen. Wir empfehlen jedoch, die Einstellungen genau an Ihre Bedürfnisse anzupassen.

Genau wie OpenSearch Anwendungsprotokolle und langsame Protokolle veröffentlicht OpenSearch Service CloudWatch Auditprotokolle in Logs. Wenn diese Option aktiviert ist, gelten die CloudWatch Standardpreise.

> **Note**
>
> Um Audit-Logs zu aktivieren, muss Ihre Benutzerrolle der `security_manager` Rolle zugeordnet sein, die Ihnen Zugriff auf die OpenSearch `plugins/_security` REST-API gewährt. Weitere Informationen hierzu finden Sie unter the section called “Hauptbenutzer ändern”.

Themen

- Einschränkungen
- Aktivieren von Prüfprotokollen
- Aktivieren Sie die Auditprotokollierung mit dem AWS CLI
- Aktivieren der Prüfungsprotokollierung über die Konfigurations-API
- Protokollebenen und -Kategorien prüfen
- Prüfprotokolleinstellungen
- Prüfungsprotokollbeispiel
- Konfigurieren von Prüfungsprotokollen mit der REST-API

Einschränkungen

Prüfungsprotokolle haben folgende Einschränkungen:

- Prüfungsprotokolle enthalten keine clusterübergreifenden Suchanforderungen, die von der Domain-Zugriffsrichtlinie des Ziels abgelehnt wurden.
- Die Maximalgröße jeder Prüfungsprotokollmeldung beträgt 10 000 Zeichen. Die Prüfungsprotokollmeldung wird abgeschnitten, wenn sie diesen Grenzwert überschreitet.

Aktivieren von Prüfprotokollen

Die Aktivierung des Prüfungsprotokolls für einen Cluster ist ein zweistufiger Prozess. Zunächst konfigurieren Sie Ihre Domain so, dass Audit-Logs in Logs veröffentlicht werden CloudWatch . Anschließend aktivieren Sie Audit-Logs in OpenSearch Dashboards und konfigurieren sie so, dass sie Ihren Anforderungen entsprechen.

> **Important**
>
> Wenn beim Ausführen dieser Schritte ein Fehler auftritt, finden Sie unter the section called "Prüfungsprotokolle können nicht aktiviert werden" Informationen zur Fehlerbehebung.

Schritt 1: Aktivieren von Überwachungsprotokolle und Konfigurieren einer Zugriffsrichtlinie

In diesen Schritten wird beschrieben, wie Sie mithilfe der Konsole Prüfungsprotokolle aktivieren. Sie können sie auch mithilfe der oder der AWS CLIOpenSearch Service-API aktivieren.

Um Audit-Logs für eine OpenSearch Service-Domain (Konsole) zu aktivieren

1. Wählen Sie die Domain aus, um ihre Konfiguration zu öffnen, und wechseln Sie dann zur Registerkarte Protokolle.
2. Wählen Sie Prüfungsprotokolle und dann Aktivieren aus.
3. Erstellen Sie eine CloudWatch Protokollgruppe oder wählen Sie eine bestehende aus.
4. Wählen Sie eine Zugriffsrichtlinie mit den entsprechenden Berechtigungen aus, oder erstellen Sie eine Richtlinie mit dem in der Konsole verfügbaren JSON:

   JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "es.amazonaws.com"
      },
```

```
      "Action": [
        "logs:PutLogEvents",
        "logs:CreateLogStream"
      ],
      "Resource": "cw_log_group_arn"
    }
  ]
}
```

Wir empfehlen Ihnen, die `aws:SourceAccount`- und `aws:SourceArn`-Bedingungsschlüssel zur Richtlinie hinzuzufügen, um sich vor dem Problem des verwirrten Stellvertreters zu schützen. Das Quellkonto ist der Eigentümer der Domain und der Quell-ARN ist der ARN der Domain. Ihre Domain muss zum Hinzufügen dieser Bedingungsschlüssel über Service-Software R20211203 oder höher verfügen.

Beispielsweise können Sie der Richtlinie den folgenden Bedingungsblock hinzufügen:

```
"Condition": {
    "StringEquals": {
        "aws:SourceAccount": "account-id"
    },
    "ArnLike": {
        "aws:SourceArn": "arn:aws:es:region:account-id:domain/domain-name"
    }
}
```

5. Wählen Sie Aktivieren aus.

Schritt 2: Aktivieren Sie Audit-Logs in OpenSearch Dashboards

Nachdem Sie die Auditprotokolle in der OpenSearch Servicekonsole aktiviert haben, müssen Sie sie auch in den OpenSearch Dashboards aktivieren und entsprechend Ihren Anforderungen konfigurieren.

1. Öffnen Sie OpenSearch Dashboards und wählen Sie im Menü auf der linken Seite Sicherheit aus.
2. Wählen Sie Prüfungsprotokolle aus.
3. Wählen Sie Überwachungsprotokollierung aktivieren aus.

Die Dashboards-Benutzeroberfläche bietet vollständige Kontrolle über die Prüfungsprotokolleinstellungen unter Allgemeine Einstellungen und Compliance-Einstellungen. Eine Beschreibung aller Konfigurationsoptionen finden Sie unter Prüfungsprotokolleinstellungen.

Aktivieren Sie die Auditprotokollierung mit dem AWS CLI

Der folgende AWS CLI Befehl aktiviert Audit-Logs für eine bestehende Domain:

```
aws opensearch update-domain-config --domain-name my-domain --log-publishing-options
 "AUDIT_LOGS={CloudWatchLogsLogGroupArn=arn:aws:logs:us-east-1:123456789012:log-
group:my-log-group,Enabled=true}"
```

Sie können Prüfungsprotokolle auch aktivieren, wenn Sie eine Domain erstellen. Weitere Informationen finden Sie in der AWS CLI -Befehlsreferenz.

Aktivieren der Prüfungsprotokollierung über die Konfigurations-API

Die folgende Anfrage an die Konfigurations-API aktiviert Prüfungsprotokolle für eine vorhandene Domain:

```
POST https://es.us-east-1.amazonaws.com/2021-01-01/opensearch/domain/my-domain/config
{
  "LogPublishingOptions": {
    "AUDIT_LOGS": {
      "CloudWatchLogsLogGroupArn":"arn:aws:logs:us-east-1:123456789012:log-
group1:sample-domain",
      "Enabled":true
    }
  }
}
```

Weitere Informationen finden Sie in der Amazon OpenSearch Service API-Referenz.

Protokollebenen und -Kategorien prüfen

Cluster-Kommunikation erfolgt über zwei separate Ebenen: die REST- und die Transportebene.

- Die REST-Schicht deckt die Kommunikation mit HTTP-Clients wie curl, Logstash, OpenSearch Dashboards, dem Java-High-Level-REST-Client und der Python-Anforderungsbibliothek ab — alle HTTP-Anfragen, die im Cluster ankommen.

- Die Transportebene deckt die Kommunikation zwischen Knoten ab. Nachdem beispielsweise eine Suchanfrage im Cluster (über die REST-Ebene) eintrifft, sendet der koordinierende Knoten, der die Anfrage bedient, die Anfrage an andere Knoten, empfängt deren Antworten, sammelt die erforderlichen Dokumente und fasst sie in der endgültigen Antwort zusammen. Operationen wie Shard-Zuweisung und Neuverteilung erfolgen ebenfalls über die Transportebene.

Sie können Prüfungsprotokolle für ganze Ebenen sowie einzelne Prüfungskategorien für eine Ebene aktivieren oder deaktivieren. Die folgende Tabelle enthält eine Zusammenfassung der Überwachungskategorien und die Ebene, für die sie verfügbar sind.

Kategorie	Beschreibung	Für REST verfügbar	Transportfähig
FAILED_LOGIN	Eine Anforderung enthielt ungültige Anmeldeinformationen und die Authentifizierung ist fehlgeschlagen.	Ja	Ja
MISSING_PRIVILEGES	Ein Benutzer hatte nicht die Berechtigung, die Anforderung zu stellen.	Ja	Ja
GRANTED_PRIVILEGES	Ein Benutzer hatte die Berechtigung, die Anforderung zu stellen.	Ja	Ja
OPENSEARCH_SECURITY_INDEX_ATTEMPT	Eine Anforderung hat versucht, den `.opendistro_security` -Index zu ändern.	Nein	Ja
AUTHENTICATED	Eine Anforderung enthielt gültige Anmeldeinformationen und die	Ja	Ja

Kategorie	Beschreibung	Für REST verfügbar	Transportfähig
	Authentifizierung ist erfolgreich.		
INDEX_EVENT	Eine Anforderung führte einen administrativen Vorgang für einen Index aus, z. B. das Erstellen eines Indexes, das Festlegen eines Alias oder das Ausführen einer erzwungenen Zusammenführung. Die vollständige Liste der `indices:admin/` Aktionen, die diese Kategorie umfasst, ist in der Dokumentation verfügbar. OpenSearch	Nein	Ja

Zusätzlich zu diesen Standardkategorien bietet die fein abgestufte Zugriffskontrolle mehrere zusätzliche Kategorien, die darauf ausgelegt sind, die Anforderungen an die Daten-Compliance zu erfüllen.

Kategorie	Beschreibung
COMPLIANCE_DOC_READ	Eine Anforderung führte ein Leseereignis für ein Dokument in einem Index aus.
COMPLIANCE_DOC_WRITE	Eine Anforderung führte ein Schreibereignis für ein Dokument in einem Index aus.

Kategorie	Beschreibung
COMPLIANCE_INTERNAL_CONFIG_READ	Eine Anforderung führte ein Leseereignis auf dem `.opendistro_security` -Index aus.
COMPLIANCE_INTERNAL_CONFIG_WRITE	Eine Anforderung führte ein Schreibereignis auf dem `.opendistro_security` -Index aus.

Es kann eine beliebige Kombination von Kategorien und Nachrichtenattributen vorliegen. Wenn Sie beispielsweise eine REST-Anforderung senden, um ein Dokument zu indizieren, werden möglicherweise die folgenden Zeilen in den Prüfungsprotokollen angezeigt:

- Authentifiziert auf REST-Ebene (Authentifizierung)
- GRANTED_PRIVILEGE auf Transportebene (Autorisierung)
- COMPLIANCE_DOC_WRITE (Dokument in einen Index geschrieben)

Prüfprotokolleinstellungen

Prüfungsprotokolle verfügen über zahlreiche Konfigurationsoptionen.

Allgemeine Einstellungen

Mit den allgemeinen Einstellungen können Sie einzelne Kategorien oder ganze Ebenen aktivieren oder deaktivieren. Wir empfehlen, GRANTED_PRIVILEGES und AUTHENTICATED als ausgeschlossene Kategorien. Andernfalls werden diese Kategorien für jede gültige Anforderung an den Cluster protokolliert.

Name	Backend-Einstellung	Beschreibung
REST-Ebene	enable_rest	Aktivieren oder Deaktivieren von Ereignissen, die auf der REST-Ebene auftreten.
REST-Kategorien	disabled_rest_categories	Geben Sie Prüfungskategorien an, die auf der REST-Ebene ignoriert werden sollen. Durch Ändern dieser Kategorie

Name	Backend-Einstellung	Beschreibung
		n kann die Größe der Prüfungsprotokolle erheblich erhöht werden.
Transportebene	enable_transport	Aktivieren oder deaktivieren Sie Ereignisse, die auf der Transportebene auftreten.
Transportkategorien	disabled_transport_categories	Geben Sie Prüfungskategorien an, die auf der Transportebene ignoriert werden müssen. Durch Ändern dieser Kategorien kann die Größe der Prüfungsprotokolle erheblich erhöht werden.

Mit Attributeinstellungen können Sie die Detailmenge in jeder Protokollzeile anpassen.

Name	Backend-Einstellung	Beschreibung
Massenanfragen	resolve_bulk_requests	Wenn Sie diese Einstellung aktivieren, wird für jedes Dokument in einer Massenanforderung ein Protokoll generiert, das die Größe der Prüfungsprotokolle erheblich erhöhen kann.
Anforderungstext	log_request_body	Fügen Sie den Anforderungstext der Anforderungen ein.
Lösen von Indizes	resolve_indices	Alias in Indizes auflösen.

Verwenden Sie Ignorier-Einstellungen, um eine Gruppe von Benutzern oder API-Pfaden auszuschließen:

Name	Backend-Einstellung	Beschreibung
Ignorierte Benutzer	ignore_users	Geben Sie die Benutzer an, die Sie ausschließen möchten.
Ignorierte Anforderungen	ignore_requests	Geben Sie Anforderungsmuster an, die Sie ausschließen möchten.

Compliance-Einstellungen

Mit den Compliance-Einstellungen können Sie den Zugriff auf Index-, Dokument- oder Feldebene optimieren.

Name	Backend-Einstellung	Beschreibung
Compliance-Protokollierung	enable_compliance	Aktivieren oder deaktivieren Sie die Compliance-Protokollierung.

Sie können die folgenden Einstellungen für die Lese- und Schreibereignisprotokollierung festlegen.

Name	Backend-Einstellung	Beschreibung
Interne Konfigurationsprotokollierung	internal_config	Aktivieren oder deaktivieren Sie die Protokollierung von Ereignissen im `.opendistro_security` -Index.

Sie können die folgenden Einstellungen für Lese-Ereignisse festlegen.

Name	Backend-Einstellung	Beschreibung
Lesen von Metadaten	read_metadata_only	Nur Metadaten für Leseereignisse einschließen. Fügen Sie keine Dokumentfelder ein.
Ignorierte Benutzer	read_ignore_users	Schließen Sie bestimmte Benutzer nicht für Leseereignisse ein.
Beobachtete Felder	read_watched_fields	Geben Sie die Indizes und Felder an, die auf Leseereignisse überwacht werden sollen. Durch das Hinzufügen überwachter Felder wird ein Protokoll pro Dokumentzugriff generiert, wodurch die Größe der Prüfungsprotokolle erheblich vergrößert wird. Beobachtete Felder unterstützen Indexmuster und Feldmuster: `{ "index-name-pattern": [ "field-name-pattern" ], "logs*": [ "message" ], "twitter": [ "id", "user*" ] }`

Sie können die folgenden Einstellungen für Schreibereignisse festlegen.

Name	Backend-Einstellung	Beschreibung
Schreiben von Metadaten	write_metadata_only	Nur Metadaten für Schreibereignisse einschließen. Fügen Sie keine Dokumentfelder ein.

Name	Backend-Einstellung	Beschreibung
Protokoll-Differenzen	write_log_diffs	Wenn write_metadata_only false ist, schließen Sie nur die Unterschiede zwischen Schreibereignissen ein.
Ignorierte Benutzer	write_ignore_users	Geben Sie bestimmte Benutzer für Schreibereignisse nicht ein.
Angesehene Indizes	write_watched_indices	Geben Sie die Indizes oder Indexmuster an, die auf Schreibereignisse überwacht werden sollen. Durch das Hinzufügen überwachter Felder wird ein Protokoll pro Dokumentzugriff generiert, wodurch die Größe der Prüfungsprotokolle erheblich vergrößert wird.

Prüfungsprotokollbeispiel

Dieser Abschnitt enthält eine Beispielkonfiguration, eine Suchanforderung und das resultierende Prüfungsprotokoll für alle Lese- und Schreibereignisse eines Indexes.

Schritt 1: Konfigurieren von Prüfungsprotokollen

Nachdem Sie die Veröffentlichung von Audit-Logs in einer CloudWatch Logs-Gruppe aktiviert haben, navigieren Sie zur Seite „Audit-Protokollierung“ der OpenSearch Dashboards und wählen Sie Audit-Protokollierung aktivieren aus.

1. Wählen Sie unter Allgemeine Einstellungen Konfigurieren und stellen Sie sicher, dass die REST-Ebene aktiviert ist.
2. Wählen Sie in den Compliance-Einstellungen die Option Konfigurieren aus.
3. Fügen Sie unter Schreiben in Beobachtete Felder `accounts` für alle Schreibereignisse zu diesem Index hinzu.
4. Fügen Sie unter Lesen in Beobachtete Felder `ssn`- und `id`--Felder des `accounts`-Index hinzu:

```
{
  "accounts-": [
    "ssn",
    "id-"
  ]
```

```
}
```

Schritt 2: Ausführen von Lese- und Schreibereignissen

1. Navigieren Sie zu OpenSearch Dashboards, wählen Sie Dev Tools und indexieren Sie ein Beispieldokument:

   ```
   PUT accounts/_doc/0
   {
     "ssn": "123",
     "id-": "456"
   }
   ```

2. Um ein Leseereignis zu testen, senden Sie die folgende Anforderung:

   ```
   GET accounts/_search
   {
     "query": {
       "match_all": {}
     }
   }
   ```

Schritt 3: Beobachten der Protokolle

1. Öffnen Sie die CloudWatch Konsole unter. https://console.aws.amazon.com/cloudwatch/
2. Wählen Sie im Navigationsbereich Protokollgruppen aus.
3. Wählen Sie die Protokollgruppe aus, die Sie beim Aktivieren von Prüfungsprotokollen festgelegt haben. Innerhalb der Protokollgruppe erstellt OpenSearch Service einen Protokollstream für jeden Knoten in Ihrer Domain.
4. Wählen Sie unter Protokollströme die Option Alle durchsuchen aus.
5. Die Lese- und Schreibereignisse finden Sie in den entsprechenden Protokollen. Sie können eine Verzögerung von 5 Sekunden erwarten, bevor das Protokoll angezeigt wird.

   Beispiel für Schreibprüfungsprotokoll

   ```
   {
     "audit_compliance_operation": "CREATE",
     "audit_cluster_name": "824471164578:audit-test",
   ```

```
  "audit_node_name": "be217225a0b77c2bd76147d3ed3ff83c",
  "audit_category": "COMPLIANCE_DOC_WRITE",
  "audit_request_origin": "REST",
  "audit_compliance_doc_version": 1,
  "audit_node_id": "3xNJhm4XS_yTzEgDWcGRjA",
  "@timestamp": "2020-08-23T05:28:02.285+00:00",
  "audit_format_version": 4,
  "audit_request_remote_address": "3.236.145.227",
  "audit_trace_doc_id": "lxnJGXQBqZSlDB91r_uZ",
  "audit_request_effective_user": "admin",
  "audit_trace_shard_id": 8,
  "audit_trace_indices": [
    "accounts"
  ],
  "audit_trace_resolved_indices": [
    "accounts"
  ]
}
```


Beispiel für Leseprüfungsprotokoll


```
{
  "audit_cluster_name": "824471164578:audit-docs",
  "audit_node_name": "806f6050cb45437e2401b07534a1452f",
  "audit_category": "COMPLIANCE_DOC_READ",
  "audit_request_origin": "REST",
  "audit_node_id": "saSevm9ASte0-pjAtYi2UA",
  "@timestamp": "2020-08-31T17:57:05.015+00:00",
  "audit_format_version": 4,
  "audit_request_remote_address": "54.240.197.228",
  "audit_trace_doc_id": "config:7.7.0",
  "audit_request_effective_user": "admin",
  "audit_trace_shard_id": 0,
  "audit_trace_indices": [
    "accounts"
  ],
  "audit_trace_resolved_indices": [
    "accounts"
  ]
}
```

Um den Anfragetext einzubeziehen, kehren Sie zu den Compliance-Einstellungen in OpenSearch Dashboards zurück und deaktivieren Sie die Option Metadaten schreiben. Um Ereignisse eines bestimmten Benutzers auszuschließen, fügen Sie den Benutzer zu Ignorierte Benutzer hinzu.

Eine Beschreibung der einzelnen Prüfungsprotokoll-Felder finden Sie unter Referenz des Prüfungsprotokolls. Informationen zur Suche und Analyse Ihrer Audit-Protokolldaten finden Sie unter Analysieren von Protokolldaten mit CloudWatch Logs Insights im Amazon CloudWatch Logs-Benutzerhandbuch.

Konfigurieren von Prüfungsprotokollen mit der REST-API

Wir empfehlen die Verwendung von OpenSearch Dashboards zur Konfiguration von Audit-Logs, Sie können aber auch die detaillierte REST-API für die Zugriffskontrolle verwenden. Dieser Abschnitt enthält eine Beispielanforderung. Die vollständige Dokumentation zur REST-API ist in der Dokumentation verfügbar. OpenSearch

```
PUT _opendistro/_security/api/audit/config
{
  "enabled": true,
  "audit": {
    "enable_rest": true,
    "disabled_rest_categories": [
      "GRANTED_PRIVILEGES",
      "AUTHENTICATED"
    ],
    "enable_transport": true,
    "disabled_transport_categories": [
      "GRANTED_PRIVILEGES",
      "AUTHENTICATED"
    ],
    "resolve_bulk_requests": true,
    "log_request_body": true,
    "resolve_indices": true,
    "exclude_sensitive_headers": true,
    "ignore_users": [
      "kibanaserver"
    ],
    "ignore_requests": [
      "SearchRequest",
      "indices:data/read/*",
      "/_cluster/health"
    ]
```

```
  },
  "compliance": {
    "enabled": true,
    "internal_config": true,
    "external_config": false,
    "read_metadata_only": true,
    "read_watched_fields": {
      "read-index-1": [
        "field-1",
        "field-2"
      ],
      "read-index-2": [
        "field-3"
      ]
    },
    "read_ignore_users": [
      "read-ignore-1"
    ],
    "write_metadata_only": true,
    "write_log_diffs": false,
    "write_watched_indices": [
      "write-index-1",
      "write-index-2",
      "log-*",
      "*"
    ],
    "write_ignore_users": [
      "write-ignore-1"
    ]
  }
}
```

Überwachung von OpenSearch Service-Ereignissen mit Amazon EventBridge

Amazon OpenSearch Service ist in Amazon integriert EventBridge , um Sie über bestimmte, Ihre Domains betreffende Ereignisse zu informieren. Ereignisse von AWS -Services werden für EventBridge nahezu in Echtzeit bereitgestellt. Die gleichen Ereignisse werden auch an Amazon CloudWatch Events gesendet, dem Vorgänger von Amazon EventBridge. Sie können einfache Regeln schreiben, um anzugeben, welche Ereignisse für Sie interessant sind und welche automatisierten Aktionen durchgeführt werden sollen, wenn sich für ein Ereignis eine

Übereinstimmung mit einer Regel ergibt. Die folgenden Aktionen können beispielsweise automatisch ausgelöst werden:

- Aufrufen einer -Funktion AWS Lambda
- Aufrufen eines Amazon EC2 Run-Befehls
- Weiterleiten des Ereignisses an Amazon Kinesis Data Streams
- Aktivieren eines AWS -Step-Functions-Zustandsautomaten
- Benachrichtigen eines Amazon SNS-Themas oder einer Amazon SQS-Warteschlange

Weitere Informationen finden Sie unter Erste Schritte mit Amazon EventBridge im EventBridge Amazon-Benutzerhandbuch.

Themen

- Aktualisieren der Software
- Automatische Optimierung von Ereignissen
- Ereignisse zum Cluster-Zustand
- VPC-Endpunktereignisse
- Ausmusterung von Knoten
- Ereignisse, bei denen der Knoten heruntergefahren ist
- Ereignisse für Domain-Fehler
- Tutorial: Überwachung von Amazon OpenSearch EventBridge Service-Ereignissen
- Tutorial: Senden von Amazon-SNS-Warnungen für verfügbare Softwareupdates

Aktualisieren der Software

OpenSearch Service sendet Ereignisse, EventBridge wenn eines der folgenden Service-Software-Update -Ereignisse auftritt.

Service-Software-Update verfügbar

OpenSearch Service sendet dieses Ereignis, wenn ein Service-Software-Update verfügbar ist.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Available",
    "severity": "Informational",
    "description": "Service software update R20220928 available. Service Software
 Deployment Mechanism:
                   Blue/Green. For more information on deployment configuration,
 please
                   see: https://docs.aws.amazon.com/opensearch-service/latest/
developerguide/managedomains-configuration-changes.html"
  }
}
```

Service-Softwareaktualisierung geplant

OpenSearch Service sendet dieses Ereignis, wenn ein Service-Software-Update geplant wurde. Bei optionalen Updates erhalten Sie die Benachrichtigung am geplanten Datum und können den Termin jederzeit verschieben. Bei erforderlichen Aktualisierungen erhalten Sie die Benachrichtigung drei Tage vor dem geplanten Datum, und Sie haben die Möglichkeit, den Termin innerhalb des obligatorischen Zeitfensters zu verschieben.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
```

```
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Scheduled",
    "severity": "High",
    "description": "A new service software update [R20200330-p1] has been scheduled at
 [21st May 2023 12:40 GMT].
                    Please see documentation for more information on scheduling
 software updates:
                    https://docs.aws.amazon.com/opensearch-service/latest/
developerguide/service-software.html."
  }
}
```

Service-Softwareaktualisierung verschoben

OpenSearch Service sendet dieses Ereignis, wenn ein optionales Service-Software-Update verschoben wurde. Weitere Informationen finden Sie unter the section called “Optionale und erforderliche Updates”.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Rescheduled",
    "severity": "High",
    "description": "The service software update [R20200330-p1], which was originally
 scheduled for
                    [21st May 2023 12:40 GMT], has been rescheduled to [23rd May 2023
 12:40 GMT].
                    Please see documentation for more information on scheduling
 software updates:
```

```
                    https://docs.aws.amazon.com/opensearch-service/latest/
developerguide/service-software.html."
  }
}
```

Service-Software-Update gestartet

OpenSearch Service sendet dieses Ereignis, wenn ein Service-Software-Update gestartet wurde.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Started",
    "severity": "Informational",
    "description": "Service software update [R20200330-p1] started.
  }
}
```

Service-Software-Update abgeschlossen

OpenSearch Service sendet dieses Ereignis, wenn ein Service-Software-Update abgeschlossen ist.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
```

```
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Completed",
    "severity": "Informational",
    "description": "Service software update [R20200330-p1] completed."
  }
}
```

Service-Software-Update abgebrochen

OpenSearch Service sendet dieses Ereignis, wenn ein Service-Software-Update abgebrochen wurde.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Cancelled",
    "severity": "Informational",
    "description": "The scheduled service software update [R20200330-p1] has been
 cancelled as a
                   newer update is available. Please schedule the latest update."
  }
}
```

Geplantes Service-Software-Update abgebrochen

OpenSearch Service sendet dieses Ereignis, wenn ein Service-Software-Update, das zuvor für die Domain geplant war, abgesagt wurde.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Cancelled",
    "severity": "Informational",
    "description": "The scheduled service software update [R20200330-p1] has been
 cancelled."
  }
}
```

Service-Softwareaktualisierung wurde nicht ausgeführt

OpenSearch Service sendet dieses Ereignis, wenn er ein Service-Software-Update nicht initiieren kann.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Unexecuted",
```

```
    "severity": "Informational",
    "description": "The scheduled service software update [R20200330-p1] cannot be
 started. Reason: [reason]"
  }
}
```

Service-Software-Update fehlgeschlagen

OpenSearch Service sendet dieses Ereignis, wenn ein Service-Software-Update fehlgeschlagen ist.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Failed",
    "severity": "High",
    "description": "Installation of service software update [R20200330-p1] failed.
 [reason].
  }
}
```

Aktualisierung der Servicesoftware erforderlich

OpenSearch Service sendet dieses Ereignis, wenn ein Service-Software-Update erforderlich ist. Weitere Informationen finden Sie unter the section called “Optionale und erforderliche Updates”.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
```

```
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Required",
    "severity": "High",
    "description": "Service software update [R20200330-p1] available. Update
                    will be automatically installed after [21st May 2023] if no
                    action is taken. Service Software Deployment Mechanism: Blue/Green.
                    For more information on deployment configuration, please see:
                    https://docs.aws.amazon.com/opensearch-service/latest/
developerguide/managedomains-configuration-changes.html"
  }
}
```

Automatische Optimierung von Ereignissen

OpenSearch Service sendet Ereignisse an, EventBridge wenn eines der folgenden automatische Optimierungs -Ereignisse auftritt.

Automatische Optimierung ausstehend

OpenSearch Service sendet dieses Ereignis, wenn die automatische Optimierung Empfehlungen für eine verbesserte Clusterleistung und -verfügbarkeit identifiziert hat. Dieses Ereignis wird nur für Domains angezeigt, bei denen die automatische Optimierung deaktiviert ist.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version": "0",
  "id": "3acb26c8-397c-4c89-a80a-ce672a864c55",
  "detail-type": "Amazon OpenSearch Service Auto-Tune Notification",
  "source": "aws.es",
  "account": "123456789012",
```

```
  "time": "2020-10-30T22:06:31Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Auto-Tune Event",
    "severity": "Informational",
    "status": "Pending",
    "description": "Auto-Tune recommends the following new settings for your
 domain: { JVM Heap size : 60%}. Enable Auto-Tune to improve cluster stability and
 performance.",
    "scheduleTime": "{iso8601-timestamp}"
  }
}
```

Automatische Optimierung gestartet

OpenSearch Service sendet dieses Ereignis, wenn die automatische Optimierung beginnt, neue Einstellungen auf Ihre Domain anzuwenden.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version": "0",
  "id": "3acb26c8-397c-4c89-a80a-ce672a864c55",
  "detail-type": "Amazon OpenSearch Service Auto-Tune Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2020-10-30T22:06:31Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Auto-Tune Event",
    "severity": "Informational",
    "status": "Started",
    "scheduleTime": "{iso8601-timestamp}",
    "startTime": "{iso8601-timestamp}",
    "description" : "Auto-Tune is applying the following settings to your domain: { JVM
 Heap size : 60%}."
  }
}
```

Die automatische Optimierung erfordert eine geplante blau/grüne Bereitstellung

OpenSearch Service sendet dieses Ereignis, wenn die automatische Optimierung Empfehlungen identifiziert hat, die eine geplante blau/grüne Bereitstellung erfordern.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version": "0",
  "id": "3acb26c8-397c-4c89-a80a-ce672a864c55",
  "detail-type": "Amazon OpenSearch Service Auto-Tune Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2020-10-30T22:06:31Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Auto-Tune Event",
    "severity": "Low",
    "status": "Pending",
    "startTime": "{iso8601-timestamp}",
    "description": "Auto-Tune has identified the following settings for your domain
 that require a blue/green deployment: { JVM Heap size : 60%}.
                    You can schedule the deployment for your preferred time."
  }
}
```

Automatische Optimierung abgebrochen

OpenSearch Service sendet dieses Ereignis, wenn der automatische Optimierungszeitplan abgebrochen wurde, da keine ausstehenden Optimierungsempfehlungen vorliegen.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version": "0",
  "id": "3acb26c8-397c-4c89-a80a-ce672a864c55",
```

```
  "detail-type": "Amazon OpenSearch Service Auto-Tune Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2020-10-30T22:06:31Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Auto-Tune Event",
    "severity": "Low",
    "status": "Cancelled",
    "scheduleTime": "{iso8601-timestamp}",
    "description": "Auto-Tune has cancelled the upcoming blue/green deployment."
  }
}
```

Automatische Optimierung abgeschlossen

OpenSearch Service sendet dieses Ereignis, wenn automatische Optimierung die blau/grüne Bereitstellung abgeschlossen hat und der Cluster mit neuen JVM-Einstellungen betriebsbereit ist.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version": "0",
  "id": "3acb26c8-397c-4c89-a80a-ce672a864c55",
  "detail-type": "Amazon OpenSearch Service Auto-Tune Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2020-10-30T22:06:31Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Auto-Tune Event",
    "severity": "Informational",
    "status": "Completed",
    "completionTime": "{iso8601-timestamp}",
    "description": "Auto-Tune has completed the blue/green deployment and successfully
 applied the following settings: { JVM Heap size : 60%}."
  }
}
```

Automatische Optimierung deaktiviert und Änderungen zurückgesetzt

OpenSearch Service sendet dieses Ereignis, wenn automatische Optimierung deaktiviert wurde und die angewendeten Änderungen zurückgesetzt wurden.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version": "0",
  "id": "3acb26c8-397c-4c89-a80a-ce672a864c55",
  "detail-type": "Amazon OpenSearch Service Auto-Tune Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2020-10-30T22:06:31Z",
  "region": "us-east-1",
  "resources": [ "arn:aws:es:us-east-1:123456789012:domain/test-domain" ],
  "detail": {
    "event": "Auto-Tune Event",
    "severity": "Informational",
    "status": "Completed",
    "description": "Auto-Tune is now disabled. All settings have been reverted. Auto-
Tune will continue to evaluate
                    cluster performance and provide recommendations.",
    "completionTime": "{iso8601-timestamp}"
  }
}
```

Automatische Optimierung deaktiviert und Änderungen beibehalten

OpenSearch Service sendet dieses Ereignis, wenn automatische Optimierung deaktiviert wurde und die angewendeten Änderungen beibehalten wurden.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version": "0",
  "id": "3acb26c8-397c-4c89-a80a-ce672a864c55",
  "detail-type": "Amazon OpenSearch Service Auto-Tune Notification",
  "source": "aws.es",
```

```
  "account": "123456789012",
  "time": "2020-10-30T22:06:31Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Auto-Tune Event",
    "severity": "Informational",
    "status": "Completed",
    "description": "Auto-Tune is now disabled. The most-recent settings by Auto-Tune
 have been retained.
                    Auto-Tune will continue to evaluate cluster performance and provide
 recommendations.",
    "completionTime": "{iso8601-timestamp}"
  }
}
```

Ereignisse zum Cluster-Zustand

OpenSearch Service sendet bestimmte Ereignisse an, EventBridge wenn die Integrität Ihres Clusters beeinträchtigt ist.

Wiederherstellung roter Cluster gestartet

OpenSearch Service sendet dieses Ereignis, nachdem Ihr Clusterstatus länger als eine Stunde lang kontinuierlich rot ist. Es versucht, einen oder mehrere rote Indizes aus einem Snapshot automatisch wiederherzustellen, um den Clusterstatus zu beheben.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
   "version":"0",
   "id":"01234567-0123-0123-0123-012345678901",
   "detail-type":"Amazon OpenSearch Service Cluster Status Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2016-11-01T13:12:22Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-domain"
   ],
   "detail":{
```

```
      "event":"Automatic Snapshot Restore for Red Indices",
      "status":"Started",
      "severity":"High",
      "description":"Your cluster status is red. We have started automatic snapshot
 restore for the red indices.
                    No action is needed from your side. Red indices [red-index-0, red-
index-1]"
   }
}
```

Wiederherstellung des roten Clusters teilweise abgeschlossen

OpenSearch Service sendet dieses Ereignis, wenn er nur in der Lage war, eine Teilmenge roter Indizes aus einem Snapshot wiederherzustellen, während er versuchte, einen roten Clusterstatus zu beheben.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
   "version":"0",
   "id":"01234567-0123-0123-0123-012345678901",
   "detail-type":"Amazon OpenSearch Service Cluster Status Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2016-11-01T13:12:22Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-domain"
   ],
   "detail":{
      "event":"Automatic Snapshot Restore for Red Indices",
      "status":"Partially Restored",
      "severity":"High",
      "description":"Your cluster status is red. We were able to restore the following
 Red indices from
                   snapshot: [red-index-0]. Indices not restored: [red-index-1].
 Please refer https://docs.aws.amazon.com/opensearch-service/latest/developerguide/
handling-errors.html#handling-errors-red-cluster-status for troubleshooting steps."
   }
}
```

Wiederherstellung roter Cluster fehlgeschlagen

OpenSearch Service sendet dieses Ereignis, wenn er nicht in der Lage war, rote Indizes wiederherzustellen, während er versuchte, einen roten Clusterstatus zu beheben.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
   "version":"0",
   "id":"01234567-0123-0123-0123-012345678901",
   "detail-type":"Amazon OpenSearch Service Cluster Status Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2016-11-01T13:12:22Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-domain"
   ],
   "detail":{
      "event":"Automatic Snapshot Restore for Red Indices",
      "status":"Failed",
      "severity":"High",
      "description":"Your cluster status is red. We were unable to restore the Red
 indices automatically.
                    Indices not restored: [red-index-0, red-index-1]. Please refer
 https://docs.aws.amazon.com/opensearch-service/latest/developerguide/handling-
errors.html#handling-errors-red-cluster-status for troubleshooting steps."
   }
}
```

Zu löschende Shards

OpenSearch Service sendet dieses Ereignis, wenn er versucht hat, Ihren roten Clusterstatus automatisch zu beheben, nachdem er 14 Tage lang kontinuierlich rot war, aber ein oder mehrere Indizes rot bleiben. Nach 7 weiteren Tagen (insgesamt 21 Tage nach kontinuierlichem Rot) fährt der OpenSearch Service mit dem Löschen nicht zugewiesene Shards auf allen roten Indizes fort.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
   "version":"0",
   "id":"01234567-0123-0123-0123-012345678901",
   "detail-type":"Amazon OpenSearch Service Cluster Status Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2022-04-09T10:36:48Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-domain"
   ],
   "detail":{
      "severity":"Medium",
      "description":"Your cluster status is red. Please fix the red indices as soon as
 possible.
                    If not fixed by 2022-04-12 01:51:47+00:00, we will delete all
 unassigned shards,
                    the unit of storage and compute, for these red indices to recover
 your domain and make it green.
                    Please refer to https://docs.aws.amazon.com/opensearch-service/
latest/developerguide/handling-errors.html#handling-errors-red-cluster-status for
 troubleshooting steps.
                    test_data, test_data1",
      "event":"Automatic Snapshot Restore for Red Indices",
      "status":"Shard(s) to be deleted"
   }
}
```

Shards gelöscht

OpenSearch Service sendet dieses Ereignis, nachdem Ihr Clusterstatus länger als 21 Tage lang kontinuierlich rot ist. Er löscht die nicht zugewiesenen Shards (Speicher und Berechnung) auf allen roten Indizes. Details hierzu finden Sie unter the section called “Automatische Behebung von roten Clustern”.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
   "version":"0",
   "id":"01234567-0123-0123-0123-012345678901",
   "detail-type":"Amazon OpenSearch Service Cluster Status Notification",
```

```
   "source":"aws.es",
   "account":"123456789012",
   "time":"2022-04-09T10:54:48Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-domain"
   ],
   "detail":{
      "severity":"High",
      "description":"We have deleted unassinged shards, the unit of storage and
 compute, in
                    red indices: index-1, index-2 because these indices were red for
 more than
                    21 days and could not be restored with the automated restore
 process.
                    Please refer to https://docs.aws.amazon.com/opensearch-service/
latest/developerguide/handling-errors.html#handling-errors-red-cluster-status for
 troubleshooting steps.",
      "event":"Automatic Snapshot Restore for Red Indices",
      "status":"Shard(s) deleted"
   }
}
```

Warnung mit hoher Shard-Anzahl

OpenSearch Service sendet dieses Ereignis, wenn die durchschnittliche Shard-Anzahl auf Ihren aktiven Datenknoten 90% des empfohlenen Standardlimits von 1.000 Shards überschritten hat. Obwohl neuere Versionen von Elasticsearch eine konfigurierbare maximale Shard-Anzahl pro Knoten OpenSearch unterstützen, empfehlen wir Ihnen nicht mehr als 1.000 Shards pro Knoten. Siehe Auswahl der Anzahl der Shards

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2016-11-01T13:12:22Z",
  "region":"us-east-1",
```

```
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"High Shard Count",
     "status":"Warning",
     "severity":"Low",
     "description":"One or more data nodes have close to 1000 shards. To ensure optimum
 performance and stability of your
                   cluster, please refer to the best practice guidelines - https://
docs.aws.amazon.com/opensearch-service/latest/developerguide/sizing-domains.html#bp-
sharding."
  }
}
```

Limit für Shard-Anzahl überschritten

OpenSearch Service sendet dieses Ereignis, wenn die durchschnittliche Shard-Anzahl auf Ihren aktiven Datenknoten das empfohlene Standardlimit von 1.000 Shards überschritten hat. Obwohl neuere Versionen von Elasticsearch eine konfigurierbare maximale Shard-Anzahl pro Knoten OpenSearch unterstützen, empfehlen wir Ihnen nicht mehr als 1.000 Shards pro Knoten. Siehe Auswahl der Anzahl der Shards

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2016-11-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"High Shard Count",
     "status":"Warning",
     "severity":"Medium",
     "description":"One or more data nodes have more than 1000 shards. To ensure
 optimum performance and stability of your
                   cluster, please refer to the best practice guidelines - https://
docs.aws.amazon.com/opensearch-service/latest/developerguide/sizing-domains.html#bp-
sharding."
```

```
  }
}
```

Geringer Speicherplatz

OpenSearch Service sendet dieses Ereignis, wenn ein oder mehrere Knoten in Ihrem Cluster weniger als 25% des verfügbaren Speicherplatzes oder weniger als 25 GB aufweisen.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2017-12-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"Low Disk Space",
     "status":"Warning",
     "severity":"Medium",
     "description":"One or more data nodes in your cluster has less than 25% of storage
 space or less than 25GB.
                  Your cluster will be blocked for writes at 20% or 20GB. Please refer
 to the documentation for more information - https://docs.aws.amazon.com/opensearch-
service/latest/developerguide/handling-errors.html#troubleshooting-cluster-block"
  }
}
```

Geringer Speicherplatz

OpenSearch Service sendet dieses Ereignis, wenn alle Knoten in Ihrem Cluster weniger als 10% des verfügbaren Speicherplatzes oder weniger als 10 GB aufweisen. Wenn alle Knoten das Wasserzeichen für den niedrigen Festplattenwert überschreiten, führt jeder neue Index zu einem gelben Cluster, und wenn alle Knoten das Wasserzeichen für die hohe Festplatte unterschreiten, führt dies zu einem roten Cluster.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2017-12-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"Low Disk Watermark Breach",
     "status":"Warning",
     "severity":"Medium",
     "description":"Low Disk Watermark threshold is about to be breached. Once the
 threshold is breached, new index creation will be blocked on all
                   nodes to prevent the cluster status from turning red. Please
 increase disk size to suit your storage needs. For more information,
                   see https://docs.aws.amazon.com/opensearch-service/latest/
developerguide/handling-errors.html#troubleshooting-cluster-block".
  }
}
```

EBS-Burst-Balance unter 70 %

OpenSearch Service sendet dieses Ereignis, wenn die EBS-Balance auf einem oder mehreren Datenknoten unter 70% fällt. Eine Erschöpfung der EBS-Burst-Balance kann zu einer weit verbreiteten Nichtverfügbarkeit des Clusters und zur Drosselung von E/A-Anfragen führen, was hohe Latenzzeiten und Timeouts bei Indizierungs- und Suchanfragen zur Folge haben kann. Schritte zur Behebung dieses Problems finden Sie unter the section called “Niedrige EBS-Burst-Balance”.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
```

```
  "time":"2017-12-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"EBS Burst Balance",
     "status":"Warning",
     "severity":"Medium",
     "description":"EBS burst balance on one or more data nodes is below 70%.
                    Follow https://docs.aws.amazon.com/opensearch-service/latest/
developerguide/handling-errors.html#handling-errors-low-ebs-burst
                    to fix this issue."
  }
}
```

EBS-Burst-Balance unter 20 %

OpenSearch Service sendet dieses Ereignis, wenn die EBS-Balance auf einem oder mehreren Datenknoten unter 20% fällt. Eine Erschöpfung der EBS-Burst-Balance kann zu einer weit verbreiteten Nichtverfügbarkeit des Clusters und zur Drosselung von E/A-Anfragen führen, was hohe Latenzzeiten und Timeouts bei Indizierungs- und Suchanfragen zur Folge haben kann. Schritte zur Behebung dieses Problems finden Sie unter the section called “Niedrige EBS-Burst-Balance”.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2017-12-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"EBS Burst Balance",
     "status":"Warning",
     "severity":"High",
     "description":"EBS burst balance on one or more data nodes is below 20%.
                    Follow https://docs.aws.amazon.com/opensearch-service/latest/
developerguide/handling-errors.html#handling-errors-low-ebs-burst
                    to fix this issue.
```

```
  }
}
```

Drosselung des Festplattendurchsatzes

OpenSearch Service sendet dieses Ereignis, wenn Lese- und Schreibanforderungen an Ihre Domain aufgrund der Durchsatzbeschränkungen Ihrer EBS-Volumes oder -Instance gedrosselt werden. EC2 Wenn Sie diese Benachrichtigung erhalten, sollten Sie eine Hochskalierung Ihrer Volumes oder Instances gemäß den AWS -empfohlenen bewährten Methoden in Erwägung ziehen. Wenn Ihr Datenträgertyp istgp2, erhöhen Sie die Volumegröße. Wenn Ihr Datenträgertyp istgp3, sorgen Sie für mehr Durchsatz. Sie können auch überprüfen, ob Ihre Instance-Basis und der maximale EBS-Durchsatz größer oder gleich dem bereitgestellten Volumendurchsatz sind, und können entsprechend skalieren.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2017-12-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"Disk Throughput Throttle",
     "status":"Warning",
     "severity":"Medium",
     "description":"Your domain is experiencing throttling due to instance or volume
 throughput limitations.
                    Please consider scaling your domain to suit your throughput needs.
 In July 2023, we improved
                    the accuracy of throughput throttle calculation by replacing ‘Max
 volume throughput’ with
                    ‘Provisioned volume throughput’. Please refer to the documentation
 for more information."
   }
}
```

Große Shard-Größe

OpenSearch Service sendet dieses Ereignis, wenn ein oder mehrere Shards in Ihrem Cluster entweder 50 GiB oder 65 GiB überschritten haben. Um eine optimale Leistung und Stabilität des Clusters zu gewährleisten, sollten Sie die Shard-Größe reduzieren.

Weitere Informationen finden Sie unter Bewährte Methoden für Sharding.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2017-12-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"Large Shard Size",
     "status":"Warning",
     "severity":"Medium",
     "description":"One or more shards are larger than 65GiB. To ensure optimum cluster
 performance and stability, reduce shard sizes.
                   For more information, see https://docs.aws.amazon.com/opensearch-
service/latest/developerguide/monitoring-events.html#monitoring-events-large-shard-
size."
  }
}
```

Hohe JVM-Nutzung

OpenSearch Der Service sendet dieses Ereignis, wenn die `JVMMemoryPressure` Metrik für Ihre Domain 80% überschritten hat. Wenn der Wert 30 Minuten lang 92% überschreitet, werden alle Schreibvorgänge in Ihrem Cluster blockiert. Um eine optimale Clusterstabilität zu gewährleisten, reduzieren Sie den Datenverkehr zum Cluster oder skalieren Sie Ihre Domain, um ausreichend Arbeitsspeicher für Ihre Arbeitslast bereitzustellen.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2017-12-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"High JVM Usage",
     "status":"Warning",
     "severity":"High",
     "description":"JVM memory pressure has exceeded 80%. If it exceeds 92% for 30
 minutes, all write operations to your cluster
                   will be blocked. To ensure optimum cluster stability, reduce
 traffic to the cluster or use larger instance types.
                   For more information, see https://docs.aws.amazon.com/opensearch-
service/latest/developerguide/monitoring-events.html#monitoring-events-high-jvm."
  }
}
```

Unzureichende GC

OpenSearch Der Dienst sendet dieses Ereignis, wenn der maximale JVM-Wert über 70% liegt und der Unterschied zwischen dem Maximum und dem Minimum weniger als 30% beträgt. Dies kann darauf hindeuten, dass die JVM während der Garbage-Collection-Zyklen nicht in der Lage ist, ausreichend Speicher für Ihre Arbeitslast zurückzugewinnen. Dies kann zu immer langsameren Reaktionen und höheren Latenzen führen. In einigen Fällen kann es sogar zu Knotenausfällen aufgrund von Integritätsprüfungen kommen, bei denen das Timeout abgelaufen ist. Um eine optimale Clusterstabilität zu gewährleisten, reduzieren Sie den Datenverkehr zum Cluster oder skalieren Sie Ihre Domain so, dass ausreichend Arbeitsspeicher für Ihre Arbeitslast zur Verfügung steht.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version":"0",
```

```
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2017-12-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"Insufficient GC",
     "status":"Warning",
     "severity":"Medium",
     "description":"Maximum JVM is above 70% and JVM range is less than 30%. This may
 indicate insufficient garbage collection for your workload.
                   For more information, see https://docs.aws.amazon.com/opensearch-
service/latest/developerguide/monitoring-events.html#monitoring-events-insufficient-
gc."
  }
}
```

Warnung beim benutzerdefinierten Index-Routing

OpenSearch Der Dienst sendet dieses Ereignis, wenn sich Ihre Domain im Verarbeitungsstatus befindet und Indizes mit benutzerdefinierten index.routing.allocation-Einstellungen enthält, was dazu führen kann, dass blaugrüne Bereitstellungen hängen bleiben. Stellen Sie sicher, dass die Einstellungen ordnungsgemäß angewendet wurden.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2017-12-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"Custom Index Routing Warning",
     "status":"Warning",
     "severity":"Medium",
```

```
     "description":"Your domain is in processing state and contains indice(s) with
 custom index.routing.allocation
                    settings which can cause blue-green deployments to get stuck.
 Verify settings are applied properly.
                    For more information, see https://docs.aws.amazon.com/opensearch-
service/latest/developerguide/monitoring-events.html#monitoring-events-index-routing."
  }
}
```

Fehlgeschlagene Shard-Sperre fehlgeschlagen

OpenSearch Der Service sendet dieses Ereignis, wenn Ihre Domain aufgrund nicht zugewiesener Shards mit defekt ist. `[ShardLockObtainFailedException]` Weitere Informationen finden Sie unter Wie behebe ich die In-Memory-Shard-Sperrausnahme in Amazon OpenSearch Service?

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2017-12-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"Failed Shard Lock",
     "status":"Warning",
     "severity":"Medium",
     "description":"Your domain is unhealthy due to unassigned shards with
 [ShardLockObtainFailedException]. For more information,
                    see https://docs.aws.amazon.com/opensearch-service/latest/
developerguide/monitoring-events.html#monitoring-events-failed-shard-lock."
}
```

VPC-Endpunktereignisse

OpenSearch Service sendet bestimmte Ereignisse an EventBridge AWS PrivateLink -Schnittstellen-Endpunkte.

Erstellung eines VPC-Endpunkts fehlgeschlagen

OpenSearch Service sendet dieses Ereignis, wenn es einen angeforderten VPC-Endpunkt nicht erstellen kann. Dieser Fehler kann auftreten, weil Sie das Limit für die Anzahl der in einer Region zulässigen VPC-Endpunkte erreicht haben. Dieser Fehler wird auch angezeigt, wenn ein bestimmtes Subnetz oder eine Sicherheitsgruppe nicht vorhanden ist.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
   "version":"0",
   "id":"01234567-0123-0123-0123-012345678901",
   "detail-type":"Amazon OpenSearch Service VPC Endpoint Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2016-11-01T13:12:22Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-domain"
   ],
   "detail":{
      "event":"VPC Endpoint Create Validation",
      "status":"Failed",
      "severity":"High",
      "description":"Unable to create VPC endpoint aos-0d4c74c0342343 for domain
                     arn:aws:es:eu-south-1:123456789012:domain/my-domain due to the
 following validation failures: You've reached the limit on the
                     number of VPC endpoints that you can create in the AWS Region."
   }
}
```

VPC-Endpunkt-Update fehlgeschlagen

OpenSearch Service sendet dieses Ereignis, wenn es einen angeforderten VPC-Endpunkt nicht löschen kann.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
   "version":"0",
   "id":"01234567-0123-0123-0123-012345678901",
   "detail-type":"Amazon OpenSearch Service VPC Endpoint Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2016-11-01T13:12:22Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-domain"
   ],
   "detail":{
      "event":"VPC Endpoint Update Validation",
      "status":"Failed",
      "severity":"High",
      "description":"Unable to update VPC endpoint aos-0d4c74c0342343 for domain
                     arn:aws:es:eu-south-1:123456789012:domain/my-domain due to the
 following validation failures: <failure message>."
    }
}
```

Löschen des VPC-Endpunkts fehlgeschlagen

OpenSearch Service sendet dieses Ereignis, wenn es einen angeforderten VPC-Endpunkt nicht löschen kann.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
   "version":"0",
   "id":"01234567-0123-0123-0123-012345678901",
   "detail-type":"Amazon OpenSearch Service VPC Endpoint Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2016-11-01T13:12:22Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-domain"
   ],
   "detail":{
      "event":"VPC Endpoint Delete Validation",
```

```
      "status":"Failed",
      "severity":"High",
      "description":"Unable to delete VPC endpoint aos-0d4c74c0342343 for domain
                  arn:aws:es:eu-south-1:123456789012:domain/my-domain due to the
 following validation failures: Specified subnet doesn't exist."
   }
}
```

Ausmusterung von Knoten

OpenSearch Service sendet Ereignisse an, EventBridge wenn eines der folgenden Ausmusterung eines Knotens auftritt.

Ausmusterung von Knoten geplant

OpenSearch Service sendet dieses Ereignis, wenn ein Ausmusterung eines Knotens geplant wurde.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2023-04-07T10:07:33Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Node Retirement Notification",
    "status": "Scheduled",
    "severity": "Medium",
    "description": "An automated action to retire and replace a node has been scheduled
 on your domain.
                  The node will be replaced in the next off-peak window. For more
 information, see
                  https://docs.aws.amazon.com/opensearch-service/latest/
developerguide/monitoring-events.html."
  }
}
```

Node-Außerbetriebnahme abgeschlossen

OpenSearch Service sendet dieses Ereignis, wenn ein Knoten abgeschlossen ist.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2023-04-07T10:07:33Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Node Retirement Notification",
    "status": "Completed",
    "severity": "Medium",
    "description": "The node has been retired and replaced with a new node."
  }
}
```

Ausmusterung eines Nodes

OpenSearch Service sendet dieses Ereignis, wenn ein Ausmusterung eines Knotens fehlgeschlagen ist.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2023-04-07T10:07:33Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
```

```
  "detail": {
    "event": "Node Retirement Notification",
    "status": "Failed",
    "severity": "Medium",
    "description": "Node retirement failed. No actions are required from your end. We
 will automatically
                    retry replacing the node."
  }
}
```

Ereignisse, bei denen der Knoten heruntergefahren ist

OpenSearch Der Dienst sendet diese Ereignisse, wenn aufgrund einer heruntergekommenen Hardware auf einem Knoten ein Austausch eines Knotens erforderlich ist.

Benachrichtigung über die Außerbetriebnahme eines heruntergekommenen

OpenSearch Der Service sendet dieses Ereignis, wenn die automatische Aktion zur Außerbetriebnahme und zum Austausch eines heruntergekommenen Knotens für Ihre Domain geplant wurde.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
   "version":"0",
   "id":"db233454-aad1-7676-3b15-10a84b052baa",
   "detail-type":"Amazon OpenSearch Service Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2024-01-11T08:16:06Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-node-replacement"
   ],
   "detail":{
      "severity":"Medium",
      "description":"An automated action to retire and replace a node has
 been scheduled on your domain. For more information, please see https://
docs.aws.amazon.com/opensearch-service/latest/developerguide/monitoring-events.html.",
      "event":"Degraded Node Retirement Notification",
```

```
      "status":"Scheduled"
   }
}
```

Außerbetriebnahme eines heruntergestuften Knotens abgeschlossen

OpenSearch Der Dienst sendet dieses Ereignis, wenn ein heruntergestufter Knoten ausgemustert und durch einen neuen Knoten ersetzt wurde.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
   "version":"0",
   "id":"7444215c-90f9-a52d-bcda-e85973a9a762",
   "detail-type":"Amazon OpenSearch Service Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2024-01-11T10:20:30Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-node-replacement"
   ],
   "detail":{
      "severity":"Medium",
      "description":"The node has been retired and replaced with a new node.",
      "event":"Degraded Node Retirement Notification",
      "status":"Completed"
   }
}
```

Die Außerbetriebnahme eines heruntergestuften Knotens

OpenSearch Der Dienst sendet dieses Ereignis, wenn die Außerbetriebnahme des heruntergestuften Knotens fehlgeschlagen ist.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
```

```
   "version":"0",
   "id":"c328e9bb-93b9-c0b2-b17a-df527fdf96b6",
   "detail-type":"Amazon OpenSearch Service Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2024-01-11T08:31:38Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-node-replacement"
   ],
   "detail":{
      "severity":"Medium",
      "description":"Node retirement failed. No actions are required from your end. We
 will automatically re-try replacing the node.",
      "event":"Degraded Node Retirement Notification",
      "status":"Failed"
   }
}
```

Ereignisse für Domain-Fehler

OpenSearch Service sendet Ereignisse an, EventBridge wenn einer der folgenden Domäne-Fehler auftritt.

Fehler bei Validierung von Domain-Updates

OpenSearch Service sendet dieses Ereignis, wenn ein oder mehrere Validierungsfehler auftreten, wenn versucht wird, eine Domain zu aktualisieren oder eine Konfigurationsänderung durchzuführen. Wie Sie diese Fehler beheben erfahren Sie unter the section called “Beheben von Validierungsfehlern”.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
   "version":"0",
   "id":"01234567-0123-0123-0123-012345678901",
   "detail-type":"Amazon OpenSearch Service Domain Update Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2016-11-01T13:12:22Z",
```

```
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-domain"
   ],
   "detail":{
      "event":"Domain Update Validation",
      "status":"Failed",
      "severity":"High",
      "description":"Unable to perform updates to your domain due to the following
 validation failures: <failures>
                    Please see the documentation for more information https://
docs.aws.amazon.com/opensearch-service/latest/developerguide/managedomains-
configuration-changes.html#validation"
   }
}
```

KMS-Schlüssel unzugänglich

OpenSearch Service sendet dieses Ereignis, wenn er nicht auf Ihre AWS KMS -Schlüssel zugreifen kann.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Domain Error Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2016-11-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"KMS Key Inaccessible",
     "status":"Error",
     "severity":"High",
     "description":"The KMS key associated with this domain is inaccessible. You are at
 risk of losing access to your domain.
                    For more information, please refer to https://docs.aws.amazon.com/
opensearch-service/latest/developerguide/encryption-at-rest.html#disabled-key."
  }
```

```
}
```

Domäne-Isolierung

OpenSearch Der Dienst sendet dieses Ereignis, wenn Ihre Domain isoliert ist und keine Anfragen empfangen, lesen oder schreiben kann, weil sie für das Netzwerk nicht erreichbar ist.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2023-11-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"Domain Isolation Notification",
     "status":"Error",
     "severity":"High",
     "description":"Your OpenSearch Service domain has been isolated. An isolated
 domain is unreachable by network and cannot receive, read, or write requests. For more
 information and assistance, please contact AWS Support at https://docs.aws.amazon.com/
opensearch-service/latest/developerguide/encryption-at-rest.html#disabled-key."
  }
}
```

Tutorial: Überwachung von Amazon OpenSearch EventBridge Service-Ereignissen

In diesem Tutorial richten Sie eine einfache AWS Lambda -Funktion ein, die OpenSearch Amazon-Service-Aufgabenereignisse überwacht und sie in einen CloudWatch Logs-Protokoll-Stream schreibt.

Voraussetzungen

Dieses Tutorial setzt voraus, dass Sie über eine vorhandene OpenSearch Service-Domäne verfügen. Wenn Sie noch keine Domain erstellt haben, führen Sie die Schritte unter Erstellen und Verwalten von Domains aus, um eine zu erstellen.

Schritt 1: Erstellen der Lambda-Funktion

In diesem Verfahren erstellen Sie eine einfache Lambda-Funktion, die als Ziel für OpenSearch Service-Ereignis-Nachrichten dient.

So erstellen Sie eine Lambda-Zielfunktion

1. Öffnen Sie die AWS Lambda Konsole unter. https://console.aws.amazon.com/lambda/
2. Wählen Sie Eine Funktion erstellen und Von Grund auf neu erstellen aus.
3. Geben Sie für Funktionsname den Event-Handler an.
4. Wählen Sie für Runtime (Laufzeit) die Option Python 3.8 aus.
5. Wählen Sie Funktion erstellen.
6. Bearbeiten Sie im Bereich Function code den Beispiel-Code entsprechend dem folgenden Beispiel:

   ```
   import json

   def lambda_handler(event, context):
       if event["source"] != "aws.es":
           raise ValueError("Function only supports input from events with a source
    type of: aws.es")

       print(json.dumps(event))
   ```

   Dies ist eine einfache Python-3.8-Funktion, mit der von OpenSearch Service gesendete Ereignisse gedruckt werden. Wenn alles richtig konfiguriert ist, sehen Sie am Ende dieses Tutorials, wie die Ereignisdetails in dem CloudWatch Protokollstream angezeigt werden, der dieser Lambda-Funktion zugeordnet ist.
7. Wählen Sie Bereitstellen.

Schritt 2: Registrieren von Ereignisregeln

In diesem Schritt erstellen Sie eine EventBridge Regel, die Ereignisse aus Ihren OpenSearch Service-Domänen erfasst. Diese Regel erfasst alle Ereignisse in dem Konto, in dem sie definiert ist. Die Ereignisnachrichten selbst enthalten Informationen über die Ereignisquelle, einschließlich der Domain, aus der sie stammen. Sie können diese Informationen verwenden, um Ereignisse programmgesteuert zu filtern und zu sortieren.

Um eine EventBridge Regel zu erstellen

1. Öffnen Sie die EventBridge Konsole unter https://console.aws.amazon.com/events/.
2. Wählen Sie Regel erstellen aus.
3. Nennen Sie die Regel Event-Regel.
4. Wählen Sie Weiter aus.
5. Wählen Sie für das Ereignismuster AWS Services, Amazon OpenSearch Service und All Events aus. Dieses Muster gilt für alle OpenSearch Service-Domänen und für jedes OpenSearch Service-Ereignis. Alternativ können Sie ein spezifischeres Muster erstellen, damit bestimmte Ergebnisse gefiltert werden.
6. Wählen Sie Weiter aus.
7. Wählen Sie für das Ziel Lambda-Funktion aus. Wählen Sie im Funktions-Dropdown-Menü Ereignis-Handler aus.
8. Wählen Sie Weiter aus.
9. Überspringen Sie die Tags und wählen Sie erneut Weiter aus.
10. Prüfen Sie die Konfiguration und wählen Sie Regel erstellen aus.

Schritt 3: Testen der Konfiguration

Wenn Sie das nächste Mal eine Benachrichtigung im Abschnitt Benachrichtigungen der OpenSearch Servicekonsole erhalten und alles richtig konfiguriert ist, wird Ihre Lambda-Funktion ausgelöst und schreibt die Ereignisdaten in einen CloudWatch Protokollstream für die Funktion.

So testen Sie die Konfiguration

1. Öffnen Sie die CloudWatch Konsole unter. https://console.aws.amazon.com/cloudwatch/
2. Wählen Sie im Navigationsbereich Logs (Protokolle) und die Protokollgruppe für Ihre Lambda-Funktion aus (z. B./aws/lambda/event-handler).
3. Wählen Sie einen Protokollstream aus, um die Ereignisdaten anzuzeigen.

Tutorial: Senden von Amazon-SNS-Warnungen für verfügbare Softwareupdates

In diesem Tutorial konfigurieren Sie eine EventBridge Amazon-Ereignisregel, die Benachrichtigungen für verfügbare Servicesoftware-Updates in Amazon OpenSearch Service erfasst und Ihnen eine E-Mail-Benachrichtigung über Amazon Simple Notification Service (Amazon SNS) sendet.

Voraussetzungen

Dieses Tutorial setzt voraus, dass Sie über eine vorhandene OpenSearch Service-Domäne verfügen. Wenn Sie noch keine Domain erstellt haben, führen Sie die Schritte unter Erstellen und Verwalten von Domains aus, um eine zu erstellen.

Schritt 1: Erstellen und Abonnieren eines Amazon-SNS-Themas

Konfigurieren Sie ein Amazon-SNS-Thema, das als Ereignisziel für Ihre neue Ereignisregel dient.

So erstellen Sie ein Amazon-SNS-Ziel

1. Öffnen Sie die Amazon-SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home.
2. Klicken Sie auf Themen und Erstellen eines Themas.
3. Wählen Sie als Auftragstyp Standard aus und benennen Sie den Auftrag software-update.
4. Wählen Sie Thema erstellen aus.
5. Nachdem das Thema erstellt wurde, wählen Sie Erstellen eines Abonnements.
6. Wählen Sie unter Protocol (Protokoll) die Option Email (E-Mail) aus. Geben Sie für Endpunkt eine E-Mail-Adresse ein, auf die Sie aktuell Zugriff haben, und wählen Sie Abonnement erstellen aus.
7. Überprüfen Sie Ihr E-Mail-Konto und warten Sie auf eine E-Mail-Nachricht zur Bestätigung Ihres Abonnements. Wenn Sie sie erhalten, wählen Sie Confirm Abonnement aus.

Schritt 2: Registrieren von Ereignisregeln

Als nächstes registrieren Sie eine Ereignisregel, die nur Service-Software-Updateereignisse erfasst.

So erstellen Sie eine Ereignisregel

1. Öffnen Sie die Konsole unter EventBridge . https://console.aws.amazon.com/events/

2. Wählen Sie Regel erstellen aus.
3. Benennen Sie die Regel softwareupdate-rule.
4. Wählen Sie Weiter aus.
5. Wählen Sie für das Ereignismuster AWS Services, Amazon OpenSearch Service und Amazon OpenSearch Service Software Update Notification aus. Dieses Muster entspricht jedem Service-Software-Update-Ereignis von OpenSearch Service. Weitere Informationen zu Ereignismustern finden Sie unter EventBridge Amazon-Ereignismuster im EventBridgeAmazon-Benutzerhandbuch.
6. Optional können Sie auch auf bestimmte Schweregrade filtern. Die Schweregrade jedes Ereignisses finden Sie unter the section called “Aktualisieren der Software”.
7. Wählen Sie Weiter aus.
8. Wählen Sie für das Ziel SNS-Thema und dann Software-Update aus.
9. Wählen Sie Weiter aus.
10. Überspringen Sie die Tags und wählen Sie Weiter aus.
11. Prüfen Sie die Regelkonfiguration und wählen Sie Regel erstellen aus.

Wenn Sie das nächste Mal eine Benachrichtigung von OpenSearch Service Software-Update erhalten und alles richtig konfiguriert ist, sollte Amazon SNS Ihnen eine E-Mail-Benachrichtigung über das Update senden, wenn alles richtig konfiguriert ist.

Überwachung von Amazon OpenSearch Service API-Aufrufen mit AWS CloudTrail

Amazon OpenSearch Service ist in einen Service integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem AWS Service in OpenSearch Service ausgeführt wurden. CloudTrail erfasst alle Konfigurations-API-Aufrufe für OpenSearch Service als Ereignisse.

> **Note**
>
> CloudTrail erfasst nur Aufrufe der Konfigurations-API, z. B. `CreateDomain` und`GetUpgradeStatus`. CloudTrail erfasst keine Aufrufe an die OpenSearch APIs, z. B. `_search` und`_bulk`. Informationen zu diesen Aufrufen finden Sie unter the section called “Überwachen der Prüfprotokolle”.

Zu den erfassten Anrufen gehören Anrufe von der OpenSearch Servicekonsole oder einem AWS SDK. AWS CLI Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Übermittlung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für OpenSearch Service. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem auf der CloudTrail Konsole im Ereignisverlauf anzeigen. Anhand der von CloudTrail gesammelten Informationen können Sie die Anfrage an den OpenSearch Service, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details ermitteln.

Weitere Informationen CloudTrail dazu finden Sie im AWS CloudTrail Benutzerhandbuch.

Amazon OpenSearch Service-Informationen in CloudTrail

CloudTrail ist auf Ihrem aktiviert AWS-Konto , wenn Sie das Konto erstellen. Wenn im OpenSearch Service eine Aktivität stattfindet, wird diese Aktivität zusammen mit anderen AWS Serviceereignissen im CloudTrail Event-Verlauf in einem Ereignis aufgezeichnet. Sie können die neusten Ereignisse in Ihr AWS-Konto -Konto herunterladen und dort suchen und anzeigen. Weitere Informationen finden Sie unter Ereignisse mit CloudTrail Ereignisverlauf anzeigen.

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS-Konto Konto, einschließlich der Ereignisse für den OpenSearch Service, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3 S3-Bucket. Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie hier:

- Erstellen Sie einen Trail für Ihren AWS-Konto
- AWS Service-Integrationen mit CloudTrail Logs
- Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien von mehreren Konten

Alle API-Aktionen für die OpenSearch Servicekonfiguration werden von der Amazon OpenSearch Service API-Referenz protokolliert CloudTrail und sind in dieser dokumentiert.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Root- oder AWS Identity and Access Management (IAM-) Benutzeranmeldedaten gestellt wurde
- Ob die Anfrage mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen föderierten Benutzer ausgeführt wurde
- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde

Weitere Informationen finden Sie unter CloudTrail userIdentity-Element.

Grundlegendes zu Amazon OpenSearch Service-Protokolldateieinträgen

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der den `CreateDomain` Vorgang demonstriert:

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::123456789012:user/test-user",
    "accountId": "123456789012",
    "accessKeyId": "access-key",
    "userName": "test-user",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2018-08-21T21:59:11Z"
      }
    },
    "invokedBy": "signin.amazonaws.com"
  },
```

```
  "eventTime": "2018-08-21T22:00:05Z",
  "eventSource": "es.amazonaws.com",
  "eventName": "CreateDomain",
  "awsRegion": "us-west-1",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "signin.amazonaws.com",
  "requestParameters": {
    "engineVersion": "OpenSearch_1.0",
    "clusterConfig": {
      "instanceType": "m4.large.search",
      "instanceCount": 1
    },
    "snapshotOptions": {
      "automatedSnapshotStartHour": 0
    },
    "domainName": "test-domain",
    "encryptionAtRestOptions": {},
    "eBSOptions": {
      "eBSEnabled": true,
      "volumeSize": 10,
      "volumeType": "gp2"
    },
    "accessPolicies": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect\":\"Allow
\",\"Principal\":{\"AWS\":[\"123456789012\"]},\"Action\":[\"es:*\"],\"Resource\":
\"arn:aws:es:us-west-1:123456789012:domain/test-domain/*\"}]}",
    "advancedOptions": {
      "rest.action.multi.allow_explicit_index": "true"
    }
  },
  "responseElements": {
    "domainStatus": {
      "created": true,
      "clusterConfig": {
        "zoneAwarenessEnabled": false,
        "instanceType": "m4.large.search",
        "dedicatedMasterEnabled": false,
        "instanceCount": 1
      },
      "cognitoOptions": {
        "enabled": false
      },
      "encryptionAtRestOptions": {
        "enabled": false
      },
```

```
      "advancedOptions": {
        "rest.action.multi.allow_explicit_index": "true"
      },
      "upgradeProcessing": false,
      "snapshotOptions": {
        "automatedSnapshotStartHour": 0
      },
      "eBSOptions": {
        "eBSEnabled": true,
        "volumeSize": 10,
        "volumeType": "gp2"
      },
      "engineVersion": "OpenSearch_1.0",
      "processing": true,
      "aRN": "arn:aws:es:us-west-1:123456789012:domain/test-domain",
      "domainId": "123456789012/test-domain",
      "deleted": false,
      "domainName": "test-domain",
      "accessPolicies": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect\":\"Allow
\",\"Principal\":{\"AWS\":\"arn:aws:iam::123456789012:root\"},\"Action\":\"es:*\",
\"Resource\":\"arn:aws:es:us-west-1:123456789012:domain/test-domain/*\"}]}"
    }
  },
  "requestID": "12345678-1234-1234-1234-987654321098",
  "eventID": "87654321-4321-4321-4321-987654321098",
  "eventType": "AwsApiCall",
  "recipientAccountId": "123456789012"
}
```

Sicherheit bei Amazon OpenSearch Service

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame Verantwortung von Ihnen AWS und Ihnen. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS Dienste in der AWS Cloud ausführt. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Auditoren von Drittanbietern testen und überprüfen die Effektivität unserer Sicherheitsmaßnahmen im Rahmen der AWS -Compliance-Programme regelmäßig. Weitere Informationen zu den Compliance-Programmen, die für Amazon OpenSearch Service gelten, finden Sie unter AWS Services in Scope by Compliance Program.
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Service, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Nutzung des OpenSearch Service anwenden können. In den folgenden Themen erfahren Sie, wie Sie den OpenSearch Service so konfigurieren, dass er Ihre Sicherheits- und Compliance-Ziele erfüllt. Sie erfahren auch, wie Sie andere AWS Dienste verwenden können, die Sie bei der Überwachung und Sicherung Ihrer OpenSearch Serviceressourcen unterstützen.

Themen

- Datenschutz bei Amazon OpenSearch Service
- Identity and Access Management in Amazon OpenSearch Service
- Serviceübergreifende Confused-Deputy-Prävention
- Feinkörnige Zugriffskontrolle in Amazon Service OpenSearch
- Konformitätsprüfung für Amazon OpenSearch Service
- Ausfallsicherheit von Amazon OpenSearch Service
- JWT-Authentifizierung und Autorisierung für Amazon Service OpenSearch
- Infrastruktursicherheit in Amazon OpenSearch Service

- SAML-Authentifizierung für Dashboards OpenSearch
- Konfiguration der Amazon Cognito Cognito-Authentifizierung für Dashboards OpenSearch
- Verwendung von serviceverknüpften Rollen für Amazon OpenSearch Service

Datenschutz bei Amazon OpenSearch Service

Das AWS Modell der mit gilt für den Datenschutz bei Amazon OpenSearch Service. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle Systeme laufen AWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz. Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag AWS -Modell der geteilten Verantwortung und in der DSGVO im AWS -Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Wird verwendet SSL/TLS , um mit AWS Ressourcen zu kommunizieren. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein AWS CloudTrail. Informationen zur Verwendung von CloudTrail Pfaden zur Erfassung von AWS Aktivitäten finden Sie unter Arbeiten mit CloudTrail Pfaden im AWS CloudTrail Benutzerhandbuch.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-3-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-3.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit dem OpenSearch Service oder anderen AWS-Services über die Konsole, API oder arbeiten. AWS CLI AWS SDKs Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Verschlüsselung von Daten im Ruhezustand für Amazon OpenSearch Service

OpenSearch Service-Domains bieten die Verschlüsselung von Daten im Ruhezustand, eine Sicherheitsfunktion, die dazu beiträgt, unbefugten Zugriff auf Ihre Daten zu verhindern. Die Funktion verwendet AWS Key Management Service (AWS KMS) zum Speichern und Verwalten Ihrer Verschlüsselungsschlüssel und den Advanced Encryption Standard-Algorithmus mit 256-Bit-Schlüsseln (AES-256) zur Durchführung der Verschlüsselung. Wenn die Funktion aktiviert ist, verschlüsselt sie die folgenden Aspekte einer Domain:

- Alle Indizes (einschließlich der Indizes im Speicher) UltraWarm
- OpenSearch Protokolle
- Swap-Dateien
- Alle anderen Daten im Anwendungsverzeichnis
- Automatisierte Snapshots

Die folgenden Dinge werden nicht verschlüsselt, wenn Sie die Verschlüsselung gespeicherter Daten aktivieren, aber Sie können weitere Schritte zu ihrem Schutz unternehmen:

- Manuelle Schnappschüsse: Sie können derzeit keine AWS KMS Schlüssel verwenden, um manuelle Schnappschüsse zu verschlüsseln. Sie können jedoch eine serverseitige Verschlüsselung mit in S3 verwalteten Schlüsseln oder KMS-Schlüsseln zum Verschlüsseln des Buckets verwenden, den Sie als Snapshot-Repository verwenden. Detaillierte Anweisungen finden Sie unter the section called “Registrieren eines manuellen Snapshot-Repositorys”.
- Langsame Protokolle und Fehlerprotokolle: Wenn Sie Protokolle veröffentlichen und diese verschlüsseln möchten, können Sie die zugehörige CloudWatch Protokollgruppe mit demselben AWS KMS Schlüssel wie die Dienstdomäne verschlüsseln. OpenSearch Weitere Informationen

finden Sie unter Verschlüsseln von Protokolldaten in CloudWatch Logs using AWS Key Management Service im Amazon CloudWatch Logs-Benutzerhandbuch.

> **Note**
>
> Sie können die Verschlüsselung im Ruhezustand für eine bestehende Domain nicht aktivieren, wenn UltraWarm oder Cold Storage auf der Domain aktiviert ist. Sie müssen zuerst Cold Storage UltraWarm deaktivieren, Verschlüsselung im Ruhezustand aktivieren und dann Cold Storage wieder aktivieren UltraWarm . Wenn Sie Indizes im Cold Storage UltraWarm oder Cold Storage behalten möchten, müssen Sie sie zunächst in den Hot-Storage verschieben, bevor Sie sie deaktivieren UltraWarm oder Cold Storage aktivieren.

OpenSearch Der Service unterstützt nur KMS-Schlüssel mit symmetrischer Verschlüsselung, keine asymmetrischen Schlüssel. Informationen zum Erstellen symmetrischer Schlüssel finden Sie unter Erstellen eines KMS-Schlüssels im AWS Key Management Service Entwicklerhandbuch.

Unabhängig davon, ob die Verschlüsselung im Ruhezustand aktiviert ist, verschlüsseln alle Domänen automatisch benutzerdefinierte Pakete mithilfe von AES-256 und vom Service verwalteten Schlüsseln. OpenSearch

Berechtigungen

Um die OpenSearch Service-Konsole zur Konfiguration der Verschlüsselung von Daten im Ruhezustand zu verwenden, benötigen Sie Leseberechtigungen AWS KMS, z. B. für die folgende identitätsbasierte Richtlinie:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:List*",
        "kms:Describe*"
      ],
```

```
      "Resource": "*"
    }
  ]
}
```

Wenn Sie einen anderen Schlüssel als den AWS eigenen Schlüssel verwenden möchten, müssen Sie auch über die erforderlichen Berechtigungen verfügen, um Berechtigungen für den Schlüssel zu erstellen. Diese Berechtigung erfolgt in der Regel über eine ressourcenbasierte Richtlinie, die Sie beim Erstellen des Schlüssels angeben.

Wenn Sie Ihren Schlüssel ausschließlich für OpenSearch Service behalten möchten, können Sie dieser Schlüsselrichtlinie die ViaService Bedingung kms: hinzufügen:

```
"Condition": {
  "StringEquals": {
    "kms:ViaService": "es.us-west-1.amazonaws.com"
  },
  "Bool": {
    "kms:GrantIsForAWSResource": "true"
  }
}
```

Weitere Informationen finden Sie unter Schlüsselrichtlinien in AWS KMS im Entwicklerhandbuch für AWS Key Management Service .

Verschlüsselung gespeicherter Daten aktivieren

Für die Verschlüsselung ruhender Daten auf neuen Domains ist entweder OpenSearch Elasticsearch 5.1 oder höher erforderlich. Für die Aktivierung auf bestehenden Domains ist entweder Elasticsearch 6.7 OpenSearch oder höher erforderlich.

So aktivieren Sie die Verschlüsselung von Data-at-Rest (Konsole)

1. Öffnen Sie die Domain in der AWS Konsole und wählen Sie dann Aktionen und Sicherheitskonfiguration bearbeiten aus.
2. Wählen Sie unter Verschlüsselung die Option Verschlüsselung von Data-at-Rest aktivieren aus.
3. Wählen Sie einen AWS KMS Schlüssel aus, den Sie verwenden möchten, und klicken Sie dann auf Änderungen speichern.

Sie können die Verschlüsselung auch über die Konfigurations-API aktivieren. Die folgende Anforderung ermöglicht die Verschlüsselung von Daten im Ruhezustand, die sich auf einer vorhandenen Domain befinden:

```
{
   "ClusterConfig":{
      "EncryptionAtRestOptions":{
         "Enabled": true,
         "KmsKeyId":"arn:aws:kms:us-east-1:123456789012:alias/my-key"
      }
   }
}
```

Deaktivierter oder gelöschter KMS-Schlüssel

Wenn du den Schlüssel, mit dem du eine Domain verschlüsselt hast, deaktivierst oder löschst, kann nicht mehr auf die Domain zugegriffen werden. OpenSearch Der Dienst sendet Ihnen eine Benachrichtigung, in der Sie darüber informiert werden, dass er nicht auf den KMS-Schlüssel zugreifen kann. Aktivieren Sie den Schlüssel erneut umgehend, um auf Ihre Domain zuzugreifen.

Das OpenSearch Serviceteam kann Ihnen nicht helfen, Ihre Daten wiederherzustellen, wenn Ihr Schlüssel gelöscht wird. AWS KMS löscht Schlüssel erst nach einer Wartezeit von mindestens sieben Tagen. Wenn Ihr Schlüssel gelöscht werden soll, brechen Sie entweder die Löschung ab oder machen Sie einen manuellen Snapshot der Domain, um den Verlust Ihrer Daten zu verhindern.

Verschlüsselung gespeicherter Daten deaktivieren

Nachdem Sie eine Domain zum Verschlüsseln von Daten im Ruhezustand konfiguriert haben, können Sie die Einstellung nicht mehr deaktivieren. Stattdessen können Sie einen manuellen Snapshot der vorhandenen Domain erstellen, eine andere Domain erstellen, Ihre Daten migrieren und die alte Domain löschen.

Überwachen von Domains, die Daten im Ruhezustand verschlüsseln

Domains, die Daten im Ruhezustand verschlüsseln, haben zwei zusätzliche Metriken: `KMSKeyError` und `KMSKeyInaccessible`. Diese Metriken werden nur angezeigt, wenn die Domain ein Problem mit Ihrem Verschlüsselungsschlüssel feststellt. Vollständige Beschreibungen dieser Metriken finden Sie unter the section called “Cluster-Metriken”. Sie können sie entweder über die OpenSearch Service-Konsole oder die CloudWatch Amazon-Konsole anzeigen.

> **Tip**
>
> Jede Metrik stellt ein erhebliches Problem für eine Domain dar. Wir empfehlen daher, CloudWatch Alarme für beide zu erstellen. Weitere Informationen finden Sie unter the section called “Empfohlene CloudWatch Alarme”.

Weitere Überlegungen

- Bei der automatischen Schlüsselrotation bleiben die Eigenschaften Ihrer AWS KMS Schlüssel erhalten, sodass die Rotation keine Auswirkungen auf Ihre Fähigkeit hat, auf Ihre OpenSearch Daten zuzugreifen. Verschlüsselte OpenSearch Dienstdomänen unterstützen keine manuelle Schlüsselrotation, bei der ein neuer Schlüssel erstellt und alle Verweise auf den alten Schlüssel aktualisiert werden müssen. Weitere Informationen finden Sie im AWS Key Management Service Entwicklerhandbuch unter AWS KMS Schlüssel drehen.
- Bestimmte Instance-Typen unterstützen die Verschlüsselung gespeicherter Daten nicht. Details hierzu finden Sie unter the section called “Unterstützte Instance-Typen”.
- Domains, die gespeicherte Daten verschlüsseln, verwenden einen anderen Repository-Namen für ihre automatischen Snapshots. Weitere Informationen finden Sie unter the section called “Wiederherstellen von Snapshots”.
- Während wir dringend empfehlen, die Verschlüsselung im Ruhezustand zu aktivieren, kann dies zusätzlichen CPU-Overhead und einige Millisekunden Latenz verursachen. Die meisten Anwendungsfälle reagieren jedoch nicht empfindlich auf diese Unterschiede, und das Ausmaß der Auswirkungen hängt von der Konfiguration Ihres Clusters, Ihrer Clients und Ihres Nutzungsprofils ab.

Node-to-node Verschlüsselung für Amazon OpenSearch Service

Node-to-node Die Verschlüsselung bietet zusätzlich zu den Standardfunktionen von Amazon OpenSearch Service eine zusätzliche Sicherheitsebene.

Jede OpenSearch Dienstdomäne — unabhängig davon, ob die Domäne VPC-Zugriff verwendet — befindet sich in einer eigenen, dedizierten VPC. Diese Architektur verhindert, dass potenzielle Angreifer den Datenverkehr zwischen Knoten abfangen, und sorgt für die Sicherheit des Clusters. OpenSearch Standardmäßig ist der Verkehr innerhalb der VPC jedoch unverschlüsselt. Node-

to-nodeVerschlüsselung aktiviert die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der VPC.

Wenn Sie Daten über HTTPS an den OpenSearch Service senden, trägt die node-to-node Verschlüsselung dazu bei, dass Ihre Daten bei der OpenSearch Verteilung (und Weiterverteilung) im gesamten Cluster verschlüsselt bleiben. Wenn Daten unverschlüsselt über HTTP ankommen, verschlüsselt der OpenSearch Service sie, nachdem sie den Cluster erreicht haben. Mithilfe der Konsole oder der Konfigurations-API können Sie verlangen, AWS CLI dass der gesamte Datenverkehr zur Domain über HTTPS eingeht.

Node-to-node Verschlüsselung ist erforderlich, wenn Sie eine differenzierte Zugriffskontrolle aktivieren.

Verschlüsselung aktivieren node-to-node

Node-to-node Für die Verschlüsselung neuer Domains ist eine beliebige Version von OpenSearch oder Elasticsearch 6.0 oder höher erforderlich. Für die Aktivierung der node-to-node Verschlüsselung auf bestehenden Domains ist eine beliebige Version von OpenSearch oder Elasticsearch 6.7 oder höher erforderlich. Wählen Sie die vorhandene Domain in der AWS -Konsole, Aktionen und Sicherheitskonfiguration bearbeiten aus.

Alternativ können Sie die Konfigurations-API AWS CLI oder verwenden. Weitere Informationen finden Sie in der AWS CLI Befehlsreferenz und der OpenSearch Service-API-Referenz.

Verschlüsselung wird deaktiviert node-to-node

Nachdem Sie eine Domain für die node-to-node Verschlüsselung konfiguriert haben, können Sie die Einstellung nicht deaktivieren. Stattdessen können Sie einen manuellen Snapshot der verschlüsselten Domain erstellen, eine andere Domain erstellen, Ihre Daten migrieren und die alte Domain löschen.

Identity and Access Management in Amazon OpenSearch Service

Amazon OpenSearch Service bietet verschiedene Möglichkeiten, den Zugriff auf Ihre Domains zu kontrollieren. Dieses Thema geht auf die verschiedenen Richtlinientypen, deren Interaktion miteinander und die Erstellung eigener, benutzerdefinierter Richtlinien ein.

> **Important**
>
> Die VPC-Unterstützung führt zu einigen zusätzlichen Überlegungen zur OpenSearch Dienstzugriffskontrolle. Weitere Informationen finden Sie unter the section called “Zugriffsrichtlinien für VPC-Domänen”.

Arten von Richtlinien

OpenSearch Der Service unterstützt drei Arten von Zugriffsrichtlinien:

- the section called “Ressourcenbasierte Richtlinien”
- the section called “Identitätsbasierte Richtlinien”
- the section called “IP-basierte Richtlinien”

Ressourcenbasierte Richtlinien

Beim Erstellen einer Domain fügen Sie eine ressourcenbasierte Richtlinie hinzu, die oft als Domain-Zugriffsrichtlinie bezeichnet wird. Diese Richtlinien legen fest, welche Aktionen ein Prinzipal auf den Subressourcen der Domain durchführen kann (mit Ausnahme der clusterübergreifenden Suche). Zu den Unterressourcen gehören OpenSearch Indizes und. APIs Das JSON-Richtlinienelement „Principal“ in IAM spezifiziert die Konten, Benutzer oder Rollen, denen Zugriff gewährt wird. Das JSON-Richtlinienelement Resource gibt an, auf welche Unterressourcen diese Prinzipale zugreifen können.

Beispielsweise gewährt die folgende ressourcenbasierte Richtlinie `test-user` vollen Zugriff (`es:*`) auf die Unterressourcen auf `test-domain`:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::123456789012:user/test-user"
```

```
        ]
      },
      "Action": [
        "es:*"
      ],
      "Resource": "arn:aws:es:us-west-1:987654321098:domain/test-domain/*"
    }
  ]
}
```

Zwei wichtige Überlegungen treffen auf diese Richtlinie zu:

- Diese Berechtigungen gelten nur für diese Domain. Sofern Sie keine ähnlichen Richtlinien auf anderen Domains erstellen, kann `test-user` nur auf `test-domain` zugreifen.
- Das nachgestellte `/*` im `Resource`-Element ist wichtig und weist darauf hin, dass ressourcenbasierte Richtlinien nur für die Unterressourcen der Domain gelten, nicht für die Domain selbst. In ressourcenbasierten Richtlinien entspricht die `es:*`-Aktion `es:ESHttp*`.

  Beispielsweise kann `test-user` zwar Anforderungen an einen Index (`GET https://search-test-domain.us-west-1.es.amazonaws.com/test-index`) richten, aber nicht die Konfiguration der Domain (`POST https://es.us-west-1.amazonaws.com/2021-01-01/opensearch/domain/test-domain/config`) aktualisieren. Beachten Sie den Unterschied zwischen den beiden Endpunkten. Für den Zugriff auf die Konfigurations-API ist eine identitätsbasierte Richtlinie erforderlich.

Sie können einen partiellen Indexnamen angeben, indem Sie einen Platzhalter hinzufügen. Dieses Beispiel identifiziert alle Indizes, die mit `commerce` beginnen:

```
arn:aws:es:us-west-1:987654321098:domain/test-domain/commerce*
```

In diesem Fall bedeutet der Platzhalter, dass `test-user` Anfragen an Indizes innerhalb von `test-domain` stellen kann, deren Namen mit `commerce` beginnen.

Um `test-user` weiter einzuschränken, können Sie die folgende Richtlinie anwenden:

JSON

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::123456789012:user/test-user"
        ]
      },
      "Action": [
        "es:ESHttpGet"
      ],
      "Resource": "arn:aws:es:us-west-1:987654321098:domain/test-domain/commerce-
data/_search"
    }
  ]
}
```

Nun kann `test-user` nur noch eine Operation durchführen: die Suche nach dem Index `commerce-data`. Auf alle anderen Indizes innerhalb der Domain kann nicht zugegriffen werden, und ohne die Berechtigung, die Aktionen `es:ESHttpPut` oder `es:ESHttpPost` zu verwenden, kann `test-user` keine Dokumente hinzufügen oder ändern.

Als nächstes möchten Sie vielleicht eine Rolle für Hauptbenutzer konfigurieren. Diese Richtlinie gewährt `power-user-role` Zugriff auf die HTTP-Methoden GET und PUT für alle URIs im Index:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::123456789012:role/power-user-role"
        ]
      },
      "Action": [
        "es:ESHttpGet",
        "es:ESHttpPut"
```

```
      ],
      "Resource": "arn:aws:es:us-west-1:987654321098:domain/test-domain/commerce-
data/*"
    }
  ]
}
```

Wenn sich Ihre Domain in einer VPC befindet oder eine differenzierte Zugriffssteuerung verwendet, können Sie eine offene Domain-Zugriffsrichtlinie verwenden. Andernfalls muss Ihre Domain-Zugriffsrichtlinie eine Einschränkung enthalten, entweder nach Prinzipal oder IP-Adresse.

Weitere Informationen zu allen verfügbaren Aktionen finden Sie unter the section called “Richtlinienelementreferenz”. Für eine weitaus detailliertere Kontrolle über Ihre Daten verwenden Sie eine offene Domain-Zugriffsrichtlinie mit differenzierte Zugriffssteuerung.

Identitätsbasierte Richtlinien

Im Gegensatz zu ressourcenbasierten Richtlinien, die Teil jeder OpenSearch Dienstdomäne sind, hängen Sie identitätsbasierte Richtlinien an Benutzer oder Rollen an, die den AWS Identity and Access Management (IAM-) Dienst verwenden. Genauso wie ressourcenbasierte Richtlinien legen identitätsbasierte Richtlinien fest, welche Personen auf einen Service zugreifen können, welche Aktionen sie ausführen können und, sofern zutreffend, für welche Ressourcen sie diese Aktionen ausführen können.

Identitätsbasierte Richtlinien sind in der Regel allgemeiner, dies muss aber nicht unbedingt so sein. Sie regeln oft nur die Konfigurations-API-Aktionen, die ein Benutzer durchführen darf. Sobald Sie diese Richtlinien eingerichtet haben, können Sie ressourcenbasierte Richtlinien (oder eine differenzierte Zugriffskontrolle) in OpenSearch Service verwenden, um Benutzern Zugriff auf Indizes und zu gewähren. OpenSearch APIs

> **Note**
>
> Benutzer mit der AWS verwalteten `AmazonOpenSearchServiceReadOnlyAccess` Richtlinie können den Cluster-Integritätsstatus auf der Konsole nicht sehen. Damit sie den Cluster-Integritätsstatus (und andere OpenSearch Daten) sehen können, fügen Sie die `es:ESHttpGet` Aktion einer Zugriffsrichtlinie hinzu und fügen Sie sie ihren Konten oder Rollen hinzu.

Da identitätsbasierte Richtlinien an Benutzer oder Rollen (Prinzipale) angefügt werden, gibt JSON keinen Prinzipal an. Die folgende Richtlinie gewährt Zugriff auf Aktionen, die mit `Describe` und `List` beginnen. Diese Kombination von Aktionen bietet schreibgeschützten Zugriff auf Domain-Konfigurationen, jedoch nicht direkt auf die in der Domain gespeicherten Daten:

JSON

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

Ein Administrator hat möglicherweise vollen Zugriff auf den OpenSearch Dienst und alle in allen Domänen gespeicherten Daten:

JSON

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

Mit identitätsbasierten Richtlinien können Sie Tags verwenden, um den Zugriff auf die Konfigurations-API zu steuern. Die folgende Richtlinie ermöglicht es beispielsweise angehängten Prinzipalen, die Konfiguration einer Domain anzuzeigen und zu aktualisieren, wenn die Domain über das Tag `team:devops` verfügt:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": [
      "es:UpdateDomainConfig",
      "es:DescribeDomain",
      "es:DescribeDomainConfig"
    ],
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:ResourceTag/team": [
          "devops"
        ]
      }
    }
  }]
}
```

Sie können auch Tags verwenden, um den Zugriff auf die OpenSearch API zu kontrollieren. Tag-basierte Richtlinien für die OpenSearch API gelten nur für HTTP-Methoden. Mit der folgenden Richtlinie können beispielsweise angehängte Principals GET- und PUT-Anfragen an die OpenSearch API senden, wenn die Domain über das `environment:production` Tag verfügt:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": [
      "es:ESHttpGet",
```

```
      "es:ESHttpPut"
    ],
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:ResourceTag/environment": [
          "production"
        ]
      }
    }
  }]
}
```

Für eine detailliertere Steuerung der OpenSearch API sollten Sie eine differenzierte Zugriffskontrolle in Betracht ziehen.

> **Note**
>
> Nachdem Sie einer Tag-basierten Richtlinie eine oder mehrere OpenSearch APIs hinzugefügt haben, müssen Sie eine einzelne Tag-Operation durchführen (z. B. ein Tag hinzufügen, entfernen oder ändern), damit die Änderungen für eine Domain wirksam werden. Sie müssen die Servicesoftware R20211203 oder höher verwenden, um OpenSearch API-Operationen in tagbasierte Richtlinien aufnehmen zu können.

OpenSearch Der Service unterstützt die `RequestTag` und die `TagKeys` globalen Bedingungsschlüssel für die Konfigurations-API, nicht für die API. OpenSearch Diese Bedingungen gelten nur für API-Aufrufe, die Tags in der Anfrage enthalten, z. B. `CreateDomain`, `AddTags` und `RemoveTags`. Mit der folgenden Richtlinie können angehängte Prinzipale Domains erstellen, jedoch nur, wenn sie das `team:it`-Tag in die Anfrage aufnehmen:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
```

```
      "es:CreateDomain",
      "es:AddTags"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:RequestTag/team": [
          "it"
        ]
      }
    }
  }
}
```

Weitere Informationen zur Verwendung von Tags für die Zugriffskontrolle und zu den Unterschieden zwischen ressourcenbasierten und identitätsbasierten Richtlinien finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung im IAM-Benutzerhandbuch.

IP-basierte Richtlinien

IP-basierte Richtlinien beschränken den Zugriff auf eine Domain auf eine oder mehrere IP-Adressen oder CIDR-Blöcke. Aus technischer Sicht sind IP-basierte Richtlinien kein eigener Richtlinientyp. Stattdessen handelt es sich lediglich um ressourcenbasierte Richtlinien, die einen anonymen Prinzipal spezifizieren und eine spezielle Bedingung enthalten. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.

Der Hauptvorteil IP-basierter Richtlinien besteht darin, dass sie unsignierte Anfragen an eine OpenSearch Service-Domain zulassen, sodass Sie Clients wie Curl und OpenSearch Dashboards verwenden oder über einen Proxyserver auf die Domain zugreifen können. Weitere Informationen hierzu finden Sie unter the section called “Verwenden eines Proxys für den Zugriff auf den Service über Dashboards OpenSearch ”.

> **Note**
>
> Wenn für die Domain VPC-Zugriff aktiviert wurde, können Sie keine IP-basierte Richtlinie konfigurieren. Stattdessen können Sie `security groups` damit steuern, welche IP-Adressen auf die Domain zugreifen können. Weitere Informationen finden Sie unter den folgenden Themen:
>
> - the section called “Zugriffsrichtlinien für VPC-Domänen”

- Steuern Sie den Datenverkehr zu Ihren AWS Ressourcen mithilfe von Sicherheitsgruppen im Amazon VPC-Benutzerhandbuch

Die folgende Richtlinie gewährt allen HTTP-Anforderungen, die vom angegebenen IP-Bereich stammen, den Zugriff auf `test-domain`:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": [
        "es:ESHttp*"
      ],
      "Condition": {
        "IpAddress": {
          "aws:SourceIp": [
            "192.0.2.0/24"
          ]
        }
      },
      "Resource": "arn:aws:es:us-west-1:987654321098:domain/test-domain/*"
    }
  ]
}
```

Wenn Ihre Domain über einen öffentlichen Endpunkt verfügt und keine differenzierte Zugriffssteuerung verwendet, empfehlen wir, IAM-Prinzipale und IP-Adressen zu kombinieren. Diese Richtlinie gewährt `test-user` HTTP-Zugriff nur, wenn die Anforderung aus dem angegebenen IP-Bereich stammt:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Principal": {
      "AWS": [
        "arn:aws:iam::987654321098:user/test-user"
      ]
    },
    "Action": [
      "es:ESHttp*"
    ],
    "Condition": {
      "IpAddress": {
        "aws:SourceIp": [
          "192.0.2.0/24"
        ]
      }
    },
    "Resource": "arn:aws:es:us-west-1:987654321098:domain/test-domain/*"
  }]
}
```

OpenSearch Serviceanfragen stellen und signieren

Selbst wenn Sie eine vollständig offene, ressourcenbasierte Zugriffsrichtlinie konfigurieren, müssen alle Anfragen an die OpenSearch Service-Konfigurations-API signiert werden. Wenn in Ihren Richtlinien IAM-Rollen oder -Benutzer angegeben sind, müssen Anfragen an die OpenSearch APIs ebenfalls mit AWS Signature Version 4 signiert werden. Die Signaturmethode ist je nach API verschieden:

- Um Aufrufe an die OpenSearch Service-Konfigurations-API zu tätigen, empfehlen wir Ihnen, eine der AWS SDKsfolgenden Optionen zu verwenden. Sie vereinfachen den Vorgang SDKs erheblich und können Ihnen im Vergleich zum Erstellen und Signieren Ihrer eigenen Anfragen viel Zeit sparen. Die Konfigurations-API-Endpunkte verwenden das folgende Format:

  ```
  es.region.amazonaws.com/2021-01-01/
  ```

Beispiel: Die folgende Anforderung versendet eine Konfigurationsänderung an die `movies`-Domain, aber Sie müssen sie selbst signieren (nicht empfohlen):

```
POST https://es.us-east-1.amazonaws.com/2021-01-01/opensearch/domain/movies/config
{
  "ClusterConfig": {
    "InstanceType": "c5.xlarge.search"
  }
}
```

Wenn Sie eine der folgenden Optionen verwenden SDKs, z. B. Boto 3, übernimmt das SDK automatisch die Signierung der Anfrage:

```
import boto3

client = boto3.client(es)
response = client.update_domain_config(
  DomainName='movies',
  ClusterConfig={
    'InstanceType': 'c5.xlarge.search'
  }
)
```

Ein Java-Codebeispiel finden Sie unter the section called “Mit dem AWS SDKs”.

- Um Anrufe an die zu tätigen OpenSearch APIs, müssen Sie Ihre eigenen Anfragen signieren. OpenSearch APIs Sie verwenden das folgende Format:

```
domain-id.region.es.amazonaws.com
```

Beispiel: Die folgende Anforderung durchsucht den `movies`-Index nach thor:

```
GET https://my-domain.us-east-1.es.amazonaws.com/movies/_search?q=thor
```

> **Note**
>
> Der Dienst ignoriert Parameter, die URLs für HTTP-POST-Anfragen übergeben wurden, die mit Signature Version 4 signiert sind.

Konflikte in Richtlinien

Komplexitäten entstehen, wenn Richtlinien einander widersprechen oder den Benutzer nicht explizit erwähnen. So funktioniert IAM Im IAM-Benutzerhandbuch finden Sie eine kurze Zusammenfassung der Bewertungslogik von Richtlinien:

- Standardmäßig werden alle Anforderungen verweigert.
- Dieser Standardwert kann durch eine explizite Zugriffserlaubnis überschrieben werden.
- Eine explizite Zugriffsverweigerung überschreibt jedwede Zugriffserlaubnis.

Wenn Ihnen beispielsweise eine ressourcenbasierte Richtlinie Zugriff auf eine Domain-Unterressource (einen OpenSearch Index oder eine API) gewährt, Ihnen aber eine identitätsbasierte Richtlinie den Zugriff verweigert, wird Ihnen der Zugriff verweigert. Wenn eine identitätsbasierte Richtlinien den Zugriff gewährt, eine ressourcenbasierte Richtlinie aber nicht festlegt, ob Ihnen Zugriff gewährt werden soll oder ob nicht, wird Ihnen der Zugriff gewährt. In der folgenden Tabelle sich überschneidender Richtlinien finden Sie eine vollständige Übersicht der Ergebnisse für Domains-Subressourcen.

	Zugelassen in ressourcenbasierter Richtlinie	Verweigert in ressourcenbasierter Richtlinie	Weder zugelassen noch verweigert in ressourcenbasierter Richtlinie
Allowed in identity-based policy	Sobald Sie die Details auf dieser Seite überprüft haben, klicken Sie auf	Deny	Sobald Sie die Details auf dieser Seite überprüft haben, klicken Sie auf
Denied in identity-based policy	Deny	Deny	Deny
Neither allowed nor denied in identity-based policy	Sobald Sie die Details auf dieser Seite überprüft haben, klicken Sie auf	Deny	Deny

Richtlinienelementreferenz

OpenSearch Der Service unterstützt die meisten Richtlinienelemente in der IAM-Referenz für Richtlinienelemente, mit Ausnahme von. `NotPrincipal` Die folgende Tabelle zeigt die gängigsten Elemente.

JSON-Richtlinienelement	Übersicht
`Version`	Die aktuelle Version der Richtliniensprache ist `2012-10-17` . Alle vordefinierten Zugriffsrichtlinien sollten diesen Wert angeben.
`Effect`	Dieses Element legt fest, ob die Anweisung den Zugriff auf die angegebenen Aktionen zulässt oder verweigert. Gültige Werte sind `Allow` oder `Deny`.
`Principal`	Dieses Element gibt die AWS-Konto oder die IAM-Rolle oder den Benutzer an, dem der Zugriff auf eine Ressource gewährt oder verweigert wird. Es kann verschiedene Formen annehmen: • AWS Konten: oder `"Principal":{"AWS": ["123456789012"]}` `"Principal":{"AWS": ["arn:aws:iam::123456789012:root"]}` • IAM-Benutzer: `"Principal":{"AWS": ["arn:aws:iam::123456789012:user/test-user"]}` • IAM-Rollen: `"Principal":{"AWS": ["arn:aws:iam::123456789012:role/test-role"]}` **Important** Durch die Angabe des Platzhalters * wird der anonyme Zugriff auf die Domain ermöglicht. Dies wird nur empfohlen, wenn Sie eine IP-basierte Bedingung hinzufügen, VPC-Support verwenden oder eine feinkörnige Zugriffssteuerung aktivieren. Prüfen Sie außerdem sorgfältig die folgenden Richtlinien, um sicherzustellen, dass sie keinen breiten Zugang gewähren:

JSON-Richtlinienelement	Übersicht
	• Identitätsbasierte Richtlinien, die mit zugehörigen AWS -Principalen verknüpft sind (z. B. IAM-Rollen) • Ressourcenbasierte Richtlinien, die mit zugehörigen AWS Ressourcen verknüpft sind (z. B. AWS Key Management Service KMS-Schlüssel)

JSON-Richtlinienelement	Übersicht
`Action`	OpenSearch Der Dienst verwendet `ESHttp*` Aktionen für OpenSearch HTTP-Methoden. Die restlichen Aktionen gelten für die Konfigurations-API. Bestimmte `es:`-Aktionen unterstützen Berechtigungen auf Ressource nebene. Sie können einem Benutzer z. B. Berechtigungen zum Löschen einer bestimmten Domain erteilen, ohne ihn zum Löschen beliebiger Domains zu berechtigen. Andere Aktionen gelten nur für den Service selbst. `es:ListDomainNames` ist im Kontext einer einzelnen Domain ohne Bedeutung und benötigt folglich einen Platzhalter. Eine Liste aller verfügbaren Aktionen und ob sie für die Domain-Su bressourcen (`test-domain/*`), für die Domain-Konfiguration () oder nur für den Service (`test-domain *`) gelten, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon OpenSearch Service in der Service Authorization Reference Ressourcenbasierte Richtlinien unterscheiden sich von Berechtig ungen auf Ressourcenebene. Ressourcenbasierte Richtlinien sind vollständige JSON-Richtlinien, die an Domains angefügt werden. Mithilfe von Berechtigungen auf Ressourcenebene können Sie Aktionen auf bestimmte Domains oder Unterressourcen einschränken. In der Praxis können Sie sich Berechtigungen auf Ressourcenebene als optionaler Teil einer ressourcen- oder identitätsbasierten Richtlinien vorstellen. Während Berechtigungen auf Ressourcenebene für `es:CreateDomain` nicht allzu sinnvoll erscheinen – denn warum sollte man einem Benutzer Berechtigungen zum Erstellen einer Domain gewähren, die bereits vorhanden ist? – können Sie mithilfe eines Platzhalters ein einfaches Benennungsschema für Ihre Domains (z. B. `"Resource": "arn:aws:es:us-west-1:987654321098:domain/my-team-name-*"`) erzwingen. Natürlich kann nichts Sie daran hindern, Aktionen zusammen mit weniger restriktiven Ressourcen einzuschließen, wie z. B. die folgenden Elemente:

JSON-Richtlinienelement	Übersicht
	JSON `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "es:ESHttpGet", "es:DescribeDomain" ], "Resource": "*" } ] }` Weitere Informationen zum Kombinieren von Aktionen mit Ressourcen finden Sie unter dem Element `Resource` in dieser Tabelle.

JSON-Richtlinienelement	Übersicht
`Condition`	OpenSearch Der Service unterstützt die meisten Bedingungen, die im IAM-Benutzerhandbuch unter den Kontextschlüsseln für AWS globale Bedingungen beschrieben sind. Zu den nennenswerten Ausnahmen gehört der `aws:PrincipalTag` Schlüssel, den der OpenSearch Service nicht unterstützt. Bei der Konfiguration einer IP-basierten Richtlinien geben Sie die IP-Adressen oder den CIDR-Block als Bedingung an, wie im folgenden Beispiel: `"Condition": { "IpAddress": { "aws:SourceIp": [ "192.0.2.0/32" ] } }` Wie unter erwähntthe section called “Identitätsbasierte Richtlinien”, gelten die Bedingungsschlüssel `aws:ResourceTag` `aws:RequestTag` , und die `aws:TagKeys` Bedingungsschlüssel sowohl für die Konfigurations-API als auch für die OpenSearch APIs.

JSON-Richtlinienelement	Übersicht

`Resource`	OpenSearch Der Service verwendet `Resource` Elemente auf drei grundlegende Arten:
	
	• Verwenden Sie für Aktionen, die sich auf den OpenSearch Dienst selbst beziehen`es:ListDomainNames` , z. B. um vollen Zugriff zu gewähren, die folgende Syntax:
	
	`"Resource": "*"`
	
	• Für Aktionen, die mit der Konfiguration einer Domain zusammenhängen, wie `es:DescribeDomain` , können Sie die folgende Syntax verwenden:
	
	`"Resource": "arn:aws:es:` *region*`:`*aws-account-id*`:domain/`*domain-name*`"`
	
	• Für Aktionen, die für Unterressourcen einer Domain gelten, wie `es:ESHttpGet` , können Sie die folgende Syntax verwenden:
	
	`"Resource": "arn:aws:es:` *region*`:`*aws-account-id*`:domain/`*domain-name*`/*"`
	
	Sie müssen keinen Platzhalter verwenden. OpenSearch Mit dem Service können Sie für jeden OpenSearch Index oder jede API eine andere Zugriffsrichtlinie definieren. Unter Umständen möchten Sie die Berechtigungen eines Benutzers für den Index `test-index` einschränken:
	
	`"Resource": "arn:aws:es:` *region*`:`*aws-account-id*`:domain/`*domain-name*`/test-index"`
	
	Anstelle eines uneingeschränkten Zugriffs auf `test-index` können Sie die Richtlinie auch nur auf die Such-API beschränken.

JSON-Richtlinienelement	Übersicht

	`"Resource": "arn:aws:es:region:aws-account-id:domain/domain-name /test-index/_search"`
	
	Sie können sogar den Zugriff auf einzelne Dokumente kontrollieren:
	
	`"Resource": "arn:aws:es:region:aws-account-id:domain/domain-name /test-index/test-type/1"`
	
	Wenn die Unterressource als URI OpenSearch ausgedrückt wird, können Sie im Wesentlichen den Zugriff darauf mithilfe einer Zugriffsrichtlinie steuern. Weitere Informationen dazu, auf welche Ressourcen ein Benutzer zugreifen kann, finden Sie unter the section called “Differenzierte Zugriffskontrolle”.
	
	Weitere Informationen dazu, welche Aktionen Berechtigungen auf Ressourcenebene unterstützten, finden Sie unter dem Element `Action` in dieser Tabelle.

Erweiterte Optionen und Überlegungen zur API

OpenSearch Der Dienst verfügt über mehrere erweiterte Optionen, von denen eine Auswirkungen auf die Zugriffskontrolle hat:. `rest.action.multi.allow_explicit_index` Bei ihrer Standardeinstellung „true" können Benutzer Unterressourcen-Berechtigungen unter bestimmten Bedingungen umgehen.

Beachten Sie beispielsweise die folgende ressourcenbasierte Richtlinie:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::123456789012:user/test-user"
        ]
      },
      "Action": [
        "es:ESHttp*"
      ],
      "Resource": [
        "arn:aws:es:us-west-1:987654321098:domain/test-domain/test-index/*",
        "arn:aws:es:us-west-1:987654321098:domain/test-domain/_bulk"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::123456789012:user/test-user"
        ]
      },
      "Action": [
        "es:ESHttpGet"
      ],
      "Resource": "arn:aws:es:us-west-1:987654321098:domain/test-domain/
restricted-index/*"
    }
  ]
}
```

Diese Richtlinie gewährt `test-user` vollen Zugriff auf `test-index` und die OpenSearch Bulk-API. Außerdem ermöglicht sie GET-Anforderungen an `restricted-index`.

Wie zu erwarten, schlägt die folgende Indizierungsanforderung aufgrund eines Berechtigungsfehlers fehl:

```
PUT https://search-test-domain.us-west-1.es.amazonaws.com/restricted-index/movie/1
{
  "title": "Your Name",
  "director": "Makoto Shinkai",
  "year": "2016"
}
```

Im Gegensatz zur Index-API ermöglicht Ihnen die Massen-API, in einem einzelnen Aufruf viele Dokumente zu erstellen, zu aktualisieren und zu löschen. Sie geben diese Operationen jedoch oft im Anforderungstext anstatt in der Anforderungs-URL an. Da OpenSearch Service URLs den Zugriff auf Domain-Subressourcen steuert, `test-user` kann er tatsächlich die Bulk-API verwenden, um Änderungen daran vorzunehmen. `restricted-index` Auch wenn der Benutzer über keine `POST`-Berechtigungen für den Index verfügt, ist die folgende Anforderung erfolgreich:

```
POST https://search-test-domain.us-west-1.es.amazonaws.com/_bulk
{ "index" : { "_index": "restricted-index", "_type" : "movie", "_id" : "1" } }
{ "title": "Your Name", "director": "Makoto Shinkai", "year": "2016" }
```

In diesem Fall funktioniert die Zugriffsrichtlinie nicht wie beabsichtigt. Um Benutzer daran zu hindern, diese Arten von Einschränkungen zu umgehen, können Sie `rest.action.multi.allow_explicit_index` in „false" ändern. Wenn dieser Wert falsch ist, funktionieren alle Aufrufe von bulk, mget und msearch, die Indexnamen im Hauptteil der Anfrage angeben APIs , nicht mehr. Mit anderen Worten: Aufrufe an `_bulk` funktionieren nicht mehr, aber Aufrufe an `test-index/_bulk` sind hiervon nicht betroffen. Da dieser zweite Endpunkt einen Indexnamen enthält, müssen Sie im Anforderungstext keinen angeben.

OpenSearch Dashboards sind stark von mget und msearch abhängig, weshalb es nach dieser Änderung unwahrscheinlich ist, dass es ordnungsgemäß funktioniert. Bei teilweiser Korrektur können Sie den Wert auf „true“ `rest.action.multi.allow_explicit_index` belassen und bestimmten Benutzern den Zugriff auf eine oder mehrere dieser Optionen verweigern. APIs

Weitere Informationen zum Ändern dieser Einstellung finden Sie unter the section called “Erweiterte Clustereinstellungen”.

Dementsprechend enthalt die folgende ressourcenbasierte Richtlinie zwei geringfügige Probleme:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/test-user"
      },
```

```
      "Action": "es:ESHttp*",
      "Resource": "arn:aws:es:us-west-1:987654321098:domain/test-domain/*"
    },
    {
      "Effect": "Deny",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/test-user"
      },
      "Action": "es:ESHttp*",
      "Resource": "arn:aws:es:us-west-1:987654321098:domain/test-domain/
restricted-index/*"
    }
  ]
}
```

- Trotz der expliziten Verweigerung kann `test-user` weiterhin Aufrufe wie `GET https://search-test-domain.us-west-1.es.amazonaws.com/_all/_search` und `GET https://search-test-domain.us-west-1.es.amazonaws.com/*/_search` für den Zugriff auf die Dokumente in `restricted-index` ausführen.
- Da das `Resource`-Element auf `restricted-index/*` verweist, ist `test-user` nicht zum direkten Zugriff auf die Dokumente des Index berechtigt. Der Benutzer verfügt jedoch über Berechtigungen zum Löschen des gesamten Index. Damit der Zugriff und das Löschen verhindert werden, muss die Richtlinie stattdessen `restricted-index*` angeben.

Anstatt großzügige Berechtigungen und gezielte Verweigerungen miteinander zu mischen, ist eine sicherere Strategie, der Regel der geringsten Rechte zu folgen und nur die Berechtigungen zu gewähren, die zum Ausführen einer Aufgabe erforderlich sind. Weitere Informationen zur Steuerung des Zugriffs auf einzelne Indizes oder OpenSearch Operationen finden Sie unter. the section called “Differenzierte Zugriffskontrolle”

> **Important**
>
> Die Angabe des Platzhalters* ermöglicht den anonymen Zugriff auf Ihre Domain. Es wird nicht empfohlen, den Platzhalter zu verwenden. Überprüfen Sie außerdem sorgfältig die folgenden Richtlinien, um sicherzustellen, dass sie keinen breiten Zugriff gewähren:
>
> - Identitätsbasierte Richtlinien, die mit zugehörigen AWS Prinzipalen verknüpft sind (z. B. IAM-Rollen)

- Ressourcenbasierte Richtlinien, die mit zugehörigen AWS Ressourcen verknüpft sind (z. B. KMS-Schlüssel) AWS Key Management Service

Konfigurieren von Zugriffsrichtlinien

- Anweisungen zum Erstellen oder Ändern von ressourcen- und IP-basierten Richtlinien in OpenSearch Service finden Sie unter. the section called “Konfigurieren von Zugriffsrichtlinien”
- Anweisungen zum Erstellen oder Ändern identitätsbasierter Richtlinien in IAM finden Sie im IAM-Benutzerhandbuch unter Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien.

Zusätzliche Beispielrichtlinien

Obwohl dieses Kapitel viele Beispielrichtlinien enthält, ist die AWS Zugriffskontrolle ein komplexes Thema, das sich am besten anhand von Beispielen verstehen lässt. Weitere Informationen finden Sie unter Beispiel für identitätsbasierte IAM-Richtlinien im IAM-Benutzerhandbuch.

Referenz zu Amazon OpenSearch Service API-Berechtigungen

Wenn Sie die Zugriffskontrolle einrichten, schreiben Sie Berechtigungsrichtlinien, die Sie einer IAM-Identität zuordnen können (identitätsbasierte Richtlinien). Weitere Informationen finden Sie in den folgenden Themen in der Service-Authorization-Referenz:

- Aktionen, Ressourcen und Bedingungsschlüssel für den Service. OpenSearch
- Aktionen, Ressourcen und Bedingungsschlüssel für OpenSearch Ingestion.

Diese Referenz enthält Informationen darüber, welche -API-Operationen in einer IAM-Richtlinie verwendet werden können. Dazu gehören auch die AWS Ressource, für die Sie die Berechtigungen erteilen können, sowie Bedingungsschlüssel, die Sie für eine differenzierte Zugriffskontrolle verwenden können.

Sie geben die Aktionen im Feld `Action` der Richtlinie, den Ressourcenwert im Feld `Resource` der Richtlinie und die Bedingungen im Feld `Condition` der Richtlinie an. Um eine Aktion für OpenSearch Service anzugeben, verwenden Sie das `es:` Präfix, gefolgt vom Namen des API-Vorgangs (z. B.`es:CreateDomain`). Um eine Aktion für OpenSearch Ingestion anzugeben, verwenden Sie das `osis:` Präfix gefolgt von der API-Operation (z. B.`osis:CreatePipeline`).

AWS verwaltete Richtlinien für Amazon OpenSearch Service

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet wird AWS. AWS Verwaltete Richtlinien sind so konzipiert, dass sie Berechtigungen für viele gängige Anwendungsfälle bereitstellen, sodass Sie damit beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass AWS verwaltete Richtlinien für Ihre speziellen Anwendungsfälle möglicherweise keine Berechtigungen mit den geringsten Rechten gewähren, da sie allen AWS Kunden zur Verfügung stehen. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Sie können die in AWS verwalteten Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert werden, wirkt sich das Update auf alle Prinzidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWS aktualisiert eine AWS verwaltete Richtlinie höchstwahrscheinlich, wenn eine neue Richtlinie eingeführt AWS-Service wird oder neue API-Operationen für bestehende Dienste verfügbar werden.

Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien im IAM-Benutzerhandbuch.

AmazonOpenSearchDirectQueryGlueCreateAccess

Gewährt Amazon OpenSearch Service Direct Query Service Zugriff auf `CreateDatabaseCreatePartition`,`CreateTable`, und `BatchCreatePartition` AWS Glue API.

Sie finden die AmazonOpenSearchDirectQueryGlueCreateAccessRichtlinie in der IAM-Konsole.

AmazonOpenSearchServiceFullAccess

Gewährt vollen Zugriff auf die API-Operationen und Ressourcen der OpenSearch Dienstkonfiguration für einen AWS-Konto.

Sie finden die AmazonOpenSearchServiceFullAccessRichtlinie in der IAM-Konsole.

AmazonOpenSearchServiceReadOnlyAccess

Gewährt schreibgeschützten Zugriff auf alle OpenSearch Serviceressourcen für einen. AWS-Konto

Sie finden die AmazonOpenSearchServiceReadOnlyAccessRichtlinie in der IAM-Konsole.

AmazonOpenSearchServiceRolePolicy

Sie können `AmazonOpenSearchServiceRolePolicy` nicht an Ihre IAM-Entitäten anhängen. Diese Richtlinie ist einer dienstbezogenen Rolle zugeordnet, die es dem OpenSearch Service ermöglicht, auf Kontoressourcen zuzugreifen. Weitere Informationen finden Sie unter the section called “Berechtigungen”.

Sie finden die AmazonOpenSearchServiceRolePolicyRichtlinie in der IAM-Konsole.

AmazonOpenSearchServiceCognitoAccess

Bietet die Mindestberechtigungen für Amazon Cognito, die erforderlich sind, um die Cognito-Authentifizierung zu aktivieren.

Sie finden die AmazonOpenSearchServiceCognitoAccessRichtlinie in der IAM-Konsole.

AmazonOpenSearchIngestionServiceRolePolicy

Sie können `AmazonOpenSearchIngestionServiceRolePolicy` nicht an Ihre IAM-Entitäten anhängen. Diese Richtlinie ist mit einer serviceverknüpften Rolle verknüpft, die es OpenSearch Ingestion ermöglicht, VPC-Zugriff für Erfassungspipelines zu aktivieren, Tags zu erstellen und aufnahmebezogene Metriken für Ihr Konto zu veröffentlichen. CloudWatch Weitere Informationen finden Sie unter the section called “Verwenden von serviceverknüpften Rollen”.

Sie finden die Richtlinie in der IAM-Konsole. AmazonOpenSearchIngestionServiceRolePolicy

OpenSearchIngestionSelfManagedVpcePolicy

Sie können `OpenSearchIngestionSelfManagedVpcePolicy` nicht an Ihre IAM-Entitäten anhängen. Diese Richtlinie ist mit einer serviceverknüpften Rolle verknüpft, die es OpenSearch Ingestion ermöglicht, selbstverwalteten VPC-Zugriff für Erfassungspipelines zu aktivieren, Tags zu erstellen und aufnahmebezogene Metriken für Ihr Konto zu veröffentlichen. CloudWatch Weitere Informationen finden Sie unter the section called “Verwenden von serviceverknüpften Rollen”.

OpenSearchIngestionSelfManagedVpcePolicySie finden die Richtlinie in der IAM-Konsole.

AmazonOpenSearchIngestionFullAccess

Gewährt vollen Zugriff auf die Operationen und Ressourcen der OpenSearch Ingestion-API für einen. AWS-Konto

Sie finden die AmazonOpenSearchIngestionFullAccessRichtlinie in der IAM-Konsole.

AmazonOpenSearchIngestionReadOnlyAccess

Gewährt schreibgeschützten Zugriff auf alle OpenSearch Ingestion-Ressourcen für einen. AWS-Konto

Sie finden die AmazonOpenSearchIngestionReadOnlyAccessRichtlinie in der IAM-Konsole.

AmazonOpenSearchServerlessServiceRolePolicy

Stellt die Amazon CloudWatch Mindestberechtigungen bereit, die erforderlich sind, um OpenSearch serverlose Metrikdaten an zu senden. CloudWatch

Sie finden die AmazonOpenSearchServerlessServiceRolePolicyRichtlinie in der IAM-Konsole.

OpenSearch Service-Updates für AWS verwaltete Richtlinien

Sehen Sie sich Details zu Aktualisierungen der AWS verwalteten Richtlinien für OpenSearch Service an, seit dieser Dienst mit der Nachverfolgung von Änderungen begonnen hat.

Änderung	Beschreibung	Datum
Das wurde aktualisiert `AmazonOpenSearchServiceRolePolicy`	Der Richtlinie wurde die folgende Erklärung hinzugefügt. Wenn Amazon OpenSearch Service die `AWSServiceRoleForAmazonOpenSearchService` dienstbezogene Rolle übernimmt, ermöglicht diese neue Erklärung in der Richtlinie, den Zugriffsbereich jeder AWS IAM Identity Center Anwendung OpenSearch zu aktualisieren, die nur von OpenSearch verwaltet wird. `{ "Effect": "Allow",`	31. März 2025

Änderung	Beschreibung	Datum
	"Action": "sso:PutApplicationAccessScope", "Resource": "arn:aws:sso::*:application/*/*", "Condition": { "StringEquals": { "aws:ResourceOrgID": "${aws:PrincipalOrgID}" } } }	
`AmazonOpenSearchServerlessServiceRolePolicy` aktualisiert	Der Sid wurde `AllowAOSSCloudwatchMetrics` der Richtlinie hinzugefügt`AmazonOpenSearchServerlessServiceRolePolicy` . Eine Sid ist eine Anweisungs-ID, die als optionale Kennung für die Richtlinienanweisung dient.	12. Juli 2024

Änderung	Beschreibung	Datum
`OpenSearchIngestionSelfManagedVpcePolicy` hinzugefügt	Eine neue Richtlinie, die es OpenSearch Ingestion ermöglicht, selbstverwalteten VPC-Zugriff für Erfassungspipelines zu aktivieren, Tags zu erstellen und aufnahmebezogene Metriken in Ihrem Konto zu veröffentlichen. CloudWatch Informationen zum Richtlinien-JSON finden Sie unter IAM-Konsole.	12. Juni 2024
Hinzugefügt `AmazonOpenSearchDirectQueryGlueCreateAccess`	Gewährt Amazon OpenSearch Service Direct Query Service Zugriff auf `CreateDatabase` `CreatePartition` ,`CreateTable` , und `BatchCreatePartition` AWS Glue API.	6. Mai 2024

Änderung	Beschreibung	Datum
`AmazonOpenSearchServiceRolePolicy` und `AmazonElasticsearchServiceRolePolicy` wurden aktualisiert	Die für die dienstbezogene Rolle erforderlichen Berechtigungen zum Zuweisen und Aufheben IPv6 der Zuweisung von Adressen wurden hinzugefügt. Die veraltete Elasticsearch-Richtlinie wurde ebenfalls aktualisiert, um die Abwärtskompatibilität sicherzustellen.	18. Oktober 2023
`AmazonOpenSearchIngestionServiceRolePolicy` hinzugefügt	Eine neue Richtlinie, die es OpenSearch Ingestion ermöglicht, den VPC-Zugriff für Erfassungspipelines zu aktivieren, Tags zu erstellen und aufnahmebezogene Metriken in Ihrem Konto zu veröffentlichen. CloudWatch Informationen zum Richtlinien-JSON finden Sie unter IAM-Konsole.	26. April 2023
`AmazonOpenSearchIngestionFullAccess` hinzugefügt	Eine neue Richtlinie, die vollen Zugriff auf die Operationen und Ressourcen der OpenSearch Ingestion-API für einen gewährt. AWS-Konto Informationen zum Richtlinien-JSON finden Sie unter IAM-Konsole.	26. April 2023

Änderung	Beschreibung	Datum
`AmazonOpenSearchIngestionReadOnlyAccess` hinzugefügt	Eine neue Richtlinie, die Lesezugriff auf alle OpenSearch Ingestion -Ressourcen für einen gewährt. AWS-Konto Informationen zum Richtlinien-JSON finden Sie unter IAM-Konsole.	26. April 2023
`AmazonOpenSearchServerlessServiceRolePolicy` hinzugefügt	Eine neue Richtlinie, die die Mindestberechtigungen bereitstellt, die erforderlich sind, um OpenSearch serverlose Metrikdaten an zu Amazon CloudWatch senden. Informationen zum Richtlinien-JSON finden Sie unter IAM-Konsole.	29. November 2022

Änderung	Beschreibung	Datum
`AmazonOpenSearchServiceRolePolicy` und `AmazonElasticsearchServiceRolePolicy` wurden aktualisiert	Es wurden die Berechtigungen hinzugefügt, die für die serviceverknüpfte Rolle erforderlich sind, um vom OpenSearch Service verwaltete VPC-Endpunkte zu erstellen. Einige Aktionen können nur ausgeführt werden, wenn die Anforderung das Tag `OpenSearchManaged=true` enthält. Die veraltete Elasticsearch-Richtlinie wurde ebenfalls aktualisiert, um die Abwärtskompatibilität sicherzustellen.	7. November 2022
`AmazonOpenSearchServiceRolePolicy` und `AmazonElasticsearchServiceRolePolicy` wurden aktualisiert	Unterstützung für die `PutMetricData` Aktion hinzugefügt, die für die Veröffentlichung von OpenSearch Cluster-Metriken auf Amazon erforderlich ist CloudWatch. Die veraltete Elasticsearch-Richtlinie wurde ebenfalls aktualisiert, um die Abwärtskompatibilität sicherzustellen. Informationen zum Richtlinien-JSON finden Sie unter IAM-Konsole.	12. September 2022

Änderung	Beschreibung	Datum
`AmazonOpenSearchServiceRolePolicy` und `AmazonElasticsearchServiceRolePolicy` wurden aktualisiert	Unterstützung für den Ressourcentyp `acm` hinzugefügt. Die Richtlinie bietet die Mindestberechtigung AWS Certificate Manager (ACM), die für die serviceverknüpfte Rolle erforderlich ist, um ACM-Ressourcen zu verifizieren und zu validieren, um benutzerdefinierte Domänen mit aktivierten Endpunkten zu erstellen und zu aktualisieren. Die veraltete Elasticsearch-Richtlinie wurde ebenfalls aktualisiert, um die Abwärtskompatibilität sicherzustellen.	28. Juli 2022

Änderung	Beschreibung	Datum
`AmazonOpenSearchServiceCognitoAccess` und `AmazonESCognitoAccess` wurden aktualisiert	Unterstützung für die `UpdateUserPoolClient` Aktion hinzugefügt, die erforderlich ist, um die Cognito-Benutzerpool-Konfiguration während des Upgrades von Elasticsearch auf festzulegen. OpenSearch Korrigierte Berechtigungen für die `SetIdentityPoolRoles` -Aktion, um Zugriff auf alle Ressourcen zu gewähren. Die veraltete Elasticsearch-Richtlinie wurde ebenfalls aktualisiert, um die Abwärtskompatibilität sicherzustellen.	20. Dezember 2021
`AmazonOpenSearchServiceRolePolicy` aktualisiert	Unterstützung für den Ressourcentyp `security-group` hinzugefügt. Die Richtlinie bietet die Mindestberechtigungen für Amazon EC2 und Elastic Load Balancing, die für die serviceverknüpfte Rolle erforderlich sind, um den VPC-Zugriff zu ermöglichen.	9. September 2021

Änderung	Beschreibung	Datum
• `AmazonOpenSearchServiceFullAccess` hinzugefügt • `AmazonESFullAccess` – Veraltet	Diese neue Richtlinie soll die alte Richtlinie ersetzen. Beide Richtlinien bieten vollen Zugriff auf die OpenSearch Service-Konfigurations-API und alle HTTP-Methoden für. OpenSearch APIs Feinkörnige Zugriffssteuerung und ressourcenbasierte Richtlinien können den Zugriff weiterhin einschränken.	7. September 2021
• `AmazonOpenSearchServiceReadOnlyAccess` hinzugefügt • `AmazonESReadOnlyAccess` – Veraltet	Diese neue Richtlinie soll die alte Richtlinie ersetzen. Beide Richtlinien bieten nur Lesezugriff auf die OpenSearch Dienstkonfigurations-API (`es:Describe* es:List*`, und`es:Get*`) und keinen Zugriff auf die HTTP-Methoden für. OpenSearch APIs	7. September 2021
• `AmazonOpenSearchServiceCognitoAccess` hinzugefügt • `AmazonESCognitoAccess` – Veraltet	Diese neue Richtlinie soll die alte Richtlinie ersetzen. Beide Richtlinien bieten die Mindestberechtigungen für Amazon Cognito, die erforderlich sind, um die Cognito-Authentifizierung zu aktivieren.	7. September 2021

Änderung	Beschreibung	Datum
• AmazonOpenSearchServiceRolePolicy hinzugefügt • `AmazonElasticsearchServiceRolePolicy` – Veraltet	Diese neue Richtlinie soll die alte Richtlinie ersetzen. Beide Richtlinien bieten die Mindestberechtigungen für Amazon EC2 und Elastic Load Balancing, die für die serviceverknüpfte Rolle erforderlich sind, um den VPC-Zugriff zu ermöglichen.	7. September 2021
Änderungsverfolgung gestartet	Amazon OpenSearch Service verfolgt jetzt Änderungen an AWS verwalteten Richtlinien.	7. September 2021

Serviceübergreifende Confused-Deputy-Prävention

Das Problem des verwirrten Stellvertreters ist ein Sicherheitsproblem, bei dem eine Entität, die keine Berechtigung zur Durchführung einer Aktion hat, eine privilegiertere Entität zur Durchführung der Aktion zwingen kann. Serviceübergreifender Identitätswechsel kann zum Problem des verwirrten Stellvertreters führen. AWS Ein dienstübergreifender Identitätswechsel kann auftreten, wenn ein Dienst (der Anruf-Dienst) einen anderen Dienst anruft (den aufgerufenen Dienst). Der aufrufende Service kann manipuliert werden, um seine Berechtigungen zu verwenden, um Aktionen auf die Ressourcen eines anderen Kunden auszuführen, für die er sonst keine Zugriffsberechtigung haben sollte. Um dies zu verhindern, bietet AWS Tools, mit denen Sie Ihre Daten für alle Services mit Serviceprinzipalen schützen können, die Zugriff auf Ressourcen in Ihrem Konto erhalten haben.

Wir empfehlen, die Kontextschlüssel `aws:SourceArn` und die `aws:SourceAccount` globalen Bedingungsschlüssel in Ressourcenrichtlinien zu verwenden, um die Berechtigungen einzuschränken, die Amazon OpenSearch Service einem anderen Service für die Ressource erteilt. Wenn der `aws:SourceArn`-Wert die Konto-ID nicht enthält, z. B. einen Amazon-S3-Bucket-ARN, müssen Sie beide globale Bedingungskontextschlüssel verwenden, um Berechtigungen einzuschränken. Wenn Sie beide globale Bedingungskontextschlüssel verwenden und der `aws:SourceArn`-Wert die Konto-ID enthält, müssen der `aws:SourceAccount`-Wert und

das Konto im `aws:SourceArn`-Wert dieselbe Konto-ID verwenden, wenn sie in der gleichen Richtlinienanweisung verwendet wird. Verwenden Sie `aws:SourceArn`, wenn Sie nur eine Ressource mit dem betriebsübergreifenden Zugriff verknüpfen möchten. Verwenden Sie `aws:SourceAccount`, wenn Sie zulassen möchten, dass Ressourcen in diesem Konto mit der betriebsübergreifenden Verwendung verknüpft werden.

Der Wert von `aws:SourceArn` muss der ARN der OpenSearch Service-Domain sein.

Der effektivste Weg, um sich vor dem Confused-Deputy-Problem zu schützen, ist die Verwendung des globalen Bedingungskontext-Schlüssels `aws:SourceArn` mit dem vollständigen ARN der Ressource. Wenn Sie den vollständigen ARN der Ressource nicht kennen oder wenn Sie mehrere Ressourcen angeben, verwenden Sie den globalen Bedingungskontext-Schlüssel `aws:SourceArn` mit Platzhaltern (*) für die unbekannten Teile des ARN. Beispiel, `arn:aws:es:*:123456789012:*`.

Das folgende Beispiel zeigt, wie Sie die Kontextschlüssel `aws:SourceArn` und die `aws:SourceAccount` globalen Bedingungsschlüssel in OpenSearch Service verwenden können, um das Problem des verwirrten Stellvertreters zu verhindern.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":{
      "Sid":"ConfusedDeputyPreventionExamplePolicy",
      "Effect":"Allow",
      "Principal":{
         "Service":"es.amazonaws.com"
      },
      "Action":"sts:AssumeRole",
      "Condition":{
         "StringEquals":{
            "aws:SourceAccount":"123456789012"
         },
         "ArnLike":{
            "aws:SourceArn":"arn:aws:es:region:123456789012:domain/my-domain"
         }
      }
   }
}
```

Feinkörnige Zugriffskontrolle in Amazon Service OpenSearch

Eine detaillierte Zugriffskontrolle bietet zusätzliche Möglichkeiten, den Zugriff auf Ihre Daten bei Amazon OpenSearch Service zu kontrollieren. Je nachdem, wer die Anforderung ausstellt, kann es sein, dass eine Suche Ergebnisse aus nur einem Index zurückgibt. Sie können bestimmte Felder in Ihren Dokumenten ausblenden oder bestimmte Dokumente ganz ausschließen.

Die differenzierte Zugriffskontrolle bietet folgende Nutzen:

- Rollenbasierte Zugriffskontrolle
- Sicherheit auf Index-, Dokument- und Feldebene
- OpenSearch Dashboards, Mehrmandantenfähigkeit
- HTTP-Basisauthentifizierung für und Dashboards OpenSearch OpenSearch

Themen

- Das Gesamtbild: detaillierte Zugriffskontrolle und Servicesicherheit OpenSearch
- Die wichtigsten Konzepte
- Über den Masterbenutzer
- Aktivieren der differenzierten Zugriffskontrolle
- Als Masterbenutzer auf OpenSearch Dashboards zugreifen
- Verwalten von Berechtigungen
- Empfohlene Konfigurationen
- Einschränkungen
- Hauptbenutzer ändern
- Zusätzliche Hauptbenutzer
- Manuelle Snapshots
- Integrationen
- REST-API-Unterschiede
- Tutorial: Konfigurieren einer Domain mit einem IAM-Hauptbenutzer und Amazon-Cognito-Authentifizierung
- Tutorial: Konfigurieren einer Domain mit der internen Benutzerdatenbank und HTTP-Basisauthentifizierung

Das Gesamtbild: detaillierte Zugriffskontrolle und Servicesicherheit OpenSearch

Die Sicherheit von Amazon OpenSearch Service besteht aus drei Hauptebenen:

Netzwerk

Die erste Sicherheitsebene ist das Netzwerk, das bestimmt, ob Anfragen eine OpenSearch Service-Domain erreichen. Wenn Sie beim Erstellen einer Domain Öffentlichen Zugriff auswählen, können Anforderungen von jedem mit dem Internet verbundenen Client den Domain-Endpunkt erreichen. Wenn Sie VPC-Zugriff auswählen, müssen Clients eine Verbindung zur VPC herstellen (und die zugeordneten Sicherheitsgruppen müssen dies zulassen), damit eine Anforderung den Endpunkt erreichen kann. Weitere Informationen finden Sie unter the section called “VPC-Unterstützung”.

Domain-Zugriffsrichtlinie

Die zweite Sicherheitsebene ist die Domain-Zugriffsrichtlinie. Nachdem eine Anforderung einen Domain-Endpunkt erreicht hat, erlaubt oder verweigert die ressourcenbasierte Zugriffsrichtlinie den Anforderungszugriff auf einen bestimmten URI. Die Zugriffsrichtlinie akzeptiert oder lehnt Anforderungen am „Rand“ der Domäne ab, bevor sie OpenSearch selbst erreichen.

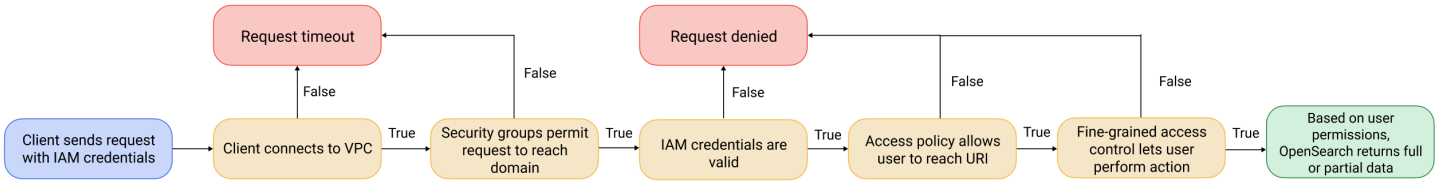
Differenzierte Zugriffskontrolle

Die dritte und letzte Sicherheitsebene ist eine differenzierte Zugriffskontrolle. Nachdem eine ressourcenbasierte Zugriffsrichtlinie eine Anforderung einen Domain-Endpunkt erreichen lässt, werden die Benutzeranmeldeinformationen durch eine differenzierte Zugriffskontrolle ausgewertet und entweder der Benutzer authentifiziert oder die Anforderung verweigert. Wenn eine differenzierte Zugriffskontrolle Zugriffssteuerung den Benutzer authentifiziert, ruft sie alle dem Benutzer zugeordneten Rollen ab und verwendet den vollständigen Satz von Berechtigungen, um zu bestimmen, wie die Anforderung behandelt werden soll.

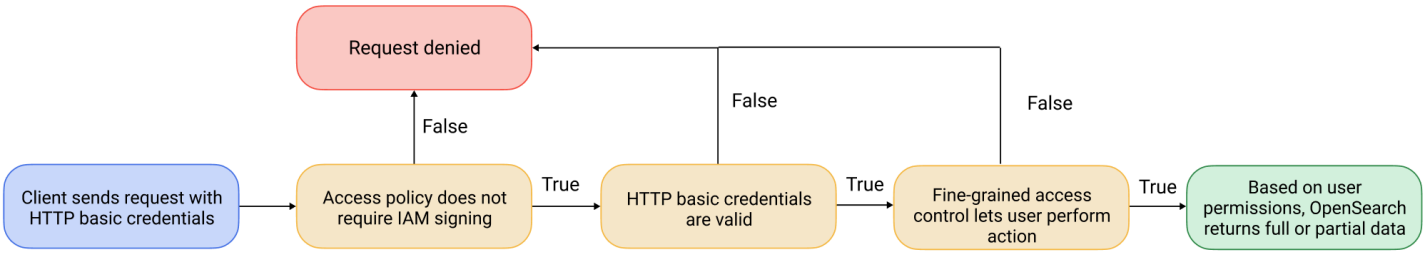
> **Note**
>
> Wenn eine ressourcenbasierte Zugriffsrichtlinie IAM-Rollen oder -Benutzer enthält, müssen Clients signierte Anfragen mit AWS Signature Version 4 senden. Daher können Zugriffsrichtlinien in Konflikt mit einer differenzierten Zugriffskontrolle stehen, insbesondere

wenn Sie die interne Benutzerdatenbank und die HTTP-Standardauthentifizierung verwenden. Sie können eine Anfrage nicht mit einem Benutzernamen und einem Passwort sowie mit IAM-Anmeldeinformationen signieren. Wenn Sie die differenzierte Zugriffskontrolle aktivieren, wird im Allgemeinen empfohlen, eine Domain-Zugriffsrichtlinie zu verwenden, die keine signierten Anforderungen erfordert.

Das folgende Diagramm veranschaulicht eine typische Konfiguration: eine VPC-Zugriff-Domain mit aktivierter differenzierter Zugriffskontrolle, eine IAM-basierte Zugriffsrichtlinie und ein IAM-Master-Benutzer.



Das folgende Diagramm veranschaulicht eine weitere typische Konfiguration: eine öffentliche Zugriff-Domain mit aktivierter differenzierter Zugriffskontrolle, eine Zugriffsrichtlinie, die keine IAM-Prinzipale verwendet, und ein Master-Benutzer in der internen Benutzerdatenbank.



Beispiel

Nehmen wir eine GET-Anfrage an `movies/_search?q=thor` an. Hat der Benutzer die Berechtigung, den `movies`-Index zu durchsuchen? Wenn ja: Hat der Benutzer die Berechtigung, alle darin befindlichen Dokumente anzuzeigen? Sollte die Antwort Felder auslassen oder anonymisieren? Für den Master-Benutzer könnte die Antwort folgendermaßen aussehen:

```
{
  "hits": {
    "total": 7,
    "max_score": 8.772789,
    "hits": [{
        "_index": "movies",
```

```
        "_type": "_doc",
        "_id": "tt0800369",
        "_score": 8.772789,
        "_source": {
          "directors": [
            "Kenneth Branagh",
            "Joss Whedon"
          ],
          "release_date": "2011-04-21T00:00:00Z",
          "genres": [
            "Action",
            "Adventure",
            "Fantasy"
          ],
          "plot": "The powerful but arrogant god Thor is cast out of Asgard to
 live amongst humans in Midgard (Earth), where he soon becomes one of their finest
 defenders.",
          "title": "Thor",
          "actors": [
            "Chris Hemsworth",
            "Anthony Hopkins",
            "Natalie Portman"
          ],
          "year": 2011
        }
      },
      ...
    ]
  }
}
```

Wenn ein Benutzer mit eingeschränkten Berechtigungen genau dieselbe Anforderung ausgibt, könnte die Antwort folgendermaßen aussehen:

```
{
  "hits": {
    "total": 2,
    "max_score": 8.772789,
    "hits": [{
        "_index": "movies",
        "_type": "_doc",
        "_id": "tt0800369",
        "_score": 8.772789,
```

```
        "_source": {
          "year": 2011,
          "release_date":
 "3812a72c6dd23eef3c750c2d99e205cbd260389461e19d610406847397ecb357",
          "plot": "The powerful but arrogant god Thor is cast out of Asgard to
 live amongst humans in Midgard (Earth), where he soon becomes one of their finest
 defenders.",
          "title": "Thor"
        }
      },
      ...
    ]
  }
}
```

Die Antwort hat weniger Treffer und weniger Felder für jeden Treffer. Außerdem ist das `release_date`-Feld anonymisiert. Wenn ein Benutzer ohne Berechtigungen dieselbe Anforderung stellt, gibt der Cluster einen Fehler zurück:

```
{
  "error": {
    "root_cause": [{
      "type": "security_exception",
      "reason": "no permissions for [indices:data/read/search] and User [name=limited-
user, roles=[], requestedTenant=null]"
    }],
    "type": "security_exception",
    "reason": "no permissions for [indices:data/read/search] and User [name=limited-
user, roles=[], requestedTenant=null]"
  },
  "status": 403
}
```

Wenn ein Benutzer ungültige Anmeldeinformationen bereitstellt, gibt der Cluster eine `Unauthorized`-Ausnahme zurück.

Die wichtigsten Konzepte

Wenn Sie mit der detaillierten Zugriffskontrolle beginnen, sollten Sie die folgenden Konzepte berücksichtigen:

- Rollen — Die wichtigste Methode zur Verwendung einer differenzierten Zugriffskontrolle. In diesem Fall unterscheiden sich die Rollen von IAM-Rollen. Rollen enthalten eine beliebige Kombination von Berechtigungen: clusterweit, indexspezifisch, auf Dokumentebene oder auf Feldebene.
- Zuordnung — Nachdem Sie eine Rolle konfiguriert haben, ordnen Sie sie einem oder mehreren Benutzern zu. Beispielsweise können Sie einem einzelnen Benutzer drei Rollen zuordnen: eine Rolle, die Zugriff auf Dashboards bietet, eine mit schreibgeschütztem Zugriff auf `index1` und eine mit Schreibzugriff auf `index2`. Sie können auch alle diese Berechtigungen in eine einzige Rolle aufnehmen.
- Benutzer — Personen oder Anwendungen, die Anfragen an den OpenSearch Cluster stellen. Benutzer verfügen über Anmeldeinformationen — entweder IAM-Zugriffsschlüssel oder einen Benutzernamen und ein Passwort —, die sie angeben, wenn sie Anfragen stellen.

Über den Masterbenutzer

Der Masterbenutzer in OpenSearch Service ist entweder eine Kombination aus Benutzername und Passwort oder ein IAM-Prinzipal, der über vollständige Berechtigungen für den zugrunde liegenden OpenSearch Cluster verfügt. Ein Benutzer gilt als Masterbenutzer, wenn er uneingeschränkten Zugriff auf den OpenSearch Cluster hat und über die Möglichkeit verfügt, interne Benutzer, Rollen und Rollenzuordnungen in Dashboards zu erstellen. OpenSearch

Ein in der OpenSearch Service Console oder über die CLI erstellter Masterbenutzer wird automatisch zwei vordefinierten Rollen zugeordnet:

- `all_access`— Bietet vollen Zugriff auf alle clusterweiten Operationen, Schreibberechtigungen für alle Clusterindizes und Schreibberechtigungen für alle Mandanten.
- `security_manager`— Ermöglicht den Zugriff auf das Security-Plugin und die Verwaltung von Benutzern und Berechtigungen.

Mit diesen beiden Rollen erhält der Benutzer Zugriff auf die Registerkarte Sicherheit in OpenSearch Dashboards, wo er Benutzer und Berechtigungen verwalten kann. Wenn Sie einen weiteren internen Benutzer erstellen und ihn nur der `all_access` Rolle zuordnen, hat der Benutzer keinen Zugriff auf den Tab Sicherheit. Sie können zusätzliche Masterbenutzer erstellen, indem Sie sie explizit `all_access` sowohl den `security_manager` Rollen als auch zuordnen. Detaillierte Anweisungen finden Sie unter the section called “Zusätzliche Hauptbenutzer”.

Wenn Sie einen Masterbenutzer für Ihre Domain erstellen, können Sie entweder einen vorhandenen IAM-Prinzipal angeben oder einen Masterbenutzer in der internen Benutzerdatenbank erstellen. Beachten Sie bei der Entscheidung, welche Sie verwenden möchten, Folgendes:

- IAM-Prinzipal — Wenn Sie einen IAM-Prinzipal für Ihren Masterbenutzer wählen, müssen alle Anfragen an den Cluster mit AWS Signature Version 4 signiert werden.

  OpenSearch Der Service berücksichtigt keine der Berechtigungen des IAM-Prinzipals. Der IAM-Benutzer oder die IAM-Rolle dient ausschließlich der Authentifizierung. Die Richtlinien für diesen Benutzer oder diese Rolle haben keinen Einfluss auf die Autorisierung des Masterbenutzers. Die Autorisierung erfolgt über die verschiedenen Berechtigungen im OpenSearch Security-Plugin.

  Sie können beispielsweise einem IAM-Prinzipal keine IAM-Berechtigungen zuweisen, und solange sich der Computer oder die Person bei diesem Benutzer oder dieser Rolle authentifizieren kann, hat sie die Macht des Masterbenutzers in Service. OpenSearch

  Wir empfehlen IAM, wenn Sie dieselben Benutzer auf mehreren Clustern verwenden möchten, wenn Sie Amazon Cognito für den Zugriff auf Dashboards verwenden möchten oder wenn Sie OpenSearch Clients haben, die Signature Version 4-Signaturen unterstützen.
- Interne Benutzerdatenbank — Wenn Sie in der internen Benutzerdatenbank einen Master erstellen (mit einer Kombination aus Benutzername und Passwort), können Sie die HTTP-Basisauthentifizierung (sowie IAM-Anmeldeinformationen) verwenden, um Anfragen an den Cluster zu stellen. Die meisten Clients unterstützen die Standardauthentifizierung, einschließlich Curl, die auch AWS Signature Version 4 mit der Option --aws-sigv4 unterstützt. Die interne Benutzerdatenbank wird in einem OpenSearch Index gespeichert, sodass Sie sie nicht mit anderen Clustern teilen können.

  Wir empfehlen die interne Benutzerdatenbank, wenn Sie Benutzer nicht über mehrere Cluster hinweg wiederverwenden müssen, wenn Sie HTTP-Standardauthentifizierung für den Zugriff auf Dashboards verwenden möchten (statt Amazon Cognito), oder wenn Sie Clients haben, die nur die Standardauthentifizierung unterstützen. Die interne Benutzerdatenbank ist der einfachste Weg, um mit OpenSearch Service zu beginnen.

Aktivieren der differenzierten Zugriffskontrolle

Ermöglichen Sie eine detaillierte Zugriffskontrolle mithilfe der Konsole oder der Konfigurations-API. AWS CLI Informationen zu den erforderlichen Schritten finden Sie unter Erstellen und Verwalten von Domains.

Für eine detaillierte Zugriffskontrolle ist Elasticsearch 6.7 OpenSearch oder höher erforderlich. Außerdem sind HTTPS für den gesamten Datenverkehr zur Domain, Verschlüsselung ruhender Daten und Verschlüsselung erforderlich. node-to-node Je nachdem, wie Sie die erweiterten Funktionen der detaillierten Zugriffskontrolle konfigurieren, kann die zusätzliche Verarbeitung Ihrer Anfragen Rechen- und Speicherressourcen auf einzelnen Datenknoten erfordern. Nachdem Sie die differenzierte Zugriffskontrolle aktiviert haben, können Sie sie nicht mehr deaktivieren.

Aktivieren der differenzierten Zugriffskontrolle für vorhandene Domains

Sie können eine differenzierte Zugriffskontrolle für bestehende Domains aktivieren, auf denen Elasticsearch 6.7 OpenSearch oder höher ausgeführt wird.

So aktivieren Sie die differenzierte Zugriffskontrolle für eine vorhandene Domain (Konsole)

1. Wählen Sie die Domain aus und wählen Sie Aktionen und Sicherheitskonfiguration bearbeiten.
2. „True“ zur Aktivierung der differenzierten Zugriffskontrolle.
3. Auswahl zur Erstellung des Hauptbenutzers:

   - Wenn Sie IAM für die Benutzerverwaltung verwenden möchten, wählen Sie IAM-ARN als Haupt-Benutzer festlegen, und geben Sie den ARN für eine IAM-Rolle an.
   - Wenn Sie die interne Benutzerdatenbank verwenden möchten, wählen Sie Masterbenutzer erstellen und geben Sie einen Benutzernamen und ein Passwort an.
4. (Optional) Wählen Sie Migrationszeitraum für offene/IP-basierte Zugriffsrichtlinie aktivieren aus. Diese Einstellung aktiviert einen 30-tägigen Übergangszeitraum, in dem Ihre bestehenden Benutzer weiterhin ohne Unterbrechungen auf die Domain zugreifen können, sowie vorhandene offene und IP-basierte Zugriffsrichtlinien weiterhin mit Ihrer Domain arbeiten werden. Während diesem Migrationszeitraum empfehlen wir Administratoren, die notwendigen Rollen zu erstellen und diese Benutzern für die Domain zuzuordnen. Wenn Sie identitätsbasierte Richtlinien anstelle einer offenen oder IP-basierten Zugriffsrichtlinie verwenden, können Sie diese Einstellung deaktivieren.

   Sie müssen Ihre Clients ebenfalls aktualisieren, um während des Migrationszeitraums mit einer differenzierten Zugriffskontrolle arbeiten zu können. Wenn Sie beispielsweise IAM-Rollen mit detaillierter Zugriffskontrolle zuordnen, müssen Sie Ihre Clients aktualisieren, damit sie Anfragen mit AWS Signature Version 4 signieren können. Wenn Sie die HTTP-Standardauthentifizierung mit einer differenzierten Zugriffskontrolle konfigurieren, müssen Sie Ihre Clients aktualisieren, um in Anfragen entsprechende grundlegende Anmeldeinformationen zur Authentifizierung bereitzustellen.

Während der Migrationsphase landen Benutzer, die auf den OpenSearch Dashboards-Endpunkt für die Domain zugreifen, direkt auf der Discover-Seite und nicht auf der Anmeldeseite. Administratoren und Master-Benutzer können Anmeldung auswählen, um sich mit Administrator-Anmeldeinformationen anzumelden und das Rollen-Mapping zu konfigurieren.

> **Important**
>
> OpenSearch Der Service deaktiviert den Migrationszeitraum automatisch nach 30 Tagen. Wir empfehlen die Beendigung des Migrationszeitraums, sobald Sie die erforderlichen Rollen erstellt und sie Benutzern zugeordnet haben. Nach Beendigung des Migrationszeitraums können Sie ihn nicht erneut aktivieren.

5. Wählen Sie Änderungen speichern aus.

Die Änderung löst ein Blau/Grün-Bereitstellung aus, in der der Cluster-Zustand rot wird. Alle Cluster-Operationen bleiben davon jedoch unberührt.

So aktivieren Sie die differenzierte Zugriffskontrolle für eine vorhandene Domain (CLI)

Ändern Sie `AnonymousAuthEnabled` zu `true`, um den Migrationszeitraum mit einer differenzierten Zugriffskontrolle zu aktivieren:

```
aws opensearch update-domain-config --domain-name test-domain --region us-east-1 \
      --advanced-security-options '{ "Enabled": true,
 "InternalUserDatabaseEnabled":true, "MasterUserOptions": {"MasterUserName":"master-
username","MasterUserPassword":"master-password"},"AnonymousAuthEnabled": true}'
```

Über die Rolle „default_role“

Die differenzierte Zugriffskontrolle erfordert das Rollen-Mapping. Wenn Ihre Domain identitätsbasierte Zugriffsrichtlinien verwendet, ordnet OpenSearch Service Ihre Benutzer automatisch einer neuen Rolle namens default_role zu, um Sie bei der ordnungsgemäßen Migration vorhandener Benutzer zu unterstützen. Diese temporäre Zuordnung stellt sicher, dass Ihre Benutzer weiterhin erfolgreich IAM-signierte GET- und PUT-Anfragen senden können, bis Sie Ihr eigenes Rollen-Mapping erstellen.

Die Rolle fügt Ihrer Service-Domain keine Sicherheitslücken oder -mängel hinzu. OpenSearch Wir empfehlen die Löschung der Standardrolle, sobald Sie Ihre eigenen Rollen erstellt und entsprechend zugeordnet haben.

Migrationszenarien

In der folgenden Tabelle wird das Verhalten für jede Authentifizierungsmethode vor und nach dem Aktivieren der differenzierten Zugriffskontrolle für eine vorhandene Domain beschrieben und die Schritte, die Administratoren durchführen müssen, um ihre Benutzer ordnungsgemäß Rollen zuzuordnen:

Authentifizierungsmethode	Vor der Aktivierung der differenzierten Zugriffskontrolle	Nach der Aktivierung der differenzierten Zugriffskontrolle	Aufgaben des Administrators
Identitätsbasierte Richtlinien	Alle Benutzer, die die IAM-Richtlinie erfüllen, können auf die Domain zugreifen.	Sie müssen den Migrationszeitraum nicht aktivieren. OpenSearch Der Service ordnet automatisch alle Benutzer, die die IAM-Richtlinie erfüllen, der Rolle default_role zu, sodass sie weiterhin auf die Domain zugreifen können.	1. Benutzerdefiniertes Rollen-Mapping für die Domäne erstellen. 2. Löschen Sie die Rolle default_role.
IP-basierte Richtlinien	Alle Benutzer von den zulässigen IP-Adressen oder CIDR-Blöcken können auf die Domain zugreifen.	Während des 30-tägigen Migrationszeitraums können alle Benutzer von den zulässigen IP-Adressen oder CIDR-Blöcken weiterhin auf die Domain zugreifen.	1. Benutzerdefiniertes Rollen-Mapping für die Domain erstellen. 2. Aktualisieren Sie Ihre Clients, um je nach Konfiguration des Rollen-Mapping entweder Anmeldeinformationen für die grundlegende Authentifizierung oder IAM-Anmeldeinformationen bereitzustellen.

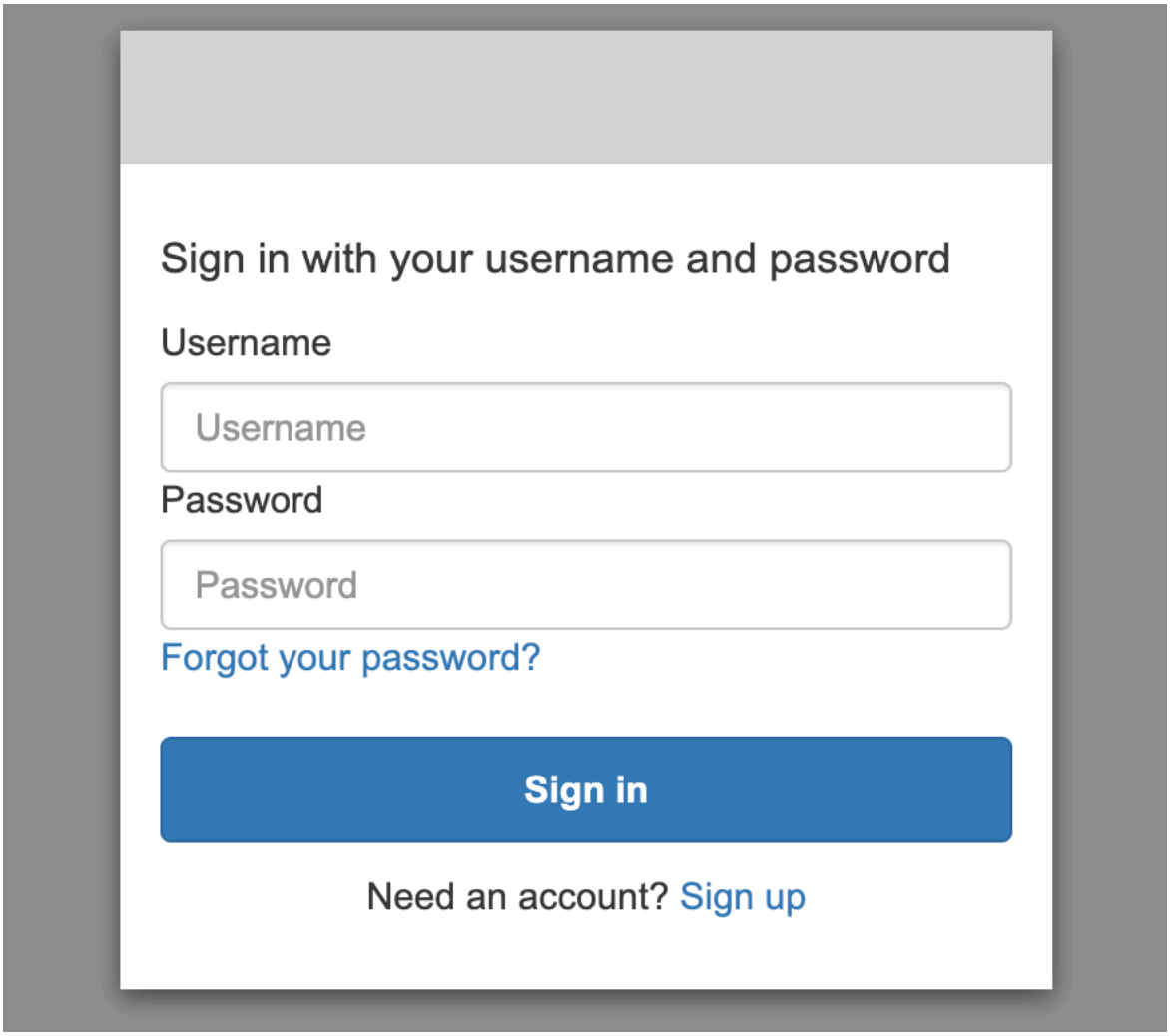
Authentifizierungsmethode	Vor der Aktivierung der differenzierten Zugriffskontrolle	Nach der Aktivierung der differenzierten Zugriffskontrolle	Aufgaben des Administrators
			3. Den Migrationszeitraum deaktivieren. Benutzer von den zulässigen IP-Adressen oder CIDR-Blöcken, die Anfragen ohne grundlegende Authentifizierung oder IAM-Anmeldeinformationen senden, verlieren den Zugriff auf die Domain.
Offene Zugriffsrichtlinien	Alle Benutzer im Internet können auf die Domain zugreifen.	Während des 30-tägigen Migrationszeitraums können alle Benutzer über das Internet weiterhin auf die Domain zugreifen.	1. Erstellen Sie Rollenzuordnungen in der Domain. 2. Aktualisieren Sie Ihre Clients, um je nach Konfiguration des Rollen-Mapping entweder Anmeldeinformationen für die grundlegende Authentifizierung oder IAM-Anmeldeinformationen bereitzustellen. 3. Den Migrationszeitraum deaktivieren. Benutzer, die Anfragen ohne grundlegende Authentifizierung oder IAM-Anmeldeinformationen senden, verlieren den Zugriff auf die Domain.

Als Masterbenutzer auf OpenSearch Dashboards zugreifen

Die differenzierte Zugriffskontrolle verfügt über ein OpenSearch Dashboards-Plugin, das Verwaltungsaufgaben vereinfacht. Mit Dashboards können Sie Benutzer, Rollen, Zuweisungen, Aktionsgruppen und Mandanten verwalten. Die Anmeldeseite von OpenSearch Dashboards und die zugrunde liegende Authentifizierungsmethode unterscheiden sich jedoch, je nachdem, wie Sie Benutzer verwalten und Ihre Domain konfiguriert haben.

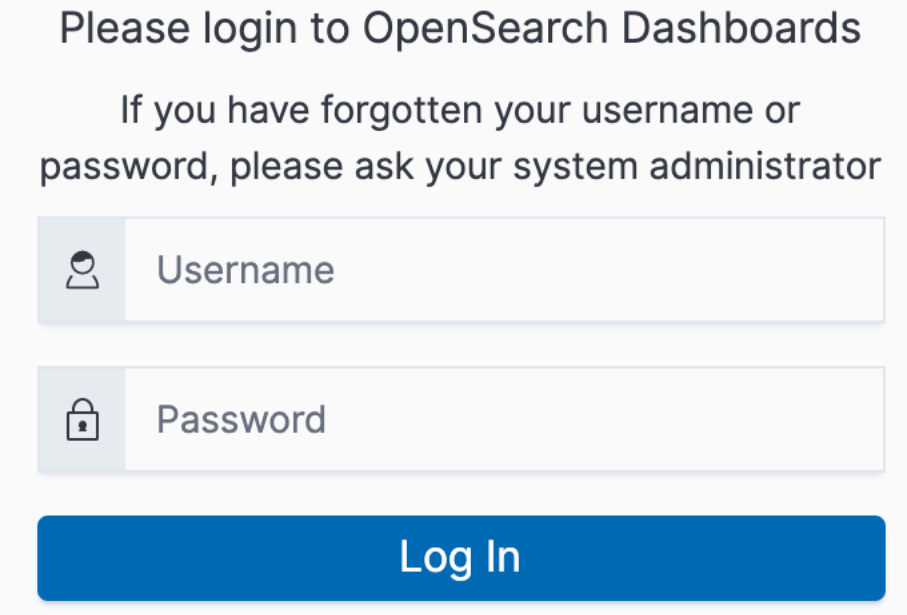
- Wenn Sie IAM für die Benutzerverwaltung verwenden möchten, verwenden Sie the section called “Amazon Cognito Cognito-Authentifizierung für Dashboards OpenSearch ”, um auf Dashboards zuzugreifen. Andernfalls zeigt Dashboards eine nicht funktionierende Anmeldeseite an. Siehe the section called “Einschränkungen”.

  Bei der Amazon-Cognito-Authentifizierung muss eine der angenommenen Rollen aus dem Identitätspool mit der IAM-Rolle übereinstimmen, die Sie für den Hauptbenutzer angegeben haben. Weitere Informationen zu dieser Konfiguration finden Sie unter the section called “(Optional) Konfigurieren von individuell festgelegtem Zugriff” und the section called “Tutorial: Detaillierte Zugriffskontrolle mit Cognito-Authentifizierung”.



- Wenn Sie die interne Benutzerdatenbank verwenden möchten, können Sie sich mit Ihrem Hauptbenutzernamen und Passwort bei Dashboards anmelden. Sie müssen über HTTPS auf Dashboards zugreifen. Amazon Cognito und SAML-Authentifizierung für Dashboards ersetzen beide diesen Anmeldebildschirm.

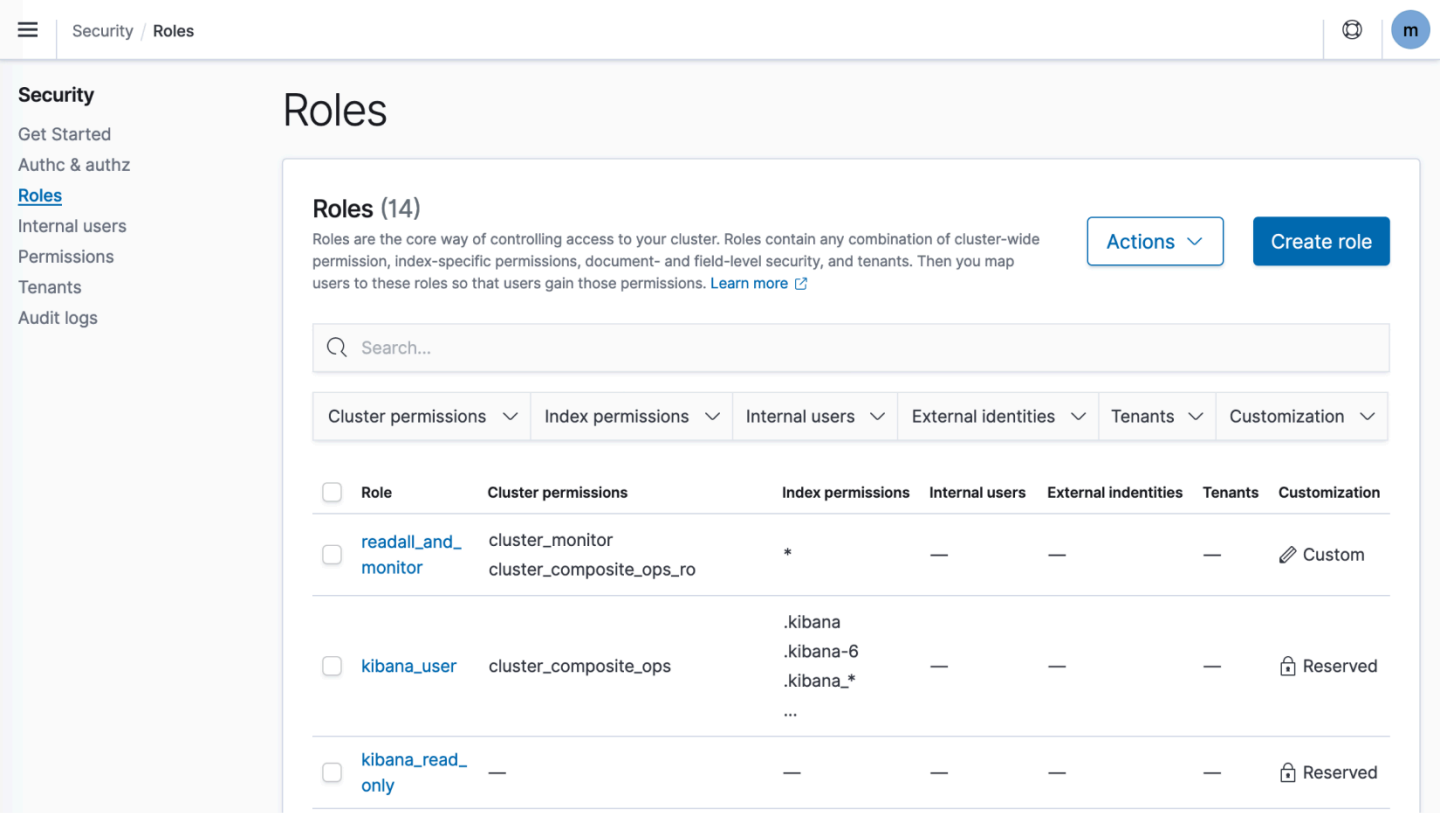
Weitere Informationen zu dieser Konfiguration finden Sie unter the section called “Tutorial: Interne Benutzerdatenbank mit einfacher Authentifizierung”.



- Falls Sie die SAML-Authentifizierung verwenden, können Sie sich mit den Anmeldeinformationen eines externen Identitätsanbieters anmelden. Weitere Informationen finden Sie unter the section called “SAML-Authentifizierung für Dashboards OpenSearch ”.

Verwalten von Berechtigungen

Wie in the section called “Die wichtigsten Konzepte” erwähnt, verwalten Sie differenzierte Zugriffskontrollberechtigungen mithilfe von Rollen, Benutzern und Zuweisungen. In diesem Abschnitt wird beschrieben, wie diese Ressourcen erstellt und angewendet werden. Wir empfehlen Ihnen, sich bei Dashboards als Hauptbenutzer anzumelden, um diese Operationen auszuführen.



> **Note**
>
> Die Berechtigungen, die Sie Ihren Benutzern gewähren möchten, variieren je nach Anwendungsfall stark. Wir können nicht alle Szenarien in dieser Dokumentation durchführbar abdecken. Achten Sie bei der Entscheidung, welche Berechtigungen Sie Ihren Benutzern gewähren möchten, darauf, die in den folgenden Abschnitten genannten OpenSearch Cluster- und Indexberechtigungen zu referenzieren und stets das Prinzip der geringsten Rechte zu beachten.

Erstellen von Rollen

Sie können mithilfe von OpenSearch Dashboards oder dem `_plugins/_security` Vorgang in der REST-API neue Rollen für eine detaillierte Zugriffskontrolle erstellen. Weitere Informationen finden Sie unter Rollen erstellen.

Die differenzierte Zugriffskontrolle umfasst auch eine Reihe vordefinierter Rollen. Clients wie OpenSearch Dashboards und Logstash stellen eine Vielzahl von Anfragen an OpenSearch, was es schwierig machen kann, Rollen mit den Mindestberechtigungen manuell zu erstellen.

Die `opensearch_dashboards_user` Rolle umfasst beispielsweise die Berechtigungen, die ein Benutzer benötigt, um mit Indexmustern, Visualisierungen, Dashboards und Mandanten zu arbeiten. Es wird empfohlen, sie einer beliebigen Benutzer- oder Backend-Rolle zuzuweisen, die auf Dashboards zugreift, zusammen mit zusätzlichen Rollen, die den Zugriff auf andere Indizes ermöglichen.

Amazon OpenSearch Service bietet die folgenden OpenSearch Rollen nicht an:

- `observability_full_access`
- `observability_read_access`
- `reports_read_access`
- `reports_full_access`

Amazon OpenSearch Service bietet mehrere Rollen an, die nicht verfügbar sind bei OpenSearch:

- `ultrawarm_manager`
- `ml_full_access`
- `cold_manager`
- `notifications_full_access`
- `notifications_read_access`

Sicherheit auf Clusterebene

Berechtigungen auf Clusterebene beinhalten die Möglichkeit, breite Anforderungen wie `_mget`, `_msearch` und `_bulk` zu machen, die Integrität zu überwachen, Snapshots zu erstellen und vieles mehr. Verwalten Sie diese Berechtigungen mithilfe des Abschnitts Clusterberechtigungen beim Erstellen einer Rolle. Eine vollständige Liste der Berechtigungen auf Clusterebene finden Sie unterCluster-Berechtigungen.

Anstelle einzelner Berechtigungen können Sie häufig Ihren gewünschten Sicherheitsstatus mithilfe einer Kombination der Standard-Aktionsgruppen erreichen. Eine Liste der Aktionsgruppen auf Cluster-Ebene finden Sie unter Clusterebene.

Sicherheit auf Index-Ebene

Berechtigungen auf Index-Ebene beinhalten die Möglichkeit, neue Indizes zu erstellen, Indizes zu durchsuchen, Dokumente zu lesen und zu schreiben, Dokumente zu löschen, Aliase zu verwalten

und vieles mehr. Verwalten Sie diese Berechtigungen beim Erstellen einer Rolle mithilfe des Abschnitts Index Permissions (Indexberechtigungen). Eine vollständige Liste der Berechtigungen auf Indexebene finden Sie unter Berechtigungen indizieren.

Anstelle einzelner Berechtigungen können Sie häufig Ihren gewünschten Sicherheitsstatus mithilfe einer Kombination der Standard-Aktionsgruppen erreichen. Eine Liste der Aktionsgruppen auf Index-Ebene finden Sie unter Index-Ebene.

Sicherheit auf Dokumentebene

Mit der Sicherheit auf Dokumentebene können Sie einschränken, welche Dokumente in einem Index ein Benutzer anzeigen kann. Geben Sie beim Erstellen einer Rolle ein Indexmuster und eine OpenSearch Abfrage an. Alle Benutzer, die Sie dieser Rolle zuordnen, können nur die Dokumente sehen, die mit der Abfrage übereinstimmen. Die Sicherheit auf Dokumentebene wirkt sich auf die Anzahl der Treffer aus, die Sie bei der Suche erhalten.

Weitere Informationen finden Sie unter Sicherheit auf Dokumentenebene.

Sicherheit auf Feldebene

Mit der Sicherheit auf Feldebene können Sie steuern, welche Dokumentfelder ein Benutzer anzeigen kann. Fügen Sie beim Erstellen einer Rolle eine Liste von Feldern hinzu, die entweder eingeschlossen oder ausgeschlossen werden sollen. Wenn Sie Felder einschließen, können alle Benutzer, die Sie dieser Rolle zuordnen, nur diese Felder sehen. Wenn Sie Felder ausschließen, können sie alle Felder mit Ausnahme der ausgeschlossenen sehen. Die Sicherheit auf Feldebene wirkt sich auf die Anzahl der Felder aus, die bei der Suche in Treffer enthalten sind.

Weitere Informationen finden Sie unter Sicherheit auf Feldebene.

Feldmaskierung

Die Feldmaskierung ist eine Alternative zur Sicherheit auf Feldebene, mit der Sie die Daten in einem Feld anonymisieren können, anstatt sie vollständig zu entfernen. Fügen Sie beim Erstellen einer Rolle eine Liste von Feldern hinzu, die maskiert werden sollen. Die Feldmaskierung wirkt sich darauf aus, ob beim Suchen der Inhalt eines Feldes angezeigt wird.

> **Tip**
>
> Wenn Sie die Standardmaskierung auf ein Feld anwenden, verwendet OpenSearch Service einen sicheren, zufälligen Hash, der zu ungenauen Aggregationsergebnissen führen kann.

Verwenden Sie stattdessen die musterbasierte Maskierung, um Aggregationen für maskierte Felder durchzuführen.

Erstellen von Benutzern

Wenn Sie die interne Benutzerdatenbank aktiviert haben, können Sie Benutzer mithilfe von OpenSearch Dashboards oder der `_plugins/_security` Operation in der REST-API erstellen. Weitere Informationen finden Sie unter Benutzer erstellen.

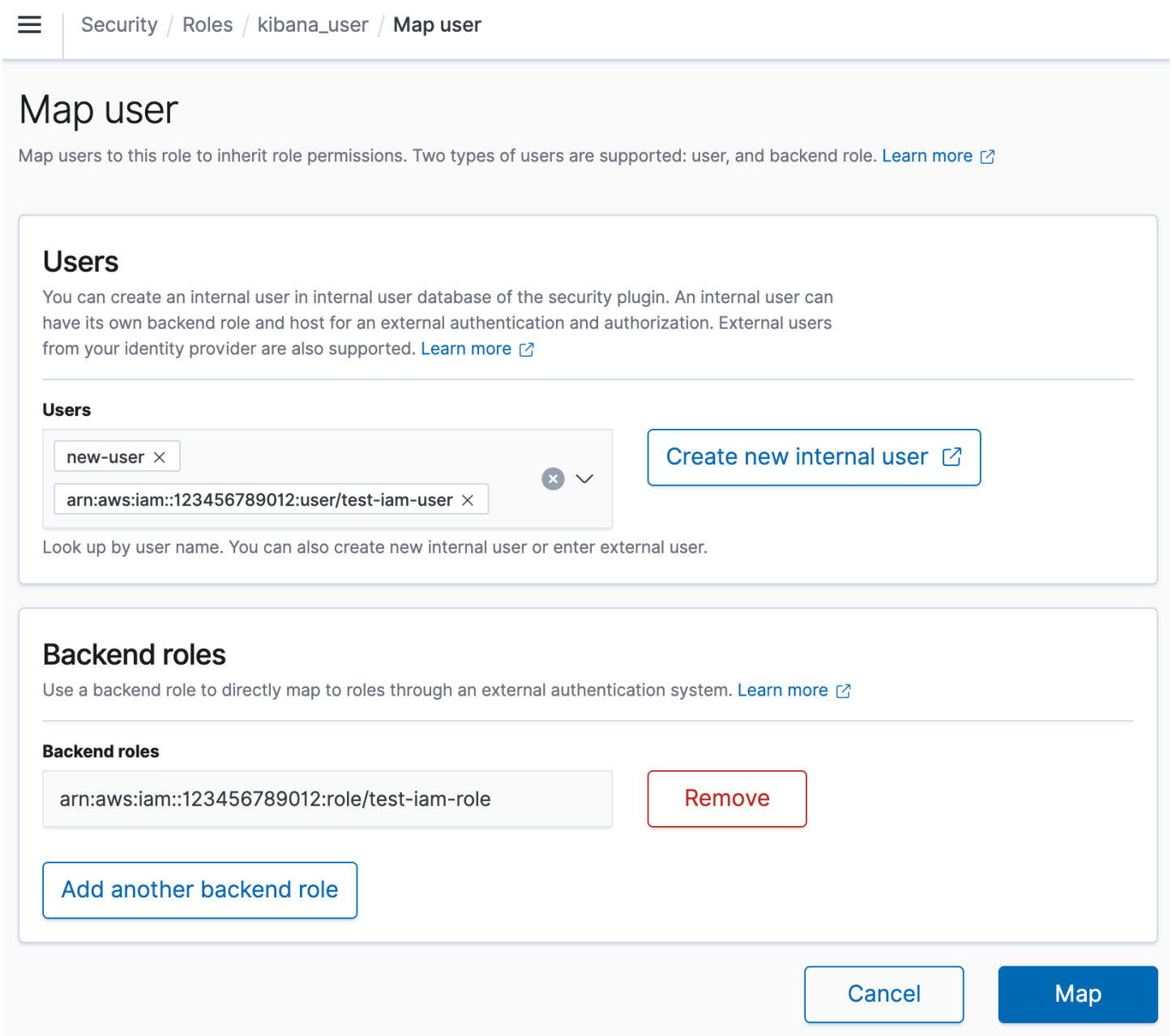
Wenn Sie sich für IAM als Ihren Hauptbenutzer entschieden haben, ignorieren Sie diesen Teil von Dashboards. Erstellen Sie stattdessen IAM-Rollen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch.

Rollen an Benutzer zuweisen

Das Rollen-Mapping ist der kritischste Aspekt der differenzierten Zugriffskontrolle. Die differenzierte Zugriffskontrolle verfügt über einige vordefinierte Rollen, die Ihnen beim Einstieg helfen. Wenn Sie jedoch nicht den Benutzern Rollen zuordnen, endet jede Anforderung an den Cluster mit einem Berechtigungsfehler.

Backend-Rollen können dazu beitragen, den Rollenzuordnungsprozess zu vereinfachen. Anstatt dieselbe Rolle 100 einzelnen Benutzern zuzuordnen, können Sie die Rolle einer einzelnen Backend-Rolle zuordnen, die sich alle 100 Benutzer teilen. Backend-Rollen können IAM-Rollen oder beliebige Zeichenfolgen sein.

- Geben Sie Benutzer ARNs, Benutzer und Amazon Cognito Cognito-Benutzerzeichenfolgen im Abschnitt Benutzer an. Cognito-Benutzerzeichenfolgen haben die Form von `Cognito/`*`user-pool-id`*`/`*`username`*.
- Geben Sie im Abschnitt Backend-Rollen die Backend-Rollen und die IAM-Rolle ARNs an.



Sie können Benutzern Rollen mithilfe von OpenSearch Dashboards oder der `_plugins/_security` Operation in der REST-API zuordnen. Weitere Informationen finden Sie unter Zuordnen von Benutzern zu Rollen.

Aktionsgruppen erstellen

Aktionsgruppen sind Gruppen von Berechtigungen, die Sie über verschiedene Ressourcen hinweg wiederverwenden können. Sie können mithilfe von OpenSearch Dashboards oder der `_plugins/_security` Operation in der REST-API neue Aktionsgruppen erstellen, obwohl die

Standardaktionsgruppen für die meisten Anwendungsfälle ausreichend sind. Weitere Informationen zu den Standardaktionsgruppen finden Sie unter Standardaktionsgruppen.

OpenSearch Dashboards, Mehrmandantenfähigkeit

Mandanten (Tenants) sind Räume zum Speichern von Indexmustern, Visualisierungen, Dashboards und anderen Dashboards-Objekten. Mit der Mehrmandantenfähigkeit von Dashboards können Sie Ihre Arbeit sicher mit anderen Dashboard-Benutzern teilen (oder privat halten) und Mandanten dynamisch konfigurieren. Sie können steuern, welche Rollen Zugriff auf einen Mandanten haben, und ob diese Rollen Lese- oder Schreibzugriff haben. Der globale Mandant ist der Standardmandant. Weitere Informationen finden Sie unter Mehrmandantenfähigkeit von Dashboards. OpenSearch

So zeigen Sie Ihren aktuellen Mandanten an oder ändern Mandanten:

1. Navigieren Sie zu OpenSearch Dashboards und melden Sie sich an.
2. Wählen Sie oben rechts Ihr Benutzersymbol aus und wählen Sie Tenant wechseln.
3. Überprüfen Sie Ihren Mandanten, bevor Sie Visualisierungen oder Dashboards erstellen. Wenn Sie Ihre Arbeit mit allen anderen Dashboards-Benutzern teilen möchten, wählen Sie Global. Um Ihre Arbeit für eine Teilmenge von Dashboards-Benutzern freizugeben, wählen Sie einen anderen freigegebenen Mandanten aus. Andernfalls wählen Sie Private (Privat).

> **Note**
>
> OpenSearch Dashboards verwaltet einen separaten Index für jeden Mandanten und erstellt eine Indexvorlage namens. `tenant_template` Löschen oder ändern Sie den `tenant_template` Index nicht, da dies zu Fehlfunktionen der OpenSearch Dashboards führen kann, wenn die Indexzuordnung des Mandanten falsch konfiguriert ist.

Empfohlene Konfigurationen

Aufgrund der Interaktion der differenzierten Zugriffskontrolle mit anderen Sicherheitsfunktionen empfehlen wir mehrere differenzierte Zugriffskontrollkonfigurationen, die für die meisten Anwendungsfälle gut funktionieren.

Beschreibung	Hauptbenutzer	Domain-Zugriffsrichtlinie

Verwenden Sie IAM-Anmeldeinformationen für Aufrufe an die und verwenden Sie die SAML-Authentifizierung OpenSearch APIs, um auf Dashboards zuzugreifen. Verwalten Sie differenzierte Zugriffskontrollrollen mithilfe von Dashboards oder der REST-API.	IAM-Rolle oder -Benutzer	JSON
		{
		"Version": "2012-10-17",
		"Statement": [
		{
		"Effect": "Allow",
		"Principal": {
		"AWS": "*"
		},
		"Action": "es:ESHttp*",
		"Resource": " *domain-arn* /*"
		}
		]
		}

Verwenden Sie IAM-Anmeldeinformationen oder die Standardauthentifizierung für Anrufe an die. OpenSearch APIs Verwalten Sie differenzierte Zugriffskontrollrollen mithilfe von Dashboards oder der REST-API.
 	
Diese Konfiguration bietet viel Flexibilität, insbesondere wenn Sie OpenSearch Clients haben, die nur die Standardauthentifizierung unterstützen.
 	
Wenn Sie über einen vorhandenen Identität
	Nutzername und Passwort	JSON
		{
		"Version": "2012-10-17",
		"Statement": [
		{
		"Effect": "Allow",
		"Principal": {
		"AWS": "*"
		},
		"Action": "es:ESHttp*",
		"Resource": " *domain-arn* /*"
		}
		]
		}

Beschreibung	Hauptbenutzer	Domain-Zugriffsrichtlinie
sanbieter verfügen, verwenden Sie die SAML-Authentifizierung, um auf Dashboards zuzugreifen. Andernfalls verwalten Sie Dashboards-Benutzer in der internen Benutzerdatenbank.		
Verwenden Sie IAM-Anmeldeinformationen für Anrufe an die und verwenden Sie Amazon Cognito OpenSearch APIs, um auf Dashboards zuzugreifen. Verwalten Sie differenzierte Zugriffskontrollrollen mithilfe von Dashboards oder der REST-API.	IAM-Rolle oder -Benutzer	JSON `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "AWS": "*" }, "Action": "es:ESHttp*", "Resource": " domain-arn /*" } ] }`

Beschreibung	Hauptbenutzer	Domain-Zugriffsrichtlinie
Verwenden Sie IAM-Anmeldeinformationen für Anrufe an die Dashboards und blockieren Sie die OpenSearch APIs meisten Zugriffe auf Dashboards. Verwalten Sie differenzierte Zugriffskontrollrollen mithilfe oder der REST-API.	IAM-Rolle oder -Benutzer	JSON `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "AWS": "*" }, "Action": "es:ESHttp*", "Resource": " domain-arn /*" }, { "Effect": "Deny", "Principal": { "AWS": "*" }, "Action": "es:ESHttp*", "Resource": " domain-arn /_dashboards*" } ] }`

Einschränkungen

Die differenzierte Zugriffskontrolle hat mehrere wichtige Einschränkungen:

- Der `hosts`-Aspekt von Rollen-Mappings, der Rollen Hostnamen oder IP-Adressen zuweist, funktioniert nicht, wenn sich die Domain innerhalb einer VPC befindet. Sie können jedoch Rollen weiterhin Benutzern und Backend-Rollen zuordnen.
- Wenn Sie IAM für den Master-Benutzer auswählen und die Amazon-Cognito- oder SAML-Authentifizierung nicht aktivieren, zeigt Dashboards eine nicht funktionierende Anmeldeseite an.

- Wenn Sie IAM für den Master-Benutzer auswählen, können Sie weiterhin Benutzer in der internen Benutzerdatenbank erstellen. Da die HTTP-Standardauthentifizierung unter dieser Konfiguration nicht aktiviert ist, werden jedoch alle mit diesen Benutzeranmeldeinformationen signierten Anforderungen abgelehnt.
- Wenn Sie SQL verwenden, um einen Index abzufragen, auf den Sie keinen Zugriff haben, erhalten Sie den Fehler „No permissions (Keine Berechtigungen)“. Wenn der Index nicht existiert, erhalten Sie den Fehler „no such index (Kein solcher Index vorhanden)“. Dieser Unterschied bei den Fehlermeldungen bedeutet, dass Sie die Existenz eines Index bestätigen können, wenn Sie zufällig seinen Namen erraten.

  Um das Problem zu minimieren, geben Sie keine vertraulichen Informationen in Indexnamen ein. Um jeden Zugriff auf SQL zu verweigern, fügen Sie der Domainszugriffsrichtlinie das folgende Element hinzu:

```
{
  "Effect": "Deny",
  "Principal": {
    "AWS": [
      "*"
    ]
  },
  "Action": [
    "es:*"
  ],
  "Resource": "arn:aws:es:us-east-1:123456789012:domain/my-domain/_plugins/_sql"
}
```

- Wenn Ihre Domain-Version 2.3 oder höher ist und Sie eine differenzierte Zugriffskontrolle aktiviert haben, führt die Einstellung auf 1 `max_clause_count` zu Problemen mit Ihrer Domain. Wir empfehlen, für dieses Konto eine höhere Zahl festzulegen.
- Wenn Sie die differenzierte Zugriffskontrolle in einer Domäne aktivieren, in der keine differenzierte Zugriffskontrolle eingerichtet ist, müssen Sie für Datenquellen, die für direkte Abfragen erstellt wurden, die detaillierten Zugriffssteuerungsrollen selbst einrichten. Weitere Informationen zum Einrichten detaillierter Zugriffsrollen finden Sie unter Erstellen von Amazon OpenSearch Service-Datenquellenintegrationen mit Amazon S3.

Hauptbenutzer ändern

Wenn Sie die Details des Master-Benutzers vergessen haben, können Sie ihn mithilfe der Konsole, AWS CLI, oder der Konfigurations-API neu konfigurieren.

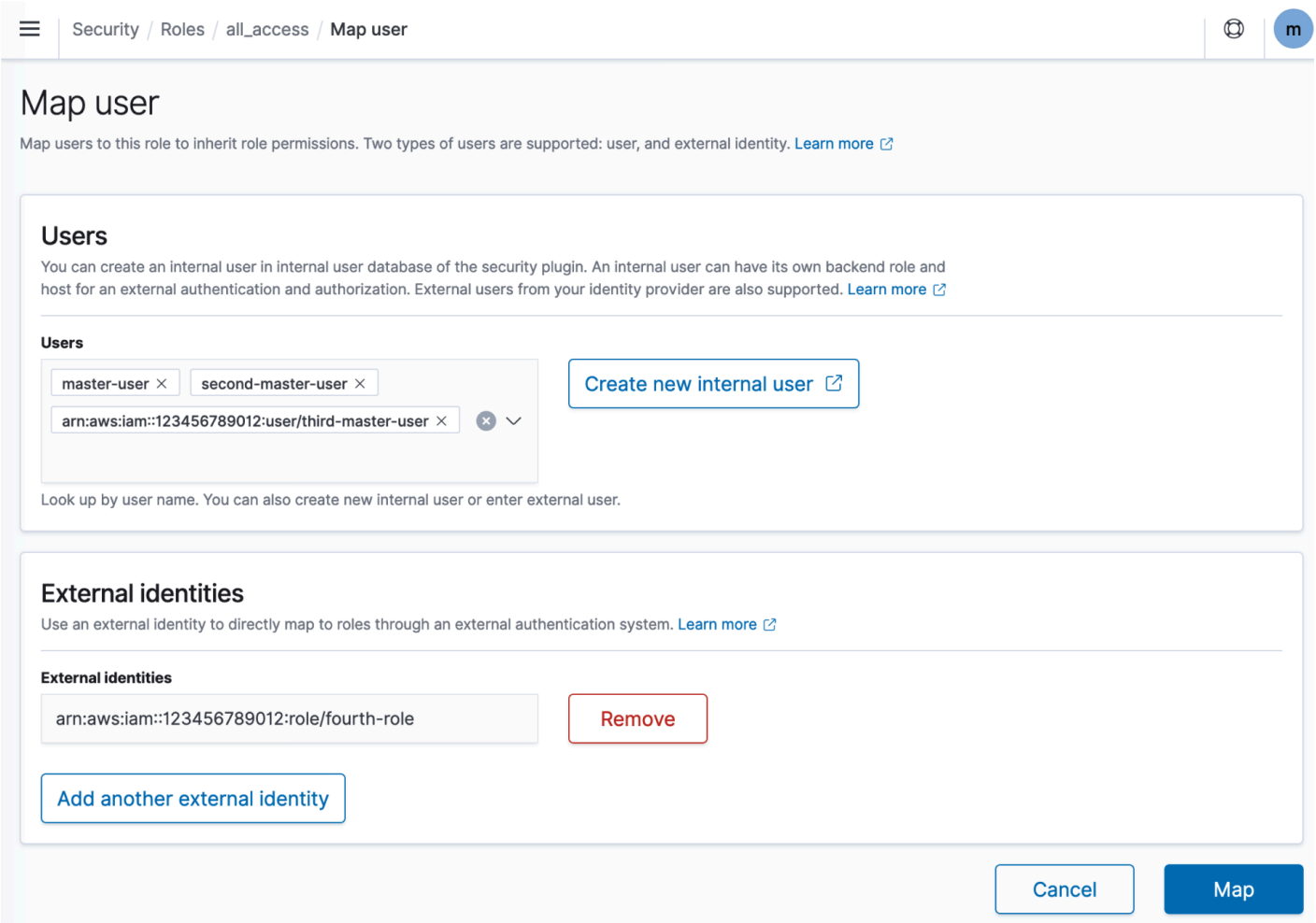
So ändern Sie den Master-Benutzer (Konsole):

1. Navigieren Sie zu der Amazon OpenSearch Service-Konsole zu https://console.aws.amazon.com/aos/Hause/.
2. Wählen Sie Ihre Domain aus und wählen Sie Actions (Aktionen), Edit security configuration (Sicherheitskonfiguration bearbeiten).
3. Wählen Sie entweder IAM-ARN als Hauptbenutzer festlegen oder Neuen Hauptbenutzer erstellen aus.
   - Wenn Sie zuvor einen IAM-Master-Benutzer verwendet haben, ordnet die differenzierte Zugriffskontrolle die `all_access`-Rolle dem von Ihnen angegebenen neuen IAM-ARN neu zu.
   - Wenn Sie zuvor die interne Benutzerdatenbank verwendet haben, erstellt die differenzierte Zugriffskontrolle einen neuen Master-Benutzer. Sie können den neuen Master-Benutzer verwenden, um den alten zu löschen.
   - Beim Wechsel von der internen Benutzerdatenbank zu einem IAM-Hauptbenutzer werden keine Benutzer aus der internen Benutzerdatenbank gelöscht. Stattdessen deaktiviert es nur die HTTP-Basisauthentifizierung. Löschen Sie Benutzer manuell aus der internen Benutzerdatenbank oder behalten Sie sie für den Fall, dass Sie die HTTP-Basisauthentifizierung je wieder aktivieren müssen.
4. Wählen Sie Änderungen speichern aus.

Zusätzliche Hauptbenutzer

Sie bestimmen einen Master-Benutzer, wenn Sie eine Domain erstellen, aber wenn Sie möchten, können Sie diesen Master-Benutzer verwenden, um zusätzliche Master-Benutzer zu erstellen. Sie haben zwei Optionen: OpenSearch Dashboards oder die REST-API.

- Wählen Sie in Dashboards Sicherheit, Rollen und weisen Sie den neuen Hauptbenutzer den Rollen `all_access` und `security_manager` zu.



- Um die REST-API zu verwenden, senden Sie die folgenden Anforderungen:

```
PUT _plugins/_security/api/rolesmapping/all_access
{
  "backend_roles": [
    "arn:aws:iam::123456789012:role/fourth-master-user"
  ],
  "hosts": [],
  "users": [
    "master-user",
    "second-master-user",
    "arn:aws:iam::123456789012:user/third-master-user"
  ]
}
```

```
PUT _plugins/_security/api/rolesmapping/security_manager
{
```

```
  "backend_roles": [
    "arn:aws:iam::123456789012:role/fourth-master-user"
  ],
  "hosts": [],
  "users": [
    "master-user",
    "second-master-user",
    "arn:aws:iam::123456789012:user/third-master-user"
  ]
}
```

Diese Anforderungen ersetzen die aktuellen Rollen-Mappings. Führen Sie daher zuerst GET-Anforderungen aus, damit Sie alle aktuellen Rollen in die PUT-Anforderungen aufnehmen können. Die REST-API ist besonders nützlich, wenn Sie nicht auf Dashboards zugreifen können und der `all_access`-Rolle eine IAM-Rolle aus Amazon Cognito zuordnen möchten.

Manuelle Snapshots

Die differenzierte Zugriffskontrolle bringt einige zusätzliche Komplikationen bei der Erstellung manueller Snapshots mit sich. Um ein Snapshot-Repository zu registrieren – auch wenn Sie die HTTP-Basisauthentifizierung für alle anderen Zwecke verwenden – müssen Sie die `manage_snapshots`-Rolle einer IAM-Rolle zuordnen, die über `iam:PassRole` Berechtigungen zum Annehmen von `TheSnapshotRole` verfügt, wie in the section called “Voraussetzungen” definiert.

Verwenden Sie dann diese IAM-Rolle, um eine signierte Anforderung an die Domain zu senden, wie in the section called “Registrieren eines manuellen Snapshot-Repositorys” beschrieben.

Integrationen

Wenn Sie andere AWS Dienste mit OpenSearch Service verwenden, müssen Sie den IAM-Rollen für diese Dienste die entsprechenden Berechtigungen zuweisen. Beispielsweise verwenden Firehose-Lieferstreams häufig eine IAM-Rolle namens. `firehose_delivery_role` Erstellen Sie in Dashboards eine Rolle für die differenzierte Zugriffskontrolle, und ordnen Sie dieser die IAM-Rolle zu. In diesem Fall benötigt die neue Rolle die folgenden Berechtigungen:

```
{
  "cluster_permissions": [
    "cluster_composite_ops",
    "cluster_monitor"
  ],
```

```
  "index_permissions": [{
    "index_patterns": [
      "firehose-index*"
    ],
    "allowed_actions": [
      "create_index",
      "manage",
      "crud"
    ]
  }]
}
```

Berechtigungen variieren je nach den Aktionen, die jeder Service ausführt. Eine AWS IoT Regel oder AWS Lambda Funktion, die Daten indexiert, benötigt wahrscheinlich ähnliche Berechtigungen wie Firehose, während eine Lambda-Funktion, die nur Suchen durchführt, einen eingeschränkteren Satz verwenden kann.

REST-API-Unterschiede

Die REST-API für die differenzierte Zugriffskontrolle unterscheidet sich je nach OpenSearch/ Elasticsearch -Version geringfügig. Bevor Sie eine PUT-Anforderung stellen, stellen Sie eine GET-Anforderung, um den erwarteten Anforderungsinhalt zu überprüfen. Beispielsweise gibt eine GET-Anforderung an `_plugins/_security/api/user` alle Benutzer zurück, die Sie dann ändern und verwenden können, um gültige PUT-Anforderungen zu stellen.

Auf Elasticsearch 6.x sehen Anforderungen zum Erstellen von Benutzern wie folgt aus:

```
PUT _opendistro/_security/api/user/new-user
{
  "password": "some-password",
  "roles": ["new-backend-role"]
}
```

Auf OpenSearch oder Elasticsearch 7.x sehen Anfragen so aus (ändern Sie `_plugins` zu`_opendistro`, wenn Sie Elasticsearch verwenden):

```
PUT _plugins/_security/api/user/new-user
{
  "password": "some-password",
  "backend_roles": ["new-backend-role"]
}
```

Außerdem sind Tenants Eigenschaften von Rollen in Elasticsearch 6.x:

```
GET _opendistro/_security/api/roles/all_access

{
  "all_access": {
    "cluster": ["UNLIMITED"],
    "tenants": {
      "admin_tenant": "RW"
    },
    "indices": {
      "*": {
        "*": ["UNLIMITED"]
      }
    },
    "readonly": "true"
  }
}
```

In OpenSearch und Elasticsearch 7.x handelt es sich um Objekte mit eigener URI (ändern Sie `_plugins` zu, `_opendistro` wenn Sie Elasticsearch verwenden):

```
GET _plugins/_security/api/tenants

{
  "global_tenant": {
    "reserved": true,
    "hidden": false,
    "description": "Global tenant",
    "static": false
  }
}
```

Die Dokumentation zur OpenSearch REST-API finden Sie in der API-Referenz für das Sicherheits-Plugin.

> **Tip**
>
> Wenn Sie die interne Benutzerdatenbank verwenden, können Sie curl verwenden, um Anforderungen zu stellen und Ihre Domain zu testen. Probieren Sie die folgenden Beispielbefehle aus:

```
curl -XGET -u 'master-user:master-user-password' 'domain-endpoint/_search'
curl -XGET -u 'master-user:master-user-password' 'domain-endpoint/_plugins/
_security/api/user'
```

Tutorial: Konfigurieren einer Domain mit einem IAM-Hauptbenutzer und Amazon-Cognito-Authentifizierung

Dieses Tutorial behandelt einen beliebten Amazon OpenSearch Service-Anwendungsfall für eine differenzierte Zugriffskontrolle: einen IAM-Master-Benutzer mit Amazon Cognito Cognito-Authentifizierung für Dashboards. OpenSearch

Im Tutorial konfigurieren wir eine Haupt-IAM-Rolle und eine eingeschränkte IAM-Rolle, die wir dann Benutzern in Amazon Cognito zuordnen. Der Masterbenutzer kann sich dann bei OpenSearch Dashboards anmelden, den eingeschränkten Benutzer einer Rolle zuordnen und mithilfe einer detaillierten Zugriffskontrolle die Benutzerberechtigungen einschränken.



Obwohl diese Schritte den Amazon-Cognito-Benutzerpool für die Authentifizierung verwenden, funktioniert derselbe grundlegende Prozess für jeden Cognito-Authentifizierungsanbieter, mit dem Sie verschiedenen Benutzern unterschiedliche IAM-Rollen zuweisen können.

In diesem Tutorial führen Sie die folgenden Schritte durch:

1. Erstellen von Haupt- und eingeschränkten IAM-Rollen
2. Erstellen einer Domain mit Cognito-Authentifizierung
3. Konfigurieren Sie einen Cognito-Benutzerpool und einen Identitätspool
4. Ordnen Sie Rollen in Dashboards zu OpenSearch

5. Testen der Berechtigungen

Schritt 1: Erstellen von Haupt- und eingeschränkten IAM-Rollen

Navigieren Sie zur AWS Identity and Access Management (IAM-) Konsole und erstellen Sie zwei separate Rollen:

- `MasterUserRole` – Der Hauptbenutzer, der über vollständige Berechtigungen für den Cluster verfügt und Rollen und Rollenzuordnungen verwaltet.
- `LimitedUserRole` – Eine eingeschränktere Rolle, der Sie als Hauptbenutzer eingeschränkten Zugriff gewähren.

Anweisungen zum Erstellen der Rollen finden Sie unter Erstellen einer Rolle mithilfe benutzerdefinierter Vertrauensrichtlinien im IAM-Benutzerhandbuch.

Beide Rollen müssen über die folgende Vertrauensrichtlinie verfügen, die es Ihrem Cognito-Identitätspool ermöglicht, die Rollen zu übernehmen:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Principal": {
      "Federated": "cognito-identity.amazonaws.com"
    },
    "Action": "sts:AssumeRoleWithWebIdentity",
    "Condition": {
      "StringEquals": {
        "cognito-identity.amazonaws.com:aud": "{identity-pool-id}"
      },
      "ForAnyValue:StringLike": {
        "cognito-identity.amazonaws.com:amr": "authenticated"
      }
    }
  }]
}
```

> **Note**
>
> Ersetzen Sie `identity-pool-id` durch die eindeutige Kennung Ihres Amazon-Cognito-Identitätspools. Beispiel, `us-east-1:0c6cdba7-3c3c-443b-a958-fb9feb207aa6`.

Schritt 2: Erstellen einer Domain mit Cognito-Authentifizierung

Rufen Sie die Amazon OpenSearch Service-Konsole unter https://console.aws.amazon.com/aos/home/ auf und erstellen Sie eine Domain mit den folgenden Einstellungen:

- OpenSearch 1.0 oder höher oder Elasticsearch 7.8 oder höher
- Öffentlicher Zugriff
- Detallierte Zugriffskontrolle, die mit `MasterUserRole` als Hauptbenutzer aktiviert ist (im vorherigen Schritt erstellt)
- Amazon Cognito Cognito-Authentifizierung für OpenSearch Dashboards aktiviert. Anweisungen zum Aktivieren der Cognito-Authentifizierung und zum Auswählen eines Benutzer- und Identitätspools finden Sie unter the section called “Konfigurieren einer Domain zur Verwendung der Amazon-Cognito-Authentifizierung”.
- Die folgende Domain-Zugriffsrichtlinie:

  JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::{account-id}:root"
      },
      "Action": [
        "es:ESHttp*"
      ],
      "Resource": "arn:aws:es:{region}:{account-id}:domain/{domain-name}/*"
    }
  ]
}
```

- HTTPS für den gesamten Datenverkehr zur Domain erforderlich

- Node-to-node Verschlüsselung
- Verschlüsselung gespeicherter Daten

Schritt 3: Cognito-Benutzer konfigurieren

Während Ihre Domain erstellt wird, konfigurieren Sie die Master- und eingeschränkten Benutzer in Amazon Cognito, indem Sie im Amazon Cognito Developer Guide unter Create a user pool nachlesen. Konfigurieren Sie abschließend Ihren Identitätspool, indem Sie die Schritte unter Erstellen eines Identitätspools in Amazon Cognito befolgen. Der Benutzer- und der Identitätenpool müssen sich in derselben AWS-Region befinden.

Schritt 4: Rollen in OpenSearch Dashboards zuordnen

Nachdem Ihre Benutzer konfiguriert sind, können Sie sich als Hauptbenutzer bei OpenSearch Dashboards anmelden und Benutzer Rollen zuordnen.

1. Kehren Sie zur OpenSearch Servicekonsole zurück und navigieren Sie zur OpenSearch Dashboard-URL für die von Ihnen erstellte Domain. Die URL weist folgendes Format auf: *domain-endpoint*`/_dashboards/`.
2. Melden Sie sich mit den `master-user`-Anmeldeinformationen an.
3. Wählen Sie Add sample data (Beispieldaten hinzufügen) und fügen Sie die Beispielflugdaten hinzu.
4. Wählen Sie im linken Navigationsbereich Security (Sicherheit), Roles (Rollen), Create role (Rolle erstellen) aus.
5. Benennen Sie die Rolle `new-role`.
6. Geben Sie für Index `opensearch_dashboards_sample_data_fli*` (`kibana_sample_data_fli*` auf Elasticsearch-Domains) an.
7. Wählen Sie für Index permissions (Indexberechtigungen) die Option read (Lesen) aus.
8. Geben Sie für Sicherheitsabfrage auf Dokumentebene die folgende Abfrage an:

```
{
  "match": {
    "FlightDelay": true
  }
}
```

9. Wählen Sie für die Sicherheit auf Feldebene Ausschließen und geben Sie `FlightNum` an.
10. Fü rAnonymisierung, geben Sie `Dest` an.
11. Wählen Sie Erstellen aus.
12. Wählen Sie Zugeordnete Benutzer, Mapping verwalten. Fügen Sie den Amazon-Ressourcennamen (ARN) für `LimitedUserRole` als externe Identität hinzu und wählen Sie Map (Zuordnen) aus.
13. Kehren Sie zur Liste der Rollen zurück und wählen Sie opensearch_dashboards_useraus. Wählen Sie Zugeordnete Benutzer, Mapping verwalten. Fügen Sie den ARN für `LimitedUserRole` als Backend-Rolle hinzu und wählen Sie Zuordnen aus.

Schritt 5: Testen der Berechtigungen

Wenn Ihre Rollen korrekt zugeordnet sind, können Sie sich als Benutzer mit eingeschränkten Rechten anmelden und die Berechtigungen testen.

1. Navigieren Sie in einem neuen, privaten Browserfenster zur OpenSearch Dashboard-URL für die Domain, melden Sie sich mit den `limited-user` Anmeldeinformationen an und wählen Sie Auf eigene Faust erkunden aus.
2. Wählen Sie Entwicklerwerkzeuge aus und führen Sie dann die Standardsuche aus:

   ```
   GET _search
   {
     "query": {
       "match_all": {}
     }
   }
   ```

   Beachten Sie den Berechtigungsfehler. `limited-user` hat keine Berechtigungen zum Ausführen von clusterweiten Suchvorgängen.
3. Führen Sie eine weitere Suche aus:

   ```
   GET opensearch_dashboards_sample_data_flights/_search
   {
     "query": {
       "match_all": {}
     }
   }
   ```

Beachten Sie, dass alle übereinstimmenden Dokumente ein `FlightDelay`-Feld von `true`, ein anonymisiertes `Dest`- Feld und kein `FlightNum`-Feld haben.

4. Wählen Sie in Ihrem ursprünglichen Browserfenster, angemeldet als `master-user`, Dev Tools, und führen Sie dann die gleichen Suchvorgänge durch. Beachten Sie die Unterschiede zwischen Berechtigungen, Anzahl der Treffer, übereinstimmenden Dokumenten und eingeschlossenen Feldern.

Tutorial: Konfigurieren einer Domain mit der internen Benutzerdatenbank und HTTP-Basisauthentifizierung

Dieses Tutorial behandelt einen weiteren beliebten Anwendungsfall für die detaillierte Zugriffskontrolle: einen Masterbenutzer in der internen Benutzerdatenbank und die HTTP-Basisauthentifizierung für Dashboards. OpenSearch Der Hauptbenutzer kann sich dann bei OpenSearch Dashboards anmelden, einen internen Benutzer erstellen, den Benutzer einer Rolle zuordnen und mithilfe einer detaillierten Zugriffskontrolle die Benutzerberechtigungen einschränken.

In diesem Tutorial führen Sie die folgenden Schritte durch:

1. Erstellen Sie eine Domain mit einem Masterbenutzer
2. Konfigurieren Sie einen internen Benutzer in OpenSearch Dashboards
3. Ordnen Sie Rollen in Dashboards zu OpenSearch
4. Testen der Berechtigungen

Schritt 1: Erstellen einer Domäne

Rufen Sie die Amazon OpenSearch Service-Konsole unter https://console.aws.amazon.com/aos/home/ auf und erstellen Sie eine Domain mit den folgenden Einstellungen:

- OpenSearch 1.0 oder höher oder Elasticsearch 7.9 oder höher
- Öffentlicher Zugriff
- Differenzierte Zugriffskontrolle mit einem Master-Benutzer in der internen Benutzerdatenbank (`TheMasterUser` für den Rest dieses Lernprogramms)
- Amazon Cognito-Authentifizierung für Dashboards deaktiviert
- Die folgende Zugriffsrichtlinie:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::{account-id}:root"
      },
      "Action": [
        "es:ESHttp*"
      ],
      "Resource": "arn:aws:es:{region}:{account-id}:domain/{domain-name}/*"
    }
  ]
}
```

- HTTPS für den gesamten Datenverkehr zur Domain erforderlich
- Node-to-node Verschlüsselung
- Verschlüsselung gespeicherter Daten

Schritt 2: Erstellen Sie einen internen Benutzer in OpenSearch Dashboards

Da Sie nun eine Domain haben, können Sie sich bei OpenSearch Dashboards anmelden und einen internen Benutzer erstellen.

1. Kehren Sie zur OpenSearch Servicekonsole zurück und navigieren Sie zur OpenSearch Dashboard-URL für die von Ihnen erstellte Domain. Die URL weist folgendes Format auf: *domain-endpoint*`/_dashboards/`.
2. Melden Sie sich mit dem an`TheMasterUser`.
3. Wählen Sie Add sample data (Beispieldaten hinzufügen) und fügen Sie die Beispielflugdaten hinzu.
4. Wählen Sie im linken Navigationsbereich Sicherheit, Interne Benutzer, Internen Benutzer erstellen aus.
5. Benennen Sie den Benutzer `new-user` und geben Sie ein Passwort an. Wählen Sie die Option Erstellen aus.

Schritt 3: Rollen in OpenSearch Dashboards zuordnen

Nachdem Ihr Benutzer konfiguriert ist, können Sie ihn einer Rolle zuordnen.

1. Bleiben Sie im Bereich Sicherheit der OpenSearch Dashboards und wählen Sie Rollen, Rolle erstellen aus.
2. Benennen Sie die Rolle `new-role`.
3. Geben Sie für Index `opensearch_dashboards_sample_data_fli*` (`kibana_sample_data_fli*`bei Elasticsearch-Domains) das Indexmuster an.
4. Wählen Sie für die Aktionsgruppe lesen aus.
5. Geben Sie für Sicherheitsabfrage auf Dokumentebene die folgende Abfrage an:

   ```
   {
     "match": {
       "FlightDelay": true
     }
   }
   ```

6. Wählen Sie für die Sicherheit auf Feldebene Ausschließen und geben Sie `FlightNum` an.
7. Fü rAnonymisierung, geben Sie `Dest` an.
8. Wählen Sie Erstellen aus.
9. Wählen Sie Zugeordnete Benutzer, Mapping verwalten. Fügen Sie dann `new-user` zu Benutzern hinzu und wählen Sie Zuordnen.
10. Kehren Sie zur Liste der Rollen zurück und wählen Sie opensearch_dashboards_useraus. Wählen Sie Zugeordnete Benutzer, Mapping verwalten. Fügen Sie dann `new-user` zu Benutzern hinzu und wählen Sie Zuordnen.

Schritt 4: Testen Sie die Berechtigungen

Wenn Ihre Rollen korrekt zugeordnet sind, können Sie sich als Benutzer mit eingeschränkten Rechten anmelden und die Berechtigungen testen.

1. Navigieren Sie in einem neuen, privaten Browserfenster zur OpenSearch Dashboard-URL für die Domain, melden Sie sich mit den `new-user` Anmeldeinformationen an und wählen Sie Auf eigene Faust erkunden aus.
2. Wählen Sie Entwicklerwerkzeuge aus und führen Sie dann die Standardsuche aus:

```
GET _search
{
  "query": {
    "match_all": {}
  }
}
```

Beachten Sie den Berechtigungsfehler. `new-user` hat keine Berechtigungen zum Ausführen von clusterweiten Suchvorgängen.

3. Führen Sie eine weitere Suche aus:

```
GET dashboards_sample_data_flights/_search
{
  "query": {
    "match_all": {}
  }
}
```

Beachten Sie, dass alle übereinstimmenden Dokumente ein `FlightDelay`-Feld von `true`, ein anonymisiertes `Dest`- Feld und kein `FlightNum`-Feld haben.

4. Wählen Sie in Ihrem ursprünglichen Browserfenster, angemeldet als `TheMasterUser`, Dev Tools, und führen Sie dann die gleichen Suchvorgänge durch. Beachten Sie die Unterschiede zwischen Berechtigungen, Anzahl der Treffer, übereinstimmenden Dokumenten und eingeschlossenen Feldern.

Konformitätsprüfung für Amazon OpenSearch Service

Externe Prüfer bewerten die Sicherheit und Konformität von Amazon OpenSearch Service im Rahmen mehrerer AWS Compliance-Programme. Zu diesen Programmen gehören SOC, PCI und HIPAA.

Wenn Sie Compliance-Anforderungen haben, sollten Sie erwägen, eine beliebige Version von OpenSearch Elasticsearch 6.0 oder höher zu verwenden. Frühere Versionen von Elasticsearch bieten keine Kombination aus Verschlüsselung ruhender Daten und node-to-node Verschlüsselung und erfüllen daher wahrscheinlich nicht Ihre Anforderungen. Sie könnten auch erwägen, eine beliebige Version von Elasticsearch 6.7 OpenSearch oder höher zu verwenden, wenn eine detaillierte Zugriffskontrolle für Ihren Anwendungsfall wichtig ist. Unabhängig davon garantiert die Wahl einer

bestimmten Version OpenSearch oder einer Elasticsearch-Version bei der Erstellung einer Domain nicht die Einhaltung der Vorschriften.

Informationen darüber, ob AWS-Service ein in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter AWS-Services Umfang nach Compliance-Programm AWS-Services unter . Wählen Sie dort das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter AWS Compliance-Programme AWS .

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter Berichte herunterladen unter .

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS stellt die folgenden Ressourcen zur Verfügung, die Sie bei der Einhaltung der Vorschriften unterstützen:

- Compliance und Governance im Bereich Sicherheit – In diesen Anleitungen für die Lösungsimplementierung werden Überlegungen zur Architektur behandelt. Außerdem werden Schritte für die Bereitstellung von Sicherheits- und Compliance-Features beschrieben.
- Referenz für berechtigte HIPAA-Services – Listet berechtigte HIPAA-Services auf. Nicht alle AWS-Services sind HIPAA-fähig.
- AWS Compliance-Ressourcen — Diese Sammlung von Arbeitsmappen und Leitfäden gilt möglicherweise für Ihre Branche und Ihren Standort.
- AWS Leitfäden zur Einhaltung von Vorschriften für Kunden — Verstehen Sie das Modell der gemeinsamen Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Verfahren zur Sicherung zusammengefasst AWS-Services und die Leitlinien den Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zugeordnet.
- Evaluierung von Ressourcen anhand von Regeln im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub— Auf diese AWS-Service Weise erhalten Sie einen umfassenden Überblick über Ihren internen Sicherheitsstatus. AWS Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Die Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerelementreferenz.

- Amazon GuardDuty — Dies AWS-Service erkennt potenzielle Bedrohungen für Ihre Workloads AWS-Konten, Container und Daten, indem es Ihre Umgebung auf verdächtige und böswillige Aktivitäten überwacht. GuardDuty kann Ihnen helfen, verschiedene Compliance-Anforderungen wie PCI DSS zu erfüllen, indem es die in bestimmten Compliance-Frameworks vorgeschriebenen Anforderungen zur Erkennung von Eindringlingen erfüllt.
- AWS Audit Manager— Auf diese AWS-Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um das Risikomanagement und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

Ausfallsicherheit von Amazon OpenSearch Service

Im Zentrum der AWS globalen -Infrastruktur stehen die AWS-Regionen und -Availability Zones. AWS-Regionen stellen mehrere physisch getrennte und isolierte Availability Zones bereit, die über hoch redundante Netzwerke mit niedriger Latenz und hohen Durchsätzen verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Availability Zones ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser hoch verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen über AWS-Regionen und Availability Zones finden Sie unter AWS Globale -Infrastruktur.

Neben der AWS globalen -Infrastruktur stellt OpenSearch Service verschiedene Funktionen bereit, um Ihren Anforderungen an Ausfallsicherheit und Datensicherung gerecht zu werden:

- Multi-AZ-Domänen und Replikat-Shards
- Automatisierte und manuelle Snapshots

JWT-Authentifizierung und Autorisierung für Amazon Service OpenSearch

Amazon OpenSearch Service ermöglicht es Ihnen jetzt, JSON Web Tokens (JWTs) für die Authentifizierung und Autorisierung zu verwenden. JWTs sind JSON-basierte Zugriffstoken, die verwendet werden, um Single Sign-On (SSO) -Zugriff zu gewähren. Sie können JWTs in OpenSearch Service verwenden, um Single Sign-On-Token zu erstellen, um Anfragen an Ihre Service-Domain zu validieren. OpenSearch Für die Verwendung JWTs müssen Sie die detaillierte Zugriffskontrolle

aktiviert haben und einen gültigen öffentlichen Schlüssel im RSA- oder ECDSA-PEM-Format angeben. Weitere Informationen zur feinkörnigen Zugriffskontrolle finden Sie unter Feinkörnige Zugriffskontrolle in Amazon Service. OpenSearch

Sie können JSON-Web-Tokens mithilfe der OpenSearch Service-Konsole, der AWS Command Line Interface (AWS CLI) oder der konfigurieren. AWS SDKs

Überlegungen

Bevor Sie Amazon OpenSearch Service verwenden JWTs , müssen Sie Folgendes beachten:

- Aufgrund der Größe der öffentlichen RSA-Schlüssel in der PEM-Formatierung empfehlen wir, die JWT-Authentifizierung und -Autorisierung über die AWS Konsole zu konfigurieren.
- Sie müssen gültige Benutzer und Rollen angeben, wenn Sie die Felder für Themen und Rollen angeben. JWTs Andernfalls werden Anfragen abgelehnt.
- OpenSearch 2.11 ist die früheste kompatible Version, die für die JWT-Authentifizierung verwendet werden kann.

Ändern der Domainzugriffsrichtlinie

Bevor Sie Ihre Domain für die Verwendung der JWT-Authentifizierung und -Autorisierung konfigurieren können, müssen Sie Ihre Domain-Zugriffsrichtlinie aktualisieren, damit JWT-Benutzer auf die Domain zugreifen können. Andernfalls werden alle eingehenden autorisierten JWT-Anfragen abgelehnt. Die empfohlene Domänenzugriffsrichtlinie für den vollständigen Zugriff auf die Unterressourcen (/*) lautet:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": "es:ESHttp*",
      "Resource": "domain-arn/*"
    }
```

```
  ]
}
```

Konfiguration der JWT-Authentifizierung und -Autorisierung

Sie können die JWT-Authentifizierung und -Autorisierung während der Domainerstellung oder durch Aktualisierung einer vorhandenen Domain aktivieren. Die Einrichtungsschritte variieren geringfügig, je nachdem, welche Option Sie wählen.

In den folgenden Schritten wird erklärt, wie Sie eine vorhandene Domäne für die JWT-Authentifizierung und -Autorisierung in der OpenSearch Servicekonsole konfigurieren:

1. Navigieren Sie unter Domänenkonfiguration zu JWT-Authentifizierung und Autorisierung für OpenSearch und wählen Sie JWT-Authentifizierung und Autorisierung aktivieren aus.
2. Konfigurieren Sie den öffentlichen Schlüssel, der für Ihre Domain verwendet werden soll. Dazu können Sie entweder eine PEM-Datei hochladen, die einen öffentlichen Schlüssel enthält, oder ihn manuell eingeben.

   > **Note**
   >
   > Wenn der hochgeladene oder eingegebene Schlüssel nicht gültig ist, erscheint über dem Textfeld eine Warnung, die das Problem angibt.

3. (Optional) Unter Zusätzliche Einstellungen können Sie die folgenden optionalen Felder konfigurieren

   - Betreffschlüssel — Sie können dieses Feld leer lassen, um den `sub` Standardschlüssel für Ihren zu verwenden JWTs.
   - Rollenschlüssel — Sie können dieses Feld leer lassen, um den `roles` Standardschlüssel für Ihre zu verwenden JWTs.

   Nachdem Sie Ihre Änderungen vorgenommen haben, speichern Sie Ihre Domain.

Verwenden eines JWT zum Senden einer Testanfrage

Nachdem Sie ein neues JWT mit einem bestimmten Betreff- und Rollenpaar erstellt haben, können Sie eine Testanfrage senden. Verwenden Sie dazu den privaten Schlüssel, um Ihre Anfrage über das

Tool zu signieren, mit dem das JWT erstellt wurde. OpenSearch Der Service kann die eingehende Anfrage validieren, indem er diese Signatur überprüft.

> **Note**
>
> Wenn Sie einen benutzerdefinierten Betreff- oder Rollenschlüssel für Ihr JWT angegeben haben, müssen Sie die richtigen Anspruchsnamen für Ihr JWT verwenden.

Im Folgenden finden Sie ein Beispiel dafür, wie Sie ein JWT-Token verwenden, um über den Suchendpunkt Ihrer Domain auf den OpenSearch Service zuzugreifen:

```
curl -XGET "$search_endpoint" -H "Authorization: Bearer <JWT>"
```

Konfiguration der JWT-Authentifizierung und -Autorisierung ()AWS CLI

Der folgende AWS CLI Befehl aktiviert die JWT-Authentifizierung und -Autorisierung, OpenSearch sofern die Domäne vorhanden ist:

```
aws opensearch update-domain-config --domain-name <your_domain_name> --advanced-
security-options '{"JWTOptions":{"Enabled":true, "PublicKey": "<your_public_key>",
 "SubjectKey": "<your_subject_key>", "RolesKey": "<your_roles_key>"}}'
```

Konfiguration der JWT-Authentifizierung und -Autorisierung (Konfiguration über API)

Die folgende Anfrage an die Konfigurations-API aktiviert die JWT-Authentifizierung und -Autorisierung für OpenSearch eine bestehende Domain:

```
POST https://es.us-east-1.amazonaws.com/2021-01-01/opensearch/domain/my-domain/config
{
  "AdvancedSecurityOptions": {
    "JWTOptions": {
      "Enabled": true,
      "PublicKey": "public-key",
      "RolesKey": "optional-roles-key",
      "SubjectKey": "optional-subject-key"
   }
  }
}
```

Ein key pair generieren

Um die Konfiguration JWTs für Ihre OpenSearch Domain vorzunehmen, müssen Sie einen öffentlichen Schlüssel im PEM-Format (Privacy-Enhanced Mail) angeben. Amazon OpenSearch Service unterstützt derzeit zwei asymetrische Verschlüsselungsalgorithmen bei der Verwendung JWTs: RSA und ECDSA.

Gehen Sie folgendermaßen vor, um ein RSA-Schlüsselpaar mit der gemeinsamen OpenSSL-Bibliothek zu erstellen:

1. `openssl genrsa -out privatekey.pem 2048`
2. `openssl rsa -in privatekey.pem -pubout -out publickey.pem`

In diesem Beispiel enthält die `publickey.pem` Datei den öffentlichen Schlüssel für die Verwendung mit Amazon OpenSearch Service und `privatekey.pem` den privaten Schlüssel zum Signieren der JWTs an den Service gesendeten Daten. Darüber hinaus haben Sie die Möglichkeit, den privaten Schlüssel in das häufig verwendete `pkcs8` Format zu konvertieren, falls Sie ihn zur Generierung Ihres benötigen JWTs.

Wenn Sie die Upload-Schaltfläche verwenden, um eine PEM-Datei direkt zur Konsole hinzuzufügen, muss die Datei eine `.pem` Erweiterung haben. Andere Dateierweiterungen wie `.crt.cert`,, oder `.key` werden derzeit nicht unterstützt.

Infrastruktursicherheit in Amazon OpenSearch Service

Als verwalteter Service ist Amazon OpenSearch Service durch die AWS globale Netzwerksicherheit von geschützt. Informationen zu AWS -Sicherheitsdiensten und wie die Infrastruktur AWS schützt, finden Sie unter AWS Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS -Umgebung anhand der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastrukturschutz im Security Pillar AWS Well-Architected Framework.

Sie verwenden durch AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf OpenSearch Service zuzugreifen. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

Sie verwenden durch AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf die OpenSearch Service-Konfigurations-API zuzugreifen. Geben Sie in den Domain-Endpunkt-Optionen den `TLSSecurityPolicy`-Wert an, um die minimal erforderliche TLS-Version für die Annahme zu konfigurieren:

```
aws opensearch update-domain-config --domain-name my-domain --domain-endpoint-options
 '{"TLSSecurityPolicy": "Policy-Min-TLS-1-2-2019-07"}'
```

Einzelheiten finden Sie in der AWS CLI -Befehlsreferenz.

Abhängig von Ihrer Domain-Konfiguration müssen Sie möglicherweise auch Anfragen an die signieren OpenSearch APIs. Weitere Informationen finden Sie unter the section called “ OpenSearch Serviceanfragen stellen und signieren”.

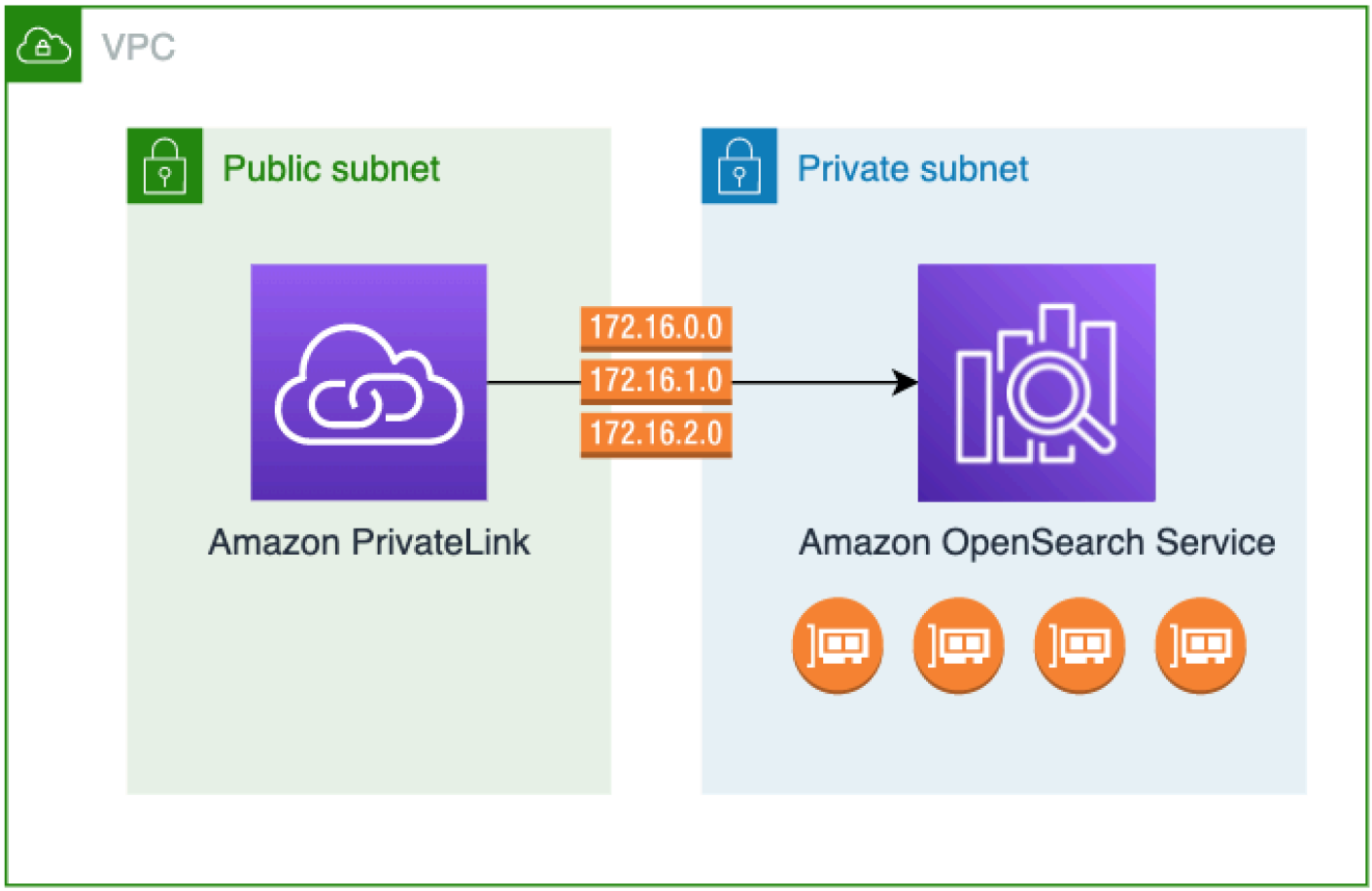
OpenSearch Der Service unterstützt öffentliche Zugriffsdomänen, die von jedem mit dem Internet verbundenen Gerät Anfragen erhalten können, und VPC-Zugriffsdomänen, die vom öffentlichen Internet isoliert sind.

Zugriff auf Amazon OpenSearch Service über einen vom Service OpenSearch verwalteten VPC-Endpunkt ()AWS PrivateLink

Sie können auf eine OpenSearch Amazon-Service-Domain zugreifen, indem Sie einen vom Service OpenSearch verwalteten VPC-Endpunkt (betrieben durch AWS PrivateLink) einrichten. Diese Endpunkte erstellen eine private Verbindung zwischen Ihrer VPC und Amazon OpenSearch Service. Sie können auf OpenSearch Service-VPC-Domains zugreifen, wenn diese sich in Ihrer VPC befinden, ohne dass dafür ein Internet-Gateway, ein NAT-Gerät, eine VPN-Verbindung oder AWS Direct Connect eine -Verbindung notwendig ist. Instances in Ihrer VPC benötigen keine öffentlichen IP-Adressen für den Zugriff auf den OpenSearch Service.

Sie können OpenSearch Service-Domains so konfigurieren, dass zusätzliche Endpunkte, die in öffentlichen oder privaten Subnetzen innerhalb derselben VPC, einer anderen VPC oder einer anderen ausgeführt werden, sichtbar werden. AWS-Konten Auf diese Weise können Sie eine zusätzliche Sicherheitsebene für den Zugriff auf Ihre Domains hinzufügen, unabhängig davon,

wo diese ausgeführt werden, ohne dass eine Infrastruktur verwaltet werden muss. Das folgende Diagramm zeigt die vom OpenSearch Service verwalteten VPC-Endpunkte innerhalb derselben VPC:



Sie stellen diese private Verbindung her, indem Sie einen von OpenSearch Service verwalteten Schnittstellen-VPC-Endpunkt erstellen, der von unterstützt wird. AWS PrivateLink Wir erstellen in jedem Subnetz, das Sie für den Schnittstellen-VPC-Endpunkt aktivieren, eine Endpunkt-Netzwerkschnittstelle. Hierbei handelt es sich um vom Service verwaltete Netzwerkschnittstellen, die als Eingangspunkt für den Datenverkehr dienen, der für den Service bestimmt ist. OpenSearch Für vom OpenSearch Service verwaltete VPC-Endpunkte, die unter abgerechnet werden, gelten die Standardpreise für AWS PrivateLink Schnittstellen-Endpunkte. AWS PrivateLink

Sie können VPC-Endpunkte für Domains erstellen, die alle Versionen von OpenSearch und ältere Elasticsearch-Versionen ausführen. Weitere Informationen finden Sie unter Zugriff auf AWS-Services über AWS PrivateLink im AWS PrivateLink -Leitfaden.

Überlegungen und Einschränkungen für den OpenSearch Service

Bevor Sie einen Schnittstellen-VPC-Endpunkt für den OpenSearch Service einrichten, lesen Sie über einen AWS Schnittstellen-VPC-Endpunkt im AWS PrivateLink -Leitfaden nach.

Berücksichtigen Sie bei der Verwendung von OpenSearch Service-verwalteten VPC-Endpunkten Folgendes:

- Sie können nur Schnittstellen-VPC-Endpunkte verwenden, um eine Verbindung zu VPC-Domains herzustellen. Öffentliche Domains werden nicht unterstützt.
- VPC-Endpunkte können nur eine Verbindung zu Domains innerhalb derselben AWS-Region herstellen.
- HTTPS ist das einzige unterstützte Protokoll für VPC-Endpunkte. HTTP ist nicht zulässig.
- OpenSearch Der Service unterstützt das Aufrufen aller unterstützten OpenSearch API-Operationen über einen Schnittstellen-VPC-Endpunkt.
- Sie können maximal 50 Endpunkte pro Konto und maximal 10 Endpunkte pro Domain konfigurieren. Eine einzelne Domain kann maximal über 10 autorisierte Prinzipale verfügen.
- Sie können derzeit nicht AWS CloudFormation zum Erstellen von Schnittstellen-VPC-Endpunkten verwenden.
- Sie können Schnittstellen-VPC-Endpunkte nur über die OpenSearch Service-Konsole oder mithilfe der OpenSearch Service-API erstellen. Sie können keine Schnittstellen-VPC-Endpunkte für OpenSearch Service mit der Amazon-VPC-Konsole erstellen.
- OpenSearch Von Service verwaltete VPC-Endpunkte sind nicht über das Internet zugänglich. Auf OpenSearch einen von Service verwalteten VPC-Endpunkt kann nur innerhalb der VPC zugegriffen werden, in der VPCs der Endpunkt gemäß den Routing-Tabellen und Sicherheitsgruppen bereitgestellt wird.
- VPC-Endpunktrichtlinien werden für OpenSearch Service nicht unterstützt. Sie können den Netzwerkschnittstellen des Endpunkts eine Sicherheitsgruppe zuordnen, um den Datenverkehr zum OpenSearch Service über die Benutzeroberfläche des Schnittstellen-VPC-Endpunkts zu steuern.
- Ihre serviceverknüpfte Rolle muss sich in demselben AWS Konto befinden, mit dem Sie den VPC-Endpunkt erstellt haben.
- Um den OpenSearch Service VPC-Endpunkt zu erstellen, zu aktualisieren und zu löschen, benötigen Sie zusätzlich zu Ihren Amazon EC2 OpenSearch Service-Berechtigungen die folgenden Amazon-Berechtigungen:

- `ec2:CreateVpcEndpoint`
- `ec2:DescribeVpcEndpoints`
- `ec2:ModifyVpcEndpoint`
- `ec2:DeleteVpcEndpoints`
- `ec2:CreateTags`
- `ec2:DescribeTags`
- `ec2:DescribeSubnets`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeVpcs`

> **Note**
>
> Derzeit können Sie die Erstellung von VPC-Endpunkten nicht auf OpenSearch Service beschränken. Wir arbeiten daran, dies in einem future Update zu ermöglichen.

Zugriff auf eine Domain bereitstellen

Wenn sich die VPC, über die Sie auf Ihre Domain zugreifen möchten, in einem anderen befindet AWS-Konto, benötigen Sie eine Autorisierung über das Konto des Eigentümers, bevor Sie einen Schnittstellen-VPC-Endpunkt erstellen können.

So gewähren Sie einer VPC in einem anderen AWS-Konto den Zugriff auf Ihre Domain

1. Öffnen Sie die Amazon OpenSearch Service-Konsole zu https://console.aws.amazon.com/aos/Hause/.
2. Wählen Sie im Navigationsbereich Domains aus und öffnen Sie die Domain, auf die Sie Zugriff gewähren möchten.
3. Wechseln Sie zur Registerkarte VPC endpoints (VPC-Endpunkte), auf der die Konten und entsprechenden angezeigt werden VPCs , die Zugriff auf Ihre Domain haben.
4. Wählen Sie Authorize principal (Prinzipal autorisieren) aus.
5. Geben Sie die AWS-Konto -ID des Kontos ein, das auf Ihre Domain zugreift. Dieser Schritt autorisiert das angegebene Konto, VPC-Endpunkte für die Domain zu erstellen.
6. Klicken Sie auf Authorize.

Erstellen eines Schnittstellen-VPC-Endpunkts für eine VPC-Domain

Sie können einen Schnittstellen-VPC-Endpunkt für OpenSearch Service erstellen, indem Sie entweder die OpenSearch Service-Konsole oder AWS Command Line Interface (AWS CLI) verwenden.

So erstellen Sie einen Schnittstellen-VPC-Endpunkt für eine OpenSearch Service-Domain

1. Öffnen Sie die Amazon OpenSearch Service-Konsole zu https://console.aws.amazon.com/aos/Hause/.
2. Wählen Sie im linken Navigationsbereich VPC endpoints (VPC-Endpunkte) aus.
3. Wählen Sie Endpunkt erstellen aus.
4. Wählen Sie, ob die Verbindung zu einer Domain im aktuellen AWS-Konto oder einem anderen hergestellt werden soll AWS-Konto.
5. Wählen Sie die Domain aus, zu der Sie mit diesem Endpunkt eine Verbindung herstellen. Wenn sich die Domain im aktuellen befindet AWS-Konto, verwenden Sie das Dropdown-Menü, um die Domain auszuwählen. Wenn sich die Domain in einem anderen Konto befindet, geben Sie den Amazon-Ressourcennamen (ARN) der Domain ein, zu der eine Verbindung hergestellt werden soll. Um eine Domain in einem anderen Konto auszuwählen, muss der Eigentümer Ihnen Zugriff auf die Domain gewähren.
6. Wählen Sie für VPC die VPC aus, von der aus Sie auf Service zugreifen OpenSearch .
7. Wählen Sie für Subnets (Subnetze) ein oder mehrere Subnetze aus, von denen aus Sie auf Service zugreifen OpenSearch möchten.
8. Wählen Sie für Sicherheitsgruppen die Sicherheitsgruppen aus, die den Security groups (Endpunkt-Netzwerkschnittstellen) zugeordnet werden sollen. Dies ist ein wichtiger Schritt, in dem Sie einschränken, welche Ports, Protokolle und Quellen für eingehenden Datenverkehr Sie für Ihren Endpunkt autorisieren. Die Sicherheitsgruppenregeln müssen den Ressourcen, die den VPC-Endpunkt für die Kommunikation mit dem OpenSearch Service verwenden, die Kommunikation mit der Netzwerkschnittstelle des Endpunkts ermöglichen.
9. Wählen Sie Endpunkt erstellen aus. Der Endpunkt sollte innerhalb von 2–5 Minuten aktiv sein.

Arbeiten mit von OpenSearch Service verwalteten VPC-Endpunkten mithilfe der Konfigurations-API

Verwenden Sie die folgenden API-Operationen, um vom OpenSearch Service verwaltete VPC-Endpunkte zu erstellen und zu verwalten.

- CreateVpcEndpoint
- ListVpcEndpoints
- UpdateVpcEndpoint
- DeleteVpcEndpoint

Verwenden Sie die folgenden API-Operationen, um den Endpunktzugriff auf VPC-Domains zu verwalten:

- AuthorizeVpcEndpointAccess
- ListVpcEndpointAccess
- ListVpcEndpointsForDomain
- RevokeVpcEndpointAccess

SAML-Authentifizierung für Dashboards OpenSearch

Mit der SAML-Authentifizierung für OpenSearch Dashboards können Sie Ihren bestehenden Identitätsanbieter verwenden, um Single Sign-On (SSO) für Dashboards auf Amazon OpenSearch Service-Domains anzubieten, auf denen Elasticsearch 6.7 OpenSearch oder höher ausgeführt wird. Um die SAML-Authentifizierung zu verwenden, müssen Sie differenzierte Zugriffssteuerung aktivieren.

Anstatt sich über Amazon Cognito oder die interne Benutzerdatenbank zu authentifizieren, können Sie mit der SAML-Authentifizierung für OpenSearch Dashboards Identitätsanbieter von Drittanbietern verwenden, um sich bei Dashboards anzumelden, eine detaillierte Zugriffskontrolle zu verwalten, Ihre Daten zu durchsuchen und Visualisierungen zu erstellen. OpenSearch Der Service unterstützt Anbieter, die den SAML 2.0-Standard verwenden, wie Okta, Keycloak, Active Directory Federation Services (ADFS), Auth0 und. AWS IAM Identity Center

Die SAML-Authentifizierung für Dashboards ist nur für den Zugriff auf Dashboards über einen Webbrowser vorgesehen. OpenSearch Mit Ihren SAML-Anmeldeinformationen können Sie keine direkten HTTP-Anfragen an die oder -Dashboards stellen. OpenSearch APIs

SAML-Konfigurationsübersicht

In dieser Dokumentation wird davon ausgegangen, dass Sie über einen vorhandenen Identitätsanbieter verfügen und damit vertraut sind. Wir können keine detaillierten

Konfigurationsschritte für Ihren genauen Anbieter bereitstellen, sondern nur für Ihre OpenSearch Service-Domain.

Der OpenSearch Anmeldevorgang für Dashboards kann eine von zwei Formen annehmen:

- Dienstanbieter (SP) initiiert: Sie navigieren zu Dashboards (z. B. `https://my-domain.us-east-1.es.amazonaws.com/_dashboards`), die Sie zum Anmeldebildschirm weiterleiten. Nachdem Sie sich angemeldet haben, leitet Sie der Identitätsanbieter zu Dashboards weiter.
- Identity Provider (IdP) initiiert: Sie navigieren zu Ihrem Identitätsanbieter, melden sich an und wählen OpenSearch Dashboards aus einem Anwendungsverzeichnis aus.

OpenSearch Der Service bietet zwei URLs Single-Sign-On-Optionen: SP-initiiert und IdP-initiiert. Sie benötigen jedoch nur das eine, das Ihrem gewünschten Dashboard-Anmeldeablauf entspricht. OpenSearch

Unabhängig davon, welchen Authentifizierungstyp Sie verwenden, besteht das Ziel darin, sich über Ihren Identitätsanbieter anzumelden und eine SAML-Assertion zu erhalten, die Ihren Benutzernamen (erforderlich) und alle Backend-Rollen (optional, aber empfohlen) enthält. Diese Informationen ermöglichen eine differenzierte Zugriffssteuerung, um SAML-Benutzern Berechtigungen zuzuweisen. Bei externen Identitätsanbietern werden Backend-Rollen normalerweise als „Rollen“ oder „Gruppen“ bezeichnet.

Überlegungen

Berücksichtigen Sie beim Konfigurieren der SAML-Authentifizierung Folgendes:

- Aufgrund der Größe der IdP-Metadatendatei empfehlen wir dringend, die SAML-Authentifizierung über die AWS Konsole zu konfigurieren.
- Domains unterstützen jeweils nur eine Dashboards-Authentifizierungsmethode. Wenn Sie die Amazon Cognito Cognito-Authentifizierung für OpenSearch Dashboards aktiviert haben, müssen Sie sie deaktivieren, bevor Sie die SAML-Authentifizierung aktivieren können.
- Wenn Sie einen Network Load Balancer mit SAML verwenden, müssen Sie zunächst einen benutzerdefinierten Endpunkt erstellen. Weitere Informationen finden Sie unter ???.
- Service Control Policies (SCP) werden im Fall von Nicht-IAM-Identitäten (wie SAML in Amazon OpenSearch Serverless und SAML und grundlegende interne Benutzerautorisierung für Amazon Service) nicht angewendet oder bewertet. OpenSearch

SAML-Authentifizierung für VPC-Domains

SAML erfordert keine direkte Kommunikation zwischen Ihrem Identitätsanbieter und Ihrem Serviceanbieter. Daher können Sie SAML auch dann verwenden, wenn Ihre OpenSearch Domain in einer privaten VPC gehostet wird, solange Ihr Browser sowohl mit Ihrem OpenSearch Cluster als auch mit Ihrem Identitätsanbieter kommunizieren kann. Ihr Browser fungiert im Wesentlichen als Vermittler zwischen Ihrem Identitätsanbieter und Ihrem Dienstanbieter. Ein nützliches Diagramm, das den SAML-Authentifizierungsablauf erklärt, finden Sie in der Okta-Dokumentation.

Ändern der Domainzugriffsrichtlinie

Bevor Sie die SAML-Authentifizierung konfigurieren, müssen Sie die Domainzugriffsrichtlinie aktualisieren, um SAML-Benutzern Zugriff auf die Domain zu gewähren. Andernfalls werden Ihnen „Zugriff verweigert“-Fehler angezeigt.

Wir empfehlen die folgende Domain-Zugriffsrichtlinie, die vollen Zugriff auf die Unterressourcen (`/*`) in der Domain bietet:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": "es:ESHttp*",
      "Resource": "domain-arn/*"
    }
  ]
}
```

Um die Richtlinie restriktiver zu gestalten, können Sie der Richtlinie eine IP-Adressbedingung hinzufügen. Diese Bedingung beschränkt den Zugriff nur auf den angegebenen IP-Adressbereich oder das angegebene Subnetz. Die folgende Richtlinie erlaubt beispielsweise den Zugriff nur vom Subnetz 192.0.2.0/24 aus:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": [
        "es:ESHttp*"
      ],
      "Condition": {
        "IpAddress": {
          "aws:SourceIp": [
            "192.0.2.0/24"
          ]
        }
      },
      "Resource": "domain-arn/*"
    }
  ]
}
```

Note

Eine offene Domänenzugriffsrichtlinie erfordert, dass eine detaillierte Zugriffskontrolle für Ihre Domain aktiviert ist. Andernfalls wird der folgende Fehler angezeigt:
`To protect domains with public access, a restrictive policy or fine-grained access control is required.`
Wenn Sie einen Masterbenutzer oder internen Benutzer mit einem sicheren Passwort konfiguriert haben, kann es aus Sicherheitsgründen akzeptabel sein, die Richtlinie offen zu lassen und gleichzeitig eine differenzierte Zugriffskontrolle zu verwenden. Weitere Informationen finden Sie unter ???.

Konfigurieren der SP- oder IDP-initiierten Authentifizierung

In diesen Schritten wird erklärt, wie die SAML-Authentifizierung mit SP-initiierter oder IDP-initiierter Authentifizierung für Dashboards aktiviert wird. OpenSearch Informationen zum zusätzlichen Schritt, der zum Aktivieren beider Authentifizierungen erforderlich ist, finden Sie unter Konfigurieren der SP- oder IdP-initiierten Authentifizierung.

Schritt 1: SAML-Authentifizierung aktivieren

Sie können die SAML-Authentifizierung entweder während der Domainerstellung aktivieren oder indem Sie für eine vorhandene Domain Actions (Aktionen), Edit security configuration (Sicherheitskonfiguration bearbeiten) auswählen. Die folgenden Schritte unterscheiden sich geringfügig, je nachdem, welchen Sie auswählen.

Wählen Sie in der Domänenkonfiguration unter SAML-Authentifizierung für OpenSearch Dashboards/Kibana die Option SAML-Authentifizierung aktivieren aus.

Schritt 2: Ihren Identitätsanbieter konfigurieren

Führen Sie die folgenden Schritte aus, je nachdem, wann Sie die SAML-Authentifizierung konfigurieren.

Wenn Sie eine Domain erstellen

Wenn Sie gerade dabei sind, eine neue Domain zu erstellen, kann OpenSearch Service noch keine Entitäts-ID oder SSO für den Dienstanbieter generieren. URLs Ihr Identitätsanbieter benötigt diese Werte, um die SAML-Authentifizierung ordnungsgemäß zu aktivieren. Sie können jedoch erst generiert werden, nachdem die Domain erstellt wurde. Um diese Interdependenz bei der Domainerstellung zu umgehen, können Sie temporäre Werte in Ihre IdP-Konfiguration eingeben, um die erforderlichen Metadaten zu generieren, und sie dann aktualisieren, sobald Ihre Domain aktiv ist.

Wenn Sie einen benutzerdefinierten Endpunkt verwenden, können Sie ableiten, welcher dieser sein URLs wird. Wenn Ihr benutzerdefinierter Endpunkt beispielsweise `www.custom-endpoint.com` lautet, lautet die Entitäts-ID des Serviceanbieters `www.custom-endpoint.com`, die IDP-initiierte SSO-URL lautet `www.custom-endpoint.com/_dashboards/_opendistro/_security/saml/acs/idpinitiated` und die SP-initiierte SSO-URL ist `www.custom-endpoint.com/_dashboards/_opendistro/_security/saml/acs`. Sie können die Werte verwenden, um Ihren Identitätsanbieter zu konfigurieren, bevor die Domain erstellt wird. Beispiele finden Sie im nächsten Abschnitt.

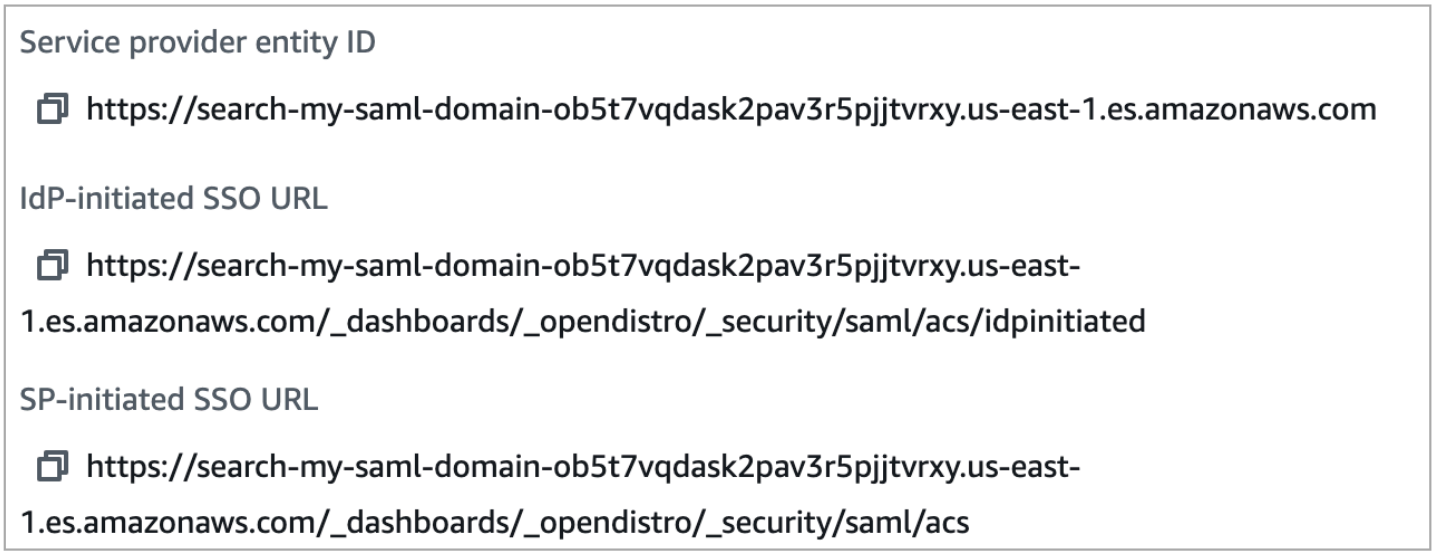
> **Note**
>
> Sie können sich nicht mit einem Dual-Stack-Endpunkt anmelden, da sich der FQDN einer HTTP-Anfrage vom FQDN einer SAML-Anfrage unterscheidet. Ein OpenSearch Administrator muss einen benutzerdefinierten Endpunkt einrichten und den CNAME-Wert auf Dual-Stack-Endpunkt setzen, wenn Sie sich mit einem Dual-Stack-Endpunkt anmelden möchten.

Wenn Sie keinen benutzerdefinierten Endpunkt verwenden, können Sie temporäre Werte in Ihren IdP eingeben, um die erforderlichen Metadaten zu generieren, und sie später aktualisieren, nachdem die Domain aktiv ist.

In Okta können Sie beispielsweise `https://temp-endpoint.amazonaws.com` in die Felder Single Sign On URL und Audience URI (SP Entity ID) eingeben, wodurch Sie die Metadaten generieren können. Sobald die Domain aktiv ist, können Sie dann die richtigen Werte aus OpenSearch Service abrufen und in Okta aktualisieren. Detaillierte Anweisungen finden Sie unter the section called “Schritt 6: Aktualisiere deinen IdP URLs”.

Wenn Sie eine bestehende Domain bearbeiten

Wenn Sie die SAML-Authentifizierung für eine bestehende Domain aktivieren, kopieren Sie die Entitäts-ID des Dienstanbieters und eine der SSO-Daten. URLs Hinweise zu der zu verwendenden URL finden Sie unter the section called “SAML-Konfigurationsübersicht”.



Verwenden Sie die Werte, um Ihren Identitätsanbieter zu konfigurieren. Dies ist der komplexeste Teil des Prozesses, und leider variieren Terminologie und Schritte je nach Anbieter stark. Schlagen Sie in der Dokumentation Ihres Anbieters nach.

In Okta erstellen Sie beispielsweise eine SAML 2.0-Webanwendung. Geben Sie für Single Sign-On-On-URL die SSO-URL an. Geben Sie für Zielgruppen-URI (SP-Entitäts-ID) die SP-Entitäts-ID an.

Anstelle von Benutzern und Backend-Rollen hat Okta Benutzer und Gruppen. Für Group Attribute Statements (Anweisungen zu Gruppenattributen) empfehlen wir, `role` zum Feld Name und den regulären Ausdruck `.+` zum Feld Filter hinzuzufügen. Diese Anweisung weist den Okta-Identitätsanbieter an, alle Benutzergruppen unter das `role`-Feld der SAML-Assertion aufzunehmen, nachdem sich ein Benutzer authentifiziert hat.

In IAM Identity Center geben Sie die SP-Entitäts-ID als SAML-Anwendungszielgruppe an. Sie müssen außerdem die folgenden Attributzuordnungen angeben: und. `Subject=${user:subject}:format=unspecified` `Role=${user:groups}:format=uri`

In Auth0 erstellen Sie eine reguläre Webanwendung und aktivieren das SAML 2.0-Add-on. In Keycloak erstellen Sie einen Client.

Schritt 3: IdP-Metadaten importen

Nachdem Sie Ihren Identitätsanbieter konfiguriert haben, wird eine IdP-Metadatendatei generiert. Diese XML-Datei enthält Informationen zum Anbieter, z. B. ein TLS-Zertifikat, Single Sign-On-Endpunkte und die Entitäts-ID des Identitätsanbieters.

Kopieren Sie den Inhalt der IdP-Metadatendatei und fügen Sie ihn in das Feld Metadaten von IdP in der OpenSearch Servicekonsole ein. Wählen Sie alternativ Aus XML-Datei importieren und laden Sie die Datei hoch. Die Metadatendatei sollte ungefähr so aussehen:

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor entityID="entity-id"
 xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
  <md:IDPSSODescriptor WantAuthnRequestsSigned="false"
 protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>tls-certificate</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
```

```
    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</
md:NameIDFormat>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</
md:NameIDFormat>
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
 Location="idp-sso-url"/>
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
Redirect" Location="idp-sso-url"/>
  </md:IDPSSODescriptor>
</md:EntityDescriptor>
```

Schritt 4: SAML-Felder konfigurieren

Nachdem Sie Ihre IdP-Metadaten eingegeben haben, konfigurieren Sie die folgenden zusätzlichen Felder in der OpenSearch Servicekonsole:

- IdP entity ID – Kopieren Sie den Wert der Eigenschaft `entityID` aus Ihrer Metadatendatei und fügen Sie ihn in dieses Feld ein. Viele Identitätsanbieter zeigen diesen Wert auch als Teil einer Zusammenfassung nach der Konfiguration an. Manche Anbieter nennen ihn „Aussteller“.
- SAML-Master-Benutzername und SAML-Master-Backend-Rolle — Die von Ihnen angegebene and/or Benutzer-Backend-Rolle erhält volle Berechtigungen für den Cluster, was einem neuen Masterbenutzer entspricht, kann diese Berechtigungen jedoch nur innerhalb von Dashboards verwenden. OpenSearch

  In Okta könnten Sie beispielsweise einen Benutzer `jdoe` haben, der zur Gruppe `admins` gehört. Wenn Sie `jdoe` zum Feld für den SAML-Hauptbenutzernamen hinzufügen, erhält nur dieser Benutzer vollständige Berechtigungen. Wenn Sie `admins` zum Feld für die SAML-Haupt-Backend-Rolle hinzufügen, erhält jeder Benutzer, der zu der `admins`-Gruppe gehört, vollständige Berechtigungen.

> **Note**
>
> Der Inhalt der SAML-Assertion muss genau mit den Zeichenfolgen übereinstimmen, die Sie für den SAML-Hauptbenutzernamen und die SAML-Hauptrolle verwenden. Einige Identitätsanbieter fügen vor ihren Benutzernamen ein Präfix hinzu, was zu einer Nichtübereinstimmung führen kann. hard-to-diagnose In der Benutzeroberfläche des Identity Providers wird möglicherweise `jdoe` angezeigt, aber die SAML-Assertion kann `auth0|jdoe` enthalten. Verwenden Sie immer die Zeichenfolge aus der SAML-Assertion.

Bei vielen Identitätsanbietern können Sie während des Konfigurationsprozesses eine Beispiel-Assertion anzeigen, und Tools wie SAML-tracer können Ihnen dabei helfen, den Inhalt echter Assertionen zu untersuchen und Fehler zu beheben. Assertions sehen in etwa wie folgt aus:

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2:Assertion ID="id67229299299259351343340162"
 IssueInstant="2020-09-22T22:03:08.633Z" Version="2.0"
  xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
  <saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">idp-issuer</
saml2:Issuer>
  <saml2:Subject>
    <saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:unspecified">username</saml2:NameID>
    <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
      <saml2:SubjectConfirmationData NotOnOrAfter="2020-09-22T22:08:08.816Z"
 Recipient="domain-endpoint/_dashboards/_opendistro/_security/saml/acs"/>
    </saml2:SubjectConfirmation>
  </saml2:Subject>
  <saml2:Conditions NotBefore="2020-09-22T21:58:08.816Z"
 NotOnOrAfter="2020-09-22T22:08:08.816Z">
    <saml2:AudienceRestriction>
      <saml2:Audience>domain-endpoint</saml2:Audience>
    </saml2:AudienceRestriction>
  </saml2:Conditions>
  <saml2:AuthnStatement AuthnInstant="2020-09-22T19:54:37.274Z">
    <saml2:AuthnContext>

 <saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport<
saml2:AuthnContextClassRef>
    </saml2:AuthnContext>
  </saml2:AuthnStatement>
  <saml2:AttributeStatement>
    <saml2:Attribute Name="role" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:unspecified">
      <saml2:AttributeValue
        xmlns:xs="http://www.w3.org/2001/XMLSchema"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:type="xs:string">GroupName Match Matches regex ".+" (case-sensitive)
      </saml2:AttributeValue>
    </saml2:Attribute>
  </saml2:AttributeStatement>
</saml2:Assertion>
```

Schritt 5: (Optional) Zusätzliche Einstellungen konfigurieren

Konfigurieren Sie unter Additional settings (Zusätzliche Einstellungen) die folgenden optionalen Felder:

- Subject key (Betreffsschlüssel) – Sie können dieses Feld leer lassen, um das Element `NameID` der SAML-Assertion für den Benutzernamen zu verwenden. Wenn Ihre Assertion dieses Standardelement nicht verwendet und stattdessen den Benutzernamen als benutzerdefiniertes Attribut enthält, geben Sie dieses Attribut hier an.
- Roles key (Rollenschlüssel) – Wenn Sie Backend-Rollen verwenden möchten (empfohlen), geben Sie in diesem Feld ein Attribut aus der Assertion an, z. B. `role` oder `group`. Dies ist eine weitere Situation, in der Tools wie SAML-tracer helfen können.
- Gültigkeitsdauer der Sitzung — Standardmäßig meldet OpenSearch Dashboards Benutzer nach 24 Stunden ab. Sie können diesen Wert auf eine beliebige Zahl zwischen 60 und 1.440 (24 Stunden) einstellen, indem Sie einen neuen Wert angeben.

Wenn Sie mit Ihrer Konfiguration zufrieden sind, speichern Sie die Domain.

Schritt 6: Aktualisiere deinen IdP URLs

Wenn Sie bei der Erstellung einer Domain die SAML-Authentifizierung aktiviert haben, mussten Sie URLs in Ihrem IdP temporär angeben, um die XML-Metadatendatei zu generieren. Nachdem sich der Domainstatus auf geändert hat`Active`, können Sie den richtigen Wert ermitteln URLs und Ihren IdP ändern.

Um den abzurufen URLs, wählen Sie die Domain aus und klicken Sie auf Aktionen, Sicherheitskonfiguration bearbeiten. Unter SAML-Authentifizierung für OpenSearch Dashboards/ Kibana finden Sie die richtige Entitäts-ID und SSO des Dienstanbieters. URLs Kopieren Sie die Werte und verwenden Sie sie, um Ihren Identitätsanbieter zu konfigurieren. Ersetzen Sie dabei den temporären Wert, den Sie in Schritt 2 URLs angegeben haben.

Schritt 7: SAML-Benutzer Rollen zuordnen

Sobald Ihr Domainstatus Aktiv ist und Ihr IdP korrekt konfiguriert ist, navigieren Sie zu OpenSearch Dashboards.

- Wenn Sie die vom SP initiierte URL gewählt haben, navigieren Sie zu *`domain-endpoint`*`/_dashboards`. Um sich direkt bei einem bestimmten Mandanten anzumelden, können Sie `?security_tenant=`*`tenant-name`* an die URL anhängen.

- Wenn Sie die vom IdP initiierte URL ausgewählt haben, navigieren Sie zum Anwendungsverzeichnis Ihres Identitätsanbieters.

Melden Sie sich in beiden Fällen entweder als SAML-Haupt-Benutzer oder als Benutzer an, der zur SAML-Haupt-Backend-Rolle gehört. Um das Beispiel ab Schritt 7 fortzusetzen, melden Sie sich entweder als `jdoe` oder als Mitglied der Gruppe `admins` an.

Wählen Sie nach dem Laden der OpenSearch Dashboards Sicherheit, Rollen aus. Ordnen Sie dann Rollen zu, damit andere Benutzer auf OpenSearch Dashboards zugreifen können.

Sie können beispielsweise Ihren vertrauenswürdigen Kollegen `jroe` den Rollen `all_access` und `security_manager` zuordnen. Sie können die Backend-Rolle `analysts` auch den Rollen `readall` und `opensearch_dashboards_user` zuordnen.

Wenn Sie lieber die API als OpenSearch Dashboards verwenden möchten, sehen Sie sich die folgende Beispielanfrage an:

```
PATCH _plugins/_security/api/rolesmapping
[
  {
    "op": "add", "path": "/security_manager", "value": { "users": ["master-user",
 "jdoe", "jroe"], "backend_roles": ["admins"] }
  },
  {
    "op": "add", "path": "/all_access", "value": { "users": ["master-user", "jdoe",
 "jroe"], "backend_roles": ["admins"] }
  },
  {
    "op": "add", "path": "/readall", "value": { "backend_roles": ["analysts"] }
  },
  {
    "op": "add", "path": "/opensearch_dashboards_user", "value": { "backend_roles":
 ["analysts"] }
  }
]
```

Konfigurieren der SP- und der IDP-initiierten Authentifizierung

Wenn Sie sowohl SP- als auch IdP-initiierte Authentifizierung konfigurieren möchten, müssen Sie dies über Ihren Identitätsanbieter tun. In Okta können Sie beispielsweise die folgenden Schritte ausführen:

1. Gehen Sie in Ihrer SAML-Anwendung zu General (Allgemeines), SAML settings (SAML-Einstellungen).
2. Geben Sie für die Single sign on URL (Single-Sign-On-URL) Ihre IdP-initiierte SSO-URL an. Beispiel, `https://search-domain-hash/_dashboards/_opendistro/_security/saml/acs/idpinitiated`.
3. Aktivieren Sie die Option Dieser App erlauben, anderes SSO URLs anzufordern.
4. Fügen Sie unter Anforderbares SSO URLs ein oder mehrere SP-initiierte SSO hinzu. URLs Beispiel, `https://search-domain-hash/_dashboards/_opendistro/_security/saml/acs`.

Konfigurieren der SAML-Authentifizierung (AWS CLI)

Der folgende AWS CLI Befehl aktiviert die SAML-Authentifizierung für OpenSearch Dashboards in einer vorhandenen Domain:

```
aws opensearch update-domain-config \
  --domain-name my-domain \
  --advanced-security-options '{"SAMLOptions":{"Enabled":true,"MasterUserName":"my-idp-user","MasterBackendRole":"my-idp-group-or-role","Idp":{"EntityId":"entity-id","MetadataContent":"metadata-content-with-quotes-escaped"},"RolesKey":"optional-roles-key","SessionTimeoutMinutes":180,"SubjectKey":"optional-subject-key"}}'
```

Sie müssen alle Anführungszeichen und Zeilenumbrüche in der Metadaten-XML maskieren. Verwenden Sie z. B.`<KeyDescriptor use=\"signing\">\n` anstelle von `<KeyDescriptor use="signing">` und einen Zeilenumbruch. Ausführliche Informationen zur Verwendung der AWS CLI finden Sie in der AWS CLI -Befehlsreferenz.

Konfigurieren der SAML-Authentifizierung (Konfigurations-API)

Die folgende Anfrage an die Konfigurations-API aktiviert die SAML-Authentifizierung für OpenSearch Dashboards in einer vorhandenen Domain:

```
POST https://es.us-east-1.amazonaws.com/2021-01-01/opensearch/domain/my-domain/config
{
  "AdvancedSecurityOptions": {
    "SAMLOptions": {
      "Enabled": true,
```

```
      "MasterUserName": "my-idp-user",
      "MasterBackendRole": "my-idp-group-or-role",
      "Idp": {
        "EntityId": "entity-id",
        "MetadataContent": "metadata-content-with-quotes-escaped"
      },
      "RolesKey": "optional-roles-key",
      "SessionTimeoutMinutes": 180,
      "SubjectKey": "optional-subject-key"
    }
  }
}
```

Sie müssen alle Anführungszeichen und Zeilenumbrüche in der Metadaten-XML maskieren. Verwenden Sie z. B.`<KeyDescriptor use=\"signing\">\n` anstelle von `<KeyDescriptor use="signing">` und einen Zeilenumbruch. Ausführliche Informationen zur Verwendung der Konfigurations-API finden Sie in der OpenSearch Service-API-Referenz.

SAML-Fehlerbehebung

Fehler	Details
Ihre Anfrage: '*/some/path* ' ist nicht zulässig.	Vergewissern Sie sich, dass Sie Ihrem Identität sanbieter die richtige SSO-URL (Schritt 3) bereitges tellt haben.
Geben Sie ein gültiges Metadaten dokument des Identitätsanbieters an, um SAML zu aktivieren.	Ihre IdP-Metadatendatei entspricht nicht dem SAML 2.0-Standard. Überprüfen Sie mit einem Validieru ngstool auf Fehler.
SAML-Konfigurationsoptionen sind in der Konsole nicht sichtbar.	Aktualisieren Sie auf die neueste Servicesoftware.
SAML-Konfigurationsfehler: Beim Abrufen der SAML-Konfiguration ist ein Fehler aufgetreten. Bitte überprüfen Sie Ihre Einstellungen.	Dieser allgemeine Fehler kann aus vielen Gründen auftreten. • Überprüfen Sie, ob Sie Ihrem Identitätsanbieter die richtige SP-Entitäts-ID und SSO-URL bereitgestellt haben.

Fehler	Details
	• Generieren Sie die IdP-Metadatendatei neu und überprüfen Sie die IdP-Entitäts-ID. Fügen Sie alle aktualisierten Metadaten in der AWS Konsole hinzu. • Vergewissern Sie sich, dass Ihre Domain-Zugriffsrichtlinie den Zugriff auf OpenSearch Dashboards und `_plugins/_security/*` ermöglicht. Generell empfehlen wir eine offene Zugriffsrichtlinie für Domains, die eine differenzierte Zugriffskontrolle verwenden. • Schritte zum Konfigurieren von SAML finden Sie in der Dokumentation Ihres Identitätsanbieters.
Fehlende Rolle: Für diesen Benutzer sind keine Rollen verfügbar, bitte wenden Sie sich an Ihren Systemadministrator.	Sie haben sich erfolgreich authentifiziert, aber der Benutzername und alle Backend-Rollen aus der SAML-Assertion sind keinen Rollen zugeordnet und haben daher keine Berechtigungen. Bei diesen Mappings muss die Groß-/Kleinschreibung beachtet werden. Ihr Systemadministrator kann den Inhalt Ihrer SAML-Assertion mit einem Tool wie SAML-Tracer überprüfen und anschließend Ihre Rollenzuweisung anhand der folgenden Anfrage überprüfen: `GET _plugins/_security/api/rolesmapping`
Ihr Browser leitet kontinuierlich um oder empfängt HTTP 500-Fehler, wenn er versucht, auf Dashboards zuzugreifen. OpenSearch	Diese Fehler können auftreten, wenn Ihre SAML-Assertion eine große Anzahl von Rollen mit insgesamt etwa 1.500 Zeichen enthält. Wenn Sie beispielsweise 80 Rollen übergeben, deren durchschnittliche Länge 20 Zeichen beträgt, überschreiten Sie möglicherweise die Größenbeschränkung für Cookies in Ihrem Webbrowser. Ab OpenSearch Version 2.7 unterstützt die SAML-Assertion Rollen mit bis zu 5000 Zeichen.

Fehler	Details
Sie können sich nicht von ADFS abmelden.	ADFS erfordert, dass alle Abmeldeanfragen signiert sind, was der OpenSearch Service nicht unterstützt. `<SingleLogoutService />` Aus der IdP-Metadatendatei entfernen, um OpenSearch Service zu zwingen, seinen eigenen internen Abmeldemechanismus zu verwenden.
`Could not find entity descriptor for __PATH__.`	Die Entitäts-ID des IdP, die in der Metadaten-XML to OpenSearch Service bereitgestellt wird, unterscheidet sich von der in der SAML-Antwort. Um dieses Problem zu beheben, stellen Sie sicher, dass sie übereinstimmen. Aktivieren Sie die CW-Anwendungsfehlerprotokolle auf Ihrer Domain, um die Fehlermeldung zum Debuggen des SAML-Integrationsproblems zu finden.
`Signature validation failed. SAML response rejected.`	OpenSearch Der Dienst kann die Signatur in der SAML-Antwort mithilfe des in Metadaten-XML bereitgestellten Zertifikats des IdP nicht überprüfen. Dies könnte entweder ein manueller Fehler sein oder Ihr IdP hat sein Zertifikat rotiert. Aktualisieren Sie das neueste Zertifikat von Ihrem IdP in der Metadaten-XML, die dem OpenSearch Service über die AWS Management Console zur Verfügung gestellt wird.
`__PATH__ is not a valid audience for this response.`	Das Zielgruppenfeld in der SAML-Antwort entspricht nicht dem Domain-Endpunkt. Um diesen Fehler zu beheben, aktualisieren Sie das SP-Zielgruppenfeld so, dass es Ihrem Domain-Endpunkt entspricht. Wenn Sie benutzerdefinierte Endpunkte aktiviert haben, sollte das Zielgruppenfeld Ihrem benutzerdefinierten Endpunkt entsprechen. Aktivieren Sie CW-Anwendungsfehlerprotokolle auf Ihrer Domain, um die Fehlermeldung zum Debuggen des SAML-Integrationsproblems zu finden.

Fehler	Details
Ihr Browser erhält in der Antwort einen HTTP 400-Fehler mit`Invalid Request Id`.	Dieser Fehler tritt im Allgemeinen auf, wenn Sie die vom IDP initiierte URL mit dem Format konfiguriert haben. *<DashboardsURL>* /_opendistro/_security/saml/acs Konfigurieren Sie die URL stattdessen mit dem Format. *<DashboardsURL>* /_opendistro/_security/saml/acs/idpinitiated
Die Antwort wurde am __PATH__ statt am empfangen__PATH__.	Das Zielfeld in der SAML-Antwort entspricht keinem der folgenden URL-Formate: • *<DashboardsURL>* /_opendistro/_security/saml/acs • *<DashboardsURL>* /_opendistro/_security/saml/acs/idpinitiated . Geben Sie je nach verwendetem Anmeldeablauf (SP-initiiert oder IDP-initiiert) ein Zielfeld ein, das mit einem der folgenden übereinstimmt. OpenSearch URLs
Die Antwort hat ein `InResponseTo` Attribut, obwohl keines erwartet wurde. `InResponseTo`	Sie verwenden die vom IdP initiierte URL für einen SP-initiierten Anmeldeablauf. Verwenden Sie stattdessen die vom SP initiierte URL.

Deaktivieren der SAML-Authentifizierung

Um die SAML-Authentifizierung für OpenSearch Dashboards zu deaktivieren (Konsole)

1. Klicken Sie auf die Domain, wählen Sie Aktionen und Sicherheitskonfiguration bearbeiten.
2. Deaktivieren Sie das Kontrollkästchen SAML-Authentifizierung aktivieren.
3. Wählen Sie Änderungen speichern aus.
4. Nachdem die Verarbeitung der Domain abgeschlossen ist, überprüfen Sie das differenzierte Mapping der Zugriffssteuerungsrollen mit der folgenden Anfrage:

```
GET _plugins/_security/api/rolesmapping
```

Durch die Deaktivierung der SAML-Authentifizierung für Dashboards werden die Zuordnungen für den SAML-Master-Benutzernamen und die SAML-Master-Backend-Rolle nicht entfernt. and/or Wenn Sie diese Zuordnungen entfernen möchten, melden Sie sich mit der internen Benutzerdatenbank (sofern aktiviert) bei Dashboards an oder verwenden Sie die API, um sie zu entfernen:

```
PUT _plugins/_security/api/rolesmapping/all_access
{
  "users": [
    "master-user"
  ]
}
```

Support für vertrauenswürdige Identitätsverbreitung durch IAM Identity Center für Amazon Service OpenSearch

Sie können jetzt Ihre zentral konfigurierten AWS IAM Identity Center-Prinzipale (Benutzer und Gruppen) über Trusted Identity Propagation verwenden, um über Serviceanwendungen auf Domänen zuzugreifen OpenSearch . OpenSearch Um die IAM Identity Center-Unterstützung für Amazon OpenSearch Service zu aktivieren, müssen Sie die Nutzung von IAM Identity Center aktivieren. Weitere Informationen dazu finden Sie unter Was ist IAM Identity Center? . Weitere Informationen finden Sie unter Wie ordnet man eine OpenSearch Domain als Datenquelle in OpenSearch Anwendungen zu? für Einzelheiten.

Sie können IAM Identity Center mithilfe der OpenSearch Servicekonsole, der AWS Command Line Interface (AWS CLI) oder der AWS SDKs konfigurieren.

> **Note**
>
> IAM Identity Center-Prinzipale werden nicht über Dashboards (zusammen mit dem Cluster) unterstützt. Sie werden nur über eine zentrale OpenSearch Benutzeroberfläche (Dashboards) unterstützt.

Überlegungen

Bevor Sie IAM Identity Center mit Amazon OpenSearch Service verwenden, müssen Sie Folgendes berücksichtigen:

- IAM Identity Center ist im Konto aktiviert.
- Die OpenSearch Domain-Version ist 1.3 oder höher.
- Fine Grained Access Control ist auf der Domain aktiviert.
- Die Domäne sollte sich in derselben Region wie die IAM Identity Center-Instanz befinden.
- Domäne und OpenSearch Anwendung sollten zu demselben AWS Konto gehören.

Ändern der Domainzugriffsrichtlinie

Bevor Sie IAM Identity Center konfigurieren, müssen Sie die Domänenzugriffsrichtlinie oder die Berechtigungen der IAM-Rolle aktualisieren, die in OpenSearch Anwendungen für Trusted Identity Propagation konfiguriert sind.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "IAM Role configured in OpenSearch application"
            },
            "Action": "es:ESHttp*",
            "Resource": "domain-arn/*"
        },
        {
        ... // Any other permissions
        }
    ]
}
```

Konfiguration der IAM Identity Center-Authentifizierung und -Autorisierung (Konsole)

Sie können die IAM Identity Center-Authentifizierung und -Autorisierung während der Domainerstellung oder durch Aktualisierung einer vorhandenen Domain aktivieren. Die Einrichtungsschritte variieren geringfügig, je nachdem, welche Option Sie wählen.

In den folgenden Schritten wird erklärt, wie Sie eine bestehende Domain für die IAM Identity Center-Authentifizierung und -Autorisierung in der Amazon OpenSearch Service Console konfigurieren:

1. Navigieren Sie unter Domain-Konfiguration zur Sicherheitskonfiguration, wählen Sie Bearbeiten und navigieren Sie zum Abschnitt IAM Identity Center-Authentifizierung und wählen Sie API-Zugriff aktivieren, der mit IAM Identity Center authentifiziert ist aus.
2. Wählen Sie den Schlüssel SubjectKey und Rollen wie folgt aus.

   - Betreff-Schlüssel — wählen Sie einen von UserId (Standard) UserName und E-Mail, um das entsprechende Attribut als Hauptbenutzer für den Zugriff auf die Domain zu verwenden.
   - Rollenschlüssel — wählen Sie einen von GroupId (Standard) und verwenden Sie GroupName die entsprechenden Attributwerte als Backend-Rolle fine-grained-access-controlfür alle Gruppen, die dem IdC-Prinzipal zugeordnet sind.

Nachdem Sie Ihre Änderungen vorgenommen haben, speichern Sie Ihre Domain.

Konfiguration von Fine Grained Access Control

Sobald Sie die IAM Identity Center-Option für Ihre OpenSearch Domain aktiviert haben, können Sie den Zugriff auf IAM Identity Center-Prinzipale konfigurieren, indem Sie eine Rollenzuweisung zur Backend-Rolle erstellen. Der Wert der Back-End-Rolle für den Principal basiert auf der Gruppenmitgliedschaft des IdC-Prinzipals und der Konfiguration von oder. RolesKey GroupId GroupName

> **Note**
>
> Amazon OpenSearch Service kann bis zu 100 Gruppen für einen einzelnen Benutzer unterstützen. Wenn Sie versuchen, mehr als die zulässige Anzahl von Instances zu verwenden, kommt es zu Inkonsistenzen bei der fine-grained-access-control Autorisierungsverarbeitung und Sie erhalten eine 403-Fehlermeldung.

Konfiguration der IAM Identity Center-Authentifizierung und -Autorisierung (CLI)

```
  aws opensearch update-domain-config \
      --domain-name my-domain \
      --identity-center-options '{"EnabledAPIAccess": true,
 "IdentityCenterInstanceARN": "instance arn",  "SubjectKey": "UserId/UserName/
UserEmail" , "RolesKey": "GroupId/GroupName"}'
```

Deaktivierung der IAM Identity Center-Authentifizierung auf der Domain

So deaktivieren Sie IAM Identity Center auf Ihrer Domain: OpenSearch

1. Klicken Sie auf die Domain, wählen Sie Aktionen und Sicherheitskonfiguration bearbeiten.
2. Deaktivieren Sie die Option API-Zugriff aktivieren, der mit IAM Identity Center authentifiziert wurde.
3. Wählen Sie Änderungen speichern aus.
4. Nachdem die Verarbeitung der Domain abgeschlossen ist, entfernen Sie die Rollenzuordnungen, die für IdC-Prinzipale hinzugefügt wurden

Um IAM Identity Center über CLI zu deaktivieren, können Sie Folgendes verwenden

```
  aws opensearch update-domain-config \
      --domain-name my-domain \
      --identity-center-options '{"EnabledAPIAccess": false}'
```

Konfiguration der Amazon Cognito Cognito-Authentifizierung für Dashboards OpenSearch

Sie können Ihre Amazon OpenSearch Service-Standardinstallation von OpenSearch Dashboards mit Amazon Cognito authentifizieren und schützen. Die Amazon Cognito Cognito-Authentifizierung ist optional und nur für Domains OpenSearch verfügbar, die Elasticsearch 5.1 oder höher verwenden. Wenn Sie die Amazon-Cognito-Authentifizierung nicht konfigurieren, können Sie

Dashboards dennoch mit einer IP-basierten Zugriffsrichtlinie und einem Proxy-Server, HTTP-Basisauthentifizierung oder SAML schützen.

Ein Großteil des Authentifizierungsprozesses findet in Amazon Cognito statt, aber dieser Abschnitt enthält Richtlinien und Anforderungen für die Konfiguration von Amazon Cognito Cognito-Ressourcen für die Verwendung mit OpenSearch Service-Domains. Die Standardpreise gelten für alle Amazon-Cognito-Ressourcen.

> **Tip**
>
> Wenn Sie eine Domain zum ersten Mal für die Verwendung der Amazon Cognito Cognito-Authentifizierung für OpenSearch Dashboards konfigurieren, empfehlen wir die Verwendung der Konsole. Amazon-Cognito-Ressourcen sind extrem anpassbar und mithilfe der Konsole können Sie die für Sie wichtigen Funktionen besser identifizieren und verstehen.

Themen

- Voraussetzungen
- Konfigurieren einer Domain zur Verwendung der Amazon-Cognito-Authentifizierung
- Zulassen der authentifizierten Rolle
- Konfigurieren von Identitätsanbietern
- (Optional) Konfigurieren von individuell festgelegtem Zugriff
- (Optional) Anpassen der Anmeldeseite
- (Optional) Konfiguration der erweiterten Sicherheit
- Testen
- Kontingente
- Häufige Konfigurationsprobleme
- Amazon Cognito Cognito-Authentifizierung für Dashboards deaktivieren OpenSearch
- Löschen von Domains, die die Amazon Cognito Cognito-Authentifizierung für OpenSearch Dashboards verwenden

Voraussetzungen

Bevor Sie die Amazon Cognito Cognito-Authentifizierung für OpenSearch Dashboards konfigurieren können, müssen Sie mehrere Voraussetzungen erfüllen. Die OpenSearch Servicekonsole hilft

dabei, die Erstellung dieser Ressourcen zu optimieren, aber das Verständnis des Zwecks der einzelnen Ressourcen hilft bei der Konfiguration und Fehlerbehebung. Für die Amazon-Cognito-Authentifizierung für Dashboards sind die folgenden Ressourcen erforderlich:

- Amazon Cognito Benutzerpool
- Amazon Cognito Identitätenpool
- IAM-Rolle, der die `AmazonOpenSearchServiceCognitoAccess`-Richtlinie zugewiesen ist (`CognitoAccessForAmazonOpenSearch`)

> **Note**
>
> Der Benutzer- und der Identitätenpool müssen sich in derselben AWS-Region befinden. Sie können denselben Benutzerpool, Identitätspool und dieselbe IAM-Rolle verwenden, um die Amazon Cognito Cognito-Authentifizierung für Dashboards zu mehreren OpenSearch Service-Domains hinzuzufügen. Weitere Informationen hierzu finden Sie unter the section called “Kontingente”.

Über den Benutzerpool

Benutzerpools haben zwei Hauptfunktionen: das Erstellen und Verwalten von Benutzerverzeichnissen und die Benutzerregistrierung und -anmeldung. Anweisungen zum Erstellen eines Benutzerpools finden Sie unter Erste Schritte mit Benutzerpools im Amazon Cognito Developer Guide.

Beachten Sie Folgendes, wenn Sie einen Benutzerpool für die Verwendung mit OpenSearch Service erstellen:

- Ihr Amazon Cognito Cognito-Benutzerpool muss einen Domainnamen haben. OpenSearch Der Service verwendet diesen Domainnamen, um Benutzer auf eine Anmeldeseite für den Zugriff auf Dashboards weiterzuleiten. Anders als für einen Domain-Namen kann für den Benutzerpool eine Standardkonfiguration verwendet werden.
- Sie müssen die für den Pool erforderlichen Standardattribute angeben – Attribute wie Name, Geburtsdatum, E-Mail-Adresse und Telefonnummer. Sie können diese Attribute nach dem Erstellen des Benutzerpools nicht mehr ändern. Wählen Sie daher diejenigen Attribute aus, die für Sie zum Zeitpunkt der Erstellung am relevantesten sind.

- Legen Sie beim Erstellen des Benutzerpools fest, ob Benutzer eigene Konten erstellen können, wie sicher Passwörter für Konten sein müssen und ob Multifaktor-Authentifizierung aktiviert werden soll. Wenn Sie vorhaben, einen externen Identitätsanbieter zu verwenden, sind diese Einstellungen nicht relevant. Theoretisch können Sie den Benutzerpool als Identitätsanbieter aktivieren und einen externen Identitätsanbieter aktivieren. Die meisten Personen ziehen jedoch eine Methode vor.

Der Benutzerpool IDs hat die Form von. *region_ID* Wenn Sie beabsichtigen, die AWS CLI oder ein AWS SDK zur Konfiguration des OpenSearch Dienstes zu verwenden, notieren Sie sich die ID.

Über den Identitätenpool

Mit Identitäten-Pools können Sie Benutzern nach der Anmeldung temporäre Rollen mit beschränkten Berechtigungen zuweisen. Anweisungen zum Erstellen eines Identitätspools finden Sie unter Übersicht über die Identity-Pools-Konsole im Amazon Cognito Developer Guide. Beachten Sie Folgendes, wenn Sie einen Identitätspool für die Verwendung mit OpenSearch Service erstellen:

- Wenn Sie die Amazon-Cognito-Konsole verwenden, müssen Sie das Kontrollkästchen Zugriff für nicht authentifizierte Identitäten aktivieren aktivieren, um den Identitätenpool zu erstellen. Nachdem Sie den Identitätspool erstellt und die OpenSearch Service-Domain konfiguriert haben, deaktiviert Amazon Cognito diese Einstellung.
- Sie müssen keine externen Identitätsanbieter zu dem Identitäten-Pool hinzufügen. Wenn Sie OpenSearch Service für die Verwendung der Amazon Cognito Cognito-Authentifizierung konfigurieren, konfiguriert er den Identitätspool so, dass er den Benutzerpool verwendet, den Sie gerade erstellt haben.
- Nachdem Sie den Identitäten-Pool erstellt haben, müssen Sie unauthentifizierte und authentifizierte IAM-Rollen auswählen. Diese Rollen legen die Zugriffsrichtlinien fest, die Benutzer vor und nach der Anmeldung haben. Wenn Sie die Amazon-Cognito-Konsole verwenden, kann diese die Rollen für Sie erstellen. Nachdem Sie die authentifizierte Rolle erstellt haben, notieren Sie sich deren ARN. Dieser hat die Form `arn:aws:iam::`*`123456789012`*`:role/Cognito_`*`identitypoolname`*`Auth_Role`.

Der Identitätspool IDs hat die Form von. *region*`:`*ID*`-`*ID*`-`*ID*`-`*ID*`-`*ID* Wenn Sie beabsichtigen, die AWS CLI oder ein AWS SDK zur Konfiguration des OpenSearch Dienstes zu verwenden, notieren Sie sich die ID.

Informationen über die CognitoAccessForAmazonOpenSearch-Rolle

OpenSearch Der Service benötigt Berechtigungen, um die Benutzer- und Identitätspools von Amazon Cognito zu konfigurieren und für die Authentifizierung zu verwenden. Zu diesem Zweck `AmazonOpenSearchServiceCognitoAccess` können Sie eine AWS verwaltete Richtlinie verwenden. `AmazonESCognitoAccess`ist eine ältere Richtlinie, die durch `AmazonOpenSearchServiceCognitoAccess` die Umbenennung des Dienstes in Amazon OpenSearch Service ersetzt wurde. Beide Richtlinien bieten die Mindestberechtigungen für Amazon Cognito, die zur Aktivierung der Amazon Cognito Cognito-Authentifizierung erforderlich sind. Einzelheiten zu den Richtlinien finden Sie AmazonOpenSearchServiceCognitoAccessim Referenzhandbuch für AWS verwaltete Richtlinien.

Wenn Sie die Konsole verwenden, um Ihre OpenSearch Service-Domain zu erstellen oder zu konfigurieren, erstellt sie eine IAM-Rolle für Sie und hängt die `AmazonOpenSearchServiceCognitoAccess` Richtlinie (oder die `AmazonESCognitoAccess` Richtlinie, wenn es sich um eine Elasticsearch-Domain handelt) an die Rolle an. Der Standardname der Rolle lautet `CognitoAccessForAmazonOpenSearch`.

`AmazonOpenSearchServiceCognitoAccess`Sowohl die Richtlinien für Rollenberechtigungen `AmazonESCognitoAccess` als auch beide ermöglichen es OpenSearch Service, die folgenden Aktionen für alle Identitäts- und Benutzerpools durchzuführen:

- Aktion: `cognito-idp:DescribeUserPool`
- Aktion: `cognito-idp:CreateUserPoolClient`
- Aktion: `cognito-idp:DeleteUserPoolClient`
- Aktion: `cognito-idp:UpdateUserPoolClient`
- Aktion: `cognito-idp:DescribeUserPoolClient`
- Aktion: `cognito-idp:AdminInitiateAuth`
- Aktion: `cognito-idp:AdminUserGlobalSignOut`
- Aktion: `cognito-idp:ListUserPoolClients`
- Aktion: `cognito-identity:DescribeIdentityPool`
- Aktion: `cognito-identity:SetIdentityPoolRoles`
- Aktion: `cognito-identity:GetIdentityPoolRoles`

Wenn Sie die AWS CLI oder eine der beiden verwenden AWS SDKs, müssen Sie Ihre eigene Rolle erstellen, die Richtlinie anhängen und den ARN für diese Rolle angeben, wenn Sie Ihre OpenSearch Service-Domain konfigurieren. Die Rolle muss über die folgende Vertrauensstellung verfügen:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "opensearchservice.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Anweisungen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen für einen AWS Dienst und Hinzufügen und Entfernen von IAM-Identitätsberechtigungen im IAM-Benutzerhandbuch.

Konfigurieren einer Domain zur Verwendung der Amazon-Cognito-Authentifizierung

Nachdem Sie die Voraussetzungen erfüllt haben, können Sie eine OpenSearch Service-Domain für die Verwendung von Amazon Cognito for Dashboards konfigurieren.

> **Note**
>
> Amazon Cognito ist nicht in allen AWS-Regionen verfügbar. Eine Liste der unterstützten Regionen finden Sie unter Service-Endpunkte für Amazon Cognito. Sie müssen nicht dieselbe Region für Amazon Cognito verwenden, die Sie für OpenSearch Service verwenden.

Konfigurieren der Amazon-Cognito-Authentifizierung (Konsole)

Da sie die `CognitoAccessForAmazonOpenSearch` Rolle für Sie erstellt, bietet die Konsole die einfachste Konfigurationserfahrung. Zusätzlich zu den standardmäßigen OpenSearch Serviceberechtigungen benötigen Sie die folgenden Berechtigungen, um mit der Konsole eine Domain zu erstellen, die die Amazon Cognito Cognito-Authentifizierung für OpenSearch Dashboards verwendet.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeVpcs",
        "cognito-identity:ListIdentityPools",
        "cognito-idp:ListUserPools",
        "iam:CreateRole",
        "iam:AttachRolePolicy"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:GetRole",
        "iam:PassRole"
      ],
      "Resource": "arn:aws:iam::123456789012:role/service-
role/CognitoAccessForAmazonOpenSearch"
    }
  ]
}
```

Anweisungen zum Hinzufügen von Berechtigungen zu einer Identität (Benutzer, Gruppe oder Rolle) finden Sie unter Hinzufügen von IAM-Identitätsberechtigungen (Konsole).

Wenn `CognitoAccessForAmazonOpenSearch` bereits vorhanden ist, benötigen Sie weniger Berechtigungen:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeVpcs",
        "cognito-identity:ListIdentityPools",
        "cognito-idp:ListUserPools"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:GetRole",
        "iam:PassRole"
      ],
      "Resource": "arn:aws:iam::123456789012:role/service-
role/CognitoAccessForAmazonOpenSearch"
    }
  ]
}
```

So konfigurieren Sie die Amazon-Cognito-Authentifizierung für Dashboards (Konsole)

1. Öffnen Sie die Amazon OpenSearch Service-Konsole zu https://console.aws.amazon.com/aos/Hause/.
2. Wählen Sie unter Domains die Domain aus, die Sie konfigurieren möchten.
3. Klicken Sie auf Aktionen, Sicherheitskonfiguration bearbeiten.
4. Wählen Sie Amazon-Cognito-Authentifizierung aktivieren aus.
5. Wählen Sie für Region die aus, AWS-Region die Ihren Amazon Cognito Cognito-Benutzerpool und Identitätspool enthält.
6. Wählen Sie für Cognito User Pool (Cognito-Benutzerpool) einen Benutzerpool aus oder erstellen Sie einen Benutzerpool. Weitere Informationen finden Sie unter the section called “Über den Benutzerpool”.

7. Wählen Sie für Cognito Identity Pool (Cognito-Identitäten-Pool) einen Identitäten-Pool aus oder erstellen Sie einen Identitäten-Pool. Weitere Informationen finden Sie unter the section called “Über den Identitätenpool”.

   > **Note**
   >
   > Über die Links Benutzerpool erstellen und Identitätenpool erstellen werden Sie zur Amazon-Cognito-Konsole geleitet und müssen diese Ressourcen dort manuell erstellen. Der Prozess erfolgt nicht automatisch. Weitere Informationen finden Sie unter the section called “Voraussetzungen”.

8. Verwenden Sie für IAM-Rollenname den Standardwert `CognitoAccessForAmazonOpenSearch` (empfohlen), oder geben Sie einen neuen Namen ein. Weitere Informationen finden Sie unter the section called “Informationen über die CognitoAccessForAmazonOpenSearch-Rolle”.
9. Wählen Sie Änderungen speichern aus.

Nachdem Ihre Domain die Verarbeitung abgeschlossen hat, finden Sie unter the section called “Zulassen der authentifizierten Rolle” und the section called “Konfigurieren von Identitätsanbietern” weitere Konfigurationsschritte.

Konfigurieren der Amazon-Cognito-Authentifizierung (AWS CLI)

Verwenden Sie den `--cognito-options` Parameter, um Ihre OpenSearch Service-Domain zu konfigurieren. Die folgende Syntax wird von den `create-domain`- und `update-domain-config`-Befehlen verwendet:

```
--cognito-options Enabled=true,UserPoolId="user-pool-id",IdentityPoolId="identity-pool-id",RoleArn="arn:aws:iam::123456789012:role/CognitoAccessForAmazonOpenSearch"
```

Beispiel

Im folgenden Beispiel wird eine Domain in der Region `us-east-1` erstellt, die Amazon-Cognito-Authentifizierung für Dashboards mit der Rolle `CognitoAccessForAmazonOpenSearch` aktiviert und der Domain Zugriff auf `Cognito_Auth_Role` erlaubt:

```
aws opensearch create-domain --domain-name my-domain --region us-east-1 --access-policies '{ "Version":"2012-10-17", "Statement":[{"Effect":"Allow","Principal":{"AWS":
```

```
 ["arn:aws:iam::123456789012:role/
Cognito_Auth_Role"]},"Action":"es:ESHttp*","Resource":"arn:aws:es:us-
east-1:123456789012:domain/*" }]}' --engine-version "OpenSearch_1.0"
 --cluster-config InstanceType=m4.xlarge.search,InstanceCount=1
 --ebs-options EBSEnabled=true,VolumeSize=10 --cognito-options
 Enabled=true,UserPoolId="us-east-1_123456789",IdentityPoolId="us-
east-1:12345678-1234-1234-1234-123456789012",RoleArn="arn:aws:iam::123456789012:role/
CognitoAccessForAmazonOpenSearch"
```

Nachdem Ihre Domain die Verarbeitung abgeschlossen hat, finden Sie unter the section called “Zulassen der authentifizierten Rolle” und the section called “Konfigurieren von Identitätsanbietern” weitere Konfigurationsschritte.

Konfiguration der Amazon Cognito Cognito-Authentifizierung ()AWS SDKs

Die AWS SDKs (außer Android und iOS SDKs) unterstützen alle Operationen, die in der Amazon OpenSearch Service API-Referenz definiert sind, einschließlich des `CognitoOptions` Parameters für die `UpdateDomainConfig` Operationen `CreateDomain` und. Weitere Informationen zur Installation und Verwendung von finden Sie AWS SDKs unter AWS Software Development Kits.

Nachdem Ihre Domain die Verarbeitung abgeschlossen hat, finden Sie unter the section called “Zulassen der authentifizierten Rolle” und the section called “Konfigurieren von Identitätsanbietern” weitere Konfigurationsschritte.

Zulassen der authentifizierten Rolle

Standardmäßig verfügt die authentifizierte IAM-Rolle, die Sie gemäß den Richtlinien unter konfiguriert haben, the section called “Über den Identitätenpool” nicht über die erforderlichen Rechte für den Zugriff auf OpenSearch Dashboards. Sie müssen der Rolle zusätzliche Berechtigungen gewähren.

> **Note**
>
> Wenn Sie eine detaillierte Zugriffskontrolle konfiguriert haben und eine offene oder IP-basierte Zugriffsrichtlinie verwenden, können Sie diesen Schritt überspringen.

Sie können diese Berechtigungen in eine identitätsbasierte Richtlinie aufnehmen. Wenn Sie jedoch nicht möchten, dass authentifizierte Benutzer Zugriff auf alle OpenSearch Dienstdomänen haben, ist eine ressourcenbasierte Richtlinie, die an eine einzelne Domäne angehängt ist, der bessere Ansatz.

Geben Sie für `Principal` den ARN der von Cognito authentifizierten Rolle an, die Sie mit den Richtlinien in the section called “Über den Identitätenpool” konfiguriert haben.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "AWS":[
               "arn:aws:iam::123456789012:role/Cognito_identitypoolnameAuth_Role"
            ]
         },
         "Action":[
            "es:ESHttp*"
         ],
         "Resource":"arn:aws:es:region:123456789012:domain/domain-name/*"
      }
   ]
}
```

Anweisungen zum Hinzufügen einer ressourcenbasierten Richtlinie zu einer Dienstdomäne finden Sie unter. OpenSearch the section called “Konfigurieren von Zugriffsrichtlinien”

Konfigurieren von Identitätsanbietern

Wenn Sie eine Domain für die Verwendung der Amazon Cognito Cognito-Authentifizierung für Dashboards konfigurieren, fügt OpenSearch Service dem Benutzerpool einen App-Client hinzu und fügt den Benutzerpool dem Identitätspool als Authentifizierungsanbieter hinzu.

> **Warning**
>
> Der App-Client darf nicht umbenannt oder gelöscht werden.

Je nachdem, wie Sie Ihren Benutzerpool konfiguriert haben, müssen Sie Benutzerkonten entweder manuell erstellen oder Benutzer können eigene Konten erstellen. Wenn Sie mit diesen Einstellungen

zufrieden sind, müssen Sie nichts weiter unternehmen. Viele Anwender verwenden jedoch lieber externe Identitätsanbieter.

Um einen SAML 2.0-Identitätsanbieter zu aktivieren, müssen Sie ein SAML-Metadatendokument bereitstellen. Um soziale Identitätsanbieter wie Login with Amazon, Facebook und Google zu aktivieren, müssen Sie über eine App-ID und einen geheimen App-Schlüssel von diesen Anbietern verfügen. Sie können Identitätsanbieter in beliebigen Kombinationen aktivieren.

Der einfachste Weg, Ihren Benutzerpool zu konfigurieren, erfolgt über die Amazon-Cognito-Konsole. Anweisungen finden Sie unter Benutzerpool-Anmeldung mit externen Identitätsanbietern und Anwendungsspezifische Einstellungen mit App-Client im Amazon Cognito Developer Guide.

(Optional) Konfigurieren von individuell festgelegtem Zugriff

Möglicherweise haben Sie bemerkt, dass die Standardeinstellungen für den Identitätspool jedem Benutzer, der sich anmeldet, dieselbe IAM-Rolle (`Cognito_`*`identitypool`*`Auth_Role`) zuweisen, was bedeutet, dass jeder Benutzer auf dieselben Ressourcen zugreifen kann. AWS Wenn Sie die differenzierte Zugriffskontrolle mit Amazon Cognito verwenden möchten – etwa weil Sie wollen, dass die Analysten Ihrer Organisation schreibgeschützt auf mehrere Indizes zugreifen, Entwickler aber Schreibzugriff auf alle Indizes haben sollen – haben Sie zwei Möglichkeiten:

- Erstellen Sie Benutzergruppen, und konfigurieren Sie Ihren Identitätsanbieter so, dass die IAM-Rolle basierend auf dem Authentifizierungstoken des Benutzers ausgewählt wird (empfohlen).
- Konfigurieren Sie Ihren Identitätsanbieter so, dass die IAM-Rolle basierend auf einer oder mehreren Regeln ausgewählt wird.

Ein Walkthrough, das die differenzierte Zugriffskontrolle enthält, finden Sie unter the section called “Tutorial: Detaillierte Zugriffskontrolle mit Cognito-Authentifizierung”.

> **Important**
>
> Genau wie die Standardrolle muss Amazon Cognito Teil der Vertrauensbeziehung jeder zusätzlichen Rolle sein. Einzelheiten finden Sie unter Rollen für die Rollenzuweisung erstellen im Amazon Cognito Developer Guide.

Benutzergruppen und Token

Wenn Sie eine Benutzergruppe erstellen, wählen Sie eine IAM-Rolle für die Mitglieder dieser Gruppe aus. Informationen zum Erstellen von Gruppen finden Sie unter Hinzufügen von Gruppen zu einem Benutzerpool im Amazon Cognito Developer Guide.

Nachdem Sie mindestens eine Benutzergruppe erstellt haben, können Sie Ihren Authentifizierungsanbieter so konfigurieren, dass er Benutzern die Rollen ihrer jeweiligen Gruppe anstelle der Standardrolle des Identitäten-Pools zuweist. Wählen Sie Rolle aus Token auswählen aus, und wählen Sie dann entweder Authentifizierte Standardrolle verwenden oder VERWEIGERN, um anzugeben, wie der Identitätenpool Benutzer behandelt, die nicht Teil einer Gruppe sind.

Regeln

Regeln bestehen im Grunde genommen aus einer Reihe von `if`-Anweisungen, die Amazon Cognito der Reihe nach auswertet. Wenn die E-Mail-Adresse eines Benutzers beispielsweise `@corporate` enthält, weist Amazon Cognito dem Benutzer `Role_A` zu. Wenn die E-Mail-Adresse eines Benutzers `@subsidiary` enthält, wird dem Benutzer `Role_B` zugewiesen. Andernfalls wird dem Benutzer die Standardauthentifizierungsrolle zugewiesen.

Weitere Informationen finden Sie unter Verwenden von regelbasierter Zuordnung zum Zuweisen von Rollen zu Benutzern im Amazon Cognito Developer Guide.

(Optional) Anpassen der Anmeldeseite

Sie können die Amazon Cognito Cognito-Konsole verwenden, um ein benutzerdefiniertes Logo hochzuladen und CSS-Änderungen an der Anmeldeseite vorzunehmen. Anweisungen und eine vollständige Liste der CSS-Eigenschaften finden Sie unter Customizing Hosted UI (classic) Branding im Amazon Cognito Developer Guide.

(Optional) Konfiguration der erweiterten Sicherheit

Amazon-Cognito-Benutzerpools unterstützen erweiterte Sicherheitsfunktionen wie Multi-Faktor-Authentifizierung, Überprüfung auf nicht mehr zuverlässige Anmeldeinformationen und die adaptive Authentifizierung. Weitere Informationen finden Sie unter Verwenden der Sicherheitsfunktionen von Amazon Cognito Cognito-Benutzerpools im Amazon Cognito Cognito-Entwicklerhandbuch.

Testen

Wenn Sie mit der Konfiguration zufrieden sind, stellen Sie sicher, dass die Benutzererfahrung Ihren Erwartungen entspricht.

So greifen Sie auf Dashboards zu OpenSearch

1. Navigieren Sie im Webbrowser zu `https://`*`opensearch-domain`*`/_dashboards`. Um sich direkt bei einem bestimmten Mandanten anzumelden, hängen Sie `?security_tenant=`*`tenant-name`* an die URL an.
2. Melden Sie sich mit Ihren bevorzugten Anmeldeinformationen an.
3. Nachdem die OpenSearch Dashboards geladen wurden, konfigurieren Sie mindestens ein Indexmuster. Dashboards identifiziert anhand dieser Muster, welche Indizes Sie analysieren möchten. Geben Sie * ein, wählen Sie Nächster Schritt aus und klicken Sie auf Create index pattern (Indexmuster erstellen).
4. Klicken Sie auf Ermitteln, um Ihre Daten zu durchsuchen.

Falls ein Schritt in diesem Prozess fehlschlägt, finden Sie unter the section called “Häufige Konfigurationsprobleme” Hilfestellung zur Problembehebung.

Kontingente

In Amazon Cognito sind Soft Limits für viele Ressourcen konfiguriert. Wenn Sie die Dashboard-Authentifizierung für eine große Anzahl von OpenSearch Service-Domains aktivieren möchten, überprüfen Sie die Kontingente in Amazon Cognito und fordern Sie bei Bedarf eine Erhöhung des Limits an.

Jede OpenSearch Service-Domain fügt dem Benutzerpool einen App-Client hinzu, wodurch dem Identitätspool ein Authentifizierungsanbieter hinzugefügt wird. Wenn Sie die OpenSearch Dashboard-Authentifizierung für mehr als 10 Domains aktivieren, stoßen Sie möglicherweise auf das Limit „maximale Amazon Cognito Cognito-Benutzerpoolanbieter pro Identitätspool“. Wenn Sie ein Limit überschreiten, können alle OpenSearch Service-Domains, die Sie für die Verwendung der Amazon Cognito Cognito-Authentifizierung für Dashboards zu konfigurieren versuchen, im Konfigurationsstatus Verarbeitung hängen bleiben.

Häufige Konfigurationsprobleme

Die folgenden Tabellen enthalten häufige Konfigurationsprobleme und deren Lösungen.

Service konfigurieren OpenSearch

Problem	Lösung
`OpenSearch Service can't create the role` (Konsole)	Sie verfügen nicht über die erforderlichen IAM-Berec htigungen. Fügen Sie die unter the section called “Konfigurieren der Amazon-Cognito-Authentifizierung (Konsole)” angegebenen Berechtigungen hinzu.
`User is not authorize d to perform: iam:PassR ole on resource CognitoAc cessForAmazonOpenSearch` (Konsole)	Sie haben keine `iam:PassRole` Berechtigungen für die CognitoAccessForAmazonOpenSearchRolle. Fügen Sie die folgende Richtlinie zu Ihrem Konto hinzu: JSON `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "iam:PassRole" ], "Resource": "arn:aws: iam:: 123456789012:role/service-role/ CognitoAccessForAmazonOpenSearch " } ] }` Alternativ können Sie die Richtlinie `IAMFullAccess` anfügen.
`User is not authorize d to perform: cognito- identity:ListIdenti tyPools on resource`	Sie verfügen nicht über die Leseberechtigung für Amazon Cognito. Fügen Sie die Richtlinie `AmazonCog nitoReadOnly` zu Ihrem Konto hinzu.

Problem	Lösung
`An error occurred (ValidationException) when calling the CreateDomain operation: OpenSearch Service must be allowed to use the passed role`	OpenSearch Der Dienst ist in der Vertrauensstellung der `CognitoAccessForAmazonOpenSearch` Rolle nicht angegeben. Stellen Sie sicher, dass Ihre Rolle die in the section called “Informationen über die CognitoAccessForAmazonOpenSearch-Rolle” angegebene Vertrauensstellung verwendet. Konfigurieren Sie alternativ mit der Konsole die Amazon-Cognito-Authentifizierung. In der Konsole wird eine Rolle für Sie erstellt.
`An error occurred (ValidationException) when calling the CreateDomain operation: User is not authorized to perform: cognito-idp: action on resource: user pool`	Die in `--cognito-options` angegebene Rolle verfügt nicht über die Berechtigung für den Zugriff auf Amazon Cognito. Vergewissern Sie sich, dass der Rolle die AWS verwaltete `AmazonOpenSearchServiceCognitoAccess` Richtlinie angehängt ist. Konfigurieren Sie alternativ mit der Konsole die Amazon-Cognito-Authentifizierung. In der Konsole wird eine Rolle für Sie erstellt.
`An error occurred (ValidationException) when calling the CreateDomain operation: User pool does not exist`	OpenSearch Der Dienst kann den Benutzerpool nicht finden. Stellen Sie sicher, dass Sie einen Benutzerpool erstellt haben und die korrekte ID verwenden. Um die ID zu finden, können Sie die Amazon Cognito Cognito-Konsole oder den folgenden AWS CLI Befehl verwenden: `aws cognito-idp list-user-pools --max-results 60 --region region`
`An error occurred (ValidationException) when calling the CreateDomain operation: IdentityPool not found`	OpenSearch Der Service kann den Identitätspool nicht finden. Stellen Sie sicher, dass Sie einen Benutzerpool erstellt haben und die korrekte ID verwenden. Um die ID zu finden, können Sie die Amazon Cognito Cognito-Konsole oder den folgenden AWS CLI Befehl verwenden: `aws cognito-identity list-identity-pools --max-results 60 --region region`

Problem	Lösung
`An error occurred (ValidationException) when calling the CreateDomain operation: Domain needs to be specified for user pool`	Der Benutzerpool verfügt nicht über einen Domain-Namen. Sie können diesen über die Amazon-Cognito-Konsole oder mit dem folgenden AWS CLI -Befehl konfigurieren: `aws cognito-idp create-user-pool-domain --domain name --user-pool-id id`

Zugreifen auf Dashboards OpenSearch

Problem	Lösung
Die Anmeldeseite enthält nicht meinen bevorzugten Identitätsanbieter.	Vergewissern Sie sich, dass Sie den Identitätsanbieter für den OpenSearch Service App-Client aktiviert haben, wie unter beschriebenthe section called “Konfigurieren von Identitätsanbietern”.
Die Anmeldeseite sieht nicht so aus, als würde sie zu meiner Organisation gehören.	Siehe the section called “(Optional) Anpassen der Anmeldeseite”.
Meine Anmeldeinformationen funktionieren nicht.	Stellen Sie sicher, dass Sie den Identitätsanbieter wie in the section called “Konfigurieren von Identitätsanbietern” angegeben konfiguriert haben. Wenn Sie den Benutzerpool als Identitätsanbieter verwenden, überprüfen Sie, ob das Konto auf der Amazon Cognito Cognito-Konsole vorhanden ist.
OpenSearch Dashboards werden entweder gar nicht geladen oder funktionieren nicht richtig.	Die von Amazon Cognito authentifizierte Rolle benötigt die Berechtigung `es:ESHttp*` für die Domain (`/*`), um auf Dashboards zugreifen und Dashboards verwenden zu können. Stellen Sie sicher, dass Sie wie in the section called “Zulassen der authentifizierten Rolle” angegeben eine Zugriffsrichtlinie hinzugefügt haben.

Problem	Lösung
Wenn ich mich von einem Tab aus OpenSearch Dashboards abmelde, wird auf den übrigen Tabs eine Meldung angezeigt, dass das Aktualisierungstoken gesperrt wurde.	Wenn Sie sich von einer OpenSearch Dashboards-Sitzung abmelden, während Sie die Amazon Cognito Cognito-Authentifizierung verwenden, führt OpenSearch Service einen AdminUserGlobalSignOutVorgang aus, der Sie von allen aktiven OpenSearch Dashboards-Sitzungen abmeldet.
`Invalid identity pool configuration. Check assigned IAM roles for this pool.`	Amazon Cognito verfügt nicht über Berechtigungen, die IAM-Rolle im Auftrag des authentifizierten Benutzers anzunehmen. Ändern Sie die Vertrauensstellung für die Rolle, so, dass sie folgendes beinhaltet: JSON `{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Principal": { "Federated": "cognito-identity.amazonaws.com" }, "Action": "sts:AssumeRoleWithWebIdentity", "Condition": { "StringEquals": { "cognito-identity.amazonaws.com:aud": " identity-pool-id " }, "ForAnyValue:StringLike": { "cognito-identity.amazonaws.com:amr": "authenticated" } } }] }`

Problem	Lösung
`Token is not from a supported provider of this identity pool.`	Dieser ungewöhnliche Fehler kann auftreten, wenn Sie den App-Client aus dem Benutzerpool entfernen. Versuchen Sie, Dashboards in einer neuen Browsersitzung zu öffnen.

Amazon Cognito Cognito-Authentifizierung für Dashboards deaktivieren OpenSearch

Gehen Sie wie folgt vor, um die Amazon-Cognito-Authentifizierung für Dashboards zu deaktivieren.

So deaktivieren Sie die Amazon-Cognito-Authentifizierung für Dashboards (Konsole)

1. Öffnen Sie die Amazon OpenSearch Service-Konsole.
2. Wählen Sie unter Domains die Domain aus, die Sie konfigurieren möchten.
3. Klicken Sie auf Aktionen, Sicherheitskonfiguration bearbeiten.
4. Heben Sie die Auswahl von Amazon-Cognito-Authentifizierung aktivieren auf.
5. Wählen Sie Änderungen speichern aus.

> **Important**
>
> Wenn Sie die Amazon-Cognito-Benutzer- und Identitätenpools nicht mehr brauchen, können Sie diese löschen. Andernfalls fallen weiterhin Gebühren an.

Löschen von Domains, die die Amazon Cognito Cognito-Authentifizierung für OpenSearch Dashboards verwenden

Um zu verhindern, dass Domänen, die Amazon Cognito Cognito-Authentifizierung für Dashboards verwenden, im Konfigurationsstatus Verarbeitung stecken bleiben, löschen Sie OpenSearch Service-Domains, bevor Sie die zugehörigen Amazon Cognito Cognito-Benutzer- und Identitätspools löschen.

Verwendung von serviceverknüpften Rollen für Amazon OpenSearch Service

Amazon OpenSearch Service verwendet AWS Identity and Access Management (IAM) serviceverknüpfte Rollen. Eine serviceverknüpfte Rolle ist ein spezieller Typ einer IAM-Rolle, die direkt mit dem Service verknüpft ist. OpenSearch Serviceverknüpfte Rollen werden von OpenSearch Service vordefiniert und schließen alle Berechtigungen ein, die der Service zum Aufrufen anderer AWS -Services in Ihrem Namen erfordert.

Eine serviceverknüpfte Rolle vereinfacht das Einrichten von OpenSearch Service, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. OpenSearch Service definiert die Berechtigungen seiner serviceverknüpften Rollen. Sofern keine andere Konfiguration festgelegt wurde, kann nur OpenSearch Service die Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden. Aktualisierungen der servicebezogenen Rollen- und Berechtigungsrichtlinien finden Sie unter Dokumentverlauf für Amazon OpenSearch Service.

Informationen zu anderen Services, die serviceverknüpfte Rollen unterstützen, finden Sie unter AWS -Services, die mit IAM funktionieren. Suchen Sie nach den Services, für die Ja in der Spalte Serviceverknüpfte Rolle angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Themen

- Verwenden von serviceverknüpften Rollen zur Erstellung von VPC-Domains und zur direkten Abfrage von Datenquellen
- Verwenden von serviceverknüpften Rollen zur Erstellung von OpenSearch Serverless-Sammlungen
- Verwenden von serviceverknüpften Rollen zur Erstellung von OpenSearch Ingestion-Pipelines

Verwenden von serviceverknüpften Rollen zur Erstellung von VPC-Domains und zur direkten Abfrage von Datenquellen

Amazon OpenSearch Service verwendet AWS Identity and Access Management (IAM) serviceverknüpfte Rollen. Eine serviceverknüpfte Rolle ist ein spezieller Typ einer IAM-Rolle, die direkt mit dem Service verknüpft ist. OpenSearch Serviceverknüpfte Rollen werden von OpenSearch

Service vordefiniert und schließen alle Berechtigungen ein, die der Service zum Aufrufen anderer AWS -Services in Ihrem Namen erfordert.

OpenSearch Service verwendet die serviceverknüpfte Rolle AWSServiceRoleForAmazonOpenSearchService, die die Mindestberechtigungen für Amazon und Elastic Load Balancing bereitstellt, die die Mindestberechtigungen für Amazon EC2 und Elastic Load Balancing bereitstellt, die die Mindestberechtigungen für Amazon und Elastic Load Balancing bereitstellt, die die Mindestberechtigungen für Amazon und Elastic Load Balancing bereitstellt.

Veraltete Elasticsearch-Rolle

Amazon OpenSearch Service verwendet eine serviceverknüpfte Rolle namens`AWSServiceRoleForAmazonOpenSearchService`. Ihre Konten enthalten möglicherweise auch eine Service-verknüpfte Rolle namens `AWSServiceRoleForAmazonElasticsearchService`, die mit den veralteten Amazon-Elasticsearch-Service-API-Endpunkten funktioniert.

Wenn die Legacy-Elasticsearch-Rolle in Ihrem Konto nicht vorhanden ist, erstellt OpenSearch Service beim ersten Erstellen einer Domain automatisch eine neue OpenSearch serviceverknüpfte Rolle. OpenSearch Andernfalls verwendet Ihr Konto weiterhin die Elasticsearch-Rolle. Damit diese automatische Erstellung möglich ist, müssen Sie über Berechtigungen für die Aktion `iam:CreateServiceLinkedRole` verfügen.

Berechtigungen

Die serviceverknüpfte Rolle `AWSServiceRoleForAmazonOpenSearchService` vertraut darauf, dass die folgenden Services die Rolle annehmen:

- `opensearchservice.amazonaws.com`

Die genannte Richtlinie für Rollenberechtigungen `AmazonOpenSearchServiceRolePolicy`erlaubt OpenSearch Service, die folgenden Aktionen auf den angegebenen Ressourcen durchzuführen:

- Aktion: `acm:DescribeCertificate` für `*`
- Aktion: `cloudwatch:PutMetricData` für `*`
- Aktion: `ec2:CreateNetworkInterface` für `*`
- Aktion: `ec2:DeleteNetworkInterface` für `*`
- Aktion: `ec2:DescribeNetworkInterfaces` für `*`

- Aktion: `ec2:ModifyNetworkInterfaceAttribute` für *
- Aktion: `ec2:DescribeSecurityGroups` für *
- Aktion: `ec2:DescribeSubnets` für *
- Aktion: `ec2:DescribeVpcs` für *
- Aktion: `ec2:CreateTags` auf allen Netzwerkschnittstellen und VPC-Endpunkten
- Aktion: `ec2:DescribeTags` für *
- Aktion: `ec2:CreateVpcEndpoint` für alle Sicherheitsgruppen VPCs, Subnetze und Routentabellen sowie für alle VPC-Endpunkte, wenn die Anfrage das Tag enthält `OpenSearchManaged=true`
- Aktion: `ec2:ModifyVpcEndpoint` für alle Sicherheitsgruppen VPCs, Subnetze und Routentabellen sowie für alle VPC-Endpunkte, wenn die Anfrage das Tag enthält `OpenSearchManaged=true`
- Aktion: `ec2:DeleteVpcEndpoints` auf allen Endpunkten, wenn die Anfrage das Tag `OpenSearchManaged=true` enthält
- Aktion: `ec2:AssignIpv6Addresses` für *
- Aktion: `ec2:UnAssignIpv6Addresses` für *
- Aktion: `elasticloadbalancing:AddListenerCertificates` für *
- Aktion: `elasticloadbalancing:RemoveListenerCertificates` für *

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter Serviceverknüpfte Rollenberechtigung im IAM-Benutzerhandbuch.

Erstellen der serviceverknüpfte -Rolle

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie eine VPC-fähige Domain oder eine direkte Abfragedatenquelle mithilfe von erstellen AWS Management Console, erstellt OpenSearch Service die serviceverknüpfte Rolle für Sie. Damit diese automatische Erstellung möglich ist, müssen Sie über Berechtigungen für die Aktion `iam:CreateServiceLinkedRole` verfügen.

Sie können auch die IAM-Konsole, den IAM-CLI oder die IAM-API verwenden, um eine Service-verknüpfte Rolle manuell zu erstellen. Weitere Informationen finden Sie unter Erstellen einer Service-verknüpften Rolle im IAM-Benutzerhandbuch.

Bearbeiten der serviceverknüpften Rolle

OpenSearch Service lässt Sie die `AWSServiceRoleForAmazonOpenSearchService` serviceverknüpfte Rolle nicht bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach der Erstellung einer serviceverknüpften Rolle nicht bearbeitet werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen der serviceverknüpften -Rolle

Wenn Sie ein Feature oder einen Dienst, die bzw. der eine serviceverknüpften Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte juristische Stelle, die nicht aktiv überwacht oder verwaltet wird. Sie müssen jedoch Ihre serviceverknüpfte Rolle zunächst bereinigen, bevor Sie sie manuell löschen können.

Bereinigen der -serviceverknüpften Rolle

Bevor Sie mit IAM eine serviceverknüpfte Rolle löschen können, müssen Sie sich zunächst vergewissern, dass die Rolle über keine aktiven Sitzungen verfügt, und alle Ressourcen entfernen, die von der Rolle verwendet werden.

So überprüfen Sie in der IAM-Konsole, ob die serviceverknüpfte Rolle über eine aktive Sitzung verfügt

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die IAM-Konsole in https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich der IAM Console Roles (Rollen) aus.
   Wählen Sie dann den Namen (nicht das Kontrollkästchen) der Rolle `AWSServiceRoleForAmazonOpenSearchService` aus.
3. Wählen Sie auf der Seite Summary für die ausgewählte Rolle die Registerkarte Access Advisor.
4. Überprüfen Sie auf der Registerkarte Access Advisor die jüngsten Aktivitäten für die serviceverknüpfte Rolle.

> **Note**
>
> Wenn Sie sich nicht sicher sind, ob OpenSearch Service die `AWSServiceRoleForAmazonOpenSearchService` Rolle verwendet, können Sie versuchen, die Rolle zu löschen. Wenn der Service die Rolle verwendet, schlägt die Löschung fehl und Sie können die Ressourcen anzeigen, in denen die Rolle verwendet

wird. Wenn die Rolle verwendet wird, müssen Sie warten, bis die Sitzung beendet wird, bevor Sie die Rolle löschen können, und/oder die Ressourcen löschen, in denen die Rolle verwendet wird. Die Sitzung für eine serviceverknüpfte Rolle können Sie nicht widerrufen.

Manuelles Löschen einer Service-verknüpften Rolle

Löschen Sie serviceverknüpfte Rollen aus der IAM-Konsole, der API oder AWS CLI. Anweisungen finden Sie unter Löschen einer Service-verknüpften Rolle im IAM-Benutzerhandbuch.

Verwenden von serviceverknüpften Rollen zur Erstellung von OpenSearch Serverless-Sammlungen

OpenSearch Serverless verwendet dienstgebundene AWS Identity and Access Management Rollen (IAM). Eine serviceverknüpfte Rolle ist ein spezieller Typ einer IAM-Rolle, die direkt mit dem Service verknüpft ist. OpenSearch Serviceverknüpfte Rollen werden von OpenSearch Service vordefiniert und schließen alle Berechtigungen ein, die der Service zum Aufrufen anderer AWS -Services in Ihrem Namen erfordert.

OpenSearch Serverless verwendet die serviceverknüpfte Rolle AWSServiceRoleForAmazonOpenSearchServerless, die die die Berechtigungen bereitstellt, die die zum Veröffentlichen von Serverless-bezogenen CloudWatch Daten in Ihrem Konto erfordert. Die zugeordnete Rollenberechtigungsrichtlinie ist benannt. AWSService RoleForAmazonOpenSearchServerless `AmazonOpenSearchServerlessServiceRolePolicy` Weitere Informationen zu der Richtlinie finden Sie AmazonOpenSearchServerlessServiceRolePolicyim Referenzhandbuch für AWS verwaltete Richtlinien.

Serviceverknüpfte Rollenberechtigungen für Serverless OpenSearch

OpenSearch Serverless verwendet die serviceverknüpfte Rolle AWSServiceRoleForAmazonOpenSearchServerless, die es OpenSearch Serverless ermöglicht, AWS -Services in Ihrem Namen aufzurufen.

Die AWSService RoleForAmazonOpenSearchServerless serviceverknüpfte Rolle vertraut darauf, dass die folgenden Services die Rolle übernehmen:

- `observability.aoss.amazonaws.com`

Die genannte Richtlinie für Rollenberechtigungen `AmazonOpenSearchServerlessServiceRolePolicy` erlaubt OpenSearch Serverless, die folgenden Aktionen auf den angegebenen Ressourcen durchzuführen:

- Aktion: `cloudwatch:PutMetricData` auf alle AWS -Ressourcen

> **Note**
>
> Die Richtlinie enthält den Bedingungsschlüssel`{"StringEquals": {"cloudwatch:namespace": "AWS/AOSS"}}`, was bedeutet, dass die dienstverknüpfte Rolle nur Metrikdaten an den `AWS/AOSS` CloudWatch Namespace senden kann.

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter Serviceverknüpfte Rollenberechtigung im IAM-Benutzerhandbuch.

Erstellen der serviceverknüpften Rolle für Serverless OpenSearch

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie eine OpenSearch Serverless-Sammlung in der - AWS Management Console, der - oder der AWS CLI AWS -API erstellen, erstellt OpenSearch Serverless die serviceverknüpfte Rolle für Sie.

> **Note**
>
> Wenn Sie zum ersten Mal eine Sammlung erstellen, muss Ihnen das `iam:CreateServiceLinkedRole` in einer identitätsbasierten Richtlinie zugewiesen werden.

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn Sie eine OpenSearch Serverless-Sammlung erstellen, erstellt OpenSearch Serverless die serviceverknüpfte Rolle erneut für Sie.

Sie können auch die IAM-Konsole verwenden, um eine serviceverknüpfte Rolle mit dem Anwendungsfall Amazon OpenSearch Serverless zu erstellen. Erstellen Sie in der API

AWS CLI oder in der AWS API eine serviceverknüpfte Rolle mit dem Servicenamen: `observability.aoss.amazonaws.com`

```
aws iam create-service-linked-role --aws-service-name
 "observability.aoss.amazonaws.com"
```

Weitere Informationen finden Sie unter Erstellen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch. Wenn Sie diese serviceverknüpfte Rolle löschen, können Sie mit demselben Verfahren die Rolle erneut erstellen.

Bearbeiten der serviceverknüpften Rolle für Serverless OpenSearch

OpenSearch Serverless erlaubt Ihnen nicht, die AWSService RoleForAmazonOpenSearchServerless serviceverknüpfte Rolle zu bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach der Erstellung einer serviceverknüpften Rolle nicht bearbeitet werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen der serviceverknüpften Rolle für Serverless OpenSearch

Wenn Sie ein Feature oder einen Service, die bzw. der eine serviceverknüpfte Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Dies verhindert, dass Sie über eine ungenutzte Entität verfügen, die nicht aktiv überwacht oder gewartet wird. Sie müssen jedoch die Ressourcen für Ihre serviceverknüpfte Rolle zunächst bereinigen, bevor Sie sie manuell löschen können.

Um die zu löschen AWSServiceRoleForAmazonOpenSearchServerless, müssen Sie zuerst alle OpenSearch Serverless-Sammlungen in Ihrem löschen. AWS-Konto

> **Note**
>
> Wenn OpenSearch Serverless die Rolle verwendet, während Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

So löschen Sie die serviceverknüpfte Rolle mit IAM

Verwenden Sie die IAM-Konsole, die oder die AWS API AWS CLI, um die AWSService RoleForAmazonOpenSearchServerless serviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Unterstützte Regionen für serviceverknüpfte -Rollen für OpenSearch Serverless

OpenSearch Serverless unterstützt die Verwendung der AWSService RoleForAmazonOpenSearchServerless serviceverknüpften Rolle in jeder Region, in der OpenSearch Serverless verfügbar ist. Eine Liste der unterstützten Regionen finden Sie unter Amazon OpenSearch Serverless Endpoints and Quotas in der. Allgemeine AWS-Referenz

Verwenden von serviceverknüpften Rollen zur Erstellung von OpenSearch Ingestion-Pipelines

Amazon OpenSearch Ingestion verwendet serviceverknüpfte AWS Identity and Access Management Rollen (IAM). Eine serviceverknüpfte Rolle ist ein spezieller Typ einer IAM-Rolle, die direkt mit Ingestion verknüpft ist. OpenSearch Serviceverknüpfte Rollen werden von OpenSearch Ingestion vordefiniert und schließen alle Berechtigungen ein, die der Service zum Aufrufen anderer AWS -Services in Ihrem Namen erfordert.

OpenSearch Bei der Aufnahme wird die angegebene dienstverknüpfte Rolle verwendet, es sei denn AWSServiceRoleForAmazonOpenSearchIngestionService, Sie verwenden eine selbstverwaltete VPC. In diesem Fall wird die dienstverknüpfte Rolle mit dem Namen verwendet. AWSServiceRoleForOpensearchIngestionSelfManagedVpce Die beigefügte Richtlinie enthält die Berechtigungen, die die Rolle zum Erstellen einer Virtual Private Cloud (VPC) zwischen Ihrem Konto und OpenSearch Ingestion sowie zum Veröffentlichen von CloudWatch Metriken in Ihrem -Konto erfordert.

Berechtigungen

Die serviceverknüpfte Rolle `AWSServiceRoleForAmazonOpenSearchIngestionService` vertraut darauf, dass die folgenden Services die Rolle annehmen:

- `osis.amazon.com`

Die genannte Richtlinie für Rollenberechtigungen `AmazonOpenSearchIngestionServiceRolePolicy` erlaubt OpenSearch Ingestion, die folgenden Aktionen auf den angegebenen Ressourcen durchzuführen:

- Aktion: `ec2:DescribeSubnets` für *
- Aktion: `ec2:DescribeSecurityGroups` für *
- Aktion: `ec2:DeleteVpcEndpoints` für *

- Aktion: `ec2:CreateVpcEndpoint` für `*`
- Aktion: `ec2:DescribeVpcEndpoints` für `*`
- Aktion: `ec2:CreateTags` für `arn:aws:ec2:*:*:network-interface/*`
- Aktion: `cloudwatch:PutMetricData` für `cloudwatch:namespace": "AWS/OSIS"`

Die serviceverknüpfte Rolle `AWSServiceRoleForOpensearchIngestionSelfManagedVpce` vertraut darauf, dass die folgenden Services die Rolle annehmen:

- `self-managed-vpce.osis.amazon.com`

Die genannte Richtlinie für Rollenberechtigungen `OpenSearchIngestionSelfManagedVpcePolicy` erlaubt OpenSearch Ingestion, die folgenden Aktionen auf den angegebenen Ressourcen durchzuführen:

- Aktion: `ec2:DescribeSubnets` für `*`
- Aktion: `ec2:DescribeSecurityGroups` für `*`
- Aktion: `ec2:DescribeVpcEndpoints` für `*`
- Aktion: `cloudwatch:PutMetricData` für `cloudwatch:namespace": "AWS/OSIS"`

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter Serviceverknüpfte Rollenberechtigung im IAM-Benutzerhandbuch.

Erstellen der serviceverknüpften Rolle für Ingestion OpenSearch

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie eine OpenSearch Ingestion-Pipeline in der AWS Management Console, der oder der AWS API erstellen AWS CLI, erstellt OpenSearch Ingestion die dienstbezogene Rolle für Sie.

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn Sie eine OpenSearch Ingestion-Pipeline erstellen, erstellt OpenSearch Ingestion die serviceverknüpfte Rolle erneut für Sie.

Bearbeiten der serviceverknüpften Rolle für Ingestion OpenSearch

OpenSearch Die Aufnahme erlaubt Ihnen nicht, die `AWSServiceRoleForAmazonOpenSearchIngestionService` serviceverknüpfte Rolle zu bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach dem Erstellen einer serviceverknüpften Rolle nicht mehr geändert werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen der serviceverknüpften Rolle für Ingestion OpenSearch

Wenn Sie ein Feature oder einen Service, die bzw. der eine serviceverknüpfte Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte Entität, die nicht aktiv überwacht oder verwaltet wird. Sie müssen jedoch die Ressourcen für Ihre serviceverknüpfte Rolle zunächst bereinigen, bevor Sie sie manuell löschen können.

Bereinigen einer serviceverknüpften Rolle

Bevor mit IAM eine serviceverknüpfte Rolle löschen können, müssen Sie zunächst alle von der Rolle verwendeten Ressourcen löschen.

> **Note**
>
> Wenn OpenSearch Ingestion die Rolle verwendet, während Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

Um OpenSearch Ingestion-Ressourcen zu löschen, die von der Rolle oder verwendet werden **`AWSServiceRoleForAmazonOpenSearchIngestionServiceAWSServiceRoleForOpensearchInge`**

1. Navigieren Sie zur Amazon OpenSearch Service-Konsole und wählen Sie Ingestion.
2. Alle Pipelines löschen. Detaillierte Anweisungen finden Sie unter the section called “Löschen von Pipelines”.

Löschen der serviceverknüpften Rolle für Ingestion OpenSearch

Sie können die OpenSearch Erfassungskonsole verwenden, um eine serviceverknüpfte Rolle zu löschen.

So löschen Sie eine serviceverknüpfte Rolle (Konsole)

1. Navigieren Sie zur IAM-Konsole.
2. Wählen Sie Rollen und suchen Sie nach der AWSServiceRoleForAmazonOpenSearchIngestionServiceRolle oder. AWSServiceRoleForOpensearchIngestionSelfManagedVpce
3. Wählen Sie die Rolle aus und klicken Sie auf Löschen.

Beispiel-Code für Amazon OpenSearch Service.

Dieses Kapitel enthält allgemeinen Beispiel-Code für das Arbeiten mit Amazon OpenSearch Service: HTTP-Anforderungssignierung in einer Vielzahl von Programmiersprachen, Komprimierung von HTTP-Anforderungskörpern und Verwendung von AWS SDKs

Themen

- Elasticsearch-Client-Kompatibilität
- Komprimieren von HTTP-Anforderungen in Amazon OpenSearch Service
- Verwenden des AWS SDKs , um mit Amazon OpenSearch Service zu interagieren

Elasticsearch-Client-Kompatibilität

Die neuesten Versionen der Elasticsearch-Clients enthalten möglicherweise Lizenz- oder Versionsprüfungen, die die Kompatibilität künstlich stören. Die folgende Tabelle enthält Empfehlungen darüber, welche Versionen dieser Clients für die optimale Kompatibilität mit OpenSearch Service verwendet werden sollen.

> **Important**
>
> Diese Client-Versionen sind veraltet und werden nicht mit den neuesten Abhängigkeiten aktualisiert, einschließlich Log4j. Wir empfehlen Ihnen, falls möglich, dringend die Verwendung der OpenSearch Versionen der Clients.

Client	Empfohlene Version
Java Low-Level-REST-Client	7.13.4
Java High-Level-REST-Clients	7.13,4
Python-Elasticsearch-Client	7.13,4
Ruby-Elasticsearch-Client	7.13,3
Node.js-Elasticsearch-Client	7.13,0

Komprimieren von HTTP-Anforderungen in Amazon OpenSearch Service

Sie können HTTP-Anfragen und Antworten in OpenSearch Amazon-Domänen mithilfe der gzip-Komprimierung komprimieren. Die gzip-Komprimierung kann Ihnen dabei helfen, die Größe Ihrer Dokumente zu reduzieren und die Bandbreitennutzung und Latenz zu senken, was zu verbesserten Übertragungsgeschwindigkeiten führt.

Die gzip-Komprimierung wird für alle Domänen unterstützt, auf denen OpenSearch oder Elasticsearch 6.0 oder höher ausgeführt wird. Einige OpenSearch Clients verfügen über integrierte Unterstützung für die gzip-Komprimierung und viele Programmiersprachen verfügen über Bibliotheken, die den Prozess vereinfachen.

Aktivieren der gzip-Komprimierung

Nicht zu verwechseln mit ähnlichen OpenSearch Einstellungen: `http_compression.enabled` ist spezifisch für den OpenSearch Service und aktiviert oder deaktiviert die gzip-Komprimierung auf einer Domäne. Domains, die auf Elasticsearch OpenSearch 7 laufen. Bei x ist die gzip-Komprimierung standardmäßig aktiviert, während bei Domänen, auf denen Elasticsearch 6 ausgeführt wird. x hat sie standardmäßig deaktiviert.

Um die gzip-Komprimierung zu aktivieren, senden Sie die folgende Anfrage:

```
PUT _cluster/settings
{
  "persistent" : {
    "http_compression.enabled": true
  }
}
```

Anforderungen an `_cluster/settings` müssen unkomprimiert sein. Daher müssen Sie möglicherweise eine separate Client- oder Standard-HTTP-Anforderung verwenden, um Clustereinstellungen zu aktualisieren.

Um zu bestätigen, dass Sie die gzip-Komprimierung erfolgreich aktiviert haben, senden Sie die folgende Anfrage:

```
GET _cluster/settings?include_defaults=true
```

Stellen Sie sicher, dass Sie die folgende Einstellung in der Antwort sehen:

```
...
"http_compression": {
  "enabled": "true"
}
...
```

Erforderliche Header

Wenn Sie einen gzip-komprimierten Anforderungstext einschließen, behalten Sie den Standard-`Content-Type: application/json`-Header und fügen Sie den `Content-Encoding: gzip`-Header hinzu. Um eine gzip-komprimierte Antwort zu akzeptieren, fügen Sie den `Accept-Encoding: gzip`-Header auch hinzu. Wenn ein OpenSearch Client die gzip-Komprimierung unterstützt, werden diese Header wahrscheinlich automatisch aufgenommen.

Beispiel-Code (Python 3)

Im folgenden Beispiel wird opensearch-py verwendet, um die Komprimierung durchzuführen und die Anforderung zu senden. Dieser Code signiert die Anforderung mit Ihren IAM-Anmeldeinformationen.

```
from opensearchpy import OpenSearch, RequestsHttpConnection
from requests_aws4auth import AWS4Auth
import boto3

host = '' # e.g. my-test-domain.us-east-1.es.amazonaws.com
region = '' # e.g. us-west-1
service = 'es'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
 session_token=credentials.token)

# Create the client.
search = OpenSearch(
    hosts = [{'host': host, 'port': 443}],
    http_auth = awsauth,
    use_ssl = True,
    verify_certs = True,
    http_compress = True, # enables gzip compression for request bodies
    connection_class = RequestsHttpConnection
)
```

```
document = {
  "title": "Moneyball",
  "director": "Bennett Miller",
  "year": "2011"
}

# Send the request.
print(search.index(index='movies', id='1', body=document, refresh=True))

# print(search.index(index='movies', doc_type='_doc', id='1', body=document,
 refresh=True))
```

Alternativ können Sie die richtigen Header angeben, den Anforderungstext selbst komprimieren und eine Standard-HTTP-Bibliothek wie Anforderungen verwenden. Dieser Code signiert die Anforderung mit grundlegenden HTTP-Anmeldeinformationen, die Ihre Domäne möglicherweise unterstützt, wenn Sie eine differenzierte Zugriffssteuerung verwenden.

```
import requests
import gzip
import json

base_url = '' # The domain with https:// and a trailing slash. For example, https://my-
test-domain.us-east-1.es.amazonaws.com/
auth = ('master-user', 'master-user-password') # For testing only. Don't store
 credentials in code.

headers = {'Accept-Encoding': 'gzip', 'Content-Type': 'application/json',
           'Content-Encoding': 'gzip'}

document = {
  "title": "Moneyball",
  "director": "Bennett Miller",
  "year": "2011"
}

# Compress the document.
compressed_document = gzip.compress(json.dumps(document).encode())

# Send the request.
path = 'movies/_doc?refresh=true'
url = base_url + path
response = requests.post(url, auth=auth, headers=headers, data=compressed_document)
print(response.status_code)
```

```
print(response.text)
```

Verwenden des AWS SDKs , um mit Amazon OpenSearch Service zu interagieren

Dieser Abschnitt enthält Beispiele für die Verwendung der AWS SDKs Amazon OpenSearch Service-Konfigurations-API. Diese Codebeispiele zeigen das Erstellen, Aktualisieren und Löschen von OpenSearch Service-Domänen.

Java

Dieser Abschnitt enthält Beispiele für Versionen 1 und 2 von AWS SDK für Java.

Version 2

In diesem Beispiel wird der OpenSearchClientBuilderKonstruktor aus Version 2 von verwendet, AWS SDK für Java um eine OpenSearch Domäne zu erstellen, ihre Konfiguration zu aktualisieren und sie zu löschen. Heben Sie die Kommentierung der Aufrufe an `waitForDomainProcessing` auf (und kommentieren Sie den Aufruf an `deleteDomain`), damit die Domäne online gehen und verwendet werden kann.

```
package com.example.samples;

import java.util.concurrent.TimeUnit;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.opensearch.OpenSearchClient;
import software.amazon.awssdk.services.opensearch.model.ClusterConfig;
import software.amazon.awssdk.services.opensearch.model.EBSOptions;
import software.amazon.awssdk.services.opensearch.model.CognitoOptions;
import software.amazon.awssdk.services.opensearch.model.NodeToNodeEncryptionOptions;
import software.amazon.awssdk.services.opensearch.model.CreateDomainRequest;
import software.amazon.awssdk.services.opensearch.model.CreateDomainResponse;
import software.amazon.awssdk.services.opensearch.model.DescribeDomainRequest;
import software.amazon.awssdk.services.opensearch.model.UpdateDomainConfigRequest;
import software.amazon.awssdk.services.opensearch.model.UpdateDomainConfigResponse;
import software.amazon.awssdk.services.opensearch.model.DescribeDomainResponse;
import software.amazon.awssdk.services.opensearch.model.DeleteDomainRequest;
import software.amazon.awssdk.services.opensearch.model.DeleteDomainResponse;
import software.amazon.awssdk.services.opensearch.model.OpenSearchException;
import software.amazon.awssdk.auth.credentials.DefaultCredentialsProvider;
```

```
/**
 * Sample class demonstrating how to use the Amazon Web Services SDK for Java to
 create, update,
 * and delete Amazon OpenSearch Service domains.
 */

public class OpenSearchSample {

    public static void main(String[] args) {

     String domainName = "my-test-domain";

     // Build the client using the default credentials chain.
        // You can use the CLI and run `aws configure` to set access key, secret
        // key, and default region.

        OpenSearchClient client = OpenSearchClient.builder()
          // Unnecessary, but lets you use a region different than your default.
          .region(Region.US_EAST_1)
          // Unnecessary, but if desired, you can use a different provider chain.
          .credentialsProvider(DefaultCredentialsProvider.create())
                    .build();

        // Create a new domain, update its configuration, and delete it.
        createDomain(client, domainName);
        //waitForDomainProcessing(client, domainName);
        updateDomain(client, domainName);
        //waitForDomainProcessing(client, domainName);
        deleteDomain(client, domainName);
    }

    /**
     * Creates an Amazon OpenSearch Service domain with the specified options.
     * Some options require other Amazon Web Services resources, such as an Amazon
 Cognito user pool
     * and identity pool, whereas others require just an instance type or instance
     * count.
     *
     * @param client
     *            The client to use for the requests to Amazon OpenSearch Service
     * @param domainName
     *            The name of the domain you want to create
     */
```

```
    public static void createDomain(OpenSearchClient client, String domainName) {

     // Create the request and set the desired configuration options

        try {

            ClusterConfig clusterConfig = ClusterConfig.builder()
                    .dedicatedMasterEnabled(true)
                    .dedicatedMasterCount(3)
                    // Small, inexpensive instance types for testing. Not
 recommended for production.
                    .dedicatedMasterType("t2.small.search")
                    .instanceType("t2.small.search")
                    .instanceCount(5)
                    .build();

            // Many instance types require EBS storage.
            EBSOptions ebsOptions = EBSOptions.builder()
                    .ebsEnabled(true)
                    .volumeSize(10)
                    .volumeType("gp2")
                    .build();

            NodeToNodeEncryptionOptions encryptionOptions =
 NodeToNodeEncryptionOptions.builder()
                    .enabled(true)
                    .build();

            CreateDomainRequest createRequest = CreateDomainRequest.builder()
                    .domainName(domainName)
                    .engineVersion("OpenSearch_1.0")
                    .clusterConfig(clusterConfig)
                    .ebsOptions(ebsOptions)
                    .nodeToNodeEncryptionOptions(encryptionOptions)
                    // You can uncomment this line and add your account ID, a
 username, and the
                    // domain name to add an access policy.
                    // .accessPolicies("{\"Version\":\"2012-10-17\",
\"Statement\":[{\"Effect\":\"Allow\",\"Principal\":{\"AWS\":
[\"arn:aws:iam::123456789012:user/user-name\"]},\"Action\":[\"es:*\"],\"Resource\":
\"arn:aws:es:region:123456789012:domain/domain-name/*\"}]}")
                    .build();

            // Make the request.
```

```
            System.out.println("Sending domain creation request...");
            CreateDomainResponse createResponse =
client.createDomain(createRequest);
            System.out.println("Domain status:
"+createResponse.domainStatus().toString());
            System.out.println("Domain ID:
"+createResponse.domainStatus().domainId());


        } catch (OpenSearchException e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
    }

    /**
     * Updates the configuration of an Amazon OpenSearch Service domain with the
     * specified options. Some options require other Amazon Web Services resources,
such as an
     * Amazon Cognito user pool and identity pool, whereas others require just an
     * instance type or instance count.
     *
     * @param client
     *             The client to use for the requests to Amazon OpenSearch Service
     * @param domainName
     *             The name of the domain to update
     */

    public static void updateDomain(OpenSearchClient client, String domainName) {

     // Updates the domain to use three data instances instead of five.
        // You can uncomment the Cognito line and fill in the strings to enable
Cognito
        // authentication for OpenSearch Dashboards.

        try {

            ClusterConfig clusterConfig = ClusterConfig.builder()
                    .instanceCount(5)
                    .build();

            CognitoOptions cognitoOptions = CognitoOptions.builder()
                    .enabled(true)
                    .userPoolId("user-pool-id")
```

```
                    .identityPoolId("identity-pool-id")
                    .roleArn("role-arn")
                    .build();

            UpdateDomainConfigRequest updateRequest =
UpdateDomainConfigRequest.builder()
                    .domainName(domainName)
                    .clusterConfig(clusterConfig)
                    //.cognitoOptions(cognitoOptions)
                    .build();

            System.out.println("Sending domain update request...");
            UpdateDomainConfigResponse updateResponse =
client.updateDomainConfig(updateRequest);
            System.out.println("Domain config:
"+updateResponse.domainConfig().toString());


        } catch (OpenSearchException e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
    }

    /**
     * Deletes an Amazon OpenSearch Service domain. Deleting a domain can take
     * several minutes.
     *
     * @param client
     *             The client to use for the requests to Amazon OpenSearch Service
     * @param domainName
     *             The name of the domain that you want to delete
     */

    public static void deleteDomain(OpenSearchClient client, String domainName) {

        try {

            DeleteDomainRequest deleteRequest = DeleteDomainRequest.builder()
                    .domainName(domainName)
                    .build();

            System.out.println("Sending domain deletion request...");
```

```
            DeleteDomainResponse deleteResponse =
client.deleteDomain(deleteRequest);
            System.out.println("Domain status: "+deleteResponse.toString());


        } catch (OpenSearchException e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
    }

    /**
     * Waits for the domain to finish processing changes. New domains typically take
15-30 minutes
     * to initialize, but can take longer depending on the configuration. Most
updates to existing domains
     * take a similar amount of time. This method checks every 15 seconds and
finishes only when
     * the domain's processing status changes to false.
     *
     * @param client
     *            The client to use for the requests to Amazon OpenSearch Service
     * @param domainName
     *            The name of the domain that you want to check
     */

    public static void waitForDomainProcessing(OpenSearchClient client, String
domainName) {
        // Create a new request to check the domain status.
        DescribeDomainRequest describeRequest = DescribeDomainRequest.builder()
                .domainName(domainName)
                .build();

        // Every 15 seconds, check whether the domain is processing.
        DescribeDomainResponse describeResponse =
client.describeDomain(describeRequest);
        while (describeResponse.domainStatus().processing()) {
            try {
                System.out.println("Domain still processing...");
                TimeUnit.SECONDS.sleep(15);
                describeResponse = client.describeDomain(describeRequest);
            } catch (InterruptedException e) {
                e.printStackTrace();
            }
```

```
        }

        // Once we exit that loop, the domain is available
        System.out.println("Amazon OpenSearch Service has finished processing
 changes for your domain.");
        System.out.println("Domain description: "+describeResponse.toString());
    }
}
```

Version 1

In diesem Beispiel wird der AWSElasticsearchClientBuilderKonstruktor der Version 1 von verwendet, AWS SDK für Java um eine ältere Elasticsearch-Domäne zu erstellen, ihre Konfiguration zu aktualisieren und sie zu löschen. Heben Sie die Kommentierung der Aufrufe an `waitForDomainProcessing` auf (und kommentieren Sie den Aufruf an `deleteDomain`), damit die Domäne online gehen und verwendet werden kann.

```
package com.amazonaws.samples;

import java.util.concurrent.TimeUnit;
import com.amazonaws.auth.DefaultAWSCredentialsProviderChain;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.elasticsearch.AWSElasticsearch;
import com.amazonaws.services.elasticsearch.AWSElasticsearchClientBuilder;
import com.amazonaws.services.elasticsearch.model.CreateElasticsearchDomainRequest;
import com.amazonaws.services.elasticsearch.model.CreateElasticsearchDomainResult;
import com.amazonaws.services.elasticsearch.model.DeleteElasticsearchDomainRequest;
import com.amazonaws.services.elasticsearch.model.DeleteElasticsearchDomainResult;
import
 com.amazonaws.services.elasticsearch.model.DescribeElasticsearchDomainRequest;
import com.amazonaws.services.elasticsearch.model.DescribeElasticsearchDomainResult;
import com.amazonaws.services.elasticsearch.model.EBSOptions;
import com.amazonaws.services.elasticsearch.model.ElasticsearchClusterConfig;
import com.amazonaws.services.elasticsearch.model.ResourceNotFoundException;
import
 com.amazonaws.services.elasticsearch.model.UpdateElasticsearchDomainConfigRequest;
import
 com.amazonaws.services.elasticsearch.model.UpdateElasticsearchDomainConfigResult;
import com.amazonaws.services.elasticsearch.model.VolumeType;

/**
 * Sample class demonstrating how to use the Amazon Web Services SDK for Java to
 create, update,
```

```
 * and delete Amazon OpenSearch Service domains.
 */

public class OpenSearchSample {

    public static void main(String[] args) {

        final String domainName = "my-test-domain";

        // Build the client using the default credentials chain.
        // You can use the CLI and run `aws configure` to set access key, secret
        // key, and default region.
        final AWSElasticsearch client = AWSElasticsearchClientBuilder
                .standard()
                // Unnecessary, but lets you use a region different than your
 default.
                .withRegion(Regions.US_WEST_2)
                // Unnecessary, but if desired, you can use a different provider
 chain.
                .withCredentials(new DefaultAWSCredentialsProviderChain())
                .build();

        // Create a new domain, update its configuration, and delete it.
        createDomain(client, domainName);
        // waitForDomainProcessing(client, domainName);
        updateDomain(client, domainName);
        // waitForDomainProcessing(client, domainName);
        deleteDomain(client, domainName);
    }

    /**
     * Creates an Amazon OpenSearch Service domain with the specified options.
     * Some options require other Amazon Web Services resources, such as an Amazon
 Cognito user pool
     * and identity pool, whereas others require just an instance type or instance
     * count.
     *
     * @param client
     *            The client to use for the requests to Amazon OpenSearch Service
     * @param domainName
     *            The name of the domain you want to create
     */
    private static void createDomain(final AWSElasticsearch client, final String
 domainName) {
```

```
        // Create the request and set the desired configuration options
        CreateElasticsearchDomainRequest createRequest = new
 CreateElasticsearchDomainRequest()
                .withDomainName(domainName)
                .withElasticsearchVersion("7.10")
                .withElasticsearchClusterConfig(new ElasticsearchClusterConfig()
                        .withDedicatedMasterEnabled(true)
                        .withDedicatedMasterCount(3)
                        // Small, inexpensive instance types for testing. Not
 recommended for production
                        // domains.
                        .withDedicatedMasterType("t2.small.elasticsearch")
                        .withInstanceType("t2.small.elasticsearch")
                        .withInstanceCount(5))
                // Many instance types require EBS storage.
                .withEBSOptions(new EBSOptions()
                        .withEBSEnabled(true)
                        .withVolumeSize(10)
                        .withVolumeType(VolumeType.Gp2));
                // You can uncomment this line and add your account ID, a username,
 and the
                // domain name to add an access policy.
                // .withAccessPolicies("{\"Version\":\"2012-10-17\",
\"Statement\":[{\"Effect\":\"Allow\",\"Principal\":{\"AWS\":
[\"arn:aws:iam::123456789012:user/user-name\"]},\"Action\":[\"es:*\"],\"Resource\":
\"arn:aws:es:region:123456789012:domain/domain-name/*\"}]}")


        // Make the request.
        System.out.println("Sending domain creation request...");
        CreateElasticsearchDomainResult createResponse =
 client.createElasticsearchDomain(createRequest);
        System.out.println("Domain creation response from Amazon OpenSearch
 Service:");
        System.out.println(createResponse.getDomainStatus().toString());
    }

    /**
     * Updates the configuration of an Amazon OpenSearch Service domain with the
     * specified options. Some options require other Amazon Web Services resources,
 such as an
     * Amazon Cognito user pool and identity pool, whereas others require just an
     * instance type or instance count.
```

```
    *
    * @param client
    *            The client to use for the requests to Amazon OpenSearch Service
    * @param domainName
    *            The name of the domain to update
    */
   private static void updateDomain(final AWSElasticsearch client, final String
domainName) {
       try {
           // Updates the domain to use three data instances instead of five.
           // You can uncomment the Cognito lines and fill in the strings to enable
Cognito
           // authentication for OpenSearch Dashboards.
           final UpdateElasticsearchDomainConfigRequest updateRequest = new
UpdateElasticsearchDomainConfigRequest()
                   .withDomainName(domainName)
                   // .withCognitoOptions(new CognitoOptions()
                           // .withEnabled(true)
                           // .withUserPoolId("user-pool-id")
                           // .withIdentityPoolId("identity-pool-id")
                           // .withRoleArn("role-arn")
                   .withElasticsearchClusterConfig(new ElasticsearchClusterConfig()
                           .withInstanceCount(3));

           System.out.println("Sending domain update request...");
           final UpdateElasticsearchDomainConfigResult updateResponse = client
                   .updateElasticsearchDomainConfig(updateRequest);
           System.out.println("Domain update response from Amazon OpenSearch
Service:");
           System.out.println(updateResponse.toString());
       } catch (ResourceNotFoundException e) {
           System.out.println("Domain not found. Please check the domain name.");
       }
   }

   /**
    * Deletes an Amazon OpenSearch Service domain. Deleting a domain can take
    * several minutes.
    *
    * @param client
    *            The client to use for the requests to Amazon OpenSearch Service
    * @param domainName
    *            The name of the domain that you want to delete
    */
```

```
   private static void deleteDomain(final AWSElasticsearch client, final String
domainName) {
       try {
           final DeleteElasticsearchDomainRequest deleteRequest = new
DeleteElasticsearchDomainRequest()
                   .withDomainName(domainName);

           System.out.println("Sending domain deletion request...");
           final DeleteElasticsearchDomainResult deleteResponse =
client.deleteElasticsearchDomain(deleteRequest);
           System.out.println("Domain deletion response from Amazon OpenSearch
Service:");
           System.out.println(deleteResponse.toString());
       } catch (ResourceNotFoundException e) {
           System.out.println("Domain not found. Please check the domain name.");
       }
   }

   /**
    * Waits for the domain to finish processing changes. New domains typically take
15-30 minutes
    * to initialize, but can take longer depending on the configuration. Most
updates to existing domains
    * take a similar amount of time. This method checks every 15 seconds and
finishes only when
    * the domain's processing status changes to false.
    *
    * @param client
    *            The client to use for the requests to Amazon OpenSearch Service
    * @param domainName
    *            The name of the domain that you want to check
    */
   private static void waitForDomainProcessing(final AWSElasticsearch client, final
String domainName) {
       // Create a new request to check the domain status.
       final DescribeElasticsearchDomainRequest describeRequest = new
DescribeElasticsearchDomainRequest()
               .withDomainName(domainName);

       // Every 15 seconds, check whether the domain is processing.
       DescribeElasticsearchDomainResult describeResponse =
client.describeElasticsearchDomain(describeRequest);
       while (describeResponse.getDomainStatus().isProcessing()) {
           try {
```

```
                System.out.println("Domain still processing...");
                TimeUnit.SECONDS.sleep(15);
                describeResponse =
 client.describeElasticsearchDomain(describeRequest);
            } catch (InterruptedException e) {
                e.printStackTrace();
            }
        }

        // Once we exit that loop, the domain is available
        System.out.println("Amazon OpenSearch Service has finished processing
 changes for your domain.");
        System.out.println("Domain description response from Amazon OpenSearch
 Service:");
        System.out.println(describeResponse.toString());
    }
}
```

Python

In diesem Beispiel wird der -Python-Client OpenSearchServiceauf niedriger Ebene aus verwendet, AWS SDK for Python (Boto) um eine Domäne zu erstellen, ihre Konfiguration zu aktualisieren und sie zu löschen.

```
import boto3
import botocore
from botocore.config import Config
import time

# Build the client using the default credential configuration.
# You can use the CLI and run 'aws configure' to set access key, secret
# key, and default region.

my_config = Config(
    # Optionally lets you specify a region other than your default.
    region_name='us-west-2'
)

client = boto3.client('opensearch', config=my_config)

domainName = 'my-test-domain'  # The name of the domain
```

```
def createDomain(client, domainName):
    """Creates an Amazon OpenSearch Service domain with the specified options."""
    response = client.create_domain(
        DomainName=domainName,
        EngineVersion='OpenSearch_1.0',
        ClusterConfig={
            'InstanceType': 't2.small.search',
            'InstanceCount': 5,
            'DedicatedMasterEnabled': True,
            'DedicatedMasterType': 't2.small.search',
            'DedicatedMasterCount': 3
        },
        # Many instance types require EBS storage.
        EBSOptions={
            'EBSEnabled': True,
            'VolumeType': 'gp2',
            'VolumeSize': 10
        },
        AccessPolicies="{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect\":\"Allow
\",\"Principal\":{\"AWS\":[\"arn:aws:iam::123456789012:user/user-name\"]},\"Action\":
[\"es:*\"],\"Resource\":\"arn:aws:es:us-west-2:123456789012:domain/my-test-domain/*
\"}]}",
        NodeToNodeEncryptionOptions={
            'Enabled': True
        }
    )
    print("Creating domain...")
    print(response)


def updateDomain(client, domainName):
    """Updates the domain to use three data nodes instead of five."""
    try:
        response = client.update_domain_config(
            DomainName=domainName,
            ClusterConfig={
                'InstanceCount': 3
            }
        )
        print('Sending domain update request...')
        print(response)

    except botocore.exceptions.ClientError as error:
```

```
        if error.response['Error']['Code'] == 'ResourceNotFoundException':
            print('Domain not found. Please check the domain name.')
        else:
            raise error


def deleteDomain(client, domainName):
    """Deletes an OpenSearch Service domain. Deleting a domain can take several
 minutes."""
    try:
        response = client.delete_domain(
            DomainName=domainName
        )
        print('Sending domain deletion request...')
        print(response)

    except botocore.exceptions.ClientError as error:
        if error.response['Error']['Code'] == 'ResourceNotFoundException':
            print('Domain not found. Please check the domain name.')
        else:
            raise error


def waitForDomainProcessing(client, domainName):
    """Waits for the domain to finish processing changes."""
    try:
        response = client.describe_domain(
            DomainName=domainName
        )
        # Every 15 seconds, check whether the domain is processing.
        while response["DomainStatus"]["Processing"] == True:
            print('Domain still processing...')
            time.sleep(15)
            response = client.describe_domain(
                DomainName=domainName)

        # Once we exit the loop, the domain is available.
        print('Amazon OpenSearch Service has finished processing changes for your
 domain.')
        print('Domain description:')
        print(response)

    except botocore.exceptions.ClientError as error:
        if error.response['Error']['Code'] == 'ResourceNotFoundException':
```

```
            print('Domain not found. Please check the domain name.')
        else:
            raise error


def main():
    """Create a new domain, update its configuration, and delete it."""
    createDomain(client, domainName)
    waitForDomainProcessing(client, domainName)
    updateDomain(client, domainName)
    waitForDomainProcessing(client, domainName)
    deleteDomain(client, domainName)
```

Knoten

In diesem Beispiel wird die Version 3 des Node.js OpenSearch -Clients von SDK für JavaScript verwendet, um eine Domäne zu erstellen, ihre Konfiguration zu aktualisieren und sie zu löschen.

```
var {
    OpenSearchClient,
    CreateDomainCommand,
    DescribeDomainCommand,
    UpdateDomainConfigCommand,
    DeleteDomainCommand
} = require("@aws-sdk/client-opensearch");
var sleep = require('sleep');

var client = new OpenSearchClient();

var domainName = 'my-test-domain'

// Create a new domain, update its configuration, and delete it.
createDomain(client, domainName)
waitForDomainProcessing(client, domainName)
updateDomain(client, domainName)
waitForDomainProcessing(client, domainName)
deleteDomain(client, domainName)

async function createDomain(client, domainName) {
    // Creates an Amazon OpenSearch Service domain with the specified options.
    var command = new CreateDomainCommand({
        DomainName: domainName,
        EngineVersion: 'OpenSearch_1.0',
```

```
        ClusterConfig: {
        'InstanceType': 't2.small.search',
        'InstanceCount': 5,
        'DedicatedMasterEnabled': 'True',
        'DedicatedMasterType': 't2.small.search',
        'DedicatedMasterCount': 3
        },
        EBSOptions:{
            'EBSEnabled': 'True',
            'VolumeType': 'gp2',
            'VolumeSize': 10
        },
        AccessPolicies: "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect\":\"Allow
\",\"Principal\":{\"AWS\":[\"arn:aws:iam::123456789012:user/user-name\"]},\"Action\":
[\"es:*\"],\"Resource\":\"arn:aws:es:us-east-1:123456789012:domain/my-test-domain/*
\"}]}",
         NodeToNodeEncryptionOptions:{
            'Enabled': 'True'
        }
    });
    const response = await client.send(command);
    console.log("Creating domain...");
    console.log(response);
}

async function updateDomain(client, domainName) {
    // Updates the domain to use three data nodes instead of five.
    var command = new UpdateDomainConfigCommand({
        DomainName: domainName,
        ClusterConfig: {
        'InstanceCount': 3
        }
    });
    const response = await client.send(command);
    console.log('Sending domain update request...');
    console.log(response);
}

async function deleteDomain(client, domainName) {
    // Deletes an OpenSearch Service domain. Deleting a domain can take several
 minutes.
    var command = new DeleteDomainCommand({
        DomainName: domainName
    });
```

```
    const response = await client.send(command);
    console.log('Sending domain deletion request...');
    console.log(response);
}

async function waitForDomainProcessing(client, domainName) {
    // Waits for the domain to finish processing changes.
    try {
        var command = new DescribeDomainCommand({
            DomainName: domainName
        });
        var response = await client.send(command);

        while (response.DomainStatus.Processing == true) {
            console.log('Domain still processing...')
            await sleep(15000) // Wait for 15 seconds, then check the status again
            function sleep(ms) {
                return new Promise((resolve) => {
                    setTimeout(resolve, ms);
                });
            }
            var response = await client.send(command);
        }
        // Once we exit the loop, the domain is available.
        console.log('Amazon OpenSearch Service has finished processing changes for your
 domain.');
        console.log('Domain description:');
        console.log(response);

    } catch (error) {
        if (error.name === 'ResourceNotFoundException') {
            console.log('Domain not found. Please check the domain name.');
            }
    };
}
```

Indizierung von Daten in Amazon Service OpenSearch

Da Amazon OpenSearch Service eine REST-API verwendet, gibt es zahlreiche Methoden für die Indizierung von Dokumenten. Sie können Standard-Clients wie curl oder eine beliebige Programmiersprache verwenden, die HTTP-Anforderungen senden können. Um den Prozess der Interaktion damit weiter zu vereinfachen, verfügt OpenSearch Service über Clients für viele Programmiersprachen. Fortgeschrittene Benutzer können direkt fortfahren mit the section called “Streaming-Daten werden in den OpenSearch Service geladen”.

Wir empfehlen Ihnen dringend, Amazon OpenSearch Ingestion für die Datenaufnahme zu verwenden. Dabei handelt es sich um einen vollständig verwalteten Datensammler, der in Service integriert ist. OpenSearch Weitere Informationen finden Sie unter Amazon OpenSearch Ingestion.

Eine Einführung in die Indizierung finden Sie in der Dokumentation. OpenSearch

Namensbeschränkungen bei Indizes

OpenSearch Für Dienstindizes gelten die folgenden Einschränkungen bei der Benennung:

- Alle Buchstaben müssen Kleinbuchstaben sein.
- Indexnamen dürfen nicht mit _ oder - beginnen.
- Indexnamen dürfen keine Leerzeichen, Kommas, :, ", *, +, /, \, |, ?, #, > oder < enthalten.

Nehmen Sie keine vertraulichen Informationen in Index-, Typ- oder Dokument-ID-Namen auf. OpenSearch Der Dienst verwendet diese Namen in seinen Uniform Resource Identifiers (URIs). Server und Anwendungen protokollieren häufig HTTP-Anfragen, was zu unnötiger Offenlegung von Daten führen kann, wenn sie vertrauliche Informationen URIs enthalten:

```
2018-10-03T23:39:43 198.51.100.14 200 "GET https://opensearch-domain/dr-jane-doe/flu-
patients-2018/202-555-0100/ HTTP/1.1"
```

Auch wenn Sie keine Berechtigungen zum Anzeigen des zugehörigen JSON-Dokuments haben, könnten Sie von dieser gefälschten Protokollzeile ableiten, dass einer von Dr. Does Patienten mit der Telefonnummer 202–555–0100 im Jahr 2018 die Grippe hatte.

Wenn der OpenSearch Dienst eine echte oder vermeintliche IP-Adresse in einem Indexnamen erkennt (z. B.`my-index-12.34.56.78.91`), maskiert er die IP-Adresse. Ein Anruf bei `_cat/indices` ergibt die folgende Antwort:

```
green open my-index-x.x.x.x.91    soY19tBERoKo71WcEScidw 5 1 0 0   2kb  1kb
```

Um unnötige Verwirrung zu vermeiden, sollten Sie es vermeiden, IP-Adressen in Indexnamen zu verwenden.

Reduzierung der Antwortgröße

Die Antworten von `_index` und `_bulk` APIs enthalten eine ganze Menge Informationen. Diese Informationen können bei der Fehlerbehebung von Anfragen oder der Implementierung von Logik für Wiederholversuche nützlich sein. Sie benötigen allerdings beträchtliche Bandbreite. In diesem Beispiel führt die Indizierung eines 32-Byte-Dokuments zu einer 339-Byte-Antwort (einschließlich Kopfzeilen):

```
PUT opensearch-domain/more-movies/_doc/1
{"title": "Back to the Future"}
```

Antwort

```
{
  "_index": "more-movies",
  "_type": "_doc",
  "_id": "1",
  "_version": 4,
  "result": "updated",
  "_shards": {
    "total": 2,
    "successful": 2,
    "failed": 0
  },
  "_seq_no": 3,
  "_primary_term": 1
}
```

Diese Antwortgröße mag minimal erscheinen, aber wenn Sie 1 000 000 Dokumente pro Tag indizieren – ungefähr 11,5 Dokumente pro Sekunde – ergeben 339 Byte pro Antwort 10,17 GB Download-Datenverkehr pro Monat.

Wenn Datenübertragungskosten ein Problem darstellen, verwenden Sie den `filter_path` Parameter, um die Größe der OpenSearch Serviceantwort zu reduzieren. Achten Sie jedoch darauf, dass Sie keine Felder herausfiltern, die Sie benötigen, um fehlgeschlagene Anfragen zu identifizieren oder erneut zu versuchen. Diese Felder variieren je nach Client. Der `filter_path` Parameter funktioniert für alle OpenSearch REST-Dienste APIs, ist aber besonders nützlich APIs , wenn Sie häufig aufrufen, z. B. mit `_index` und `_bulk` APIs:

```
PUT opensearch-domain/more-movies/_doc/1?filter_path=result,_shards.total
{"title": "Back to the Future"}
```

Antwort

```
{
  "result": "updated",
  "_shards": {
    "total": 2
  }
}
```

Anstatt Felder zu integrieren, können Sie Felder mit einem `-`-Präfix ausschließen. `filter_path` unterstützt auch Platzhalter:

```
POST opensearch-domain/_bulk?filter_path=-took,-items.index._*
{ "index": { "_index": "more-movies", "_id": "1" } }
{"title": "Back to the Future"}
{ "index": { "_index": "more-movies", "_id": "2" } }
{"title": "Spirited Away"}
```

Antwort

```
{
  "errors": false,
  "items": [
    {
      "index": {
        "result": "updated",
        "status": 200
      }
    },
    {
      "index": {
```

```
        "result": "updated",
        "status": 200
      }
    }
  ]
}
```

Indexcodecs

Index-Codecs bestimmen, wie die in einem Index gespeicherten Felder komprimiert und auf der Festplatte gespeichert werden. Der Index-Codec wird durch die statische `index.codec` Einstellung gesteuert, die den Komprimierungsalgorithmus angibt. Diese Einstellung wirkt sich auf die Größe des Index-Shards und die Betriebsleistung aus.

Eine Liste der unterstützten Codecs und ihrer Leistungsmerkmale finden Sie in der Dokumentation unter Unterstützte Codecs. OpenSearch

Beachten Sie bei der Auswahl eines Index-Codec Folgendes:

- Um die Probleme zu vermeiden, die mit der Änderung der Codec-Einstellung eines vorhandenen Indexes verbunden sind, sollten Sie zunächst einen repräsentativen Workload in einer Umgebung außerhalb der Produktionsumgebung testen, bevor Sie eine neue Codec-Einstellung verwenden. Weitere Informationen finden Sie unter Ändern eines Index-Codecs.
- Sie können keine Z-Standard-Komprimierungscodecs (`"index.codec": "zstd"`oder`"index.codec": "zstd_no_dict"`) für k-NN- oder Security Analytics-Indizes verwenden.

Streaming-Daten in Amazon OpenSearch Service laden

Sie können OpenSearch Ingestion verwenden, um Streaming-Daten direkt in Ihre Amazon OpenSearch Service-Domain zu laden, ohne Lösungen von Drittanbietern verwenden zu müssen. Um Daten an OpenSearch Ingestion zu senden, konfigurieren Sie Ihre Datenproduzenten und der Service liefert die Daten automatisch an die von Ihnen angegebene Domain oder Sammlung. Informationen zu den ersten Schritten mit OpenSearch Ingestion finden Sie unter. the section called “Tutorial: Daten in eine Sammlung aufnehmen”

Sie können weiterhin andere Quellen zum Laden von Streaming-Daten verwenden, z. B. Amazon Data Firehose und Amazon CloudWatch Logs, die über eine integrierte Unterstützung für

OpenSearch Service verfügen. Andere, wie z. B. Amazon S3, Amazon Kinesis Data Streams und Amazon DynamoDB, verwenden AWS Lambda -Funktionen als Ereignis-Handler. Die Lambda-Funktionen reagieren auf neue Daten, indem Sie sie verarbeiten und zu Ihrer Domain streamen.

> **Note**
>
> Lambda unterstützt verschiedene gängige Programmiersprachen und ist in den meisten AWS-Regionen verfügbar. Weitere Informationen finden Sie unter Getting started with Lambda im AWS Lambda Developer Guide und unter AWS Service Endpoints im. Allgemeine AWS-Referenz

Streaming-Daten aus Ingestion werden geladen OpenSearch

Sie können Amazon OpenSearch Ingestion verwenden, um Daten in eine OpenSearch Service-Domain zu laden. Sie konfigurieren Ihre Datenproduzenten so, dass sie Daten an OpenSearch Ingestion senden, und Ingestion übermittelt die Daten automatisch an die von Ihnen angegebene Sammlung. Sie können OpenSearch Ingestion auch so konfigurieren, dass Ihre Daten vor der Bereitstellung transformiert werden. Weitere Informationen finden Sie unter OpenSearch Einnahme durch Amazon.

So laden Sie Streaming-Daten aus Amazon S3

Sie können Lambda verwenden, um Daten von Amazon S3 an Ihre OpenSearch Service-Domain zu senden. Neue in einem S3-Bucket eintreffende Daten lösen eine Ereignisbenachrichtigung an Lambda aus, wodurch Ihr benutzerdefinierter Code zum Durchführen der Indizierung ausgeführt wird.

Diese Methode zum Streamen von Daten ist ausgesprochen flexibel. Sie können Objekt-Metadaten indizieren oder einige Elemente des Objekttextes analysieren und indizieren, sofern das Objekt Klartext ist. Dieser Abschnitt enthält unkomplizierten Python-Beispielcode für die Verwendung von regulären Ausdrücken zum Analysieren einer Protokolldatei und Indizieren der Übereinstimmungen.

Voraussetzungen

Zum Fortfahren benötigen Sie die folgenden Ressourcen.

Voraussetzung	Beschreibung
Amazon-S3-Bucket	Weitere Informationen finden Sie unter Erstellen Ihres ersten S3 Buckets im Benutzerhandbuch für Amazon Simple Storage Service. Der Bucket muss sich in derselben Region wie Ihre OpenSearch Service-D omain befinden.
OpenSearch Dienstdomäne	Das Ziel für die Daten, nachdem sie durch Ihre Lambda-Funktion verarbeitet wurden. Weitere Informationen finden Sie unter the section called “ OpenSearch Dienstdomänen erstellen”.

Erstellen des Lambda-Bereitstellungspakets

Bereitstellungspakete sind ZIP- oder JAR-Dateien, die Ihren Code und seine Abhängigkeiten enthalten. Dieser Abschnitt enthält Python-Beispielcode. Informationen zu anderen Programmiersprachen finden Sie unter Lambda-Bereitstellungspakete im AWS Lambda - Entwicklerhandbuch.

1. Erstellen Sie ein Verzeichnis. In diesem Beispiel verwenden wir den Namen `s3-to-opensearch`.
2. Erstellen Sie im Verzeichnis eine Datei mit dem Namen `sample.py`:

```
import boto3
import re
import requests
from requests_aws4auth import AWS4Auth

region = '' # e.g. us-west-1
service = 'es'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
 session_token=credentials.token)

host = '' # the OpenSearch Service domain, e.g. https://search-mydomain.us-
west-1.es.amazonaws.com
index = 'lambda-s3-index'
datatype = '_doc'
url = host + '/' + index + '/' + datatype
```

```
headers = { "Content-Type": "application/json" }

s3 = boto3.client('s3')

# Regular expressions used to parse some simple log lines
ip_pattern = re.compile('(\d+\.\d+\.\d+\.\d+)')
time_pattern = re.compile('\[(\d+\/\w\w\w\/\d\d\d\d:\d\d:\d\d:\d\d\s-\d\d\d\d)\]')
message_pattern = re.compile('\"(.+)\"')

# Lambda execution starts here
def handler(event, context):
    for record in event['Records']:

        # Get the bucket name and key for the new file
        bucket = record['s3']['bucket']['name']
        key = record['s3']['object']['key']

        # Get, read, and split the file into lines
        obj = s3.get_object(Bucket=bucket, Key=key)
        body = obj['Body'].read()
        lines = body.splitlines()

        # Match the regular expressions to each line and index the JSON
        for line in lines:
            line = line.decode("utf-8")
            ip = ip_pattern.search(line).group(1)
            timestamp = time_pattern.search(line).group(1)
            message = message_pattern.search(line).group(1)

            document = { "ip": ip, "timestamp": timestamp, "message": message }
            r = requests.post(url, auth=awsauth, json=document, headers=headers)
```

Bearbeiten Sie die Variablen für `region` und `host`.

3. Installieren Sie pip, falls noch nicht geschehen, und installieren Sie dann die Abhängigkeiten in einem neuen `package`-Verzeichnis:

```
cd s3-to-opensearch

pip install --target ./package requests
pip install --target ./package requests_aws4auth
```

Da in allen Lambda-Ausführungsumgebungen Boto3 installiert ist, müssen Sie es nicht in Ihr Bereitstellungspaket einschließen.

4. Paket mit Anwendungscode und Abhängigkeiten:

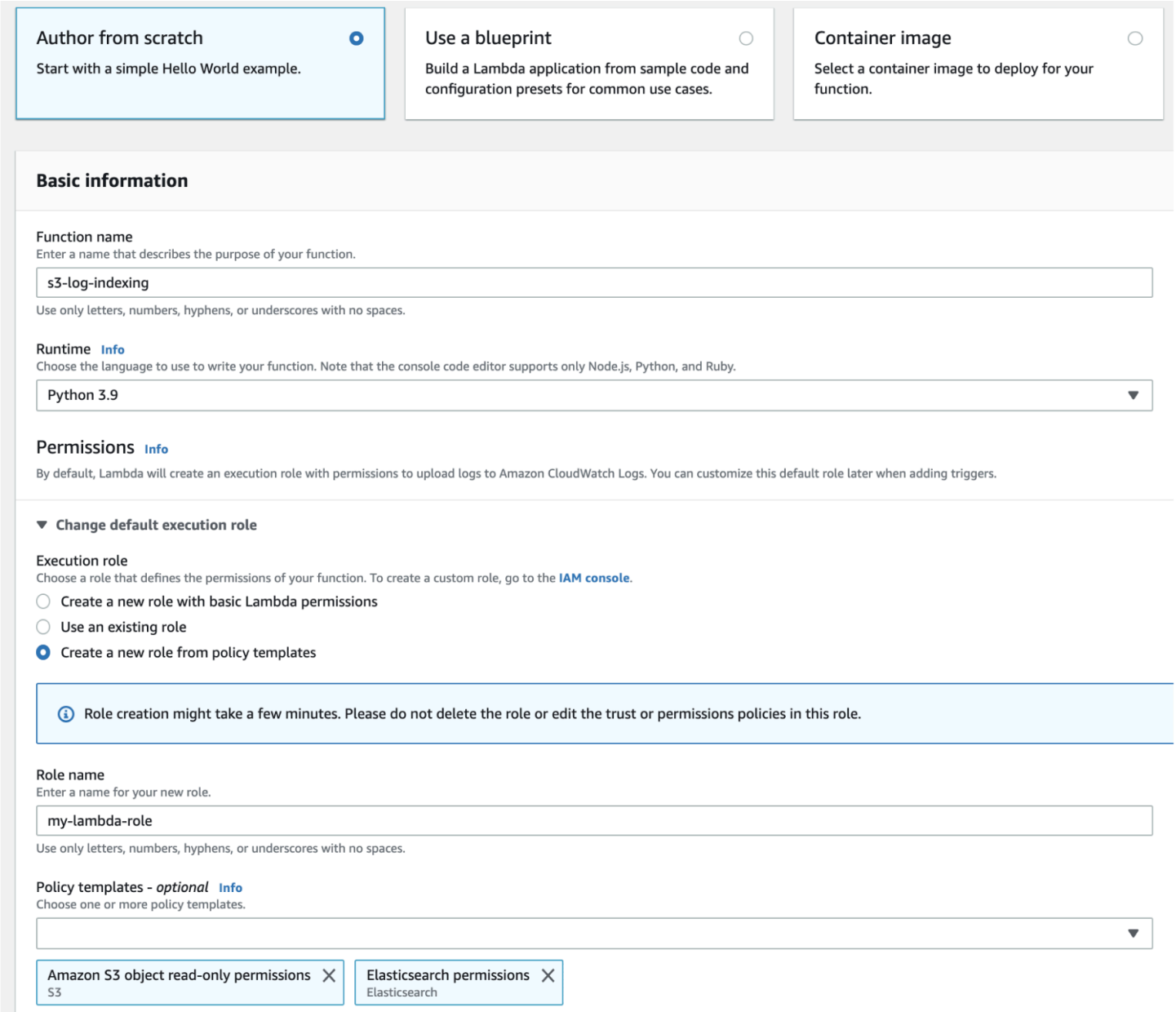
```
cd package
zip -r ../lambda.zip .

cd ..
zip -g lambda.zip sample.py
```

So erstellen Sie die Lambda-Funktion:

Nachdem Sie das Bereitstellungspaket erstellt haben, können Sie die Lambda-Funktion erstellen. Wenn Sie eine Funktion erstellen, wählen Sie einen Namen, eine Laufzeit (z. B. Python 3.8) und eine IAM-Rolle aus. Die IAM-Rolle definiert die Berechtigungen der Funktion. Detaillierte Anweisungen finden Sie unter Erstellen einer einfachen Lambda-Funktion im AWS Lambda -Entwicklerhandbuch.

In diesem Beispiel wird davon ausgegangen, dass Sie die Konsole verwenden. Wählen Sie Python 3.9 und eine Rolle mit S3-Leseberechtigungen und OpenSearch Service-Schreibberechtigungen, wie im folgenden Screenshot gezeigt:



Nachdem Sie die Funktion erstellt haben, müssen Sie einen Auslöser hinzufügen. In diesem Beispiel soll der Code immer dann ausgeführt werden, wenn im S3-Bucket ein Protokoll eintrifft:

1. Klicken Sie auf Auslöser hinzufügen und wählen Sie S3 aus.
2. Wählen Sie Ihren Bucket aus.
3. Wählen Sie unter Event type (Ereignistyp) die Option PUT aus.
4. Geben Sie für Prefix (Präfix) den Wert `logs/` ein.
5. Geben Sie für Suffix `.log` ein.
6. Bestätigen Sie die Warnung für rekursive Aufrufe und wählen Sie Hinzufügen aus.

Schließlich können Sie Ihr Bereitstellungs-Paket hochladen:

1. Wählen Sie Hochladen von und .zip-Datei und befolgen Sie dann die Anweisungen zum Hochladen Ihres Bereitstellungspakets.
2. Nachdem der Upload abgeschlossen ist, bearbeiten Sie die Laufzeit-Einstellungen und ändern Sie den Handler auf `sample.handler`. Diese Einstellung teilt Lambda die Datei (`sample.py`) und Methode (`handler`) mit, die es nach einem Auslöser ausführen soll.

Zu diesem Zeitpunkt verfügen Sie über einen vollständigen Satz von Ressourcen: einen Bucket für Protokolldateien, eine Funktion, die immer dann ausgeführt wird, wenn dem Bucket eine Protokolldatei hinzugefügt wird, Code, der das Parsen und Indizieren durchführt, und eine OpenSearch Service-Domain für die Suche und Visualisierung.

Testen der Lambda-Funktion

Nachdem Sie die Funktion erstellt haben, können Sie sie durch Hochladen einer Datei in den Amazon-S3-Bucket testen. Erstellen Sie anhand der folgenden Beispielprotokollzeilen eine Datei mit dem Namen `sample.log`:

```
12.345.678.90 - [10/Oct/2000:13:55:36 -0700] "PUT /some-file.jpg"
12.345.678.91 - [10/Oct/2000:14:56:14 -0700] "GET /some-file.jpg"
```

Laden Sie die Datei in den Ordner `logs` Ihres S3-Buckets hoch. Anweisungen finden Sie unter Hochladen eines Objekts in Ihren Bucket im Benutzerhandbuch für Amazon Simple Storage Service.

Überprüfen Sie anschließend mithilfe der OpenSearch Servicekonsole oder der OpenSearch Dashboards, ob der `lambda-s3-index` Index zwei Dokumente enthält. Sie können auch eine Standard-Suchabfrage durchführen:

```
GET https://domain-name/lambda-s3-index/_search?pretty
{
  "hits" : {
    "total" : 2,
    "max_score" : 1.0,
    "hits" : [
      {
        "_index" : "lambda-s3-index",
        "_type" : "_doc",
        "_id" : "vTYXaWIBJWV_TTkEuSDg",
```

```
        "_score" : 1.0,
        "_source" : {
          "ip" : "12.345.678.91",
          "message" : "GET /some-file.jpg",
          "timestamp" : "10/Oct/2000:14:56:14 -0700"
        }
      },
      {
        "_index" : "lambda-s3-index",
        "_type" : "_doc",
        "_id" : "vjYmaWIBJWV_TTkEuCAB",
        "_score" : 1.0,
        "_source" : {
          "ip" : "12.345.678.90",
          "message" : "PUT /some-file.jpg",
          "timestamp" : "10/Oct/2000:13:55:36 -0700"
        }
      }
    ]
  }
}
```

So laden Sie Streaming-Daten aus Amazon Kinesis Data Streams

Sie können Streaming-Daten von Kinesis Data Streams in den OpenSearch Service laden. Neue im Daten-Stream eintreffende Daten lösen eine Ereignisbenachrichtigung an Lambda aus, wodurch Ihr benutzerdefinierter Code zum Durchführen der Indizierung ausgeführt wird. Dieser Abschnitt enthält unkomplizierten Python-Beispielcode.

Voraussetzungen

Zum Fortfahren benötigen Sie die folgenden Ressourcen.

Voraussetzung	Beschreibung
Amazon Kinesis Data Stream	Die Ereignisquelle für Ihre Lambda-Funktion. Weitere Informationen finden Sie unter Kinesis Data Streams.
OpenSearch Dienstdomäne	Das Ziel für die Daten, nachdem sie durch Ihre Lambda-Funktion verarbeitet wurden. Weitere Informationen finden Sie unter the section called “ OpenSearch Dienstdomänen erstellen”

Voraussetzung	Beschreibung
IAM Role (IAM-Rolle)	Diese Rolle muss über grundlegende OpenSearch Service-, Kinesis- und Lambda-Berechtigungen verfügen, z. B. die folgenden: JSON **{** **"Version": "2012-10-17",** **"Statement": [** **{** **"Effect": "Allow",** **"Action": [** **"es:ESHttpPost",** **"es:ESHttpPut",** **"logs:CreateLogGroup",** **"logs:CreateLogStream",** **"logs:PutLogEvents",** **"kinesis:GetShardIterator",** **"kinesis:GetRecords",** **"kinesis:DescribeStream",** **"kinesis:ListStreams"** **],** **"Resource": "*"** **}** **]** **}** Die Rolle muss über die folgende Vertrauensstellung verfügen: JSON **{** **"Version": "2012-10-17",** **"Statement": [** **{** **"Effect": "Allow",** **"Principal": {** **"Service": "lambda.amazonaws.com"** **},**

Voraussetzung	Beschreibung
	<pre>"Action": "sts:AssumeRole" }] }</pre> Weitere Informationen finden Sie unter Erstellen von IAM-Rollen im IAM-Benutzerhandbuch.

So erstellen Sie die Lambda-Funktion:

Befolgen Sie die Anweisungen in the section called “Erstellen des Lambda-Bereitstellungspakets”. Erstellen Sie jedoch ein Verzeichnis mit dem Namen `kinesis-to-opensearch` und verwenden Sie den folgenden Code für `sample.py`:

```
import base64
import boto3
import json
import requests
from requests_aws4auth import AWS4Auth

region = '' # e.g. us-west-1
service = 'es'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
 session_token=credentials.token)

host = '' # the OpenSearch Service domain, e.g. https://search-mydomain.us-
west-1.es.amazonaws.com
index = 'lambda-kine-index'
datatype = '_doc'
url = host + '/' + index + '/' + datatype + '/'

headers = { "Content-Type": "application/json" }

def handler(event, context):
    count = 0
    for record in event['Records']:
        id = record['eventID']
        timestamp = record['kinesis']['approximateArrivalTimestamp']
```

```
        # Kinesis data is base64-encoded, so decode here
        message = base64.b64decode(record['kinesis']['data'])

        # Create the JSON document
        document = { "id": id, "timestamp": timestamp, "message": message }
        # Index the document
        r = requests.put(url + id, auth=awsauth, json=document, headers=headers)
        count += 1
    return 'Processed ' + str(count) + ' items.'
```

Bearbeiten Sie die Variablen für `region` und `host`.

Installieren Sie pip, falls noch nicht geschehen, und verwenden Sie dann die folgenden Befehle, um Ihre Abhängigkeiten zu installieren:

```
cd kinesis-to-opensearch

pip install --target ./package requests
pip install --target ./package requests_aws4auth
```

Befolgen Sie dann die Anweisungen in the section called “So erstellen Sie die Lambda-Funktion:”. Geben Sie jedoch die IAM-Rolle aus the section called “Voraussetzungen” und die folgenden Einstellungen für den Auslöser an:

- Kinesis-Stream: Ihr Kinesis-Stream
- Stapelgröße: 100
- Startposition: Horizont trimmen

Weitere Informationen finden Sie unter Was ist Amazon Kinesis Data Streams? im Entwicklerhandbuch für Amazon Kinesis Data Streams.

Zu diesem Zeitpunkt verfügen Sie über einen vollständigen Satz von Ressourcen: einen Kinesis-Datenstream, eine Funktion, die ausgeführt wird, nachdem der Stream neue Daten empfangen und diese Daten indexiert hat, und eine OpenSearch Service-Domäne für die Suche und Visualisierung.

Lambda-Funktion testen

Nachdem Sie die Funktion erstellt haben, können Sie sie testen, indem Sie den Data-Stream mithilfe der AWS CLI aufzeichnen:

```
aws kinesis put-record --stream-name test --data "My test data." --partition-key
 partitionKey1 --region us-west-1
```

Verwenden Sie dann die OpenSearch Servicekonsole oder die OpenSearch Dashboards, um zu überprüfen, ob das Dokument ein `lambda-kine-index` Dokument enthält. Sie können außerdem die folgenden Anforderung verwenden:

```
GET https://domain-name/lambda-kine-index/_search
{
  "hits" : [
    {
      "_index": "lambda-kine-index",
      "_type": "_doc",
      "_id":
 "shardId-000000000000:495835116157626994950129608214214566865294366804960870 42",
      "_score": 1,
      "_source": {
        "timestamp": 1523648740.051,
        "message": "My test data.",
        "id":
 "shardId-000000000000:495835116157626994950129608214214566865294366804960870 42"
      }
    }
  ]
}
```

So laden Sie Streaming-Daten aus Amazon DynamoDB

Sie können AWS Lambda es verwenden, um Daten von Amazon DynamoDB an Ihre OpenSearch Service-Domain zu senden. Neue in der Datenbanktabelle eintreffende Daten lösen eine Ereignisbenachrichtigung an Lambda aus, wodurch Ihr benutzerdefinierte Code zum Durchführen der Indizierung ausgeführt wird.

Voraussetzungen

Zum Fortfahren benötigen Sie die folgenden Ressourcen.

Voraussetzung	Beschreibung
DynamoDB-Tabelle	Die Tabelle enthält Ihre Quelldaten. Weitere Informationen finden Sie unter Grundlegende Operationen in DynamoDB-Tabellen im Amazon-DynamoDB-Entwicklerhandbuch. Die Tabelle muss sich in derselben Region wie Ihre OpenSearch Service-Domain befinden und einen Stream haben, der auf Neues Bild gesetzt ist. Weitere Informationen finden Sie unter Aktivieren eines Streams.
OpenSearch Dienstdomäne	Das Ziel für die Daten, nachdem sie durch Ihre Lambda-Funktion verarbeitet wurden. Weitere Informationen finden Sie unter the section called “ OpenSearch Dienstdomänen erstellen”.

IAM-Rolle	Diese Rolle muss über grundlegende OpenSearch Service-, DynamoDB- und Lambda-Ausführungsberechtigungen verfügen, z. B. die folgenden:
	
	JSON
	
	{
	"Version": "2012-10-17",
	"Statement": [
	{
	"Effect": "Allow",
	"Action": [
	"es:ESHttpPost",
	"es:ESHttpPut",
	"dynamodb:DescribeStream",
	"dynamodb:GetRecords",
	"dynamodb:GetShardIterator",
	"dynamodb:ListStreams",
	"logs:CreateLogGroup",
	"logs:CreateLogStream",
	"logs:PutLogEvents"
	],
	"Resource": "*"
	}
	]

Voraussetzung	Beschreibung

	}
	
	Die Rolle muss über die folgende Vertrauensstellung verfügen:
	
	JSON
	
	{
	"Version": "2012-10-17",
	"Statement": [
	{
	"Effect": "Allow",
	"Principal": {
	"Service": "lambda.amazonaws.com"
	},
	"Action": "sts:AssumeRole"
	}
	]
	}
	
	Weitere Informationen finden Sie unter Erstellen von IAM-Rollen im IAM-Benutzerhandbuch.

So erstellen Sie die Lambda-Funktion:

Befolgen Sie die Anweisungen in the section called “Erstellen des Lambda-Bereitstellungspakets”. Erstellen Sie jedoch ein Verzeichnis mit dem Namen `ddb-to-opensearch` und verwenden Sie den folgenden Code für `sample.py`:

```
import boto3
import requests
from requests_aws4auth import AWS4Auth

region = '' # e.g. us-east-1
service = 'es'
credentials = boto3.Session().get_credentials()
```

```
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
 session_token=credentials.token)

host = '' # the OpenSearch Service domain, e.g. https://search-mydomain.us-
west-1.es.amazonaws.com
index = 'lambda-index'
datatype = '_doc'
url = host + '/' + index + '/' + datatype + '/'

headers = { "Content-Type": "application/json" }

def handler(event, context):
    count = 0
    for record in event['Records']:
        # Get the primary key for use as the OpenSearch ID
        id = record['dynamodb']['Keys']['id']['S']

        if record['eventName'] == 'REMOVE':
            r = requests.delete(url + id, auth=awsauth)
        else:
            document = record['dynamodb']['NewImage']
            r = requests.put(url + id, auth=awsauth, json=document, headers=headers)
        count += 1
    return str(count) + ' records processed.'
```

Bearbeiten Sie die Variablen für `region` und `host`.

Installieren Sie pip, falls noch nicht geschehen, und verwenden Sie dann die folgenden Befehle, um Ihre Abhängigkeiten zu installieren:

```
cd ddb-to-opensearch

pip install --target ./package requests
pip install --target ./package requests_aws4auth
```

Befolgen Sie dann die Anweisungen in the section called “So erstellen Sie die Lambda-Funktion:”. Geben Sie jedoch die IAM-Rolle aus the section called “Voraussetzungen” und die folgenden Einstellungen für den Auslöser an:

- Tabelle: Ihre DynamoDB-Tabelle
- Stapelgröße: 100
- Startposition: Horizont trimmen

Weitere Informationen finden Sie unter Verarbeiten neuer Elemente mit DynamoDB-Streams und Lambda im Amazon-DynamoDB-Entwicklerhandbuch.

Zu diesem Zeitpunkt verfügen Sie über einen vollständigen Satz von Ressourcen: eine DynamoDB-Tabelle für Ihre Quelldaten, einen DynamoDB-Stream mit Änderungen an der Tabelle, eine Funktion, die nach Änderungen Ihrer Quelldaten ausgeführt wird und diese Änderungen indexiert, und eine OpenSearch Service-Domäne für die Suche und Visualisierung.

Lambda-Funktion testen

Nachdem Sie die Funktion erstellt haben, können Sie sie testen, indem Sie ein neues Element zur DynamoDB-Tabelle mithilfe der AWS CLI hinzufügen:

```
aws dynamodb put-item --table-name test --item '{"director": {"S": "Kevin
 Costner"},"id": {"S": "00001"},"title": {"S": "The Postman"}}' --region us-west-1
```

Überprüfen Sie dann mithilfe der OpenSearch Servicekonsole oder der OpenSearch Dashboards, ob das Dokument ein Dokument enthält. `lambda-index` Sie können außerdem die folgenden Anforderung verwenden:

```
GET https://domain-name/lambda-index/_doc/00001
{
    "_index": "lambda-index",
    "_type": "_doc",
    "_id": "00001",
    "_version": 1,
    "found": true,
    "_source": {
        "director": {
            "S": "Kevin Costner"
        },
        "id": {
            "S": "00001"
        },
        "title": {
            "S": "The Postman"
        }
    }
}
```

Streaming-Daten von Amazon Data Firehose laden

Firehose unterstützt OpenSearch Service als Lieferziel. Anweisungen zum Laden von Streaming-Daten in OpenSearch Service finden Sie unter Creating a Kinesis Data Firehose Delivery Stream and Choose OpenSearch Service for Your Destination im Amazon Data Firehose Developer Guide.

Bevor Sie Daten in OpenSearch Service laden, müssen Sie möglicherweise Transformationen an den Daten durchführen. Weitere Informationen über die Verwendung von Lambda-Funktionen zur Ausführung dieser Aufgabe finden Sie unter Amazon Kinesis Data Firehose Datentransformation im selben Handbuch.

Wenn Sie einen Lieferstream konfigurieren, verfügt Firehose über eine IAM-Rolle mit nur einem Klick, die dem Unternehmen den Ressourcenzugriff gewährt, den es benötigt, um Daten an OpenSearch Service zu senden, Daten auf Amazon S3 zu sichern und Daten mit Lambda zu transformieren. Aufgrund der Komplexität bei der manuellen Erstellung einer solchen Rolle empfehlen wir die Verwendung der bereitgestellten Rolle.

Streaming-Daten von Amazon laden CloudWatch

Sie können Streaming-Daten von CloudWatch Logs in Ihre OpenSearch Service-Domain laden, indem Sie ein CloudWatch Logs-Abonnement verwenden. Informationen zu CloudWatch Amazon-Abonnements finden Sie unter Echtzeitverarbeitung von Protokolldaten mit Abonnements. Informationen zur Konfiguration finden Sie unter Streaming CloudWatch Logs data to Amazon OpenSearch Service im Amazon CloudWatch Developer Guide.

Streaming-Daten werden geladen von AWS IoT

Sie können Daten AWS IoT mithilfe von Regeln senden. Weitere Informationen finden Sie in der entsprechenden OpenSearchAktion im AWS IoT Entwicklerhandbuch.

Daten mit Logstash in Amazon OpenSearch Service laden

Die Open-Source-Version von Logstash (Logstash OSS) bietet eine bequeme Möglichkeit, die Bulk-API zum Hochladen von Daten in Ihre Amazon Service-Domain zu verwenden. OpenSearch Der Service unterstützt alle Standard-Logstash-Eingabe-Plugins, einschließlich des Amazon S3 S3-Eingabe-Plugins. OpenSearch Der Service unterstützt das logstash-output-opensearchAusgabe-Plugin, das sowohl die Standardauthentifizierung als auch IAM-Anmeldeinformationen unterstützt. Das Plugin arbeitet mit Version 8.1 und niedriger von Logstash OSS.

Konfiguration

Die Logstash-Konfiguration variiert je nach Art der Authentifizierung, die Ihre Domäne verwendet.

Unabhängig davon, welche Authentifizierungsmethode Sie verwenden, müssen Sie im Abschnitt output der Konfigurationsdatei `ecs_compatibility` auf `disabled` festlegen. Logstash 8.0 führte eine bahnbrechende Änderung ein, bei der alle Plugins standardmäßig im ECS-Kompatibilitätsmodus ausgeführt werden. Sie müssen den Standard überschreiben, um das Legacy-Verhalten beizubehalten.

Differenzierte Zugriffskontrolle

Wenn Ihre OpenSearch Service-Domain eine differenzierte Zugriffskontrolle mit HTTP-Basisauthentifizierung verwendet, ähnelt die Konfiguration jedem anderen Cluster. OpenSearch Diese Beispielkonfigurationsdatei übernimmt ihre Eingabe aus der Open-Source-Version von Filebeat (Filebeat OSS):

```
input {
  beats  {
    port => 5044
  }
}

output {
  opensearch {
    hosts       => "https://domain-endpoint:443"
    user        => "my-username"
    password    => "my-password"
    index       => "logstash-logs-%{+YYYY.MM.dd}"
    ecs_compatibility => disabled
    ssl_certificate_verification => false
  }
}
```

Die Konfiguration variiert je nach Beats-Anwendung und Anwendungsfall, aber Ihre Filebeat-OSS-Konfiguration könnte folgendermaßen aussehen:

```
filebeat.inputs:
- type: log
  enabled: true
  paths:
```

```
    - /path/to/logs/dir/*.log
filebeat.config.modules:
  path: ${path.config}/modules.d/*.yml
  reload.enabled: false
setup.ilm.enabled: false
setup.ilm.check_exists: false
setup.template.settings:
  index.number_of_shards: 1
output.logstash:
  hosts: ["logstash-host:5044"]
```

IAM-Konfiguration

Wenn Ihre Domain eine IAM-basierte Domänenzugriffsrichtlinie oder eine detaillierte Zugriffskontrolle mit einem Masterbenutzer verwendet, müssen Sie alle Anfragen an Service mit IAM-Anmeldeinformationen signieren. OpenSearch Die folgende identitätsbasierte Richtlinie gewährt allen HTTP-Anfragen an die Unterressourcen Ihrer Domain.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "es:ESHttp*"
      ],
      "Resource": "arn:aws:es:region:aws-account-id:domain/domain-name/*"
    }
  ]
}
```

Um Ihre Logstash-Konfiguration einzurichten, ändern Sie Ihre Konfigurationsdatei so, dass das Plugin für die Ausgabe verwendet wird. Diese Beispielkonfigurationsdatei übernimmt ihre Eingabe von Dateien in einem S3-Bucket:

```
input {
  s3 {
    bucket => "amzn-s3-demo-"
```

```
    region => "us-east-1"
  }
}

output {
  opensearch {
    hosts => ["domain-endpoint:443"]
    auth_type => {
      type => 'aws_iam'
      aws_access_key_id => 'your-access-key'
      aws_secret_access_key => 'your-secret-key'
      region => 'us-east-1'
      }
      index  => "logstash-logs-%{+YYYY.MM.dd}"
      ecs_compatibility => disabled
  }
}
```

Wenn Sie Ihre IAM-Anmeldeinformationen nicht in der Konfigurationsdatei angeben möchten, können Sie sie exportieren (oder `aws configure` ausführen):

```
export AWS_ACCESS_KEY_ID="your-access-key"
export AWS_SECRET_ACCESS_KEY="your-secret-key"
export AWS_SESSION_TOKEN="your-session-token"
```

Wenn sich Ihre OpenSearch Service-Domain in einer VPC befindet, muss die Logstash OSS-Maschine in der Lage sein, eine Verbindung zur VPC herzustellen und über die VPC-Sicherheitsgruppen Zugriff auf die Domain zu haben. Weitere Informationen finden Sie unter the section called “Zugriffsrichtlinien für VPC-Domänen”.

Suchen nach Daten in Amazon OpenSearch Service

Es gibt mehrere gängige Methoden für die Suche nach Dokumenten in Amazon OpenSearch Service, darunter URI-Suchen und Suchen nach Anforderungstexten. OpenSearch Der Service bietet zusätzliche Funktionen, die das Sucherlebnis verbessern, wie z. B. benutzerdefinierte Pakete, SQL-Unterstützung und asynchrone Suche. Eine umfassende OpenSearch Such-API-Referenz finden Sie in der OpenSearchDokumentation.

> **Note**
>
> Die folgenden Beispielanfragen funktionieren mit OpenSearch APIs. Einige Anfragen funktionieren möglicherweise nicht mit älteren Elasticsearch-Versionen.

Themen

- URI-Suchanfragen
- Anforderungstextsuchen
- Paginieren der Suchergebnisse
- Abfragesprache für Dashboards
- Pakete in Amazon OpenSearch Service importieren und verwalten
- Abfragen Ihrer Amazon OpenSearch Service-Daten mit SQL
- k-NN-Suche (k-Nearest Neighbor) in Amazon Service OpenSearch
- Clusterübergreifende Suche in Amazon Service OpenSearch
- Learning to Rank für Amazon OpenSearch Service
- Asynchrone Suche in Amazon Service OpenSearch
- Point-in-Time-Suche in Amazon OpenSearch Service
- Semantische Suche in Amazon Service OpenSearch
- Gleichzeitige Segmentsuche in Amazon Service OpenSearch
- Generierung von Abfragen in natürlicher Sprache in Amazon OpenSearch Service

URI-Suchanfragen

Universal Resource Identifier (URI)-Suchanfragen sind die einfachste Form der Suche. Sie geben in einer URI-Suchanfrage die Abfrage als einen HTTP-Anfrageparameter an:

```
GET https://search-my-domain.us-west-1.es.amazonaws.com/_search?q=house
```

Eine Beispielantwort kann wie folgt aussehen:

```
{
  "took": 25,
  "timed_out": false,
  "_shards": {
    "total": 10,
    "successful": 10,
    "skipped": 0,
    "failed": 0
  },
  "hits": {
    "total": {
      "value": 85,
      "relation": "eq",
    },
    "max_score": 6.6137657,
    "hits": [
      {
        "_index": "movies",
        "_type": "movie",
        "_id": "tt0077975",
        "_score": 6.6137657,
        "_source": {
          "directors": [
            "John Landis"
          ],
          "release_date": "1978-07-27T00:00:00Z",
          "rating": 7.5,
          "genres": [
            "Comedy",
            "Romance"
          ],
          "image_url": "http://ia.media-imdb.com/images/M/
MV5BMTY2OTQxNTc1OF5BMl5BanBnXkFtZTYwNjA3NjI5._V1_SX400_.jpg",
```

```
          "plot": "At a 1962 College, Dean Vernon Wormer is determined to expel the
 entire Delta Tau Chi Fraternity, but those troublemakers have other plans for him.",
          "title": "Animal House",
          "rank": 527,
          "running_time_secs": 6540,
          "actors": [
            "John Belushi",
            "Karen Allen",
            "Tom Hulce"
          ],
          "year": 1978,
          "id": "tt0077975"
        }
      },
      ...
    ]
  }
}
```

Standardmäßig durchsucht diese Abfrage alle Felder aller Indizes nach dem Begriff house. Wenn Sie die Suche einschränken möchten, geben Sie einen Index- (`movies`) und ein Dokumentfeld (`title`) in der URI an:

```
GET https://search-my-domain.us-west-1.es.amazonaws.com/movies/_search?q=title:house
```

Sie können zusätzliche Parameter in die Anfrage aufnehmen, aber die unterstützten Parameter stellen nur einen kleinen Teil der OpenSearch Suchoptionen dar. Die folgende Anfrage gibt 20 Ergebnisse (statt standardmäßig 10) zurück und sortiert nach Jahr (statt nach `_score`):

```
GET https://search-my-domain.us-west-1.es.amazonaws.com/movies/_search?
q=title:house&size=20&sort=year:desc
```

Anforderungstextsuchen

Um komplexere Suchvorgänge auszuführen, verwenden Sie den HTTP-Anforderungstext und die domänenspezifische Sprache (DSL) von OpenSearch für Abfragen. Mit der Abfrage-DSL können Sie die vollständige Palette der OpenSearch -Suchoptionen angeben.

> **Note**
>
> Sie können keine Unicode-Sonderzeichen in einen Textfeldwert aufnehmen, andernfalls wird der Wert als mehrere durch das Sonderzeichen getrennte Werte analysiert. Diese fehlerhafte Analyse kann zu einer unbeabsichtigten Filterung von Dokumenten führen und möglicherweise die Kontrolle über deren Zugriff beeinträchtigen. Weitere Informationen finden Sie in der OpenSearch Dokumentation unter Ein Hinweis zu Unicode-Sonderzeichen in Textfeldern.

Die folgende `match`-Abfrage ist ähnlich wie das endgültige URI-Suchanfragen-Beispiel:

```
POST https://search-my-domain.us-west-1.es.amazonaws.com/movies/_search
{
  "size": 20,
  "sort": {
    "year": {
      "order": "desc"
    }
  },
  "query": {
    "query_string": {
      "default_field": "title",
      "query": "house"
    }
  }
}
```

> **Note**
>
> Die `_search`-API akzeptiert HTTP `GET` und `POST` für Anforderungstextsuchen, jedoch nicht alle HTTP-Clients unterstützen das Hinzufügen eines Anforderungstexts zu einer `GET`-Anforderung. `POST` ist die universellere Wahl.

In vielen Fällen möchten Sie möglicherweise mehrere Felder durchsuchen, jedoch nicht alle Felder. Verwenden Sie die `multi_match`-Abfrage:

```
POST https://search-my-domain.us-west-1.es.amazonaws.com/movies/_search
{
```

```
  "size": 20,
  "query": {
    "multi_match": {
      "query": "house",
      "fields": ["title", "plot", "actors", "directors"]
    }
  }
}
```

Boosten der Felder

Sie können die Suchrelevanz verbessern, indem Sie bestimmte Felder "boosten". Boosts sind Multiplikatoren, die Übereinstimmungen in einem Feld stärker gewichten als die in anderen Feldern. Im folgenden Beispiel beeinflusst eine Übereinstimmung für john im `title`-Feld `_score` doppelt so viel wie eine Übereinstimmung im `plot`-Feld und vier Mal so viel wie eine Übereinstimmung im `actors`- oder `directors`-Feld. Das Ergebnis ist, dass Filme wie John Wick und John Carter oben in den Suchergebnissen und Filme mit John Travolta unten angegeben werden.

```
POST https://search-my-domain.us-west-1.es.amazonaws.com/movies/_search
{
  "size": 20,
  "query": {
    "multi_match": {
      "query": "john",
      "fields": ["title^4", "plot^2", "actors", "directors"]
    }
  }
}
```

Hervorheben der Suchergebnisse

Die `highlight` Option weist OpenSearch an, dass ein zusätzliches Objekt innerhalb des `hits` Arrays zurückgegeben werden soll, wenn die Abfrage mit einem oder mehreren Feldern übereinstimmt:

```
POST https://search-my-domain.us-west-1.es.amazonaws.com/movies/_search
{
  "size": 20,
  "query": {
    "multi_match": {
      "query": "house",
```

```
      "fields": ["title^4", "plot^2", "actors", "directors"]
    }
  },
  "highlight": {
    "fields": {
      "plot": {}
    }
  }
}
```

Wenn die Abfrage mit dem Inhalt des `plot`-Feldes übereinstimmt, könnte ein Treffer folgendermaßen aussehen:

```
{
  "_index": "movies",
  "_type": "movie",
  "_id": "tt0091541",
  "_score": 11.276199,
  "_source": {
    "directors": [
      "Richard Benjamin"
    ],
    "release_date": "1986-03-26T00:00:00Z",
    "rating": 6,
    "genres": [
      "Comedy",
      "Music"
    ],
    "image_url": "http://ia.media-imdb.com/images/M/
MV5BMTIzODEzODE2OF5BMl5BanBnXkFtZTcwNjQ3ODcyMQ@@._V1_SX400_.jpg",
    "plot": "A young couple struggles to repair a hopelessly dilapidated house.",
    "title": "The Money Pit",
    "rank": 4095,
    "running_time_secs": 5460,
    "actors": [
      "Tom Hanks",
      "Shelley Long",
      "Alexander Godunov"
    ],
    "year": 1986,
    "id": "tt0091541"
  },
  "highlight": {
```

```
    "plot": [
      "A young couple struggles to repair a hopelessly dilapidated <em>house</em>."
    ]
  }
}
```

Standardmäßig OpenSearch umschließt die übereinstimmende Zeichenfolge in Tags, stellt bis zu 100 Zeichen Kontext für den Treffer bereit und teilt den Inhalt in Sätze auf, indem Satzzeichen, Leerzeichen, Tabulatoren und Zeilenumbrüche identifiziert werden. Alle diese Einstellungen sind konfigurierbar:

```
POST https://search-my-domain.us-west-1.es.amazonaws.com/movies/_search
{
  "size": 20,
  "query": {
    "multi_match": {
      "query": "house",
      "fields": ["title^4", "plot^2", "actors", "directors"]
    }
  },
  "highlight": {
    "fields": {
      "plot": {}
    },
    "pre_tags": "<strong>",
    "post_tags": "</strong>",
    "fragment_size": 200,
    "boundary_chars": ".,!? "
  }
}
```

Count-API

Wenn Sie nicht am Inhalt Ihrer Dokumente interessiert sind und einfach nur die Anzahl der Übereinstimmungen wissen möchten, können Sie die `_count`-API anstelle der `_search`-API verwenden. Die folgende Anfrage verwendet die `query_string`-Abfrage zum Identifizieren romantischer Komödien:

```
POST https://search-my-domain.us-west-1.es.amazonaws.com/movies/_count
{
  "query": {
```

```
    "query_string": {
      "default_field": "genres",
      "query": "romance AND comedy"
    }
  }
}
```

Eine Beispielantwort kann wie folgt aussehen:

```
{
  "count": 564,
  "_shards": {
    "total": 5,
    "successful": 5,
    "skipped": 0,
    "failed": 0
  }
}
```

Paginieren der Suchergebnisse

Wenn Sie eine große Anzahl von Suchergebnissen anzeigen müssen, können Sie die Paginierung mit verschiedenen Methoden implementieren.

Zeitpunkt

Die Point-in-Time-Funktion (PIT) ist eine Art von Suche, mit der Sie verschiedene Abfragen für einen Datensatz ausführen können, der zeitlich festgelegt ist. Dies ist die bevorzugte Paginierungsmethode OpenSearch, insbesondere für tiefe Paginierung. Sie können PIT mit OpenSearch Service Version 2.5 und höher verwenden. Weitere Informationen zu PIT finden Sie unter???.

Die `size` Parameter `from` und

Die einfachste Methode zum Paginieren ist die Verwendung der `size` Parameter `from` und. Die folgende Anfrage gibt Ergebnisse 20-39 der null-indizierten Liste von Suchergebnissen zurück:

```
POST https://search-my-domain.us-west-1.es.amazonaws.com/movies/_search
{
  "from": 20,
  "size": 20,
```

```
  "query": {
    "multi_match": {
      "query": "house",
      "fields": ["title^4", "plot^2", "actors", "directors"]
    }
  }
}
```

Weitere Informationen zur Suchpaginierung finden Sie in der Dokumentation unter Ergebnisse paginieren. OpenSearch

Abfragesprache für Dashboards

Sie können die Dashboards Query Language (DQL) verwenden, um in Dashboards nach Daten und Visualisierungen zu suchen. OpenSearch DQL verwendet vier primäre Abfragetypen: Begriffe, boolesch, Datum und Bereich und verschachteltes Feld.

Begriffsabfrage

Bei einer Begriffsabfrage müssen Sie den Begriff angeben, nach dem Sie suchen.

Geben Sie zum Durchführen einer Begriffsabfrage Folgendes ein:

```
host:www.example.com
```

Boolesche Abfrage

Sie können die booleschen Operatoren `AND`, `or` und `not` verwenden, um mehrere Abfragen zu kombinieren.

Fügen Sie zum Durchführen einer booleschen Abfrage Folgendes ein:

```
host.keyword:www.example.com and response.keyword:200
```

Datums- und Bereichsabfragen

Sie können eine Datums- und Bereichsabfrage verwenden, um ein Datum vor oder nach Ihrer Abfrage zu finden.

- > zeigt eine Suche nach einem Datum nach dem angegebenen Datum an.
- < zeigt eine Suche nach einem Datum vor dem angegebenen Datum an.

```
@timestamp > "2020-12-14T09:35:33"
```

Verschachtelte Feldabfrage

Wenn Sie ein Dokument mit verschachtelten Feldern haben, müssen Sie angeben, welche Teile des Dokuments Sie abrufen möchten. Im Folgenden finden Sie ein Beispieldokument, das verschachtelte Felder enthält:

```
{"NBA players":[
    {"player-name": "Lebron James",
      "player-position": "Power forward",
      "points-per-game": "30.3"
    },
    {"player-name": "Kevin Durant",
      "player-position": "Power forward",
      "points-per-game": "27.1"
    },
    {"player-name": "Anthony Davis",
      "player-position": "Power forward",
      "points-per-game": "23.2"
    },
    {"player-name": "Giannis Antetokounmpo",
      "player-position": "Power forward",
      "points-per-game":"29.9"
    }
  ]
}
```

Fügen Sie Folgendes ein, um ein bestimmtes Feld mit DQL abzurufen:

```
NBA players: {player-name: Lebron James}
```

Fügen Sie Folgendes ein, um mehrere Objekte aus dem verschachtelten Dokument abzurufen:

```
NBA players: {player-name: Lebron James} and NBA players: {player-name: Giannis
 Antetokounmpo}
```

Fügen Sie Folgendes ein, um innerhalb eines Bereichs zu suchen:

```
NBA players: {player-name: Lebron James} and NBA players: {player-name: Giannis
 Antetokounmpo and < 30}
```

Wenn Ihr Dokument ein Objekt enthält, das in einem anderen Objekt verschachtelt ist, können Sie dennoch Daten abrufen, indem Sie alle Ebenen angeben. Fügen Sie dazu Folgendes ein:

```
Top-Power-forwards.NBA players: {player-name:Lebron James}
```

Pakete in Amazon OpenSearch Service importieren und verwalten

Mit Amazon OpenSearch Service können Sie benutzerdefinierte Wörterbuchdateien (z. B. Stoppwörter und Synonyme) hochladen und Plugins mit Ihrer Domäne verknüpfen. Diese Plugins können vorkonfiguriert, benutzerdefiniert oder von Drittanbietern sein, sodass Sie die Funktionalität Ihrer Domain flexibel erweitern können. Der Oberbegriff für all diese Arten von Dateien ist Pakete.

- Wörterbuchdateien helfen dabei, Suchergebnisse OpenSearch zu verfeinern, indem sie anweisen, sehr häufige Wörter zu ignorieren oder ähnliche Begriffe wie „gefrorene Creme“, „Gelato“ und „Eis“ als gleichwertig zu behandeln. Sie können außerdem die Stammverknüpfung verbessern, wie das japanische (kuromoji) Analyse-Plugin zeigt.
- Vorgefertigte Plug-ins bieten integrierte Funktionen, wie z. B. das Amazon Personalize Personalize-Plug-in für personalisierte Suchergebnisse. Diese Plugins verwenden den `ZIP-PLUGIN` Pakettyp. Weitere Informationen finden Sie unter the section called “Plug-ins nach Engine-Version”.
- Mit benutzerdefinierten Plugins und Plugins von Drittanbietern können Sie maßgeschneiderte Funktionen hinzufügen oder in externe Systeme integrieren, was Ihrer Domain noch mehr Flexibilität bietet. Wie bei vorkonfigurierten Plugins laden Sie benutzerdefinierte Plugins als `ZIP-PLUGIN` Pakete hoch. Bei Plug-ins von Drittanbietern müssen Sie auch die Plugin-Lizenz und die Konfigurationsdateien als separate Pakete importieren und sie dann alle der Domain zuordnen.

  Weitere Informationen finden Sie unter den folgenden Themen:

  - the section called “Benutzerdefinierte Plugins”
  - the section called “Plugins von Drittanbietern”

> **Note**
>
> Sie können einer einzelnen Domain maximal 20 Plugins zuordnen. Dieses Limit umfasst alle Plugin-Typen — optionale Plug-ins, Drittanbieter-Plugins und benutzerdefinierte Plug-ins.

Themen

- Erforderliche Berechtigungen
- Hochladen von Paketen nach Amazon S3
- Importieren und Zuordnen von Paketen
- Pakete verwenden mit OpenSearch
- Aktualisieren von Paketen
- Manuelles Aktualisieren von Indizes mit einem neuen Wörterbuch
- Trennen und Entfernen von Paketen
- Verwaltung benutzerdefinierter Plugins in Amazon OpenSearch Service
- Installation von Drittanbieter-Plugins in Amazon OpenSearch Service

Erforderliche Berechtigungen

Benutzer ohne Administratorzugriff benötigen bestimmte - AWS Identity and Access Management (IAM) -Aktionen, um Pakete zu verwalten:

- `es:CreatePackage`— Erstellen Sie ein Paket
- `es:DeletePackage`— Löscht ein Paket
- `es:AssociatePackage`— Zuordnen eines Pakets zu einer Domäne
- `es:DissociatePackage`— Trennen eines Pakets von einer Domäne

Sie benötigen auch Berechtigungen für den Amazon-S3-Bucket-Pfad oder das Objekt, in dem sich das benutzerdefinierte Paket befindet.

Erteilen Sie alle Berechtigungen innerhalb von IAM, nicht in der Domänenzugriffsrichtlinie. Weitere Informationen finden Sie unter the section called “Identitäts- und Zugriffsverwaltung”.

Hochladen von Paketen nach Amazon S3

In diesem Abschnitt wird beschrieben, wie benutzerdefinierte Wörterbuchpakete hochgeladen werden, da vorkonfigurierte Plugin-Pakete bereits installiert sind. Bevor Sie ein benutzerdefiniertes Wörterbuch mit Ihrer Domäne verknüpfen können, müssen Sie es in einen Amazon-S3-Bucket hochladen. Weitere Anleitungen finden Sie unter Upload eines Objekts im Benutzerhandbuch für Amazon Simple Storage Service. Unterstützte Plugins müssen nicht hochgeladen werden.

Wenn Ihr Wörterbuch vertrauliche Informationen enthält, geben Sie beim Hochladen die serverseitige Verschlüsselung mit S3-verwalteten Schlüsseln an. OpenSearch Der Dienst kann nicht auf Dateien in S3 zugreifen, die Sie mit einem AWS KMS -Schlüssel schützen.

Nachdem Sie die Datei hochgeladen haben, notieren Sie deren S3-Pfad. Das Pfadformat lautet `s3://amzn-s3-demo-bucket/file-path/file-name`.

Sie können die folgende Synonymdatei für Testzwecke verwenden. Speichern Sie diese unter `synonyms.txt`.

```
danish, croissant, pastry
ice cream, gelato, frozen custard
sneaker, tennis shoe, running shoe
basketball shoe, hightop
```

Bestimmte Wörterbücher, wie Hunspell-Wörterbücher, verwenden mehrere Dateien und benötigen eigene Verzeichnisse im Dateisystem. Zu diesem Zeitpunkt unterstützt OpenSearch Service nur Einzeldatei-Wörterbücher.

Importieren und Zuordnen von Paketen

Die Konsole ist die einfachste Möglichkeit, ein benutzerdefiniertes Wörterbuch in OpenSearch Service zu importieren. Wenn Sie ein Wörterbuch aus Amazon S3 importieren, speichert OpenSearch Service eine eigene Kopie des Pakets und verschlüsselt diese Kopie automatisch unter Verwendung von AES-256 mit OpenSearch vom Service verwalteten Schlüsseln.

Optionale Plug-ins sind in OpenSearch Service bereits vorinstalliert, sodass Sie sie nicht selbst hochladen müssen. Sie müssen jedoch ein Plug-in mit einer Domain verknüpfen. Verfügbare Plug-ins sind auf dem Bildschirm Pakete in der Konsole aufgeführt.

Importieren eines Pakets und Zuordnen eines Pakets zu einer Domäne

1. Wählen Sie in der Amazon OpenSearch Service-Konsole Pakete aus.
2. Klicken Sie auf Packet importieren.
3. Geben Sie dem Paket einen beschreibenden Namen.
4. Geben Sie den S3-Pfad zu der Datei an und wählen Sie dann Import (Importieren) aus.
5. Kehren Sie zum Bildschirm Packages (Pakete) zurück.
6. Wenn der Paketstatus Available (Verfügbar) lautet, wählen Sie das Paket aus.
7. Wählen Sie Einer Domain zuordnen aus.

8. Wählen Sie eine Domain aus und klicken Sie dann auf Weiter. Sehen Sie sich die Pakete an und wählen Sie Associate aus.
9. Wählen Sie im Navigationsbereich Ihre Domäne und dann die Registerkarte Pakete aus.
10. Wenn es sich bei dem Paket um ein benutzerdefiniertes Wörterbuch handelt, notieren Sie sich die ID, wenn das Paket verfügbar wird. Verwenden Sie `analyzers/id` als Dateipfad für Anfragen an OpenSearch.

Pakete verwenden mit OpenSearch

In diesem Abschnitt wird beschrieben, wie Sie beide Arten von Paketen verwenden können: benutzerdefinierte Wörterbücher und vorgefertigte Plugins.

Verwenden von benutzerdefinierten Wörterbüchern

Nachdem Sie eine Datei einer Domäne zugeordnet haben, können Sie sie in Parametern wie`synonyms_path`, und verwenden`stopwords_path`, `user_dictionary` wenn Sie Tokenizer und Tokenfilter erstellen. Der genaue Parameter ist je nach Objekt unterschiedlich. Mehrere Objekte unterstützen `synonyms_path` und `stopwords_path`, `user_dictionary` gilt jedoch exklusiv für das kuromoji-Plugin.

Für das IK-Analysis-Plug-In (Chinesisch) können Sie eine benutzerdefinierte Wörterbuchdatei als benutzerdefiniertes Paket hochladen und sie einer Domäne zuordnen, und das Plug-In nimmt sie automatisch auf, ohne dass ein `user_dictionary`-Parameter erforderlich ist. Wenn es sich bei Ihrer Datei um eine Synonymdatei handelt, verwenden Sie den `synonyms_path`-Parameter.

Mit dem folgenden Beispiel wird eine Synonymdatei zu einem neuen Index hinzugefügt:

```
PUT my-index
{
  "settings": {
    "index": {
      "analysis": {
        "analyzer": {
          "my_analyzer": {
            "type": "custom",
            "tokenizer": "standard",
            "filter": ["my_filter"]
          }
        },
```

```
        "filter": {
          "my_filter": {
            "type": "synonym",
            "synonyms_path": "analyzers/F111111111",
            "updateable": true
          }
        }
      }
    }
  },
  "mappings": {
    "properties": {
      "description": {
        "type": "text",
        "analyzer": "standard",
        "search_analyzer": "my_analyzer"
      }
    }
  }
}
```

Diese Anforderung erstellt einen benutzerdefinierten Analysator für den Index, der den Standard-Tokenizer und einen Synonym-Tokenfilter verwendet.

- Tokenizer teilen Zeichendatenströme auf der Grundlage einer Reihe von Regeln in Token (im Allgemeinen Wörter) auf. Das einfachste Beispiel ist der Whitespace-Tokenizer, der die vorhergehenden Zeichen jedes Mal in ein Token unterteilt, wenn er auf ein Leerzeichen trifft. Ein komplexeres Beispiel ist der Standard-Tokenizer, der unter Verwendung einer Reihe von grammatikalischen Regeln in vielen Sprachen arbeitet.
- Tokenfilter fügen Token hinzu, ändern oder löschen Token. Ein Synonym-Tokenfilter beispielsweise fügt Token hinzu, wenn er ein Wort in der Synonymliste findet. Der Stopp-Tokenfilter entfernt Token, wenn er ein Wort in der Liste der Stoppwörter findet.

Diese Anforderung fügt auch ein Textfeld (`description`) zu der Zuweisung hinzu und weist OpenSearch an, den neuen Analysator als Such-Analysator zu verwenden. Sie können sehen, dass es immer noch den Standard-Analysator als Indexanalysator verwendet.

Notieren Sie sich schließlich die Zeile `"updateable": true` im Token-Filter. Dieses Feld gilt nur für Suchanalysatoren, nicht für Indexanalysatoren und ist wichtig, wenn Sie den Suchanalysator später automatisch aktualisieren möchten.

Fügen Sie dem Index zu Testzwecken einige Dokumente hinzu:

```
POST _bulk
{ "index": { "_index": "my-index", "_id": "1" } }
{ "description": "ice cream" }
{ "index": { "_index": "my-index", "_id": "2" } }
{ "description": "croissant" }
{ "index": { "_index": "my-index", "_id": "3" } }
{ "description": "tennis shoe" }
{ "index": { "_index": "my-index", "_id": "4" } }
{ "description": "hightop" }
```

Suchen Sie diese anschließend unter Verwendung eines Synonyms:

```
GET my-index/_search
{
  "query": {
    "match": {
      "description": "gelato"
    }
  }
}
```

In diesem Fall OpenSearch gibt die folgende -Antwort zurück:

```
{
  "hits": {
    "total": {
      "value": 1,
      "relation": "eq"
    },
    "max_score": 0.99463606,
    "hits": [{
      "_index": "my-index",
      "_type": "_doc",
      "_id": "1",
      "_score": 0.99463606,
      "_source": {
        "description": "ice cream"
      }
    }]
  }
```

```
}
```

> **Tip**
>
> Wörterbuchdateien verwenden Java-Heap-Speicherplatz proportional zu ihrer Größe. Beispielsweise kann eine 2-GiB-Wörterbuchdatei 2 GiB Heap-Speicherplatz auf einem Knoten verbrauchen. Wenn Sie große Dateien verwenden, stellen Sie sicher, dass die Knoten über genügend Heap-Speicher verfügen, um sie aufzunehmen. Überwachen Sie die `JVMMemoryPressure`-Metrik und skalieren Sie Ihren Cluster nach Bedarf.

Verwendung von vorkonfigurierten Plugins

OpenSearch Mit diesem Service können Sie vorinstallierte, optionale OpenSearch Plugins zur Verwendung mit Ihrer Domain verknüpfen. Ein vorkonfiguriertes Plugin-Paket ist mit einer bestimmten OpenSearch Version kompatibel und kann nur Domains mit dieser Version zugeordnet werden. Die Liste der verfügbaren Pakete für Ihre Domain enthält alle unterstützten Plugins, die mit Ihrer Domain-Version kompatibel sind. Nachdem Sie ein Plugin mit einer Domain verknüpft haben, beginnt ein Installationsvorgang auf der Domain. Anschließend können Sie auf das Plugin verweisen und es verwenden, wenn Sie Anfragen an den OpenSearch Service stellen.

Das Zuordnen und Trennen eines Plugins erfordert eine Blau/Grün-Bereitstellung. Weitere Informationen finden Sie unter the section called “Änderungen, die normalerweise zu Bereitstellungen führen blue/green ”.

Zu den optionalen Plugins gehören Sprachanalyseprogramme und benutzerdefinierte Suchergebnisse. Das Amazon Personalize Search Ranking-Plugin verwendet beispielsweise maschinelles Lernen, um Suchergebnisse für Ihre Kunden zu personalisieren. Weitere Informationen zu diesem Plugin finden Sie unter Suchergebnisse personalisieren von. OpenSearch Eine Liste aller unterstützten Plugins finden Sie unterthe section called “Plug-ins nach Engine-Version”.

Sudachi-Plug-In

Wenn Sie beim Sudachi-Plugin eine Wörterbuchdatei neu zuordnen, wirkt sich das nicht sofort auf die Domain aus. Das Wörterbuch wird aktualisiert, wenn die nächste blaue/grüne Bereitstellung im Rahmen einer Konfigurationsänderung oder eines anderen Updates auf der Domain ausgeführt wird. Alternativ können Sie ein neues Paket mit den aktualisierten Daten erstellen, mit diesem neuen Paket einen neuen Index erstellen, den vorhandenen Index erneut mit dem neuen Index indizieren und

dann den alten Index löschen. Wenn Sie den Ansatz der Neuindizierung bevorzugen, verwenden Sie einen Indexalias, damit Ihr Datenverkehr nicht unterbrochen wird.

Darüber hinaus unterstützt das Sudachi-Plugin nur binäre Sudachi-Wörterbücher, die Sie mit der API-Operation hochladen können. CreatePackage Informationen zum vorgefertigten Systemwörterbuch und zum Verfahren zum Kompilieren von Benutzerwörterbüchern finden Sie in der Sudachi-Dokumentation.

Das folgende Beispiel zeigt, wie Sie System- und Benutzerwörterbücher mit dem Sudachi Tokenizer verwenden. Sie müssen diese Wörterbücher als benutzerdefinierte Pakete mit Typ hochladen `TXT-DICTIONARY` und ihr Paket in den zusätzlichen Einstellungen angeben. IDs

```
PUT sudachi_sample
{
  "settings": {
    "index": {
      "analysis": {
        "tokenizer": {
          "sudachi_tokenizer": {
            "type": "sudachi_tokenizer",
            "additional_settings": "{\"systemDict\": \"<system-dictionary-package-id>\",\"userDict\": [\"<user-dictionary-package-id>\"]}"
        }
        },
        "analyzer": {
          "sudachi_analyzer": {
            "filter": ["my_searchfilter"],
            "tokenizer": "sudachi_tokenizer",
            "type": "custom"
          }
        },
        "filter":{
          "my_searchfilter": {
            "type": "sudachi_split",
            "mode": "search"
          }
        }
      }
    }
  }
}
```

Aktualisieren von Paketen

In diesem Abschnitt wird nur beschrieben, wie Sie ein benutzerdefiniertes Wörterbuchpaket aktualisieren, da vorkonfigurierte Plugin-Pakete bereits für Sie aktualisiert wurden. Das Hochladen einer neuen Version eines Wörterbuches auf Amazon S3 aktualisiert das Paket nicht automatisch bei Amazon OpenSearch Service. OpenSearch Der Service speichert eine eigene Kopie der Datei. Wenn Sie also eine neue Version auf S3 hochladen, müssen Sie diese manuell aktualisieren.

Jede Ihrer verknüpften Domänen speichert auch eine eigene Kopie der Datei. Um das Suchverhalten vorhersehbar zu halten, verwenden Domänen weiterhin ihre aktuelle Paketversion, bis Sie sie explizit aktualisieren. Um ein benutzerdefiniertes Paket zu aktualisieren, ändern Sie die Datei in Amazon S3 Control, aktualisieren Sie das Paket unter OpenSearch Service und wenden Sie dann das Update an.

Konsole

1. Wählen Sie in der OpenSearch Servicekonsole Pakete aus.
2. Wählen Sie ein Paket und Aktualisieren aus.
3. Geben Sie einen neuen S3-Pfad zu der Datei an und wählen Sie dann Paket aktualisieren aus.
4. Kehren Sie zum Bildschirm Packages (Pakete) zurück.
5. Wenn der Paketstatus auf Verfügbar wechselt, wählen Sie das Paket aus. Wählen Sie dann eine oder mehrere verknüpfte Domänen aus, übernehmen Sie die Aktualisierung und bestätigen Sie. Warten Sie, bis sich der Zuordnungsstatus in Aktiv ändert.
6. Die nächsten Schritte hängen davon ab, wie Sie Ihre Indizes konfiguriert haben:

   - Wenn Ihre Domäne läuft OpenSearch oder Elasticsearch 7.8 oder höher ist und nur Suchanalysatoren verwendet, bei denen das updateable -Feld auf „true“ gesetzt ist, müssen Sie keine weiteren Maßnahmen ergreifen. OpenSearch Der Service aktualisiert Ihre Indizes automatisch unter Verwendung der API _plugins/_search_search_search_search_search_search_search_search_search_search_searc
   - Wenn Ihre Domäne Elasticsearch 7.7 oder früher ausführt, Indexanalysatoren verwendet oder das `updateable` Feld nicht verwendet, siehe. the section called “Manuelles Aktualisieren von Indizes mit einem neuen Wörterbuch”

Obwohl die Konsole die einfachste Methode ist, können Sie OpenSearch Servicepakete auch mit AWS CLI SDKs, oder Konfigurations-API aktualisieren. Weitere Informationen finden Sie in der AWS CLI Befehlsreferenz und der Amazon OpenSearch Service API-Referenz.

AWS SDK

Anstatt ein Paket in der Konsole manuell zu aktualisieren, können Sie die SDKs zur Automatisierung des Update-Prozesses verwenden. Das folgende Python-Beispielskript lädt eine neue Paketdatei in Amazon S3 hoch, aktualisiert das Paket in OpenSearch Service und wendet das neue Paket auf die angegebene Domäne an. Nachdem bestätigt wurde, dass das Update erfolgreich war, führt es einen Beispielaufruf durch, um zu OpenSearch zeigen, dass die neuen Synonyme angewendet wurden.

Sie müssen Werte für `host`, `region`, `file_name`, `bucket_name`, `s3_key`, `package_id`, `domain_name` und `query` angeben.

```
from requests_aws4auth import AWS4Auth
import boto3
import requests
import time
import json
import sys

host = ''  # The OpenSearch domain endpoint with https:// and a trailing slash. For
 example, https://my-test-domain.us-east-1.es.amazonaws.com/
region = ''  # For example, us-east-1
file_name = ''  # The path to the file to upload
bucket_name = ''  # The name of the S3 bucket to upload to
s3_key = ''  # The name of the S3 key (file name) to upload to
package_id = ''  # The unique identifier of the OpenSearch package to update
domain_name = ''  # The domain to associate the package with
query = ''  # A test query to confirm the package has been successfully updated

service = 'es'
credentials = boto3.Session().get_credentials()
client = boto3.client('opensearch')
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key,
                   region, service, session_token=credentials.token)


def upload_to_s3(file_name, bucket_name, s3_key):
    """Uploads file to S3"""
    s3 = boto3.client('s3')
    try:
        s3.upload_file(file_name, bucket_name, s3_key)
        print('Upload successful')
        return True
    except FileNotFoundError:
```

```
        sys.exit('File not found. Make sure you specified the correct file path.')


def update_package(package_id, bucket_name, s3_key):
    """Updates the package in OpenSearch Service"""
    print(package_id, bucket_name, s3_key)
    response = client.update_package(
        PackageID=package_id,
        PackageSource={
            'S3BucketName': bucket_name,
            'S3Key': s3_key
        }
    )
    print(response)


def associate_package(package_id, domain_name):
    """Associates the package to the domain"""
    response = client.associate_package(
        PackageID=package_id, DomainName=domain_name)
    print(response)
    print('Associating...')


def wait_for_update(domain_name, package_id):
    """Waits for the package to be updated"""
    response = client.list_packages_for_domain(DomainName=domain_name)
    package_details = response['DomainPackageDetailsList']
    for package in package_details:
        if package['PackageID'] == package_id:
            status = package['DomainPackageStatus']
            if status == 'ACTIVE':
                print('Association successful.')
                return
            elif status == 'ASSOCIATION_FAILED':
                sys.exit('Association failed. Please try again.')
            else:
                time.sleep(10)  # Wait 10 seconds before rechecking the status
                wait_for_update(domain_name, package_id)


def sample_search(query):
    """Makes a sample search call to OpenSearch"""
    path = '_search'
```

```
params = {'q': query}
url = host + path
response = requests.get(url, params=params, auth=awsauth)
print('Searching for ' + '"' + query + '"')
print(response.text)
```

> **Note**
>
> Wenn Sie beim Ausführen des Skripts mit die Fehlermeldung „Paket nicht gefunden“ erhalten, bedeutet dies wahrscheinlich AWS CLI, dass Boto3 die in ~/.aws/config angegebene Region verwendet, die nicht die Region ist, in der sich Ihr S3-Bucket befindet. Führen Sie entweder `aws configure` aus und geben Sie die richtige Region an, oder fügen Sie die Region explizit zum Client hinzu:
>
> ```
> client = boto3.client('opensearch', region_name='us-east-1')
> ```

Manuelles Aktualisieren von Indizes mit einem neuen Wörterbuch

Manuelle Indexaktualisierungen gelten nur für benutzerdefinierte Wörterbücher, nicht für vorkonfigurierte Plugins. Um ein aktualisiertes Wörterbuch zu verwenden, müssen Sie Ihre Indizes manuell aktualisieren, wenn Sie eine der folgenden Bedingungen erfüllen:

- Ihre Domäne führt Elasticsearch 7.7 oder früher aus.
- Sie verwenden benutzerdefinierte Pakete als Indexanalysatoren.
- Sie verwenden benutzerdefinierte Pakete als Suchanalysatoren, schließen jedoch das aktualisierbare Feld nicht ein.

Um Analyzer mit den neuen Paketdateien zu aktualisieren, haben Sie zwei Möglichkeiten:

- Schließen und öffnen Sie alle Indizes, die Sie aktualisieren möchten:

```
POST my-index/_close
POST my-index/_open
```

- Indizieren Sie die Indizes neu. Erstellen Sie zunächst einen Index, der die aktualisierte Synonymdatei verwendet (oder eine ganz neue Datei). Beachten Sie, dass nur UTF-8 unterstützt wird.

```
PUT my-new-index
{
  "settings": {
    "index": {
      "analysis": {
        "analyzer": {
          "synonym_analyzer": {
            "type": "custom",
            "tokenizer": "standard",
            "filter": ["synonym_filter"]
          }
        },
        "filter": {
          "synonym_filter": {
            "type": "synonym",
            "synonyms_path": "analyzers/F222222222"
          }
        }
      }
    }
  },
  "mappings": {
    "properties": {
      "description": {
        "type": "text",
        "analyzer": "synonym_analyzer"
      }
    }
  }
}
```

Nehmen Sie anschließend eine Neuindizierung des alten Index in diesen neuen Index vor:

```
POST _reindex
{
  "source": {
    "index": "my-index"
  },
  "dest": {
    "index": "my-new-index"
  }
```

```
}
```

Wenn Sie häufig Index-Analysen aktualisieren, verwenden Sie Indexalias um einen konsistenten Pfad zum neuesten Index beizubehalten:

```
POST _aliases
{
  "actions": [
    {
      "remove": {
        "index": "my-index",
        "alias": "latest-index"
      }
    },
    {
      "add": {
        "index": "my-new-index",
        "alias": "latest-index"
      }
    }
  ]
}
```

Wenn Sie den alten Index nicht benötigen, löschen Sie ihn:

```
DELETE my-index
```

Trennen und Entfernen von Paketen

Das Trennen eines Pakets, unabhängig davon, ob es sich um ein benutzerdefiniertes Wörterbuch oder ein vorverpacktes Plug-In handelt, von einer Domäne zu trennen, bedeutet, dass Sie dieses Paket nicht mehr verwenden können, wenn Sie neue Indizes erstellen. Nachdem ein Paket getrennt wurde, können bestehende Indizes, die das Paket verwendet haben, es nicht mehr verwenden. Sie müssen das Paket aus einem Index entfernen, bevor Sie es trennen können. Andernfalls schlägt die Trennung fehl.

Die Konsole ist die einfachste Möglichkeit, ein Paket von einer Domäne zu trennen und aus Service zu entfernen. OpenSearch Wenn Sie ein Paket aus OpenSearch Service entfernen, wird es nicht von seinem ursprünglichen Speicherort auf Amazon S3 entfernt.

Trennen eines Pakets von einer Domäne

1. Melden Sie sich zu https://console.aws.amazon.com/aos/Hause bei der Amazon OpenSearch Service-Konsole an.
2. Wählen Sie im Navigationsbereich Domains aus.
3. Wählen Sie die Domain aus und navigieren Sie dann zur Registerkarte Pakete.
4. Wählen Sie ein Paket aus, klicken Sie dann auf die Option Aktionen und anschließend auf Trennen. Bestätigen Sie Ihre Auswahl.
5. Warten Sie, bis das Paket nicht mehr in der Liste angezeigt wird. Möglicherweise müssen Sie Ihren Browser aktualisieren.
6. Wenn Sie das Paket mit anderen Domänen verwenden möchten, hören Sie hier auf. Um mit dem Entfernen des Pakets fortzufahren (falls es sich um ein benutzerdefiniertes Wörterbuch handelt), wählen Sie im Navigationsbereich Pakete aus.
7. Wählen Sie das Paket und anschließend Delete (Löschen) aus.

Verwenden Sie alternativ die Konfigurations-API AWS CLI SDKs, oder, um Pakete zu trennen und zu entfernen. Weitere Informationen finden Sie in der AWS CLI Befehlsreferenz und der Amazon OpenSearch Service API-Referenz.

Verwaltung benutzerdefinierter Plugins in Amazon OpenSearch Service

Mithilfe benutzerdefinierter Plug-ins für OpenSearch Service können Sie die OpenSearch Funktionalität in Bereichen wie Sprachanalyse, benutzerdefinierte Filterung, Ranking und mehr erweitern, sodass Sie personalisierte Sucherlebnisse erstellen können. Benutzerdefinierte Plug-ins für OpenSearch können entwickelt werden, indem Sie die `org.opensearch.plugins.Plugin` Klasse erweitern und sie dann in eine `.zip` Datei packen.

Die folgenden Plugin-Erweiterungen werden derzeit von Amazon OpenSearch Service unterstützt:

- AnalysisPlugin— Erweitert die Analysefunktionalität, indem beispielsweise benutzerdefinierte Analysatoren, Zeichen-Tokenizer oder Filter für die Textverarbeitung hinzugefügt werden.
- SearchPlugin— Verbessert die Suchfunktionen durch benutzerdefinierte Abfragetypen, Ähnlichkeitsalgorithmen, Vorschlagsoptionen und Aggregationen.
- MapperPlugin— Ermöglicht es Ihnen, benutzerdefinierte Feldtypen und deren Zuordnungskonfigurationen in zu erstellen OpenSearch, sodass Sie definieren können, wie verschiedene Datentypen gespeichert und indexiert werden sollen.

- ScriptPlugin— Ermöglicht das Hinzufügen benutzerdefinierter Skriptfunktionen zu OpenSearch beispielsweise benutzerdefinierten Skripten für Operationen wie Bewertung, Sortierung und Feldwerttransformationen während der Suche oder Indizierung.

Sie können die OpenSearch Service-Konsole oder bestehende API-Befehle für benutzerdefinierte Pakete verwenden, um das Plugin hochzuladen und mit dem Amazon OpenSearch Service-Cluster zu verknüpfen. Sie können den DescribePackagesBefehl auch verwenden, um alle Pakete in Ihrem Konto zu beschreiben und Details wie OpenSearch Version und Fehlerdetails einzusehen. OpenSearch Der Dienst überprüft das Plugin-Paket auf Versionskompatibilität, Sicherheitslücken und zulässige Plugin-Operationen. Weitere Informationen zu benutzerdefinierten Paketen finden Sie unterthe section called “Pakete”.

OpenSearch Version und AWS-Region Unterstützung

Benutzerdefinierte Plug-ins werden in OpenSearch Service-Domänen, auf denen OpenSearch Version 2.15 ausgeführt wird, wie folgt AWS-Regionen unterstützt:

- USA Ost (Ohio): (us-east-2)
- USA Ost (Nord-Virginia): (us-east-1)
- USA West (Oregon): (us-west-2)
- Asien-Pazifik (Mumbai): (ap-south-1)
- Asien-Pazifik (Seoul): (ap-northeast-2)
- Asien-Pazifik (Singapur): (ap-southeast-1)
- Asien-Pazifik (Sydney): (ap-southeast-2)
- Asien-Pazifik (Tokyo) (ap-northeast-1)
- Kanada (Zentral): (ca-central-1)
- Europa (Frankfurt) (eu-central-1)
- Europa (Irland) (eu-west-1)
- Europa (London) (eu-west-2)
- Europa (Paris) (eu-west-3)
- Südamerika (São Paulo) (sa-east-1)

> **Note**
>
> Benutzerdefinierte Plugins enthalten vom Benutzer entwickelten Code. Für Probleme, einschließlich SLA-Verstöße, die durch von Benutzern entwickelten Code verursacht werden, können keine SLA-Gutschriften gutgeschrieben werden. Weitere Informationen finden Sie unter Amazon OpenSearch Service Level Agreement.

Themen

- Plugin-Quoten
- Voraussetzungen
- Fehlerbehebung
- Installieren eines benutzerdefinierten Plugins mit der Konsole
- Verwaltung benutzerdefinierter Plugins mit dem AWS CLI
- AWS KMS Integration benutzerdefinierter Amazon OpenSearch Service-Pakete

Plugin-Quoten

- Sie können bis zu 25 benutzerdefinierte Plugins pro Konto und Region erstellen.
- Die maximale unkomprimierte Größe für ein Plugin beträgt 1 GB.
- Die maximale Anzahl von Plugins, die einer einzelnen Domäne zugeordnet werden können, beträgt 20. Dieses Kontingent gilt für alle Plugin-Typen zusammen: optional, Drittanbieter und benutzerdefiniert.
- Benutzerdefinierte Plugins werden auf Domains unterstützt, auf denen OpenSearch Version 2.15 oder höher ausgeführt wird.
- Die `descriptor.properties` Datei für Ihr Plugin muss eine Engine-Version unterstützen, die 2.15.0 oder eine beliebige 2.x.x-Version ähnelt, wobei die Patch-Version auf Null gesetzt ist.
- Die folgenden Funktionen sind nicht verfügbar, wenn Ihre Domain benutzerdefinierte Plugins verwendet:
  - Cluster-übergreifende Suche
  - Cluster-übergreifende Replikation
  - Neuindizierung per Fernzugriff
  - Automatische Optimierung

- the section called “Multi-AZ mit Standby”
- Zentralisierte Benutzerschnittstelle OpenSearch

Voraussetzungen

Überprüfen Sie zuerst, ob die folgenden Anforderungen erfüllt sind, bevor Sie ein benutzerdefiniertes Plug-In installieren und mit einer Domäne verknüpfen:

- Die unterstützte Engine-Version für das Plugin in der `descriptor.properties` Datei sollte `2.15.0` oder ähneln`2.x.0`. Das heißt, die Patch-Version muss Null sein.
- Die folgenden Funktionen müssen auf Ihrer Domain aktiviert sein:
  - Node-to-node Verschlüsselung
  - Verschlüsselung im Ruhezustand
  - `EnforceHTTPS`ist auf 'true' gesetzt

    Siehe auch opensearch-https-requiredim AWS Config Entwicklerhandbuch.
  - Kunden müssen Policy-Min-TLS-1-2-PFS-2023-10 unterstützen. Sie können diese Unterstützung mit dem folgenden -Befehl angeben. Ersetzen Sie *`placeholder value`* durch Ihre eigenen Informationen:

    ```
    aws opensearch update-domain-config \
        --domain-name domain-name \
        --domain-endpoint-options '{"TLSSecurityPolicy":"Policy-Min-TLS-1-2-
    PFS-2023-10" }'
    ```

    Weitere Informationen finden Sie DomainEndpointOptionsin der Amazon OpenSearch Service API-Referenz.

Fehlerbehebung

Wenn das System den Fehler zurückgibt`PluginValidationFailureReason : The provided plugin could not be loaded`, finden Sie Informationen the section called “Die Installation eines benutzerdefinierten Plugins schlägt aufgrund der Versionskompatibilität fehl” zur Fehlerbehebung unter.

Installieren eines benutzerdefinierten Plugins mit der Konsole

Um ein Drittanbieter-Plugin mit einer Domain zu verknüpfen, importieren Sie zunächst die Plugin-Lizenz und die Konfiguration als Pakete.

So installieren Sie ein benutzerdefiniertes Plugin:

1. Melden Sie sich zu https://console.aws.amazon.com/aos/Hause bei der Amazon OpenSearch Service-Konsole an.
2. Wählen Sie im linken Navigationsbereich Packages aus.
3. Klicken Sie auf Packet importieren.
4. Geben Sie unter Name einen eindeutigen, leicht identifizierbaren Namen für das Plugin ein.
5. (Optional) Geben Sie unter Beschreibung alle nützlichen Informationen über das Paket oder seinen Zweck an.
6. Wählen Sie als Pakettyp die Option Plugin aus.
7. Geben Sie Package Paketquelle den Pfad ein oder suchen Sie nach der Plugin-ZIP-Datei in Amazon S3.
8. Wählen Sie als OpenSearch Engine-Version die Version aus OpenSearch , die das Plugin unterstützt.
9. Wählen Sie für Paketverschlüsselung aus, ob der Verschlüsselungsschlüssel für das Package angepasst werden soll. Standardmäßig verschlüsselt OpenSearch Service das Plugin-Paket mit einem AWS-eigener Schlüssel. Sie können stattdessen einen vom Kunden verwalteten Schlüssel verwenden.
10. Wählen Sie Importieren aus.

Nachdem Sie das Plugin-Paket importiert haben, ordnen Sie es einer Domain zu. Detaillierte Anweisungen finden Sie unter the section called “Importieren eines Pakets und Zuordnen eines Pakets zu einer Domäne”.

Verwaltung benutzerdefinierter Plugins mit dem AWS CLI

Sie können den verwenden AWS CLI , um eine Reihe von benutzerdefinierten Plugin-Aufgaben zu verwalten.

Aufgaben

- Installieren eines benutzerdefinierten Plugins mit der AWS CLI

- Aktualisieren eines benutzerdefinierten Plugins mit der AWS CLI
- Erstellen oder aktualisieren Sie ein benutzerdefiniertes Plugin mit einem AWS KMS Sicherheitsschlüssel
- Aktualisieren einer OpenSearch Dienstdomäne mit benutzerdefinierten Plugins auf eine neuere Version der OpenSearch Verwendung von AWS CLI
- Deinstallation und Anzeige des Dissoziationsstatus eines benutzerdefinierten Plug-ins

Installieren eines benutzerdefinierten Plugins mit der AWS CLI

Bevor Sie beginnen

Bevor Sie ein benutzerdefiniertes Plug-In mit Ihrer Domäne verknüpfen können, müssen Sie es in einen Amazon Simple Storage Service (Amazon S3) -Bucket hochladen. Der Bucket muss sich an derselben AWS-Region Stelle befinden, an der Sie das Plugin verwenden möchten. Informationen zum Hinzufügen eines Objekts zu einem S3-Bucket finden Sie unter Hochladen von Objekten im Amazon Simple Storage Service-Benutzerhandbuch.

Wenn Ihr Plug-In vertrauliche Informationen enthält, geben Sie beim Hochladen die serverseitige Verschlüsselung mit S3-verwalteten Schlüsseln an. Nachdem Sie die Datei hochgeladen haben, notieren Sie deren S3-Pfad. Das Pfadformat lautet `s3://amzn-s3-demo-bucket/file-path/file-name`.

> **Note**
>
> Sie können optional ein benutzerdefiniertes Plugin sichern, wenn Sie das Plugin erstellen, indem Sie einen AWS Key Management Service ()AWS KMS-Schlüssel angeben. Weitere Informationen finden Sie unter the section called “Erstellen oder aktualisieren Sie ein benutzerdefiniertes Plugin mit einem AWS KMS Sicherheitsschlüssel”.

So installieren Sie ein benutzerdefiniertes Plugin mit der AWS CLI

1. Erstellen Sie ein neues Paket für Ihr benutzerdefiniertes Plugin, indem Sie den folgenden Befehl create-package ausführen und dabei sicherstellen, dass die folgenden Anforderungen erfüllt sind:

   - Der Bucket und die Schlüsselposition müssen auf die `.zip` Plugin-Datei in einem S3-Bucket in dem Konto verweisen, in dem Sie die Befehle ausführen.

- Der S3-Bucket muss sich in derselben -Region befinden, in der das Paket erstellt wird.
- Für `ZIP-PLUGIN` Pakete werden nur `.zip` Dateien unterstützt.
- Der Inhalt der `.zip` Datei muss der Verzeichnisstruktur folgen, wie sie vom Plugin erwartet wird.
- Der Wert für `--engine-version` muss das folgende Format habenOpenSearch_*{MAJOR}.{MINOR}*. Beispiel: **`OpenSearch_2.17`**.

Ersetzen Sie *`placeholder values`* durch Ihre eigenen Informationen:

```
aws opensearch create-package \
    --package-name package-name \
    --region region \
    --package-type ZIP-PLUGIN \
    --package-source S3BucketName=amzn-s3-demo-bucket,S3Key=s3-key \
    --engine-version opensearch-version
```

2. (Optional) Mit dem Befehl describe-packages können Sie sich den Status des `create-package` Vorgangs anzeigen lassen, einschließlich aller Validierungs- und Sicherheitslücken. Ersetzen Sie *`placeholder values`* durch Ihre eigenen Informationen:

```
aws opensearch describe-packages \
    --region region  \
    --filters '[{"Name": "PackageType","Value": ["ZIP-PLUGIN"]}, {"Name":
 "PackageName","Value": ["package-name"]}]'
```

Die vom System zurückgegebenen Informationen ähneln den Folgenden:

```
{
    "PackageDetailsList": [{
        "PackageID": "pkg-identifier",
        "PackageName": "package-name",
        "PackageType": "ZIP-PLUGIN",
        "PackageStatus": "VALIDATION_FAILED",
        "CreatedAt": "2024-11-11T13:07:18.297000-08:00",
        "LastUpdatedAt": "2024-11-11T13:10:13.843000-08:00",
        "ErrorDetails": {
            "ErrorType": "",
```

```
            "ErrorMessage": "PluginValidationFailureReason : Dependency Scan
 reported 3 vulnerabilities for the plugin: CVE-2022-23307, CVE-2019-17571,
 CVE-2022-23305"
        },
        "EngineVersion": "OpenSearch_2.15",
        "AllowListedUserList": [],
        "PackageOwner": "OWNER-XXXX"
    }]
}
```

> **Note**
>
> Während des `create-package` Vorgangs überprüft Amazon OpenSearch Service den `ZIP-PLUGIN` Wert auf Versionskompatibilität, unterstützte Plugin-Erweiterungen und Sicherheitslücken. Die Sicherheitslücken werden mit dem Amazon Inspector-Service gescannt. Die Ergebnisse dieser Prüfungen werden im `ErrorDetails` Feld in der API-Antwort angezeigt.

3. Verwenden Sie den Befehl associate-package, um das Plugin mithilfe der Paket-ID des im vorherigen Schritt erstellten Pakets der OpenSearch Service-Domain Ihrer Wahl zuzuordnen.

> **Tip**
>
> Wenn Sie über mehrere Plugins verfügen, können Sie stattdessen den Befehl associate-packages verwenden, um mehrere Pakete in einem Vorgang einer Domain zuzuordnen.

Ersetzen Sie *`placeholder values`* durch Ihre eigenen Informationen:

```
aws opensearch associate-package \
    --domain-name domain-name \
    --region region \
    --package-id package-id
```

> **Note**
>
> Das Plugin wird mithilfe eines blauen/grünen Bereitstellungsprozesses installiert und deinstalliert.

4. (Optional) Verwenden Sie den list-packages-for-domainBefehl, um den Status der Zuordnung anzuzeigen. Der Zuordnungsstatus ändert sich, je weiter der Workflow von `ASSOCIATING` bis `ACTIVE` voranschreitet. Der Zuordnungsstatus ändert sich auf AKTIV, nachdem die Plugin-Installation abgeschlossen ist und das Plug-in einsatzbereit ist.

   Ersetzen Sie *`placeholder values`* durch Ihre Informationen.

   ```
   aws opensearch list-packages-for-domain \
       --region region \
       --domain-name domain-name
   ```

Aktualisieren eines benutzerdefinierten Plugins mit der AWS CLI

Verwenden Sie den Befehl update-package, um Änderungen an einem Plugin vorzunehmen.

> **Note**
>
> Sie können optional ein benutzerdefiniertes Plugin sichern, wenn Sie das Plugin aktualisieren, indem Sie einen AWS Key Management Service (AWS KMS) -Schlüssel angeben. Weitere Informationen finden Sie unter the section called “Erstellen oder aktualisieren Sie ein benutzerdefiniertes Plugin mit einem AWS KMS Sicherheitsschlüssel”.

So aktualisieren Sie ein benutzerdefiniertes Plugin mit der AWS CLI

- Führen Sie den folgenden Befehl aus. Ersetzen Sie *`placeholder values`* durch Ihre Informationen.

  ```
  aws opensearch update-package \
      --region region \
      --package-id package-id \
      --package-source S3BucketName=amzn-s3-demo-bucket,S3Key=s3-key \
      --package-description description
  ```

Nach der Aktualisierung eines Pakets können Sie den Befehl associate-package oder associate-packages verwenden, um Paketaktualisierungen auf eine Domain anzuwenden.

> **Note**
>
> Mithilfe von. Sie können Vorgänge auf dem Plug-in prüfen, erstellen, aktualisieren, zuordnen und deren Zuordnung aufheben. AWS CloudTrail Weitere Informationen finden Sie unter Überwachung von Amazon OpenSearch Service API-Aufrufen mit AWS CloudTrail.

Erstellen oder aktualisieren Sie ein benutzerdefiniertes Plugin mit einem AWS KMS Sicherheitsschlüssel

Sie können ein benutzerdefiniertes Plugin sichern, wenn Sie das Plugin erstellen oder aktualisieren, indem Sie einen AWS KMS Schlüssel angeben. Stellen `PackageEncryptionOptions` Sie dazu den Amazon-Ressourcennamen (ARN) des Schlüssels ein `true` und geben Sie ihn an, wie in den folgenden Beispielen dargestellt.

Beispiel: Erstellen Sie ein benutzerdefiniertes Plugin mit AWS KMS Schlüsselsicherheit

```
aws opensearch create-package \
    --region us-east-2  --package-name my-custom-package \
    --package-type ZIP-PLUGIN \
    --package-source S3BucketName=amzn-s3-demo-bucket,S3Key=my-s3-key
    --engine-version OpenSearch_2.15
"PackageConfigOptions": {
     ...
  }
  "PackageEncryptionOptions": {
    "Enabled": true,
    "KmsKeyId":"arn:aws:kms:us-east-2:111222333444:key/2ba228d5-1d09-456c-ash9-
daf42EXAMPLE"
  }
```

Beispiel: Aktualisieren Sie ein benutzerdefiniertes Plugin mit AWS KMS Key Security

```
aws opensearch update-package \
    --region us-east-2  --package-name my-custom-package \
    --package-type ZIP-PLUGIN \
    --package-source S3BucketName=amzn-s3-demo-bucket,S3Key=my-s3-key
    --engine-version OpenSearch_2.15
"PackageConfigOptions": {
     ...
  }
```

```
  "PackageEncryptionOptions": {
    "Enabled": true,
    "KmsKeyId":"arn:aws:kms:us-east-2:111222333444:key/2ba228d5-1d09-456c-ash9-
daf42EXAMPLE"
  }
```

> **Important**
>
> Wenn der von Ihnen angegebene AWS KMS Schlüssel deaktiviert oder gelöscht wird, kann dies dazu führen, dass der zugehörige Cluster nicht mehr funktioniert.

Weitere Informationen zur AWS KMS Integration mit benutzerdefinierten Paketen finden Sie unterthe section called “AWS KMS Integration benutzerdefinierter Amazon OpenSearch Service-Pakete”.

Aktualisieren einer OpenSearch Dienstdomäne mit benutzerdefinierten Plugins auf eine neuere Version der OpenSearch Verwendung von AWS CLI

Wenn Sie eine OpenSearch Dienstdomäne, die benutzerdefinierte Plug-ins verwendet, auf eine neuere Version von aktualisieren müssen OpenSearch, führen Sie die folgenden Schritte durch.

Um eine OpenSearch Dienstdomäne mit benutzerdefinierten Plug-ins auf eine neuere Version zu aktualisieren, OpenSearch verwenden Sie AWS CLI

1. Verwenden Sie den Befehl create-package, um ein neues Paket für Ihr Plugin zu erstellen und dabei die neue OpenSearch Version anzugeben.

   Stellen Sie sicher, dass der Paketname für das Plugin für alle Engine-Versionen derselbe ist. Eine Änderung des Paketnamens führt dazu, dass der Domain-Upgrade-Prozess während der Blau/Grün-Bereitstellung fehlschlägt.
2. Führen Sie ein Upgrade Ihrer Domain auf die höhere Version durch, indem Sie die Schritte unter befolgen. the section called “Aktualisieren von Domains”

   Während dieses Vorgangs trennt Amazon OpenSearch Service die Zuordnung zur vorherigen Version des Plugin-Pakets und installiert die neue Version mithilfe einer blauen/grünen Bereitstellung.

Deinstallation und Anzeige des Dissoziationsstatus eines benutzerdefinierten Plug-ins

Um das Plugin von einer beliebigen Domain zu deinstallieren, können Sie den Befehl dissociate-package verwenden. Wenn Sie diesen Befehl ausführen, werden auch alle zugehörigen Konfigurations- oder Lizenzpakete entfernt. Sie können den list-packages-for-domainBefehl dann zum Anzeigen des Status der Trennung verwenden.

> **Tip**
>
> Sie können auch den Befehl dissociate-packages verwenden, um mehrere Plugins aus einer Domain in einem einzigen Vorgang zu deinstallieren.

Um ein benutzerdefiniertes Plugin zu deinstallieren und den Dissoziationsstatus anzuzeigen

1. Deaktiviert das Plugin in jedem Index. Dies muss geschehen, bevor Sie das Plugin-Paket trennen.

   Wenn Sie versuchen, ein Plugin zu deinstallieren, bevor Sie es für jeden Index deaktivieren, bleibt der blaue/grüne Bereitstellungsprozess im Status hängen. `Processing`
2. Führen Sie zur Deinstallation des Plugins den folgenden Befehl aus. Ersetzen Sie *`placeholder values`* durch Ihre Informationen.

   ```
   aws opensearch dissociate-package \
       --region region \
       --package-id plugin-package-id \
       --domain-name domain name
   ```
3. (Optional) Führen Sie den list-packages-for-domainBefehl aus, um den Status der Dissoziation anzuzeigen.

AWS KMS Integration benutzerdefinierter Amazon OpenSearch Service-Pakete

Benutzerdefinierte Pakete von Amazon OpenSearch Service bieten standardmäßig Verschlüsselung, um Ihre `ZIP-PLUGIN` Pakete im Ruhezustand zu schützen Von AWS verwaltete Schlüssel.

- AWS-eigene Schlüssel— Benutzerdefinierte Pakete von Amazon OpenSearch Service verwenden diese Schlüssel standardmäßig, um Ihre `ZIP-PLUGIN` Pakete automatisch zu verschlüsseln. Sie können ihre Nutzung nicht einsehen, verwalten AWS-eigene Schlüssel oder verwenden und

auch nicht ihre Nutzung prüfen. Sie müssen jedoch keine Maßnahmen ergreifen oder Programme ändern, um die Schlüssel zu schützen, die zur Verschlüsselung Ihrer Daten verwendet werden. Weitere Informationen finden Sie unter AWS-eigene Schlüssel im AWS Key Management Service - Entwicklerhandbuch.

- Vom Kunden verwaltete Schlüssel — Sie können eine zweite Verschlüsselungsebene über der vorhandenen hinzufügen, AWS-eigene Schlüssel indem Sie bei der Erstellung Ihres `ZIP-PLUGIN` benutzerdefinierten Pakets einen vom Kunden verwalteten Schlüssel auswählen.

  Benutzerdefinierte OpenSearch Amazon-Service-Pakete unterstützen die Verwendung eines symmetrischen, vom Kunden verwalteten Schlüssels, den Sie erstellen, besitzen und verwalten, um eine zweite Verschlüsselungsebene über die bestehende AWS -eigene Verschlüsselung zu legen. Da Sie die volle Kontrolle über diese Verschlüsselungsebene haben, können Sie die folgenden Aufgaben ausführen:

  - Legen Sie wichtige Richtlinien fest und pflegen Sie sie
  - Festlegung und Aufrechterhaltung AWS Identity and Access Management (IAM) von Richtlinien und Zuschüssen
  - Aktivieren und Deaktivieren von Schlüsselrichtlinien
  - Schlüssel des kryptographischen Materials rotieren
  - Tags hinzufügen
  - Erstellen von Schlüsselaliasen
  - Schlüssel für das Löschen planen

Weitere Informationen finden Sie unter Kundenverwaltete Schlüssel im AWS Key Management Service Entwicklerhandbuch.

> **Note**
>
> Die benutzerdefinierten Pakete von Amazon OpenSearch Service aktivieren automatisch die Verschlüsselung im Ruhezustand und verwenden AWS-eigene Schlüssel diese kostenlos. Allerdings AWS KMS fallen -Gebühren an, wenn Sie einen vom Kunden verwalteten Schlüssel verwenden. Weitere Informationen zu Preisen finden Sie unter AWS Key Management Service Preise.

So verwendet der OpenSearch Service für benutzerdefinierte Pakete von Amazon Service Zuschüsse in AWS KMS

OpenSearch Für benutzerdefinierte Servicepakete ist eine Genehmigung erforderlich, um Ihren vom Kunden verwalteten Schlüssel verwenden zu können.

Wenn Sie ein `ZIP-PLUGIN` Paket erstellen, das mit einem vom Kunden verwalteten Schlüssel verschlüsselt ist, erstellt der OpenSearch Amazon-Dienst für benutzerdefinierte Pakete in Ihrem Namen eine Genehmigung, indem er eine CreateGrantAnfrage an sendet AWS KMS. Zuschüsse AWS KMS gewähren OpenSearch Service Zugriff auf einen AWS KMS Schlüssel in Ihrem Konto. Für die mit benutzerdefinierten OpenSearch Servicepaketen erstellten Berechtigungen gilt eine Einschränkung, die nur dann Operationen zulässt, wenn die Anfrage einen Verschlüsselungskontext mit Ihrer benutzerdefinierten Paket-ID enthält.

Für benutzerdefinierte Pakete von Amazon OpenSearch Service benötigen Sie die Gewährung, um Ihren vom Kunden verwalteten Schlüssel für die folgenden internen Vorgänge zu verwenden:

Operation	Beschreibung
`DescribeKey`	Sendet `DescribeKey` Anfragen an, AWS KMS um zu überprüfen, ob die bereitgestellte symmetrische vom Kunden verwaltete Schlüssel-ID gültig ist.
`GenerateDataKeyWithoutPlaintext`	Sendet `GenerateDataKeyWithoutPlaintext` Anfragen an, AWS KMS um Datenschlüssel zu generieren, die mit Ihrem vom Kunden verwalteten Schlüssel verschlüsselt sind.
`GenerateDataKey`	Sendet `GenerateDataKey` Anfragen AWS KMS zur Generierung von Datenschlüsseln zur Verschlüsselung des Pakets, wenn es intern kopiert wird.
`Decrypt`	Sendet `Decrypt` Anfragen an AWS KMS , um die verschlüsselten Datenschlüssel zu entschlüsseln, damit Sie diese zur Entschlüsselung Ihrer Daten verwenden können.

Sie können den Zugriff auf die Genehmigung jederzeit widerrufen oder den Zugriff des Services auf den vom Kunden verwalteten Schlüssel entfernen. Wenn Sie dies tun, kann OpenSearch Service nicht auf Daten zugreifen, die mit dem vom Kunden verwalteten Schlüssel verschlüsselt sind.

Dies wirkt sich auf Vorgänge aus, die von diesen Daten abhängig sind. Wenn Sie beispielsweise versuchen, ein Plugin-Paket zuzuordnen, auf das der OpenSearch Service nicht zugreifen kann, gibt der Vorgang einen `AccessDeniedException` Fehler zurück.

Einen kundenverwalteten Schlüssel erstellen

Sie können einen symmetrischen, kundenverwalteten Schlüssel erstellen, indem Sie die AWS Management Console oder die AWS KMS APIs.

Einen symmetrischen kundenverwalteten Schlüssel erstellen

- Folgen Sie den Schritten unter Erstellen eines KMS-Schlüssels im AWS Key Management Service Entwicklerhandbuch.

Schlüsselrichtlinie

Schlüsselrichtlinien steuern den Zugriff auf den vom Kunden verwalteten Schlüssel. Jeder vom Kunden verwaltete Schlüssel muss über genau eine Schlüsselrichtlinie verfügen, die aussagt, wer den Schlüssel wie verwenden kann. Wenn Sie Ihren vom Kunden verwalteten Schlüssel erstellen, können Sie eine Schlüsselrichtlinie angeben. Weitere Informationen finden Sie unter Schlüsselrichtlinien in AWS KMS im Entwicklerhandbuch für AWS Key Management Service .

Um Ihren vom Kunden verwalteten Schlüssel mit Ihren Plugin-Ressourcen zu verwenden, müssen Sie die folgenden API-Vorgänge in der Schlüsselrichtlinie zulassen:

- `kms:CreateGrant`: Fügt einem kundenverwalteten Schlüssel eine Erteilung hinzu. Gewährt Kontrollzugriff auf einen bestimmten AWS KMS Schlüssel und ermöglicht so den Zugriff auf Gewährungsvorgänge, die für benutzerdefinierte OpenSearch Servicepakete erforderlich sind. Weitere Informationen über die Verwendung von Zuweisungen finden Sie im AWS KMS Entwicklerhandbuch.

  Damit kann OpenSearch Service Folgendes tun:

  - `GenerateDataKeyWithoutPlainText`Generieren eines verschlüsselten Datenschlüssels und speichern Sie ihn für weitere Validierungen.
  - Rufen Sie `GenerateDataKey` auf, um das Plugin-Paket intern zu kopieren.
  - Rufen Sie auf`Decrypt`, um intern auf das Plugin-Paket zuzugreifen.
  - Richten Sie einen Principal ein, der in den Ruhestand geht, damit der Dienst dies tun `RetireGrant` kann.

- `kms:DescribeKey`— Stellt Details zu den vom Kunden verwalteten Schlüsseldetails bereit, damit der OpenSearch Service den Schlüssel validieren kann.
- `kms:GenerateDataKey`,`kms:GenerateDataKeyWithoutPlaintext`, `kms:Decrypt` — Gewährt dem OpenSearch Service Zugriff auf benutzerdefinierte Pakete, sodass er diese Operationen im Rahmen des Zuschusses nutzen kann.

Im Folgenden finden Sie Beispiele für Richtlinienanweisungen, die Sie für benutzerdefinierte OpenSearch Servicepakete hinzufügen können:

```
"Statement" : [
  {
    "Sid" : "Allow access to principals authorized to use OpenSearch Service custom
 packages",
    "Effect" : "Allow",
    "Principal" : {
      "AWS" : "*"
    },
    "Action" : [
      "kms:CreateGrant",
      "kms:GenerateDataKey",
      "kms:GenerateDataKeyWithoutPlaintext",
      "kms:Decrypt"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "kms:ViaService" : "custom-packages.region.amazonaws.com"
      },
      "StringEquals" : {
        "kms:EncryptionContext:packageId": "Id of the package"
      }
    }
  },
  {
    "Sid" : "Allow access to principals authorized to use Amazon OpenSearch Service
 custom packages",
    "Effect" : "Allow",
    "Principal" : {
      "AWS" : "*"
    },
    "Action" : [
```

```
      "kms:DescribeKey"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "kms:ViaService" : "custom-packages.region.amazonaws.com"
      }
    }
  }
]
```

Weitere Informationen zur Angabe von Berechtigungen in einer Richtlinie finden Sie unter Wichtige Richtlinien AWS KMS im AWS Key Management Service Entwicklerhandbuch.

Weitere Informationen zur Problembehandlung beim Zugriff auf Schlüssel finden Sie unter Problembehandlung bei AWS KMS Berechtigungen im AWS Key Management Service Entwicklerhandbuch.

Geben Sie einen vom Kunden verwalteten Schlüssel für benutzerdefinierte Amazon OpenSearch Service-Pakete an

Sie können einen vom Kunden verwalteten Schlüssel als zweite Verschlüsselungsebene für Ihre `ZIP-PLUGIN` Pakete festlegen.

Wenn Sie ein Plugin-Paket erstellen, können Sie den Datenschlüssel angeben, indem Sie eine AWS KMS Schlüssel-ID eingeben, die von den benutzerdefinierten OpenSearch Servicepaketen zum Verschlüsseln des Plugin-Pakets verwendet wird.

AWS KMS Schlüssel-ID — Eine Schlüsselkennung für einen vom AWS KMS Kunden verwalteten Schlüssel. Geben Sie eine Schlüssel-ID, einen Schlüssel-ARN, einen Alias-Namen oder einen Alias-ARN ein.

Verschlüsselungskontext für benutzerdefinierte Pakete von Amazon OpenSearch Service

Ein Verschlüsselungskontext ist ein optionaler Satz von Schlüssel-Wert-Paaren, die zusätzliche kontextbezogene Informationen zu den Daten enthalten.

AWS KMS verwendet den Verschlüsselungskontext als zusätzliche authentifizierte Daten, um die authentifizierte Verschlüsselung zu unterstützen. Wenn Sie einen Verschlüsselungskontext in eine Anforderung zur Verschlüsselung von Daten aufnehmen, AWS KMS bindet den

Verschlüsselungskontext an die verschlüsselten Daten. Zur Entschlüsselung von Daten müssen Sie denselben Verschlüsselungskontext in der Anfrage übergeben.

Verschlüsselungskontext für benutzerdefinierte Pakete von Amazon OpenSearch Service

Benutzerdefinierte Pakete von Amazon OpenSearch Service verwenden bei allen AWS KMS kryptografischen Vorgängen denselben Verschlüsselungskontext, wobei der Schlüssel `packageId` und der Wert dem `package-id` Ihres Plugin-Pakets entsprechen.

Verwenden des Verschlüsselungskontexts für die Überwachung

Wenn Sie einen symmetrischen, vom Kunden verwalteten Schlüssel verwenden, um Ihr Plugin-Paket zu verschlüsseln, können Sie den Verschlüsselungskontext in Prüfaufzeichnungen und Protokollen verwenden, um zu ermitteln, wie der vom Kunden verwaltete Schlüssel verwendet wird. Der Verschlüsselungskontext erscheint auch in Protokollen, die von AWS CloudTrail oder Amazon CloudWatch Logs generiert wurden.

Verwendung des Verschlüsselungskontextes zur Steuerung des Zugriffs auf den vom Kunden verwalteten Schlüssel

Sie können den Verschlüsselungskontext in Schlüsselrichtlinien und IAM-Richtlinien als Bedingungen verwenden, um den Zugriff auf Ihren symmetrischen, vom Kunden verwalteten Schlüssel zu kontrollieren. Sie können Verschlüsselungskontext-Einschränkungen auch in einer Genehmigung verwenden.

OpenSearch Benutzerdefinierte Servicepakete verwenden eine Einschränkung des Verschlüsselungskontextes bei Zuweisungen, um den Zugriff auf den vom Kunden verwalteten Schlüssel in Ihrem Konto oder Ihrer Region zu steuern. Eine Genehmigungseinschränkung erfordert, dass durch die Genehmigung ermöglichte Vorgänge den angegebenen Verschlüsselungskontext verwenden.

Im Folgenden finden Sie Beispiele für Schlüsselrichtlinienanweisungen zur Gewährung des Zugriffs auf einen vom Kunden verwalteten Schlüssel für einen bestimmten Verschlüsselungskontext. Die Bedingung in dieser Richtlinienanweisung setzt voraus, dass die Genehmigungen eine Einschränkung des Verschlüsselungskontextes haben, die den Verschlüsselungskontext spezifiziert.

```
{
    "Sid": "Enable DescribeKey",
    "Effect": "Allow",
    "Principal": {
```

```
        "AWS": "arn:aws:iam::111122223333:role/ExampleReadOnlyRole"
    },
    "Action": "kms:DescribeKey",
    "Resource": "*"
},
{
    "Sid": "Enable OpenSearch Service custom packages to use the key",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/ExampleReadOnlyRole"
    },
    "Action" : [
         "kms:CreateGrant",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals" : {
            "kms:EncryptionContext:packageId": "ID of the package"
         }
    }
}
```

Überwachen von Verschlüsselungsschlüsseln für den OpenSearch benutzerdefinierten Paketservice

Wenn Sie einen vom AWS KMS Kunden verwalteten Schlüssel zusammen mit Ihren OpenSearch Serviceressourcen für benutzerdefinierte Pakete verwenden, können Sie CloudTrail oder CloudWatch Logs verwenden, um Anfragen nachzuverfolgen, an die OpenSearch benutzerdefinierte Pakete gesendet AWS KMS werden.

Weitere Informationen

Die folgenden Ressourcen enthalten weitere Informationen zur Datenverschlüsselung im Ruhezustand:

- Weitere Informationen zu AWS KMS grundlegenden Konzepten finden Sie AWS KMS keysim AWS Key Management Service Entwicklerhandbuch.
- Weitere Informationen zu bewährten Sicherheitsmethoden für AWS KMS finden Sie im AWS Prescriptive Guidance Guide mit AWS Key Management Service bewährten Methoden.

Installation von Drittanbieter-Plugins in Amazon OpenSearch Service

Amazon OpenSearch Service unterstützt Drittanbieter-Plug-ins von ausgewählten Partnern. Diese Plugins können Ihr OpenSearch Setup um zusätzliche Funktionen wie benutzerdefinierte Analysatoren, Tokenizer oder Verschlüsselungsfunktionen erweitern. Folgen Sie den spezifischen Installations- und Konfigurationsanweisungen der Drittanbieter, um eine ordnungsgemäße Integration mit Ihrer Service-Domain sicherzustellen. OpenSearch

> **Note**
>
> Sie müssen gültige Lizenzen direkt von den Drittanbietern erwerben und verwalten. Einige Anbieter aktivieren ihre Plugins möglicherweise nicht vollständig AWS-Regionen. Erkundigen Sie sich daher beim Plugin-Anbieter nach der Verfügbarkeit.

Die folgenden Drittanbieter-Plugins sind für die Verwendung mit OpenSearch Service verfügbar:

- Portal26-Verschlüsselungs-Plugin (Titanium-Lockbox) — Verwendet NIST FIPS 140-2-zertifizierte Verschlüsselung, um Daten so zu verschlüsseln, wie sie indexiert sind. Es bietet Unterstützung für Bring Your Own Key (BYOK), mit der Sie Ihre Verschlüsselungsschlüssel verwalten können, um die Sicherheit zu erhöhen. Das Plugin wird von Portal26 bereitgestellt und erfordert OpenSearch Version 2.15 oder höher.
- Name Match (RNI) — Stimmt mit Namen, Organisationen, Adressen und Daten in über 24 Sprachen überein, was die Sicherheit und die Einhaltung von Vorschriften verbessert. Das Plugin wird von Babel Street bereitgestellt und benötigt OpenSearch Version 2.15 oder höher.

Themen

- Voraussetzungen
- Installieren von Plugins von Drittanbietern
- Nächste Schritte

Voraussetzungen

Bevor Sie ein Drittanbieter-Plugin installieren, führen Sie die folgenden Schritte aus:

- Die Plugin-Konfiguration und die Lizenzdateien wurden abgerufen und in einen Amazon-S3-Bucket hochgeladen. Der Bucket muss sich in derselben AWS-Region -Domäne befinden.

- Ein Drittanbieter-Plugin ist eine Art von benutzerdefiniertem Plugin. Stellen Sie sicher, dass die Domain die Voraussetzungen für benutzerdefinierte Plugins erfüllt.

Installieren von Plugins von Drittanbietern

Um ein Drittanbieter-Plugin mit einer OpenSearch Service-Domain zu verknüpfen, müssen Sie zunächst drei separate Pakete hochladen: das Lizenzpaket, das Konfigurationspaket und das Plugin-Paket.

- Das Lizenzpaket enthält die Lizenzinformationen oder Metadaten, die mit dem Plugin verknüpft sind, im Format.json oder .xml.
- Das Konfigurationspaket enthält die Plugin-Konfigurationsdateien sowie unterstützende Ressourcen und Einstellungen. Diese Dateien definieren, wie sich das Plugin verhält oder wie es integriert OpenSearch wird.
- Das Plugin-Paket enthält die kompilierte Plugin-Binärdatei, d. h. den ausführbaren Code, der OpenSearch ausgeführt wird. Dies ist der Kern der Plugin-Funktionalität.

Nachdem Sie beide Pakete hochgeladen haben, können Sie das Plugin und die Lizenz einer kompatiblen Domain zuordnen.

Konsole

Um einer Domain ein Drittanbieter-Plugin zuzuordnen, importieren Sie zunächst die Plugin-Lizenz und die Konfiguration als Pakete.

So installieren Sie ein Plugin eines Drittanbieters:

1. Melden Sie sich zu https://console.aws.amazon.com/aos/Hause bei der Amazon OpenSearch Service-Konsole an.
2. Wählen Sie im linken Navigationsbereich Packages aus.
3. Importieren Sie zunächst das Lizenzpaket. Klicken Sie auf Packet importieren.
4. Wählen Sie als Pakettyp die Option Lizenz aus.
5. Geben Sie als Paketquelle den Pfad zur Lizenz-JSON- oder XML-Datei in Amazon S3 ein.
6. Wählen Sie Importieren aus. Das Paket wird auf der Seite Pakete auf der Registerkarte Lizenzen angezeigt.
7. Importieren Sie jetzt die Plugin-Konfiguration. Wählen Sie erneut Paket importieren.

8. Wählen Sie als Pakettyp die Option Konfiguration aus.
9. Geben Sie als Paketquelle den Pfad zur Plugin-Konfigurations-ZIP-Datei in Amazon S3 ein.
10. Wählen Sie Importieren aus.
11. Importieren Sie abschließend das Plugin selbst. Klicken Sie auf Packet importieren.
12. Wählen Sie als Pakettyp die Option Plugin aus.
13. Geben Sie Package Paketquelle den Pfad zur Plugin-ZIP-Datei in Amazon S3 ein.
14. Wählen Sie die OpenSearch Engine-Version aus, die das Plugin unterstützt.
15. Wählen Sie Importieren aus.

Um ein Drittanbieter-Plugin mit einer Domain zu verknüpfen

1. Ordnen Sie nun die Plugin-Lizenz und die Konfiguration der Domain zu. Wählen Sie im linken Navigationsbereich die Option Domains aus.
2. Wählen Sie den Namen der Domäne, um deren Clusterkonfiguration zu öffnen.
3. Navigieren Sie zur Registerkarte Plugins.
4. Wählen Sie Pakete zuordnen und wählen Sie die Plugin-, Lizenz- und Konfigurationspakete aus, die Sie gerade importiert haben.
5. Wählen Sie Select (Auswählen).
6. Wählen Sie Weiter aus. Prüfen Sie die Pakete, die Sie verknüpfen möchten, und wählen Sie Associate aus.

CLI

Verwenden Sie zunächst den Befehl create-package, um ein neues Paket zu erstellen, das die Plugin-Lizenz enthält. Sie `S3Key` müssen auf eine .json- oder .xml-Datei in Amazon S3 verweisen, die den Lizenztext oder die Metadaten enthält.

```
aws opensearch create-package \
  --package-name plugin-license-package \
  --package-type PACKAGE-LICENSE \
  --package-source S3BucketName=my-bucket,S3Key=licenses/my-plugin-license.json
```

Verwenden Sie erneut den Befehl create-package, um ein Paket zu erstellen, das die Plugin-Konfiguration enthält. Sie `S3Key` müssen auf eine .zip-Datei in Amazon S3 verweisen, die der vom Plugin erwarteten Verzeichnisstruktur entspricht.

```
aws opensearch create-package \
  --package-name plugin-config-package \
  --package-type PACKAGE-CONFIG \
  --package-source S3BucketName=my-bucket,S3Key=path/to/package.zip
```

Verwenden Sie erneut den Befehl create-package, um ein Paket zu erstellen, das das Plugin selbst enthält. Sie S3Key müssen auf die .zip -Datei des Plug-ins in Amazon S3 verweisen.

```
aws opensearch create-package \
  --package-name plugin-package \
  --package-type ZIP-PLUGIN \
  --package-source S3BucketName=my-bucket,S3Key=path/to/package.zip
```

Verwenden Sie abschließend den Befehl associate-package, um das Partner-Plugin, die Lizenz und die Konfiguration mit einer kompatiblen Domain zu verknüpfen, indem Sie jeweils das Paket IDs angeben. Geben Sie die Plugin-ID als Voraussetzung für die anderen Pakete an, was bedeutet, dass sie der Domain vor den anderen Paketen zugeordnet werden muss.

```
aws opensearch associate-packages \
  --domain-name my-domain \
  --package-list '[{"PackageID": "plugin-package-id"},{"PackageID": "license-package-id","PrerequisitePackageIDList":["plugin-package-id"]},{"PackageID":"config-package-id","PrerequisitePackageIDList":["plugin-package-id"]}]'
```

Nächste Schritte

Wenn die Zuordnung abgeschlossen ist, können Sie das Plugin für bestimmte Indizes aktivieren oder es nach Bedarf entsprechend Ihren Anforderungen konfigurieren. Um Plugin-Funktionen von Drittanbietern auf bestimmte Indizes anzuwenden, ändern Sie die Indexeinstellungen während der Indexerstellung oder aktualisieren Sie bestehende Indizes. Wenn Ihr Drittanbieter-Plugin beispielsweise einen benutzerdefinierten Analyzer enthält, verweisen Sie in den Indexeinstellungen darauf.

Verwenden Sie Indexvorlagen, die die Plugin-Konfigurationen enthalten, um die Plugin-Funktionen konsistent auf mehrere Indizes anzuwenden. Konsultieren Sie immer die Plugin-Dokumentation, um zu erfahren, wie Sie die Funktionen für Ihr OpenSearch Setup konfigurieren können.

Abfragen Ihrer Amazon OpenSearch Service-Daten mit SQL

Sie können SQL verwenden, um Ihren Amazon OpenSearch Service abzufragen, anstatt die JSON-basierte OpenSearch Abfrage DSL zu verwenden. Abfragen mit SQL sind nützlich, wenn Sie bereits mit der Sprache vertraut sind oder Ihre Domain in eine Anwendung integrieren möchten, die sie verwendet. SQL-Unterstützung ist in Domänen verfügbar, in denen Elasticsearch ab Version 6.5 ausgeführt OpenSearch wird.

> **Note**
>
> Diese Dokumentation beschreibt die Versionskompatibilität zwischen OpenSearch Service und verschiedenen Versionen des SQL-Plug-ins sowie des JDBC- und ODBC-Treibers. Informationen zur Syntax für grundlegende und komplexe Abfragen, Funktionen, Metadatenabfragen und Aggregatfunktionen finden Sie in der OpenSearchOpen-Source-Dokumentation.

Verwenden Sie die folgende Tabelle, um die Version des SQL-Plugins zu finden, die von den einzelnen OpenSearch Elasticsearch-Versionen unterstützt wird.

OpenSearch

OpenSearch Version	SQL-Plug-In-Version	Bemerkenswerte Funktionen
2.19.0	2.19.0.0	
2.18.0	2.18.0.0	
2.17.0	2.17.0.0	
2.15.0	2.15.0.0	
2.13.0	2.13.0.0	
2.11.0	2.11.0.0	Unterstützung für PPL-Sprache und Abfragen hinzufügen
2.9.0	2.9.0.0	Spark-Konnektor hinzufügen und Tabellen- und PromQL-Funktionen unterstützen

OpenSearch Version	SQL-Plug-In-Version	Bemerkenswerte Funktionen
2.7.0	2.7.0.0	API hinzufügen `datasource`
2.5.0	2.5.0.0	
2.3.0	2.3.0.0	Hinzufügen von `maketime`- und `makedate`-Datum- und Uhrzeit-Funktionen
1.3.0	1.3.0.0	Support für standardmäßige Abfragelimitgröße und IN-Klausel zur Auswahl innerhalb einer Werteliste
1.2.0	1.2.0.0	Neues Protokoll für das Visualisierungs-Antwortformat hinzugefügt.
1.1.0	1.1.0.0	Match-Funktion als Filter in SQL und PPL wird unterstützt
1.0.0	1.0.0.0	Support von Abfragen eines Datenstroms

Open Distro für Elasticsearch

Elasticsearch Version	SQL-Plug-In-Version	Bemerkenswerte Funktionen
710	1,13,0	NULL FIRST und LAST für Fensterfunktionen, CAST () - Funktion, SHOW- und DESCRIBE-Befehle
7.9	1.11.0	Zusätzliche Datums-/Uhrzeitfunktionen hinzufügen, ORDER BY-Schlüsselwort
7.8	1.9.0	
7.7	1.8.0	
7.3	1.3.0	Mehrere Zeichenfolgen- und Zahlenoperatoren
7.1	1.1.0	

Beispielaufruf

Um Ihre Daten mit SQL abzufragen, senden Sie HTTP-Anforderungen im folgenden Format an `_sql`:

```
POST domain-endpoint/_plugins/_sql
{
  "query": "SELECT * FROM my-index LIMIT 50"
}
```

> **Note**
>
> Wenn auf Ihrer Domain Elasticsearch statt ausgeführt wird OpenSearch, lautet `_opendistro/_sql` das Format.

Hinweise und Unterschiede

Aufrufe an `_plugins/_sql` enthalten Indexnamen im Anforderungstext, es gelten also die gleichen Überlegungen zur Zugriffsrichtlinie wie bei den Operationen bulk, mget und msearch. Befolgen Sie wie immer das Prinzip der geringsten Rechte wenn Sie API-Operationen Berechtigungen erteilen.

Sicherheitsüberlegungen bezüglich der Verwendung von SQL mit differenzierter Zugriffskontrolle finden Sie unter Differenzierte Zugriffskontrolle in the section called “Differenzierte Zugriffskontrolle”.

Das OpenSearch SQL-Plugin enthält viele einstellbare Einstellungen. Verwenden Sie im OpenSearch Service den `_cluster/settings` Pfad, nicht den Pfad der Plugin-Einstellungen (`_plugins/_query/settings`):

```
PUT _cluster/settings
{
  "transient" : {
    "plugins.sql.enabled" : true
  }
}
```

Ersetzen Sie für ältere Elasticsearch-Domains `plugins` mit `opendistro`:

```
PUT _cluster/settings
{
  "transient" : {
```

```
    "opendistro.sql.enabled" : true
  }
}
```

SQL Workbench

Die SQL Workbench ist eine OpenSearch Dashboards-Benutzeroberfläche, mit der Sie SQL-Abfragen On-Demand ausführen, SQL in sein REST-Äquivalent übersetzen und Ergebnisse anzeigen und als Text, JSON, JDBC oder CSV speichern können. Weitere Informationen finden Sie unter Workbench abfragen.

SQL CLI

SQL-CLI ist eine eigenständige Python-Anwendung, die Sie mit dem Befehl `opensearchsql` starten können. Schritte zum Installieren, Konfigurieren und Verwenden finden Sie unter SQL CLI.

JDBC-Treiber

Der JDBC (Java Database Connectivity) -Treiber ermöglicht das Integrieren von OpenSearch Service-Domänen mit den gewünschten BI (Business Intelligence) -Anwendungen. Um den Treiber herunterzuladen, klicken Sie hier. Weitere Informationen finden Sie im Abschnitt GitHubRepository.

ODBC-Treiber

Der Open Database Connectivity (ODBC) -Treiber ist ein schreibgeschützter ODBC-Treiber für Windows und macOS, mit dem Sie Business Intelligence- und Datenvisualisierungsanwendungen wie Microsoft Excel mit dem SQL-Plugin verbinden können.

Sie können ein Beispiel für eine funktionierende Treiberdatei auf der Seite mit den Artefakten herunterladen. OpenSearch Weitere Informationen zur Installation des Treibers finden Sie im Abschnitt SQL-Repository unter GitHub

k-NN-Suche (k-Nearest Neighbor) in Amazon Service OpenSearch

Mit k-NN für Amazon OpenSearch Service können Sie nach Punkten in einem Vektorraum suchen und die nächsten Nachbarn für diese Punkte anhand des euklidischen Abstands oder der Kosinusähnlichkeit finden. Anwendungsfälle umfassen Empfehlungen (z. B. eine Funktion „andere Songs, die Ihnen vielleicht gefallen“ in einer Musikanwendung), Bilderkennung und Betrugserkennung.

> **Note**
>
> Diese Dokumentation bietet einen kurzen Überblick über das k-NN-Plug-In sowie die Einschränkungen bei der Verwendung des Plug-ins mit Managed Service. OpenSearch Eine umfassende Dokumentation des k-NN-Plug-ins, einschließlich einfacher und komplexer Beispiele, Parameterreferenzen und der vollständigen API-Referenz, finden Sie in der OpenSearch Open-Source-Dokumentation. Die Open-Source-Dokumentation behandelt auch Leistungsoptimierung und k-NN-specific Cluster-Einstellungen.

Erste Schritte mit k-NN

Um k-NN zu verwenden, müssen Sie einen Index mit der `index.knn`-Einstellung erstellen und mindestens ein Feld des `knn_vector`-Datentyps hinzufügen.

```
PUT my-index

{
  "settings": {
    "index.knn": true
  },
  "mappings": {
    "properties": {
      "my_vector1": {
        "type": "knn_vector",
        "dimension": 2
      },
      "my_vector2": {
        "type": "knn_vector",
        "dimension": 4
      }
    }
  }
}
```

Der `knn_vector`-Datentyp unterstützt eine einzelne Liste von bis zu 10.000 Gleitkommazahlen, wobei die Anzahl der Gleitkommazahlen durch den erforderlichen `dimension`-Parameter definiert wird. Nachdem Sie den Index erstellt haben, fügen Sie ihm einige Daten hinzu.

```
POST _bulk
```

```
{ "index": { "_index": "my-index", "_id": "1" } }
{ "my_vector1": [1.5, 2.5], "price": 12.2 }
{ "index": { "_index": "my-index", "_id": "2" } }
{ "my_vector1": [2.5, 3.5], "price": 7.1 }
{ "index": { "_index": "my-index", "_id": "3" } }
{ "my_vector1": [3.5, 4.5], "price": 12.9 }
{ "index": { "_index": "my-index", "_id": "4" } }
{ "my_vector1": [5.5, 6.5], "price": 1.2 }
{ "index": { "_index": "my-index", "_id": "5" } }
{ "my_vector1": [4.5, 5.5], "price": 3.7 }
{ "index": { "_index": "my-index", "_id": "6" } }
{ "my_vector2": [1.5, 5.5, 4.5, 6.4], "price": 10.3 }
{ "index": { "_index": "my-index", "_id": "7" } }
{ "my_vector2": [2.5, 3.5, 5.6, 6.7], "price": 5.5 }
{ "index": { "_index": "my-index", "_id": "8" } }
{ "my_vector2": [4.5, 5.5, 6.7, 3.7], "price": 4.4 }
{ "index": { "_index": "my-index", "_id": "9" } }
{ "my_vector2": [1.5, 5.5, 4.5, 6.4], "price": 8.9 }
```

Dann können Sie die Daten mit dem knn-Abfragetyp durchsuchen.

```
GET my-index/_search
{
  "size": 2,
  "query": {
    "knn": {
      "my_vector2": {
        "vector": [2, 3, 5, 6],
        "k": 2
      }
    }
  }
}
```

In diesem Fall ist k die Anzahl der Nachbarn, die die Abfrage zurückgeben soll, aber Sie müssen auch die `size`-Option einschließen. Andernfalls erhalten Sie k-Ergebnisse für jeden Shard (und jedes Segment) anstatt k-Ergebnisse für die gesamte Abfrage. k-NN unterstützt einen maximalen k-Wert von 10 000.

Wenn Sie die knn-Abfrage mit anderen Klauseln mischen, erhalten Sie möglicherweise weniger als k-Ergebnisse. In diesem Beispiel reduziert die `post_filter`-Klausel die Anzahl der Ergebnisse von 2 auf 1.

```
GET my-index/_search

{
  "size": 2,
  "query": {
    "knn": {
      "my_vector2": {
        "vector": [2, 3, 5, 6],
        "k": 2
      }
    }
  },
  "post_filter": {
    "range": {
      "price": {
        "gte": 6,
        "lte": 10
      }
    }
  }
}
```

Wenn Sie eine große Anzahl von Abfragen bearbeiten und gleichzeitig eine optimale Leistung beibehalten müssen, können Sie die `_msearch`API verwenden, um eine Massensuche mit JSON zu erstellen und eine einzige Anfrage zu senden, um mehrere Suchen durchzuführen:

```
GET _msearch

{ "index": "my-index"}
{ "query": { "knn": {"my_vector2":{"vector": [2, 3, 5, 6],"k":2 }} } }
{ "index": "my-index", "search_type": "dfs_query_then_fetch"}
{ "query": { "knn": {"my_vector1":{"vector": [2, 3],"k":2 }} } }
```

Das folgende Video veranschaulicht, wie Sie eine Bulk-Vektorsuche für K-NN-Abfragen einrichten.

k-NN-Unterschiede, -Optimierung und -Einschränkungen

OpenSearch ermöglicht es Ihnen, alle k-NN-Einstellungen mithilfe der `_cluster/settings` API zu ändern. Bei OpenSearch Service können Sie alle Einstellungen außer `knn.memory.circuit_breaker.enabled` und ändern`knn.circuit_breaker.triggered`. k-NN-Statistiken sind als Amazon-Statistiken enthalten CloudWatch .

Vergleichen Sie insbesondere die `KNNGraphMemoryUsage` Metrik auf jedem Datenknoten mit der `knn.memory.circuit_breaker.limit` Statistik und dem verfügbaren RAM für den Instance-Typ. OpenSearch Der Service verwendet die Hälfte des RAM einer Instance für den Java-Heap bis zu einer Heap-Größe von 32 GiB. Standardmäßig verwendet KNN bis zu 50 % der verbleibenden Hälfte, sodass ein Instance-Typ mit 32 GiB RAM 8 GiB an Graphen (32 * 0,5 * 0,5) aufnehmen kann. Die Leistung kann beeinträchtigt werden, wenn die Nutzung des Graphen-Speichers diesen Wert überschreitet.

Sie können einen in Version 2.x oder höher erstellten k-NN-Index zu oder Cold Storage auf einer Domain mit Version 2.17 UltraWarmoder höher migrieren.

Clear-Cache-API und Warmup-APIs für k-NN-Indizes sind für warme Indizes blockiert. Wenn die erste Abfrage für den Index initiiert wird, werden die Grafikdateien von Amazon S3 heruntergeladen und das Diagramm in den Speicher geladen. In ähnlicher Weise werden die Dateien automatisch aus dem Speicher entfernt, wenn die TTL für die Graphen abgelaufen ist.

Clusterübergreifende Suche in Amazon Service OpenSearch

Mit der clusterübergreifenden Suche in Amazon OpenSearch Service können Sie Abfragen und Aggregationen über mehrere verbundene Domains hinweg durchführen. Es ist oft sinnvoller, mehrere kleinere Domänen anstelle einer einzigen großen Domäne zu verwenden, insbesondere wenn Sie verschiedene Arten von Workloads ausführen.

Mit Workload-spezifischen Domänen können Sie die folgenden Aufgaben ausführen:

- Optimieren Sie jede Domäne durch die Auswahl von Instance-Typen für bestimmte Workloads.
- Richten Sie Grenzen für die Fehlerisolierung über Workloads hinweg ein. Dies bedeutet, dass, wenn einer Ihrer Workloads fehlschlägt, der Fehler in dieser bestimmten Domäne bleibt und sich nicht auf Ihre anderen Workloads auswirkt.
- Skalieren Sie einfacher über Domänen hinweg.

Die clusterübergreifende Suche unterstützt OpenSearch Dashboards, sodass Sie Visualisierungen und Dashboards für alle Ihre Domains erstellen können. Sie zahlen die Standardgebühren für die AWS Datenübertragung für Suchergebnisse, die zwischen Domains übertragen werden.

> **Note**
>
> Open Source bietet OpenSearch auch Dokumentation für die clusterübergreifende Suche. Die Einrichtung unterscheidet sich für Open-Source-Cluster erheblich von denen für verwaltete Amazon OpenSearch Service-Domains. Vor allem konfigurieren Sie in OpenSearch Service clusterübergreifende Verbindungen mit der und AWS Management Console nicht mit cURL. Darüber hinaus verwendet der verwaltete Dienst AWS Identity and Access Management (IAM) für die clusterübergreifende Authentifizierung zusätzlich zur detaillierten Zugriffskontrolle. Daher empfehlen wir, diese Dokumentation und nicht die OpenSearch Open-Source-Dokumentation zu verwenden, um die clusterübergreifende Suche für Ihre Domains zu konfigurieren.

Themen

- Einschränkungen
- Voraussetzungen für die Cluster-übergreifende Suche
- Cluster-übergreifende Suche – Preise
- Einrichten einer Verbindung
- Entfernen einer Verbindung
- Einrichten von Sicherheit und Beispiel-Walkthrough-Anleitungen
- OpenSearch Dashboards

Einschränkungen

Die Cluster-übergreifende Suche hat mehrere wichtige Einschränkungen:

- Sie können eine Elasticsearch-Domain nicht mit einer OpenSearch Domain verbinden.
- Sie können keine Verbindung zu selbstverwalteten OpenSearch/Elasticsearch Clustern herstellen.
- Um Domains regionsübergreifend zu verbinden, müssen sich beide Domains auf Elasticsearch 7.10 oder höher oder befinden. OpenSearch

- Eine Domäne kann maximal 20 ausgehende Verbindungen haben. Ebenso kann eine Domäne maximal 20 eingehende Verbindungen haben. Mit anderen Worten, eine Domäne kann sich mit maximal 20 anderen Domänen verbinden.
- Die Quelldomain muss sich in derselben oder einer höheren Version als die Zieldomain befinden. Wenn Sie eine bidirektionale Verbindung zwischen zwei Domänen einrichten und eine oder beide aktualisieren möchten, müssen Sie zuerst eine der Verbindungen löschen.
- Sie können keine benutzerdefinierten Wörterbücher oder SQL mit Cluster-übergreifender Suche verwenden.
- Sie können es nicht verwenden AWS CloudFormation , um Domänen zu verbinden.
- Sie können die Cluster-übergreifende Suche auf M3- oder (T2 und T3) Burstable Instances nicht verwenden.

Voraussetzungen für die Cluster-übergreifende Suche

Bevor Sie die Cluster-übergreifende Suche einrichten, stellen Sie sicher, dass Ihre Domänen die folgenden Anforderungen erfüllen:

- Zwei OpenSearch Domains oder Elasticsearch-Domains in Version 6.7 oder höher
- Differenzierte Zugriffskontrolle aktiviert
- Node-to-node Verschlüsselung aktiviert

Cluster-übergreifende Suche – Preise

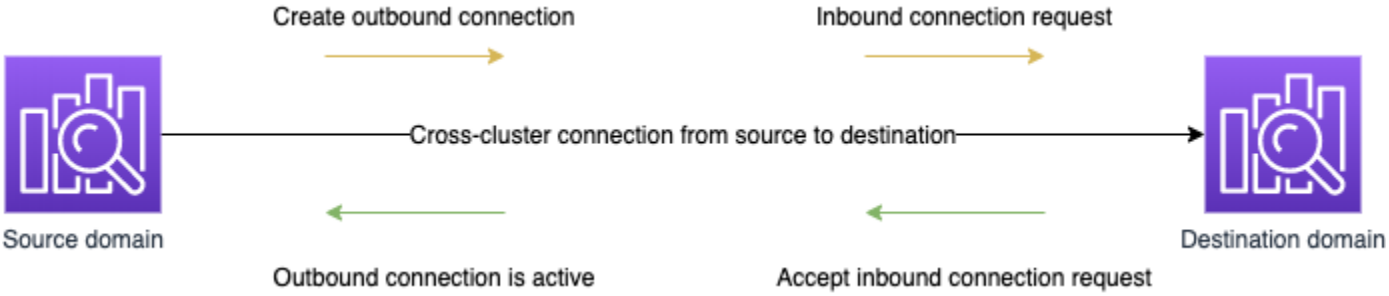
Für die Suche über Domänen hinweg fallen keine zusätzlichen Gebühren an.

Einrichten einer Verbindung

Die Domäne „Quelle“ bezieht sich auf die Domäne, von der eine Cluster-übergreifende Suchabfrage stammt. Mit anderen Worten, die Quelldomäne ist diejenige, an die Sie die erste Suchabfrage senden.

Die Domäne „Ziel“ ist die Domäne, die die Quelldomäne abfragt.

Eine Cluster-übergreifende Verbindung ist unidirektional von der Quelle zur Zieldomäne. Dies bedeutet, dass die Zieldomäne die Quelldomäne nicht abfragen kann. Sie können jedoch eine andere Verbindung in die entgegengesetzte Richtung einrichten.



Die Quelldomäne erstellt eine „ausgehende“ Verbindung zur Zieldomäne. Die Zieldomäne empfängt eine „eingehende“ Verbindungsanforderung von der Quelldomäne.

So richten Sie eine Verbindung ein

1. Wählen Sie im Domänen-Dashboard eine Domäne und anschließend die Registerkarte Verbindungen aus.
2. Wählen Sie im Abschnitt Ausgehende Verbindungen die Option Anforderung.
3. Geben Sie unter Verbindungs-Alias einen Namen für die Verbindung ein.
4. Wählen Sie, ob Sie eine Verbindung zu einer Domain in Ihrer AWS-Konto Region oder zu einem anderen Konto oder einer anderen Region herstellen möchten.
   - Um eine Verbindung zu einem Cluster in Ihrer Region AWS-Konto und Ihrer Region herzustellen, wählen Sie die Domain aus dem Drop-down-Menü aus und wählen Sie Request aus.
   - Um eine Verbindung zu einem Cluster in einer anderen Region AWS-Konto oder Region herzustellen, wählen Sie den ARN der Remotedomäne aus und wählen Sie Request. Um Domains regionsübergreifend zu verbinden, müssen auf beiden Domains Elasticsearch Version 7.10 oder höher oder ausgeführt werden. OpenSearch
5. Um nicht verfügbare Cluster für Cluster-Abfragen zu überspringen, wählen Sie Skip unavailable aus. Diese Einstellung stellt sicher, dass Ihre clusterübergreifenden Abfragen trotz Ausfällen auf einem oder mehreren Remoteclustern Teilergebnisse zurückgeben.
6. Die Cluster-übergreifende Suche überprüft zuerst die Verbindungsanforderung, um sicherzustellen, dass die Voraussetzungen erfüllt sind. Wenn die Domänen inkompatibel sind, wechselt die Verbindungsanforderung in den Status `Validation failed`.
7. Nachdem die Verbindungsanforderung erfolgreich validiert wurde, wird sie an die Zieldomäne gesendet, wo sie genehmigt werden muss. Bis diese Genehmigung erfolgt, bleibt die Verbindung im Status `Pending acceptance`. Wenn die Verbindungsanforderung in der Zieldomäne

akzeptiert wird, ändert sich der Status in `Active` und die Zieldomäne steht für Abfragen zur Verfügung.

- Auf der Domänenseite werden die allgemeinen Domänenintegritäts- und Instance-Integritätsdetails Ihrer Zieldomäne angezeigt. Nur Domänenbesitzer haben die Flexibilität, Verbindungen zu oder von ihren Domänen zu erstellen, anzuzeigen, zu entfernen und zu überwachen.

Nachdem die Verbindung hergestellt wurde, wird jeder Datenverkehr, der zwischen den Knoten der verbundenen Domänen fließt, verschlüsselt. Wenn Sie eine VPC-Domäne mit einer Nicht-VPC-Domäne verbinden und die Nicht-VPC-Domäne ein öffentlicher Endpunkt ist, der Datenverkehr aus dem Internet empfangen kann, ist der Cluster-übergreifende Datenverkehr zwischen den Domänen immer noch verschlüsselt und sicher.

Entfernen einer Verbindung

Durch das Entfernen einer Verbindung werden alle clusterübergreifenden Operationen an ihren Indizes gestoppt.

1. Wählen Sie im Domänen-Dashboard die Registerkarte Verbindungen aus.
2. Wählen Sie die Domänenverbindungen aus, die Sie entfernen möchten und klicken Sie auf Löschen, um den Löschvorgang zu bestätigen.

Sie können diese Schritte entweder in der Quell- oder der Zieldomäne ausführen, um die Verbindung zu entfernen. Nachdem Sie die Verbindung entfernt haben, ist sie noch 15 Tage lang mit einem `Deleted`-Status sichtbar.

Sie können eine Domäne mit aktiven Cluster-übergreifenden Verbindungen nicht löschen. Um eine Domäne zu löschen, entfernen Sie zuerst alle eingehenden und ausgehenden Verbindungen aus dieser Domäne. Damit stellen Sie sicher, dass Sie die Benutzer der Cluster-übergreifenden Domäne berücksichtigen, bevor Sie die Domäne löschen.

Einrichten von Sicherheit und Beispiel-Walkthrough-Anleitungen

1. Sie senden eine Cluster-übergreifende Suchabfrage an die Quelldomäne.
2. Die Quelldomäne wertet diese Anforderung anhand ihrer Domänenzugriffsrichtlinie aus. Da die Cluster-übergreifende Suche eine differenzierte Zugriffskontrolle erfordert, wird eine Open-Access-Richtlinie für die Quelldomäne empfohlen.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "*"
        ]
      },
      "Action": [
        "es:ESHttp*"
      ],
      "Resource": "arn:aws:es:region:account:domain/src-domain/*"
    }
  ]
}
```

> **Note**
>
> Wenn Sie Remote-Indizes in den Pfad einbeziehen, müssen Sie den URI im Domänen-ARN URL-codieren. Verwenden Sie beispielsweise `arn:aws:es:us-east-1:123456789012:domain/my-domain/local_index,dst%3Aremote_index` anstelle von `arn:aws:es:us-east-1:123456789012:domain/my-domain/local_index,dst:remote_index`.

Wenn Sie zusätzlich zur differenzierten Zugriffskontrolle eine restriktive Zugriffsrichtlinie verwenden möchten, muss Ihre Richtlinie mindestens den Zugriff auf `es:ESHttpGet` zulassen.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::123456789012:user/test-user"
        ]
      },
      "Action": "es:ESHttpGet",
      "Resource": "arn:aws:es:region:account:domain/src-domain/*"
    }
  ]
}
```

3. Die differenzierte Zugriffskontrolle für die Quelldomäne wertet die Anforderung aus:

   - Ist die Anforderung mit gültigen IAM- oder HTTP-Basisanmeldeinformationen signiert?
   - Ist dies der Fall, hat der Benutzer die Berechtigung, die Suche durchzuführen und auf die Daten zuzugreifen?

   Wenn die Anforderung nur Daten in der Zieldomäne durchsucht (z. B. `dest-alias:dest-index/_search`), benötigen Sie nur Berechtigungen für die Zieldomäne.

   Wenn die Anforderung Daten in beiden Domänen durchsucht (z. B. `source-index,dest-alias:dest-index/_search`), benötigen Sie Berechtigungen für beide Domänen.

   Bei der detaillierten Zugriffskontrolle müssen Benutzer zusätzlich zu den Standard `read` - oder `search` Berechtigungen für die `indices:admin/shards/search_shards` entsprechenden Indizes auch über die entsprechenden Berechtigungen verfügen.

4. Die Quelldomäne übergibt die Anforderung an die Zieldomäne. Die Zieldomäne wertet diese Anforderung anhand ihrer Domänenzugriffsrichtlinie aus. Sie müssen die `es:ESCrossClusterGet`-Berechtigung für die Zieldomäne angeben:

   JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
```

```
        "AWS": "*"
      },
      "Action": "es:ESCrossClusterGet",
      "Resource": "arn:aws:es:region:account:domain/dst-domain"
    }
  ]
}
```

Stellen Sie sicher, dass die `es:ESCrossClusterGet`-Berechtigung auf `/dst-domain` und nicht `/dst-domain/*` angewendet wird.

Diese Mindestrichtlinie erlaubt jedoch nur Cluster-übergreifende Suchvorgänge. Wenn Sie andere Operationen ausführen möchten, z. B. das Indizieren von Dokumenten und das Durchführen von Standardsuchvorgängen, benötigen Sie zusätzliche Berechtigungen. Wir empfehlen die folgende Richtlinie für die Zieldomäne:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "*"
        ]
      },
      "Action": [
        "es:ESHttp*"
      ],
      "Resource": "arn:aws:es:region:account:domain/dst-domain/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": "es:ESCrossClusterGet",
      "Resource": "arn:aws:es:region:account:domain/dst-domain"
    }
```

```
  ]
}
```

> **Note**
>
> Alle clusterübergreifenden Suchanfragen zwischen Domänen werden bei der Übertragung standardmäßig als Teil der Verschlüsselung verschlüsselt. node-to-node

5. Die Zieldomäne führt die Suche durch und gibt die Ergebnisse an die Quelldomäne zurück.
6. Die Quelldomäne kombiniert ihre eigenen Ergebnisse (falls vorhanden) mit den Ergebnissen der Zieldomäne und gibt sie an Sie zurück.
7. Wir empfehlen Postman für Testanfragen:

   - Indizieren Sie in der Zieldomäne ein Dokument:

   ```
   POST https://dst-domain.us-east-1.es.amazonaws.com/books/_doc/1

   {
     "Dracula": "Bram Stoker"
   }
   ```

   - Wenn Sie diesen Index von der Quelldomäne abfragen möchten, fügen Sie den Verbindungsalias der Zieldomäne in die Abfrage ein.

   ```
   GET https://src-domain.us-east-1.es.amazonaws.com/<connection_alias>:books/
   _search

   {
       ...
     "hits": [
       {
         "_index": "source-destination:books",
         "_type": "_doc",
         "_id": "1",
         "_score": 1,
         "_source": {
           "Dracula": "Bram Stoker"
         }
       }
     ]
   ```

```
}
```

Sie finden den Verbindungsalias auf der Registerkarte Verbindungen in Ihrem Domänen-Dashboard.

- Wenn Sie eine Verbindung zwischen `domain-a -> domain-b` mit dem Verbindungsalias `cluster_b` und `domain-a -> domain-c` mit dem Verbindungsalias `cluster_c` einrichten, suchen Sie `domain-a`, `domain-b` und `domain-c` wie folgt:

```
GET https://src-domain.us-east-1.es.amazonaws.com/
local_index,cluster_b:b_index,cluster_c:c_index/_search
{
  "query": {
    "match": {
      "user": "domino"
    }
  }
}
```

Antwort

```
{
  "took": 150,
  "timed_out": false,
  "_shards": {
    "total": 3,
    "successful": 3,
    "failed": 0,
    "skipped": 0
  },
  "_clusters": {
    "total": 3,
    "successful": 3,
    "skipped": 0
  },
  "hits": {
    "total": 3,
    "max_score": 1,
    "hits": [
      {
        "_index": "local_index",
        "_type": "_doc",
```

```
        "_id": "0",
        "_score": 1,
        "_source": {
          "user": "domino",
          "message": "This is message 1",
          "likes": 0
        }
      },
      {
        "_index": "cluster_b:b_index",
        "_type": "_doc",
        "_id": "0",
        "_score": 2,
        "_source": {
          "user": "domino",
          "message": "This is message 2",
          "likes": 0
        }
      },
      {
        "_index": "cluster_c:c_index",
        "_type": "_doc",
        "_id": "0",
        "_score": 3,
        "_source": {
          "user": "domino",
          "message": "This is message 3",
          "likes": 0
        }
      }
    ]
  }
}
```

Wenn Sie sich in Ihrer Verbindungseinrichtung nicht dafür entschieden haben, nicht verfügbare Cluster zu überspringen, müssen alle Zielcluster, die Sie durchsuchen, verfügbar sein, damit Ihre Suchanfrage erfolgreich ausgeführt werden kann. Andernfalls schlägt die gesamte Anforderung fehl, auch wenn eine der Domänen nicht verfügbar ist, werden keine Suchergebnisse zurückgegeben.

OpenSearch Dashboards

Sie können Daten aus mehreren verbundenen Domänen auf die gleiche Weise visualisieren wie aus einer einzelnen Domäne, dafür müssen Sie jedoch auf die Remote-Indizes mit `connection-alias:index` zugreifen. Ihr Indexmuster muss also mit `connection-alias:index` übereinstimmen.

Learning to Rank für Amazon OpenSearch Service

OpenSearch verwendet ein probabilistisches Ranking-Framework namens BM-25, um Relevanzbewertungen zu berechnen. Wenn ein markantes Schlüsselwort häufiger in einem Dokument erscheint, weist BM-25 diesem Dokument eine höhere Relevanzbewertung zu. Dieses Framework berücksichtigt jedoch Benutzerverhalten wie Click-Through-Daten nicht, was die Relevanz weiter verbessern könnte.

Learning to Rank ist ein Open-Source-Plug-In, mit dem Sie mittels Machine Learning und Verhaltensdaten die Relevanz von Dokumenten optimieren können. Es verwendet Modelle aus den XGBoost und Ranklib-Bibliotheken, um die Suchergebnisse erneut zu bewerten. Das Elasticsearch-LTR-Plugin wurde ursprünglich von OpenSource Connections unter maßgeblicher Mitwirkung von Wikimedia Foundation, Snagajob Engineering, Bonsai und Yelp Engineering entwickelt. Die OpenSearch Version des Plugins leitet sich vom Elasticsearch-LTR-Plugin ab.

Für Learning to Rank ist Elasticsearch 7.7 oder höher erforderlich OpenSearch . Um das Plug-In „Learning to Rank“ verwenden zu können, benötigen Sie volle Administratorberechtigungen. Weitere Informationen hierzu finden Sie unter the section called “Hauptbenutzer ändern”.

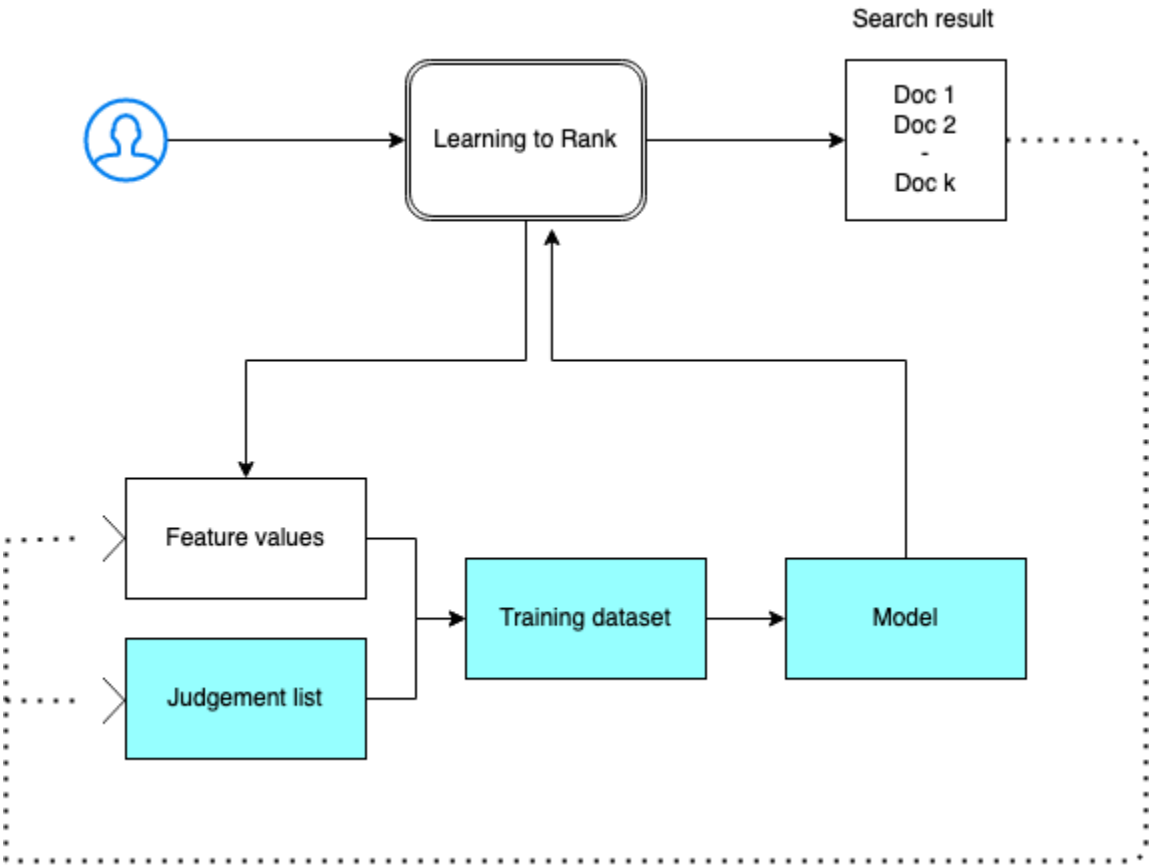
> **Note**
>
> Diese Dokumentation bietet einen allgemeinen Überblick über das Learning to Rank-Plugin und hilft Ihnen bei den ersten Schritten. Die vollständige Dokumentation, einschließlich detaillierter Schritte und API-Beschreibungen, finden Sie in der Dokumentation Learning to Rank.

Themen

- Erste Schritte mit Learning to Rank
- Learning-to-Rank-API

Erste Schritte mit Learning to Rank

Sie müssen eine Urteilsliste bereitstellen, einen Schulungsdatensatz vorbereiten und das Modell außerhalb von Amazon OpenSearch Service trainieren. Die blauen Teile kommen außerhalb von OpenSearch Service vor:



Schritt 1: Initialisieren des Plug-Ins

Um das Learning-to-Rank-Plug-In zu initialisieren, senden Sie die folgende Anfrage an Ihre OpenSearch Service-Domäne:

```
PUT _ltr
```

```
{
  "acknowledged" : true,
  "shards_acknowledged" : true,
  "index" : ".ltrstore"
}
```

Mit diesem Befehl wird ein ausgeblendeter `.ltrstore`-Index erstellt, in dem Metadateninformationen wie Funktions-Sets und Modelle gespeichert werden.

Schritt 2: Erstellen einer Urteilliste

> **Note**
>
> Sie müssen diesen Schritt außerhalb von OpenSearch Service ausführen.

Eine Urteilsliste ist eine Sammlung von Beispielen, von denen ein Machine-Learning-Modell lernt. Ihre Urteilsliste sollte Schlüsselwörter enthalten, die für Sie wichtig sind und eine Reihe von bewerteten Dokumenten für jedes Schlüsselwort.

In diesem Beispiel haben wir eine Urteilsliste für einen Film-Datensatz. Eine Bewertung von 4 weist auf eine perfekte Übereinstimmung hin. Eine Bewertung von 0 gibt die schlechteste Übereinstimmung an.

Bewertung	Stichwort	Dokument-ID	Filmname
4	rambo	7555	Rambo
3	rambo	1370	Rambo III
3	rambo	1369	Rambo: First Blood Teil II
3	rambo	1368	First Blood

Erstellen Sie Ihre Urteilsliste im folgenden Format:

```
4 qid:1 # 7555 Rambo
3 qid:1 # 1370 Rambo III
3 qid:1 # 1369 Rambo: First Blood Part II
3 qid:1 # 1368 First Blood

where qid:1 represents "rambo"
```

Ein umfassendes Beispiel für eine Urteilliste finden Sie unter Film-Urteile.

Sie können diese Urteilsliste manuell mit Hilfe von menschlichen Kommentatoren erstellen oder sie programmgesteuert aus Analysedaten ableiten.

Schritt 3: Erstellen eines Funktionssets

Eine Funktion ist ein Feld, das der Relevanz eines Dokuments entspricht, z. B. `title`, `overview`, `popularity score` (Anzahl der Ansichten) usw.

Erstellen Sie für jede Funktion einen Funktionssatz mit einer Mustache-Vorlage. Weitere Informationen zu Funktionen finden Sie unter Arbeiten mit Funktionen.

In diesem Beispiel erstellen wir einen `movie_features`-Funktionssatz mit den Feldern `title` und`overview`:

```
POST _ltr/_featureset/movie_features
{
  "featureset" : {
      "name" : "movie_features",
      "features" : [
        {
          "name" : "1",
          "params" : [
            "keywords"
          ],
          "template_language" : "mustache",
          "template" : {
            "match" : {
              "title" : "{{keywords}}"
            }
          }
        },
        {
          "name" : "2",
          "params" : [
            "keywords"
          ],
          "template_language" : "mustache",
          "template" : {
            "match" : {
              "overview" : "{{keywords}}"
            }
          }
        }
```

```
      ]
    }
}
```

Wenn Sie den ursprünglichen `.ltrstore`-Index verwenden, erhalten Sie Ihren Funktionsatz zurück:

```
GET _ltr/_featureset
```

Schritt 4: Protokollieren der Funktionswerte

Die Funktionswerte sind die Relevanzwerte, die von BM-25 für jede Funktion berechnet werden.

Kombinieren Sie den Funktionsatz und die Beurteilungsliste, um die Funktionswerte zu protokollieren. Weitere Informationen zur Protokollierung finden Sie unter Protokollieren von Funktionssätzen.

In diesem Beispiel ruft die `bool`-Abfrage die bewerteten Dokumente mit dem Filter ab und wählt dann den Funktionssatz mit der `sltr`-Abfrage aus. Die `ltr_log`-Abfrage kombiniert die Dokumente und die Funktionen, um die entsprechenden Funktionswerte zu protokollieren:

```
POST tmdb/_search
{
  "_source": {
    "includes": [
      "title",
      "overview"
    ]
  },
  "query": {
    "bool": {
      "filter": [
        {
          "terms": {
            "_id": [
              "7555",
              "1370",
              "1369",
              "1368"
            ]
          }
        },
        {
          "sltr": {
```

```
            "_name": "logged_featureset",
            "featureset": "movie_features",
            "params": {
              "keywords": "rambo"
            }
          }
        }
      ]
    }
  },
  "ext": {
    "ltr_log": {
      "log_specs": {
        "name": "log_entry1",
        "named_query": "logged_featureset"
      }
    }
  }
}
```

Eine Beispielantwort kann wie folgt aussehen:

```
{
  "took" : 7,
  "timed_out" : false,
  "_shards" : {
    "total" : 1,
    "successful" : 1,
    "skipped" : 0,
    "failed" : 0
  },
  "hits" : {
    "total" : {
      "value" : 4,
      "relation" : "eq"
    },
    "max_score" : 0.0,
    "hits" : [
      {
        "_index" : "tmdb",
        "_type" : "movie",
        "_id" : "1368",
        "_score" : 0.0,
```

```
      "_source" : {
        "overview" : "When former Green Beret John Rambo is harassed by local law
enforcement and arrested for vagrancy, the Vietnam vet snaps, runs for the hills and
rat-a-tat-tats his way into the action-movie hall of fame. Hounded by a relentless
sheriff, Rambo employs heavy-handed guerilla tactics to shake the cops off his tail.",
        "title" : "First Blood"
      },
      "fields" : {
        "_ltrlog" : [
          {
            "log_entry1" : [
              {
                "name" : "1"
              },
              {
                "name" : "2",
                "value" : 10.558305
              }
            ]
          }
        ]
      },
      "matched_queries" : [
        "logged_featureset"
      ]
    },
    {
      "_index" : "tmdb",
      "_type" : "movie",
      "_id" : "7555",
      "_score" : 0.0,
      "_source" : {
        "overview" : "When governments fail to act on behalf of captive missionaries,
ex-Green Beret John James Rambo sets aside his peaceful existence along the Salween
River in a war-torn region of Thailand to take action.  Although he's still haunted
by violent memories of his time as a U.S. soldier during the Vietnam War, Rambo can
hardly turn his back on the aid workers who so desperately need his help.",
        "title" : "Rambo"
      },
      "fields" : {
        "_ltrlog" : [
          {
            "log_entry1" : [
              {
```

```
                  "name" : "1",
                  "value" : 11.2569065
                },
                {
                  "name" : "2",
                  "value" : 9.936821
                }
              ]
            }
          ]
        },
        "matched_queries" : [
          "logged_featureset"
        ]
      },
      {
        "_index" : "tmdb",
        "_type" : "movie",
        "_id" : "1369",
        "_score" : 0.0,
        "_source" : {
          "overview" : "Col. Troutman recruits ex-Green Beret John Rambo for a highly
secret and dangerous mission. Teamed with Co Bao, Rambo goes deep into Vietnam to
rescue POWs. Deserted by his own team, he's left in a hostile jungle to fight for his
life, avenge the death of a woman and bring corrupt officials to justice.",
          "title" : "Rambo: First Blood Part II"
        },
        "fields" : {
          "_ltrlog" : [
            {
              "log_entry1" : [
                {
                  "name" : "1",
                  "value" : 6.334839
                },
                {
                  "name" : "2",
                  "value" : 10.558305
                }
              ]
            }
          ]
        },
        "matched_queries" : [
```

```
          "logged_featureset"
        ]
      },
      {
        "_index" : "tmdb",
        "_type" : "movie",
        "_id" : "1370",
        "_score" : 0.0,
        "_source" : {
          "overview" : "Combat has taken its toll on Rambo, but he's finally begun to
 find inner peace in a monastery. When Rambo's friend and mentor Col. Trautman asks for
 his help on a top secret mission to Afghanistan, Rambo declines but must reconsider
 when Trautman is captured.",
          "title" : "Rambo III"
        },
        "fields" : {
          "_ltrlog" : [
            {
              "log_entry1" : [
                {
                  "name" : "1",
                  "value" : 9.425955
                },
                {
                  "name" : "2",
                  "value" : 11.262714
                }
              ]
            }
          ]
        },
        "matched_queries" : [
          "logged_featureset"
        ]
      }
    ]
  }
}
```

Im vorherigen Beispiel hat die erste Funktion keinen Funktionswert, da das Schlüsselwort „rambo“ nicht im Titelfeld des Dokuments mit einer ID 1368 angezeigt wird. Dies ist ein fehlender Funktionswert in den Trainingsdaten.

Schritt 5: Erstellen eines Trainingdatensatzes

> **Note**
>
> Sie müssen diesen Schritt außerhalb von OpenSearch Service ausführen.

Der nächste Schritt besteht darin, die Beurteilungsliste und die Funktionswerte zu kombinieren, um einen Trainingsdatensatz zu erstellen. Wenn Ihre ursprüngliche Urteilsliste wie folgt aussieht:

```
4 qid:1 # 7555 Rambo
3 qid:1 # 1370 Rambo III
3 qid:1 # 1369 Rambo: First Blood Part II
3 qid:1 # 1368 First Blood
```

Konvertieren Sie sie in den abschließenden Trainingsdatensatz, der wie folgt aussieht:

```
4 qid:1 1:12.318474 2:10.573917 # 7555 rambo
3 qid:1 1:10.357875 2:11.950391 # 1370 rambo
3 qid:1 1:7.010513 2:11.220095 # 1369 rambo
3 qid:1 1:0.0 2:11.220095 # 1368 rambo
```

Sie können diesen Schritt manuell ausführen oder ein Programm schreiben, um es zu automatisieren.

Schritt 6: Einen Algorithmus auswählen und das Modell erstellen

> **Note**
>
> Sie müssen diesen Schritt außerhalb von OpenSearch Service ausführen.

Wenn der Trainingsdatensatz vorhanden ist, besteht der nächste Schritt darin, Ranklib-Bibliotheken zum Erstellen eines Modells zu verwenden XGBoost . XGBoost Mit Ranklib-Bibliotheken können Sie beliebte Modelle wie LambdaMart, Random Forest usw. erstellen.

Anweisungen zur Verwendung XGBoost von Ranklib zum Erstellen des Modells finden Sie in der jeweiligen Dokumentation. XGBoostRankLib Informationen zur Verwendung von Amazon SageMaker zum Erstellen des XGBoost Modells finden Sie unter XGBoostAlgorithmus.

Schritt 7: Bereitstellen des Modells

Nachdem Sie das Modell erstellt haben, stellen Sie es im Plug-In „Learning to Rank“ bereit. Weitere Informationen zur Bereitstellung eines Modells finden Sie unter Hochladen eines trainierten Modells.

In diesem Beispiel erstellen wir ein `my_ranklib_model`-Modell mit der Ranklib-Bibliothek:

```
POST _ltr/_featureset/movie_features/_createmodel?pretty
{
  "model": {
    "name": "my_ranklib_model",
    "model": {
      "type": "model/ranklib",
      "definition": """## LambdaMART
## No. of trees = 10
## No. of leaves = 10
## No. of threshold candidates = 256
## Learning rate = 0.1
## Stop early = 100

<ensemble>
   <tree id="1" weight="0.1">
      <split>
         <feature>1</feature>
         <threshold>10.357875</threshold>
         <split pos="left">
            <feature>1</feature>
            <threshold>0.0</threshold>
            <split pos="left">
               <output>-2.0</output>
            </split>
            <split pos="right">
               <feature>1</feature>
               <threshold>7.010513</threshold>
               <split pos="left">
                  <output>-2.0</output>
               </split>
               <split pos="right">
                  <output>-2.0</output>
               </split>
            </split>
         </split>
         <split pos="right">
```

```
            <output>2.0</output>
         </split>
      </split>
   </tree>
   <tree id="2" weight="0.1">
      <split>
         <feature>1</feature>
         <threshold>10.357875</threshold>
         <split pos="left">
            <feature>1</feature>
            <threshold>0.0</threshold>
            <split pos="left">
               <output>-1.67031991481781</output>
            </split>
            <split pos="right">
               <feature>1</feature>
               <threshold>7.010513</threshold>
               <split pos="left">
                  <output>-1.67031991481781</output>
               </split>
               <split pos="right">
                  <output>-1.6703200340270996</output>
               </split>
            </split>
         </split>
         <split pos="right">
            <output>1.6703201532363892</output>
         </split>
      </split>
   </tree>
   <tree id="3" weight="0.1">
      <split>
         <feature>2</feature>
         <threshold>10.573917</threshold>
         <split pos="left">
            <output>1.479954481124878</output>
         </split>
         <split pos="right">
            <feature>1</feature>
            <threshold>7.010513</threshold>
            <split pos="left">
               <feature>1</feature>
               <threshold>0.0</threshold>
               <split pos="left">
```

```
                  <output>-1.4799546003341675</output>
               </split>
               <split pos="right">
                  <output>-1.479954481124878</output>
               </split>
            </split>
            <split pos="right">
               <output>-1.479954481124878</output>
            </split>
         </split>
      </split>
   </tree>
   <tree id="4" weight="0.1">
      <split>
         <feature>1</feature>
         <threshold>10.357875</threshold>
         <split pos="left">
            <feature>1</feature>
            <threshold>0.0</threshold>
            <split pos="left">
               <output>-1.3569872379302979</output>
            </split>
            <split pos="right">
               <feature>1</feature>
               <threshold>7.010513</threshold>
               <split pos="left">
                  <output>-1.3569872379302979</output>
               </split>
               <split pos="right">
                  <output>-1.3569872379302979</output>
               </split>
            </split>
         </split>
         <split pos="right">
            <output>1.3569873571395874</output>
         </split>
      </split>
   </tree>
   <tree id="5" weight="0.1">
      <split>
         <feature>1</feature>
         <threshold>10.357875</threshold>
         <split pos="left">
            <feature>1</feature>
```

```
            <threshold>0.0</threshold>
            <split pos="left">
               <output>-1.2721362113952637</output>
            </split>
            <split pos="right">
               <feature>1</feature>
               <threshold>7.010513</threshold>
               <split pos="left">
                  <output>-1.2721363306045532</output>
               </split>
               <split pos="right">
                  <output>-1.2721363306045532</output>
               </split>
            </split>
         </split>
         <split pos="right">
            <output>1.2721362113952637</output>
         </split>
      </split>
   </tree>
   <tree id="6" weight="0.1">
      <split>
         <feature>1</feature>
         <threshold>10.357875</threshold>
         <split pos="left">
            <feature>1</feature>
            <threshold>7.010513</threshold>
            <split pos="left">
               <feature>1</feature>
               <threshold>0.0</threshold>
               <split pos="left">
                  <output>-1.2110036611557007</output>
               </split>
               <split pos="right">
                  <output>-1.2110036611557007</output>
               </split>
            </split>
            <split pos="right">
               <output>-1.2110037803649902</output>
            </split>
         </split>
         <split pos="right">
            <output>1.2110037803649902</output>
         </split>
```

```
      </split>
   </tree>
   <tree id="7" weight="0.1">
      <split>
         <feature>1</feature>
         <threshold>10.357875</threshold>
         <split pos="left">
            <feature>1</feature>
            <threshold>7.010513</threshold>
            <split pos="left">
               <feature>1</feature>
               <threshold>0.0</threshold>
               <split pos="left">
                  <output>-1.165616512298584</output>
               </split>
               <split pos="right">
                  <output>-1.165616512298584</output>
               </split>
            </split>
            <split pos="right">
               <output>-1.165616512298584</output>
            </split>
         </split>
         <split pos="right">
            <output>1.165616512298584</output>
         </split>
      </split>
   </tree>
   <tree id="8" weight="0.1">
      <split>
         <feature>1</feature>
         <threshold>10.357875</threshold>
         <split pos="left">
            <feature>1</feature>
            <threshold>7.010513</threshold>
            <split pos="left">
               <feature>1</feature>
               <threshold>0.0</threshold>
               <split pos="left">
                  <output>-1.131177544593811</output>
               </split>
               <split pos="right">
                  <output>-1.131177544593811</output>
               </split>
```

```
            </split>
            <split pos="right">
               <output>-1.131177544593811</output>
            </split>
         </split>
         <split pos="right">
            <output>1.131177544593811</output>
         </split>
      </split>
   </tree>
   <tree id="9" weight="0.1">
      <split>
         <feature>2</feature>
         <threshold>10.573917</threshold>
         <split pos="left">
            <output>1.1046180725097656</output>
         </split>
         <split pos="right">
            <feature>1</feature>
            <threshold>7.010513</threshold>
            <split pos="left">
               <feature>1</feature>
               <threshold>0.0</threshold>
               <split pos="left">
                  <output>-1.1046180725097656</output>
               </split>
               <split pos="right">
                  <output>-1.1046180725097656</output>
               </split>
            </split>
            <split pos="right">
               <output>-1.1046180725097656</output>
            </split>
         </split>
      </split>
   </tree>
   <tree id="10" weight="0.1">
      <split>
         <feature>1</feature>
         <threshold>10.357875</threshold>
         <split pos="left">
            <feature>1</feature>
            <threshold>7.010513</threshold>
            <split pos="left">
```

```
               <feature>1</feature>
               <threshold>0.0</threshold>
               <split pos="left">
                  <output>-1.0838804244995117</output>
               </split>
               <split pos="right">
                  <output>-1.0838804244995117</output>
               </split>
            </split>
            <split pos="right">
               <output>-1.0838804244995117</output>
            </split>
         </split>
         <split pos="right">
            <output>1.0838804244995117</output>
         </split>
      </split>
   </tree>
</ensemble>
"""
    }
  }
}
```

Um das Modell zu sehen, senden Sie die folgende Anfrage:

```
GET _ltr/_model/my_ranklib_model
```

Schritt 8: Suchen mit Learning to Rank

Nach der Bereitstellung des Modells können Sie suchen.

Führen Sie die `sltr`-Abfrage mit den verwendeten Funktionen und dem Namen des Modells aus, das Sie ausführen möchten:

```
POST tmdb/_search
{
  "_source": {
    "includes": ["title", "overview"]
  },
  "query": {
    "multi_match": {
```

```
      "query": "rambo",
      "fields": ["title", "overview"]
    }
  },
  "rescore": {
    "query": {
      "rescore_query": {
        "sltr": {
          "params": {
            "keywords": "rambo"
          },
          "model": "my_ranklib_model"
        }
      }
    }
  }
}
```

Mit „Learning to Ranking“ sehen Sie „Rambo“ als erstes Ergebnis, da wir ihm die höchste Bewertung in der Urteilsliste zugewiesen haben:

```
{
  "took" : 12,
  "timed_out" : false,
  "_shards" : {
    "total" : 1,
    "successful" : 1,
    "skipped" : 0,
    "failed" : 0
  },
  "hits" : {
    "total" : {
      "value" : 7,
      "relation" : "eq"
    },
    "max_score" : 13.096414,
    "hits" : [
      {
        "_index" : "tmdb",
        "_type" : "movie",
        "_id" : "7555",
        "_score" : 13.096414,
        "_source" : {
```

```
        "overview" : "When governments fail to act on behalf of captive missionaries,
ex-Green Beret John James Rambo sets aside his peaceful existence along the Salween
River in a war-torn region of Thailand to take action.  Although he's still haunted
by violent memories of his time as a U.S. soldier during the Vietnam War, Rambo can
hardly turn his back on the aid workers who so desperately need his help.",
        "title" : "Rambo"
      }
    },
    {
      "_index" : "tmdb",
      "_type" : "movie",
      "_id" : "1370",
      "_score" : 11.17245,
      "_source" : {
        "overview" : "Combat has taken its toll on Rambo, but he's finally begun to
find inner peace in a monastery. When Rambo's friend and mentor Col. Trautman asks for
his help on a top secret mission to Afghanistan, Rambo declines but must reconsider
when Trautman is captured.",
        "title" : "Rambo III"
      }
    },
    {
      "_index" : "tmdb",
      "_type" : "movie",
      "_id" : "1368",
      "_score" : 10.442155,
      "_source" : {
        "overview" : "When former Green Beret John Rambo is harassed by local law
enforcement and arrested for vagrancy, the Vietnam vet snaps, runs for the hills and
rat-a-tat-tats his way into the action-movie hall of fame. Hounded by a relentless
sheriff, Rambo employs heavy-handed guerilla tactics to shake the cops off his tail.",
        "title" : "First Blood"
      }
    },
    {
      "_index" : "tmdb",
      "_type" : "movie",
      "_id" : "1369",
      "_score" : 10.442155,
      "_source" : {
        "overview" : "Col. Troutman recruits ex-Green Beret John Rambo for a highly
secret and dangerous mission. Teamed with Co Bao, Rambo goes deep into Vietnam to
rescue POWs. Deserted by his own team, he's left in a hostile jungle to fight for his
life, avenge the death of a woman and bring corrupt officials to justice.",
```

```
          "title" : "Rambo: First Blood Part II"
        }
      },
      {
        "_index" : "tmdb",
        "_type" : "movie",
        "_id" : "31362",
        "_score" : 7.424202,
        "_source" : {
          "overview" : "It is 1985, and a small, tranquil Florida town is being rocked
by a wave of vicious serial murders and bank robberies. Particularly sickening to the
authorities is the gratuitous use of violence by two “Rambo” like killers who dress
themselves in military garb. Based on actual events taken from FBI files, the movie
depicts the Bureau’s efforts to track down these renegades.",
          "title" : "In the Line of Duty: The F.B.I. Murders"
        }
      },
      {
        "_index" : "tmdb",
        "_type" : "movie",
        "_id" : "13258",
        "_score" : 6.43182,
        "_source" : {
          "overview" : """Will Proudfoot (Bill Milner) is looking for an escape from
his family's stifling home life when he encounters Lee Carter (Will Poulter), the
school bully. Armed with a video camera and a copy of "Rambo: First Blood", Lee plans
to make cinematic history by filming his own action-packed video epic. Together, these
two newfound friends-turned-budding-filmmakers quickly discover that their imaginative
– and sometimes mishap-filled – cinematic adventure has begun to take on a life of its
own!""",
          "title" : "Son of Rambow"
        }
      },
      {
        "_index" : "tmdb",
        "_type" : "movie",
        "_id" : "61410",
        "_score" : 3.9719706,
        "_source" : {
          "overview" : "It's South Africa 1990. Two major events are about to happen:
The release of Nelson Mandela and, more importantly, it's Spud Milton's first year
at an elite boys only private boarding school. John Milton is a boy from an ordinary
background who wins a scholarship to a private school in Kwazulu-Natal, South Africa.
Surrounded by boys with nicknames like Gecko, Rambo, Rain Man and Mad Dog, Spud has
```

```
 his hands full trying to adapt to his new home. Along the way Spud takes his first
 tentative steps along the path to manhood. (The path it seems could be a rather long
 road). Spud is an only child. He is cursed with parents from well beyond the lunatic
 fringe and a senile granny. His dad is a fervent anti-communist who is paranoid that
 the family domestic worker is running a shebeen from her room at the back of the
 family home. His mom is a free spirit and a teenager's worst nightmare, whether it's
 shopping for Spud's underwear in the local supermarket",
          "title" : "Spud"
        }
      }
    ]
  }
}
```

Wenn Sie suchen, ohne das Plug-In „Learning to Rank“ zu verwenden, werden verschiedene Ergebnisse OpenSearch zurückgegeben:

```
POST tmdb/_search
{
  "_source": {
    "includes": ["title", "overview"]
  },
  "query": {
    "multi_match": {
      "query": "Rambo",
      "fields": ["title", "overview"]
    }
  }
}
```

```
{
  "took" : 5,
  "timed_out" : false,
  "_shards" : {
    "total" : 1,
    "successful" : 1,
    "skipped" : 0,
    "failed" : 0
  },
  "hits" : {
    "total" : {
      "value" : 5,
      "relation" : "eq"
```

```
    },
    "max_score" : 11.262714,
    "hits" : [
      {
        "_index" : "tmdb",
        "_type" : "movie",
        "_id" : "1370",
        "_score" : 11.262714,
        "_source" : {
          "overview" : "Combat has taken its toll on Rambo, but he's finally begun to
find inner peace in a monastery. When Rambo's friend and mentor Col. Trautman asks for
his help on a top secret mission to Afghanistan, Rambo declines but must reconsider
when Trautman is captured.",
          "title" : "Rambo III"
        }
      },
      {
        "_index" : "tmdb",
        "_type" : "movie",
        "_id" : "7555",
        "_score" : 11.2569065,
        "_source" : {
          "overview" : "When governments fail to act on behalf of captive missionaries,
ex-Green Beret John James Rambo sets aside his peaceful existence along the Salween
River in a war-torn region of Thailand to take action.  Although he's still haunted
by violent memories of his time as a U.S. soldier during the Vietnam War, Rambo can
hardly turn his back on the aid workers who so desperately need his help.",
          "title" : "Rambo"
        }
      },
      {
        "_index" : "tmdb",
        "_type" : "movie",
        "_id" : "1368",
        "_score" : 10.558305,
        "_source" : {
          "overview" : "When former Green Beret John Rambo is harassed by local law
enforcement and arrested for vagrancy, the Vietnam vet snaps, runs for the hills and
rat-a-tat-tats his way into the action-movie hall of fame. Hounded by a relentless
sheriff, Rambo employs heavy-handed guerilla tactics to shake the cops off his tail.",
          "title" : "First Blood"
        }
      },
      {
```

```
        "_index" : "tmdb",
        "_type" : "movie",
        "_id" : "1369",
        "_score" : 10.558305,
        "_source" : {
          "overview" : "Col. Troutman recruits ex-Green Beret John Rambo for a highly
 secret and dangerous mission. Teamed with Co Bao, Rambo goes deep into Vietnam to
 rescue POWs. Deserted by his own team, he's left in a hostile jungle to fight for his
 life, avenge the death of a woman and bring corrupt officials to justice.",
          "title" : "Rambo: First Blood Part II"
        }
      },
      {
        "_index" : "tmdb",
        "_type" : "movie",
        "_id" : "13258",
        "_score" : 6.4600153,
        "_source" : {
          "overview" : """Will Proudfoot (Bill Milner) is looking for an escape from
 his family's stifling home life when he encounters Lee Carter (Will Poulter), the
 school bully. Armed with a video camera and a copy of "Rambo: First Blood", Lee plans
 to make cinematic history by filming his own action-packed video epic. Together, these
 two newfound friends-turned-budding-filmmakers quickly discover that their imaginative
 – and sometimes mishap-filled – cinematic adventure has begun to take on a life of its
 own!""",
          "title" : "Son of Rambow"
        }
      }
    ]
  }
}
```

Passen Sie die Beurteilungsliste und die Funktionen an, je nachdem, wie gut das Modell Ihrer Meinung nach funktioniert. Wiederholen Sie anschließend die Schritte 2 bis 8, um die Ranglistenergebnisse im Laufe der Zeit zu verbessern.

Learning-to-Rank-API

Verwenden Sie die Operationen „Learning to Rank“, um programmgesteuert mit Funktionssätzen und Modellen zu arbeiten.

Shop erstellen

Es wird ein ausgeblendeter `.ltrstore`-Index erstellt, in dem Metadateninformationen wie Funktionssätze und Modelle gespeichert werden.

```
PUT _ltr
```

Shop löschen

Löscht den versteckten `.ltrstore`-Index und setzt das Plug-In zurück.

```
DELETE _ltr
```

Erstellen eines Funktionssatzes

Erstellt einen Funktionssatz.

```
POST _ltr/_featureset/<name_of_features>
```

Löschen eines Funktionssatzes

Löscht einen Funktionssatz.

```
DELETE _ltr/_featureset/<name_of_feature_set>
```

Abrufen eines Funktionssatzes

Ruft einen Funktionssatz ab.

```
GET _ltr/_featureset/<name_of_feature_set>
```

Erstellen eines Modells

Erstellt ein Modell.

```
POST _ltr/_featureset/<name_of_feature_set>/_createmodel
```

Löschen eines Modells

Löscht ein Modell.

```
DELETE _ltr/_model/<name_of_model>
```

Abrufen eines Modells

Ruft ein Modell ab.

```
GET _ltr/_model/<name_of_model>
```

Statistiken abrufen

Enthält Informationen darüber, wie sich das Plug-In verhält.

```
GET _ltr/_stats
```

Sie können auch Filter verwenden, um eine einzelne Statistik abzurufen:

```
GET _ltr/_stats/<stat>
```

Darüber hinaus können Sie die Informationen auf einen einzelnen Knoten im Cluster beschränken:

```
GET _ltr/_stats/<stat>/nodes/<nodeId>

{
  "_nodes" : {
    "total" : 1,
    "successful" : 1,
    "failed" : 0
  },
  "cluster_name" : "873043598401:ltr-77",
  "stores" : {
    ".ltrstore" : {
      "model_count" : 1,
      "featureset_count" : 1,
      "feature_count" : 2,
      "status" : "green"
    }
  },
  "status" : "green",
  "nodes" : {
    "DjelK-_ZSfyzstO5dhGGQA" : {
      "cache" : {
```

```
        "feature" : {
          "eviction_count" : 0,
          "miss_count" : 0,
          "entry_count" : 0,
          "memory_usage_in_bytes" : 0,
          "hit_count" : 0
        },
        "featureset" : {
          "eviction_count" : 2,
          "miss_count" : 2,
          "entry_count" : 0,
          "memory_usage_in_bytes" : 0,
          "hit_count" : 0
        },
        "model" : {
          "eviction_count" : 2,
          "miss_count" : 3,
          "entry_count" : 1,
          "memory_usage_in_bytes" : 3204,
          "hit_count" : 1
        }
      },
      "request_total_count" : 6,
      "request_error_count" : 0
    }
  }
}
```

Die Statistiken werden auf zwei Ebenen, Knoten und Cluster, bereitgestellt, wie in den folgenden Tabellen angegeben:

Statistiken auf Knotenebene

Feldname	Beschreibung
request_total_count	Gesamtzahl der Ranking-Anforderungen.
request_error_count	Gesamtzahl der fehlgeschlagenen Anforderungen.
Cache	Statistiken über alle Caches hinweg (Funktionen, Funktionssätze, Modelle). Ein Cache-Treffer tritt auf, wenn ein Benutzer das Plug-In

Feldname	Beschreibung
	abfragt und das Modell bereits in den Speicher geladen ist.
cache.eviction_count	Anzahl der Cache-Bereinigungen.
cache.hit_count	Anzahl der Cache-Treffer.
cache.miss_count	Anzahl der Cache-Fehler. Ein Cache-Fehler tritt auf, wenn ein Benutzer das Plug-In abfragt und das Modell noch nicht in den Speicher geladen ist.
cache.entry_count	Anzahl der Einträge im Cache.
cache.memory_usage_in_bytes	Gesamtspeicher, der in Bytes verwendet wird.
cache.cache_capacity_reached	Gibt an, ob das Cache-Limit erreicht ist.

Cluster-Ebenen-Statistiken

Feldname	Beschreibung
stores	Gibt an, wo die Funktionssätze und Modellmet adaten gespeichert werden. (Der Standardw ert ist „.ltrstore“. Andernfalls wird „.ltrstore_“ mit einem vom Benutzer angegebenen Namen vorangestellt).
stores.status	Der Indexstatus.
stores.feature_sets	Anzahl der Funktionssätze.
stores.features_count	Anzahl der Funktionen.
stores.model_count	Anzahl der Modelle.
Status	Der Plug-In-Status basierend auf dem Status der Funktionsspeicher-Indizes (rot, gelb oder

Feldname	Beschreibung
	grün) und des Leistungsschalterstatus (offen oder geschlossen).
cache.cache_capacity_reached	Gibt an, ob das Cache-Limit erreicht ist.

Cache-Statistiken abrufen

Gibt Statistiken über den Cache und die Speichernutzung zurück.

```
GET _ltr/_cachestats

{
    "_nodes": {
        "total": 2,
        "successful": 2,
        "failed": 0
    },
    "cluster_name": "opensearch-cluster",
    "all": {
        "total": {
            "ram": 612,
            "count": 1
        },
        "features": {
            "ram": 0,
            "count": 0
        },
        "featuresets": {
            "ram": 612,
            "count": 1
        },
        "models": {
            "ram": 0,
            "count": 0
        }
    },
    "stores": {
        ".ltrstore": {
            "total": {
                "ram": 612,
```

```
                "count": 1
            },
            "features": {
                "ram": 0,
                "count": 0
            },
            "featuresets": {
                "ram": 612,
                "count": 1
            },
            "models": {
                "ram": 0,
                "count": 0
            }
        }
    },
    "nodes": {
        "ejF6uutERF20wOFNOXB61A": {
            "name": "opensearch1",
            "hostname": "172.18.0.4",
            "stats": {
                "total": {
                    "ram": 612,
                    "count": 1
                },
                "features": {
                    "ram": 0,
                    "count": 0
                },
                "featuresets": {
                    "ram": 612,
                    "count": 1
                },
                "models": {
                    "ram": 0,
                    "count": 0
                }
            }
        },
        "Z2RZNWRLSveVcz2c6lHf5A": {
            "name": "opensearch2",
            "hostname": "172.18.0.2",
            "stats": {
                ...
```

```
            }
        }
    }
}
```

Löschen des Cache

Löscht den Plug-In-Cache. Verwenden Sie diese Option, um das Modell zu aktualisieren.

```
POST _ltr/_clearcache
```

Asynchrone Suche in Amazon Service OpenSearch

Mit der asynchronen Suche nach Amazon OpenSearch Service können Sie eine Suchanfrage senden, die im Hintergrund ausgeführt wird, den Fortschritt der Anfrage überwachen und Ergebnisse zu einem späteren Zeitpunkt abrufen. Sie können Teilergebnisse abrufen, sobald sie verfügbar sind, bevor die Suche abgeschlossen ist. Nachdem die Suche abgeschlossen ist, speichern Sie die Ergebnisse für einen späteren Abruf und Analyse.

Die asynchrone Suche erfordert OpenSearch 1.0 oder höher oder Elasticsearch 7.10 oder höher.

Diese Dokumentation bietet einen kurzen Überblick über die asynchrone Suche. Es werden auch die Einschränkungen der Verwendung der asynchronen Suche mit einer verwalteten Amazon OpenSearch Service-Domain anstelle eines OpenSearch Open-Source-Clusters erörtert. Eine vollständige Dokumentation der asynchronen Suche, einschließlich verfügbarer Einstellungen, Berechtigungen und einer vollständigen API-Referenz, finden Sie in der Dokumentation unter Asynchrone Suche. OpenSearch

Beispiele für Suchaufrufe

Um eine asynchrone Suche durchzuführen, senden Sie HTTP-Anforderungen an `_plugins/_asynchronous_search` im folgenden Format:

```
POST opensearch-domain/_plugins/_asynchronous_search
```

> **Note**
>
> Wenn Sie Elasticsearch 7.10 anstelle einer OpenSearch Version verwenden, `_plugins` ersetzen Sie `_opendistro` in allen asynchronen Suchanfragen durch.

Sie können die folgenden asynchronen Suchoptionen angeben:

Optionen	Beschreibung	Standardwert	Erforderlich
`wait_for_completion_timeout`	Gibt die Zeitspanne an, in der Sie auf die Ergebnisse warten möchten. Sie können die Ergebnisse sehen, die Sie innerhalb dieser Zeit erhalten, genau wie bei einer normalen Suche. Sie können die verbleibenden Ergebnisse anhand einer ID abfragen. Der Höchstwert beträgt 300 Sekunden.	1 Sekunde	Nein
`keep_on_completion`	Gibt an, ob die Ergebnisse nach Abschluss der Suche im Cluster gespeichert werden sollen. Sie können die gespeicherten Ergebnisse zu einem späteren Zeitpunkt untersuchen.	`false`	Nein
`keep_alive`	Gibt die Zeit an, in der das Ergebnis im Cluster gespeichert wird. `2d` bedeutet beispielsweise, dass die Ergebnisse 48 Stunden lang im Cluster gespeichert werden. Die gespeicherten Suchergebnisse werden nach diesem Zeitraum gelöscht oder wenn die Suche abgebrochen wird. Beachten Sie, dass dies die Abfragelaufzeit einschließt. Wenn die Abfrage dieses Mal überläuft, bricht der Prozess diese Abfrage automatisch ab.	12 Stunden	Nein

Beispielanforderung

```
POST _plugins/_asynchronous_search/?
pretty&size=10&wait_for_completion_timeout=1ms&keep_on_completion=true&request_cache=false
{
  "aggs": {
    "city": {
      "terms": {
        "field": "city",
        "size": 10
```

```
      }
    }
  }
}
```

> **Note**
>
> Alle Anforderungsparameter, die für eine Standard-`_search`-Abfrage gelten, werden unterstützt. Wenn Sie Elasticsearch 7.10 anstelle einer OpenSearch Version verwenden, ersetzen Sie durch`_plugins`. `_opendistro`

Asynchrone Suchberechtigungen

Die asynchrone Suche unterstützt eine abgestimmte Zugriffskontrolle. Ausführliche Informationen zum Mischen und Abgleichen von Berechtigungen für Ihren Anwendungsfall finden Sie unter Sicherheit bei der asynchronen Suche.

Für Domains, bei denen eine abgestimmte Zugriffssteuerung aktiviert ist, benötigen Sie die folgenden Mindestberechtigungen für eine Rolle:

```
# Allows users to use all asynchronous search functionality
asynchronous_search_full_access:
  reserved: true
  cluster_permissions:
    - 'cluster:admin/opensearch/asynchronous-search/*'
  index_permissions:
    - index_patterns:
        - '*'
      allowed_actions:
        - 'indices:data/read/search*'

# Allows users to read stored asynchronous search results
asynchronous_search_read_access:
  reserved: true
  cluster_permissions:
    - 'cluster:admin/opensearch/asynchronous-search/get'
```

Verwenden Sie für Domains mit deaktivierter Zugriffssteuerung den IAM-Zugriff und den geheimen Schlüssel, um alle Anforderungen zu signieren. Sie können mit der asynchronen Such-ID auf die Ergebnisse zugreifen.

Asynchrone Sucheinstellungen

OpenSearch ermöglicht es Ihnen, alle verfügbaren Einstellungen für die asynchrone Suche mithilfe der API zu ändern. `_cluster/settings` Sie können in OpenSearch Service nur die folgenden Einstellungen ändern:

- `plugins.asynchronous_search.node_concurrent_running_searches`
- `plugins.asynchronous_search.persist_search_failures`

Cluster-übergreifende Suche

Sie können eine asynchrone Suche über Cluster mit den folgenden geringfügigen Einschränkungen durchführen:

- Sie können eine asynchrone Suche nur in der Quell-Domain ausführen.
- Sie können Netzwerk-Roundtrips als Teil einer clusterübergreifenden Suchabfrage nicht minimieren.

Wenn Sie eine Verbindung zwischen `domain-a -> domain-b` mit dem Verbindungsalias `cluster_b` und `domain-a -> domain-c` mit dem Verbindungsalias `cluster_c` einrichten, suchen Sie `domain-a`, `domain-b` und `domain-c` asynchron, wie folgt:

```
POST https://src-domain.us-east-1.es.amazonaws.com/
local_index,cluster_b:b_index,cluster_c:c_index/_plugins/_asynchronous_search/?
pretty&size=10&wait_for_completion_timeout=500ms&keep_on_completion=true&request_cache=false
{
  "size": 0,
  "_source": {
    "excludes": []
  },
  "aggs": {
    "2": {
      "terms": {
        "field": "clientip",
        "size": 50,
        "order": {
          "_count": "desc"
        }
      }
```

```
    }
  },
  "stored_fields": [
    "*"
  ],
  "script_fields": {},
  "docvalue_fields": [
    "@timestamp"
  ],
  "query": {
    "bool": {
      "must": [
        {
          "query_string": {
            "query": "status:404",
            "analyze_wildcard": true,
            "default_field": "*"
          }
        },
        {
          "range": {
            "@timestamp": {
              "gte": 1483747200000,
              "lte": 1488326400000,
              "format": "epoch_millis"
            }
          }
        }
      ],
      "filter": [],
      "should": [],
      "must_not": []
    }
  }
}
```

Antwort

```
{
  "id" :
 "Fm9pYzJyVG91U19xb0hIQUJnMHJfRFEAAAAAAAknghQ1OWVBczNZQjVEa2dMYTBXaTdEagAAAAAAAAAB",
  "state" : "RUNNING",
  "start_time_in_millis" : 1609329314796,
```

```
  "expiration_time_in_millis" : 1609761314796
}
```

Weitere Informationen finden Sie unter the section called “Cluster-übergreifende Suche”.

UltraWarm

Asynchrone Suchen mit UltraWarm Indizes funktionieren weiterhin. Weitere Informationen finden Sie unter the section called “UltraWarm Speicher”.

> **Note**
>
> Sie können asynchrone Suchstatistiken in CloudWatch überwachen. Eine vollständige Liste der Metriken finden Sie unter the section called “Asynchrone Suchmetriken”.

Point-in-Time-Suche in Amazon OpenSearch Service

Point in Time (PIT) ist ein Suchtyp, mit dem Sie verschiedene Abfragen für einen Datensatz ausführen können, der zeitlich festgelegt ist. Wenn Sie dieselbe Abfrage für denselben Index zu unterschiedlichen Zeitpunkten ausführen, erhalten Sie in der Regel unterschiedliche Ergebnisse, da Dokumente ständig indexiert, aktualisiert und gelöscht werden. Mit PIT können Sie Abfragen anhand eines konstanten Zustands Ihres Datensatzes durchführen.

Der Hauptzweck der PIT-Suche besteht darin, sie mit `search_after` Funktionen zu verbinden. Dies ist die bevorzugte Paginierungsmethode OpenSearch, insbesondere für tiefe Paginierung, da sie mit einem Datensatz arbeitet, der zeitlich eingefroren ist, nicht an eine Abfrage gebunden ist und eine konsistente Paginierung vor- und rückwärts unterstützt. Sie können PIT mit einer Domain verwenden, auf der Version 2.5 ausgeführt wird. OpenSearch

> **Note**
>
> Dieses Thema bietet einen Überblick über PIT und einige Dinge, die bei der Verwendung auf einer verwalteten Amazon OpenSearch Service-Domain und nicht auf einem selbstverwalteten OpenSearch Cluster zu beachten sind. Eine vollständige Dokumentation von PIT, einschließlich einer umfassenden API-Referenz, finden Sie unter Point in Time in der OpenSearch Open-Source-Dokumentation.

Überlegungen

Berücksichtigen Sie Folgendes, wenn Sie Ihre PIT-Suchen konfigurieren:

- Wenn Sie ein Upgrade von einer Domain mit OpenSearch Version 2.3 durchführen und eine detaillierte Zugriffskontrolle für PIT-Aktionen benötigen, müssen Sie diese Aktionen und Rollen manuell hinzufügen.
- Es gibt keine Resilienz für PIT. Der Neustart von Knoten, die Kündigung des Knotens, Bereitstellungen in Blau/Grün und OpenSearch Prozessneustarts führen dazu, dass alle PIT-Daten verloren gehen.
- Wenn ein Shard während der Blau/Grün-Bereitstellung verschoben wird, werden nur Live-Datensegmente auf den neuen Knoten übertragen. Shard-Segmente, die sich im Besitz von PIT befinden (sowohl exklusiv als auch diejenigen, die gemeinsam mit aktiven Daten genutzt werden), verbleiben auf dem alten Knoten.
- PIT-Suchen funktionieren derzeit nicht mit asynchroner Suche.

Erstellen eines PIT

Um eine PIT-Abfrage auszuführen, senden Sie `_search/point_in_time` HTTP-Anforderungen im folgenden Format:

```
POST opensearch-domain/my-index/_search/point_in_time?keep_alive=time
```

Sie können die folgenden PIT-Optionen angeben:

Optionen	Beschreibung	Standardwert	Erforderlich
`keep_alive`	Die Zeitspanne für die Aufbewahrung der PIT. Jedes Mal, wenn Sie mit einer Suchanfrage auf eine PIT zugreifen, wird die PIT-Lebensdauer um den Zeitraum verlängert, der dem `keep_alive` Parameter entspricht. Dieser Abfrageparameter ist erforderlich, wenn Sie eine PIT erstellen, bei einer Suchanfrage jedoch optional.		Ja

Optionen	Beschreibung	Standardwert	Erforderlich
`preference`	Eine Zeichenfolge, die den Knoten oder den Shard angibt, der für die Suche verwendet wurde.	Random	Nein
`routing`	Eine Zeichenfolge, die angibt, Suchanfragen an einen bestimmten Shard weiterzuleiten.	Das Dokument ist `_id`	Nein
`expand_wildcards`	Eine Zeichenfolge, die den Indextyp angibt, der dem Platzhaltermuster entsprechen kann. Unterstützt kommaseparierte Werte. Gültige Werte: • `all`: Entspricht einem beliebigen Index oder Datenstrom, auch versteckten. • `open`: Ordnet offene, nicht versteckte Indizes oder nicht versteckte Datenströme zu. • `closed`: Ordnet geschlossene, nicht versteckte Indizes oder nicht versteckte Datenströme zu. • `hidden`: Ordnet versteckte Indizes oder Datenströme zu. Muss mit „offen“, „geschlossen“ oder „offen“ und „geschlossen“ kombiniert werden. • `none`: Platzhaltermuster werden nicht akzeptiert.	`open`	Nein
`allow_partial_pit_creation`	Ein boolescher Wert, der angibt, ob eine PIT mit teilweisen Fehlern erstellt werden soll.	`true`	Nein

Beispielantwort

```
{
```

```
    "pit_id":
 "o463QQEPbXktaW5kZXgtMDAwMDAxFnNOWU43ckt3U3IyaFVpbGE1UWEtMncAFjFyeXBsRGJmVFM2RTB6eVg1aVVqQncAA
    "_shards": {
        "total": 1,
        "successful": 1,
        "skipped": 0,
        "failed": 0
    },
    "creation_time": 1658146050064
}
```

Wenn Sie eine PIT erstellen, erhalten Sie in der Antwort eine PIT-ID. Dies ist die ID, die Sie verwenden, um Suchen mit der PIT durchzuführen.

Zeitpunktberechtigungen

PIT unterstützt die differenzierte Zugriffskontrolle. Wenn Sie ein Upgrade auf eine Domain der OpenSearch Version 2.5 durchführen und eine detaillierte Zugriffskontrolle benötigen, müssen Sie manuell Rollen mit den folgenden Berechtigungen erstellen:

```
# Allows users to use all point in time search search functionality
point_in_time_full_access:
  reserved: true
  index_permissions:
    - index_patterns:
        - '*'
      allowed_actions:
        - "indices:data/read/point_in_time/create"
        - "indices:data/read/point_in_time/delete"
        - "indices:data/read/point_in_time/readall"
        - "indices:data/read/search"
        - "indices:monitor/point_in_time/segments"


# Allows users to use point in time search search functionality for specific index
# All type operations like list all PITs, delete all PITs are not supported in this
 case

point_in_time_index_access:
  reserved: true
  index_permissions:
    - index_patterns:
```

```
      - 'my-index-1'
    allowed_actions:
      - "indices:data/read/point_in_time/create"
      - "indices:data/read/point_in_time/delete"
      - "indices:data/read/search"
      - "indices:monitor/point_in_time/segments"
```

Für Domänen mit OpenSearch Version 2.5 und höher können Sie die integrierte `point_in_time_full_access` Rolle verwenden. Weitere Informationen finden Sie in der OpenSearch Dokumentation unter Sicherheitsmodell.

PIT-Einstellungen

OpenSearch ermöglicht es Ihnen, alle verfügbaren PIT-Einstellungen mithilfe der `_cluster/settings` API zu ändern. Im OpenSearch Service können Sie derzeit keine Einstellungen ändern.

Cluster-übergreifende Suche

Sie können Cluster mit PIT erstellen PITs IDs, mit PIT suchen PITs, auflisten und PITs löschen, wobei die folgenden geringfügigen Einschränkungen gelten:

- Sie können PITs nur in der Quell-Domain alle auflisten und alle löschen.
- Sie können Netzwerk-Roundtrips als Teil einer clusterübergreifenden Suchabfrage nicht minimieren.

Weitere Informationen finden Sie unter the section called “Cluster-übergreifende Suche”.

UltraWarm

PIT-Suchen mit UltraWarm Indizes funktionieren weiterhin. Weitere Informationen finden Sie unter the section called “UltraWarm Speicher”.

> **Note**
>
> Sie können die PIT-Suchstatistiken in überwachen CloudWatch. Eine vollständige Liste der Metriken finden Sie unter the section called “Point-in-Time-Metriken”.

Semantische Suche in Amazon Service OpenSearch

Ab OpenSearch Version 2.9 können Sie die semantische Suche verwenden, um Suchanfragen besser zu verstehen und die Suchrelevanz zu verbessern. Sie können die semantische Suche auf zwei Arten verwenden — mit der neuronalen Suche und mit der Suche nach k-Nearest Neighbor (k-NN).

Mit OpenSearch Service können Sie KI-Konnektoren für AWS-Services und externe Dienste einrichten. Mit der -Konsole können Sie auch ein ML-Modell mit einer AWS CloudFormation -Konsole erstellen. Weitere Informationen finden Sie unter the section called “CloudFormation Vorlagen-Integrationen”.

Eine vollständige Dokumentation der semantischen Suche, einschließlich einer step-by-step Anleitung zur Verwendung der semantischen Suche, finden Sie unter Semantische Suche in der Open-Source-Dokumentation. OpenSearch

Gleichzeitige Segmentsuche in Amazon Service OpenSearch

Ab OpenSearch Version 2.17 verwendet die gleichzeitige Segmentsuche eine neue Einstellung zur Steuerung des gleichzeitigen Suchverhaltens.

- Bei neuen Domänen, die mit Version 2.17 erstellt wurden, ist die standardmäßige gleichzeitige Segmentsuche auf Knoten, die 2xl oder höher sind, standardmäßig auf den auto Modus eingestellt.
- Bei bestehenden Domains, die auf 2.17 aktualisiert werden, ist die standardmäßige gleichzeitige Segmentsuche auf auto basierend auf dem Instance-Typ für alle Knoten eingestellt, die 2xl oder höher sind, und wenn die Gesamt-CPU-Auslastung des Clusters in der letzten 1 Woche unter 45% lag.
- Weitere Informationen finden Sie unter Gleichzeitige Segmentsuche Version 2.17.

Ab OpenSearch Version 2.13 können Sie die gleichzeitige Segmentsuche verwenden, um während der Abfragephase parallel nach Segmenten zu suchen. Eine vollständige Dokumentation der gleichzeitigen Segmentsuche finden Sie unter Gleichzeitige Segmentsuche in der Open-Source-Dokumentation. OpenSearch Informationen zu CloudWatch Amazon-Metriken im Zusammenhang mit der gleichzeitigen Segmentsuche finden Sie unter Instance-Metriken und UltraWarm Metriken.

Es gibt einige zusätzliche Einschränkungen, die gelten, wenn Sie die aktuelle Segmentsuche mit Amazon OpenSearch Service verwenden:

- Sie können die gleichzeitige Segmentsuche auf Indexebene in OpenSearch Service nicht aktivieren.
- Standardmäßig verwendet OpenSearch Service eine Anzahl von 2 Slices mit dem Mechanismus „Max Slice Count“.

Generierung von Abfragen in natürlicher Sprache in Amazon OpenSearch Service

Mit der Funktion zur Generierung von Abfragen in natürlicher Sprache in Amazon OpenSearch Service können Sie Ihre Betriebs- und Sicherheitsprotokolldaten in natürlicher Sprache abfragen. OpenSearch ist eine ideale Option für die Untersuchung von Protokolldaten, da es sich um eine hochgradig skalierbare und leistungsstarke Protokollanalyse- und Suchmaschine handelt. Jetzt können Sie diese Protokolle in natürlicher Sprache untersuchen. Mit dieser Funktion können Sie Probleme identifizieren, ohne sich auf die OpenSearch Piped Processing Language (PPL) verlassen zu müssen oder beim Erstellen Ihrer Abfragen nach Datendefinitionen suchen zu müssen. Sie können die Funktion zur Generierung von Abfragen in natürlicher Sprache für OpenSearch Dienstdomänen mit Version 2.13 und höher verwenden. Sie müssen die differenzierte Zugriffskontrolle aktiviert sein.

Diese Funktion wurde mit dem OpenSearch Assistant Toolkit erstellt. Wenn Sie ähnliche Funktionen erstellen möchten, die eine Verbindung zu Ihren großen Sprachmodellen herstellen, können Sie das Toolkit verwenden, um Ihre eigenen Agenten und Tools zu konfigurieren.

Voraussetzungen

Bevor Sie die Funktion zur Generierung von Abfragen in natürlicher Sprache verwenden können, muss Ihre Domain über Folgendes verfügen:

- Version 2.13 oder höher.
- Servicesoftware R20240520-P4 oder höher.
- Differenzierte Zugriffskontrolle aktiviert Weitere Informationen finden Sie unter the section called “Aktivieren der differenzierten Zugriffskontrolle”.

Erste Schritte

Die Generierung von Abfragen in natürlicher Sprache ist standardmäßig für alle Domänen aktiviert, die mit Version 2.13 oder höher erstellt wurden und für die eine detaillierte Zugriffskontrolle aktiviert ist.

Für andere Domains aktivieren Sie es, indem Sie die Funktionen Enable Natural Language Query Generation und Amazon Q Developer auswählen.

Nachdem Sie es aktiviert haben, navigieren Sie in den OpenSearch Dashboards zur Seite Logs. Wählen Sie Event Explorer und stellen Sie mit dem Abfrageassistenten eine Frage.

Konfigurieren von Berechtigungen

Wenn Sie die Generierung von Abfragen in natürlicher Sprache in einer bereits vorhandenen OpenSearch Dienstdomäne aktivieren, ist die query_assistant_access -Rolle möglicherweise nicht für die Domäne definiert. Benutzer ohne Administratorrechte müssen dieser Rolle zugeordnet werden, um Warm-Indizes in Domains mithilfe einer fein abgestuften Zugriffskontrolle zu verwalten. Führen Sie die folgenden Schritte aus, um die query_assistant_access -Rolle manuell zu erstellen:

1. Gehen Sie in OpenSearch Dashboards zu Sicherheit und wählen Sie Rollen aus.
2. Wählen Sie Create role und konfigurieren Sie die folgenden Cluster-Berechtigungen:
   - `cluster:admin/opensearch/ml/config/get`
   - `cluster:admin/opensearch/ml/execute`
   - `cluster:admin/opensearch/ml/predict`
   - `cluster:admin/opensearch/ppl`
3. Nennen Sie die Rolle query_assistant_access.
4. Wählen Sie Rolle erstellen aus. Die Rolle query_assistant_access ist jetzt verfügbar.

> **Note**
>
> Sie müssen außerdem über die Berechtigungen `indices:admin/mappings/get` und `read` Indexberechtigungen für die Indizes verfügen, mit denen Sie Fragen in natürlicher Sprache verwenden möchten.

Automatisierung der Konfiguration

Flow Framework ist ein OpenSearch Plugin, das eine Möglichkeit bietet, OpenSearch Konfigurationen für Anwendungsfälle wie die Generierung von Abfragen und Konversationschats zu automatisieren. Da das Plugin die Ressourcen verfolgt, die die Funktion zur Generierung von Abfragen in natürlicher Sprache aktivieren, speichert der Flow Framework-Index eine Vorlage für jede Domain, die die Abfrageunterstützung verwendet.

Mit Flow Framework können Sie entweder aus einer Reihe vordefinierter Vorlagen auswählen oder Ihre eigenen Automatisierungen für Konnektoren, Tools, Agenten und andere Komponenten für maschinelles Lernen erstellen, die OpenSearch als Backend für generative Modelle dienen.

Verwenden von OpenSearch Dashboards mit Amazon Service OpenSearch

OpenSearch Dashboards ist ein Open-Source-Visualisierungstool, mit dem Sie arbeiten können. OpenSearch Amazon OpenSearch Service bietet für jede OpenSearch Service-Domain eine Installation von Dashboards. Dashboards wird auf den Hot-Data-Knoten in der Domain ausgeführt.

OpenSearch Dashboards sind ein Visualisierungstool zur Untersuchung und Analyse von Daten innerhalb einer einzigen OpenSearch Domäne. Im Gegensatz dazu ist die zentralisierte OpenSearch Benutzeroberfläche (auch als OpenSearch Anwendung bezeichnet) eine cloudbasierte Benutzeroberfläche, die eine Verbindung zu mehreren OpenSearch Domänen, OpenSearch serverlosen Sammlungen und AWS Datenquellen herstellt. Sie umfasst Arbeitsbereiche für spezifische Anwendungsfälle wie Beobachtbarkeits- und Sicherheitsanalysen und bietet ein einheitliches Erlebnis für alle Datensätze. Dashboards sind zwar an einzelne Domänen gebunden, die zentralisierte Benutzeroberfläche ermöglicht jedoch die domänenübergreifende Datenintegration und -analyse. Weitere Informationen finden Sie unter OpenSearch Benutzeroberfläche.

Einen Link zu OpenSearch Dashboards finden Sie in Ihrem Domain-Dashboard in der OpenSearch Servicekonsole. Für laufende OpenSearch Domains lautet *domain-endpoint*`/_dashboards/` die URL. Für Domains, auf denen Legacy-Elasticsearch ausgeführt wird, lautet *domain-endpoint*`/_plugin/kibana` die URL.

Abfragen, die diese Standard-Dashboards-Installation verwenden, haben ein Timeout von 300 Sekunden.

> **Note**
>
> In dieser Dokumentation werden OpenSearch Dashboards im Kontext von Amazon OpenSearch Service beschrieben, einschließlich verschiedener Verbindungsmöglichkeiten. Eine umfassende Dokumentation, einschließlich eines Leitfadens für die ersten Schritte, einer Anleitung zum Erstellen eines Dashboards, der Verwaltung von Dashboards und der Dashboards Query Language (DQL), finden Sie unter OpenSearch Dashboards in der Open-Source-Dokumentation. OpenSearch

Steuern des Zugriffs auf Dashboards

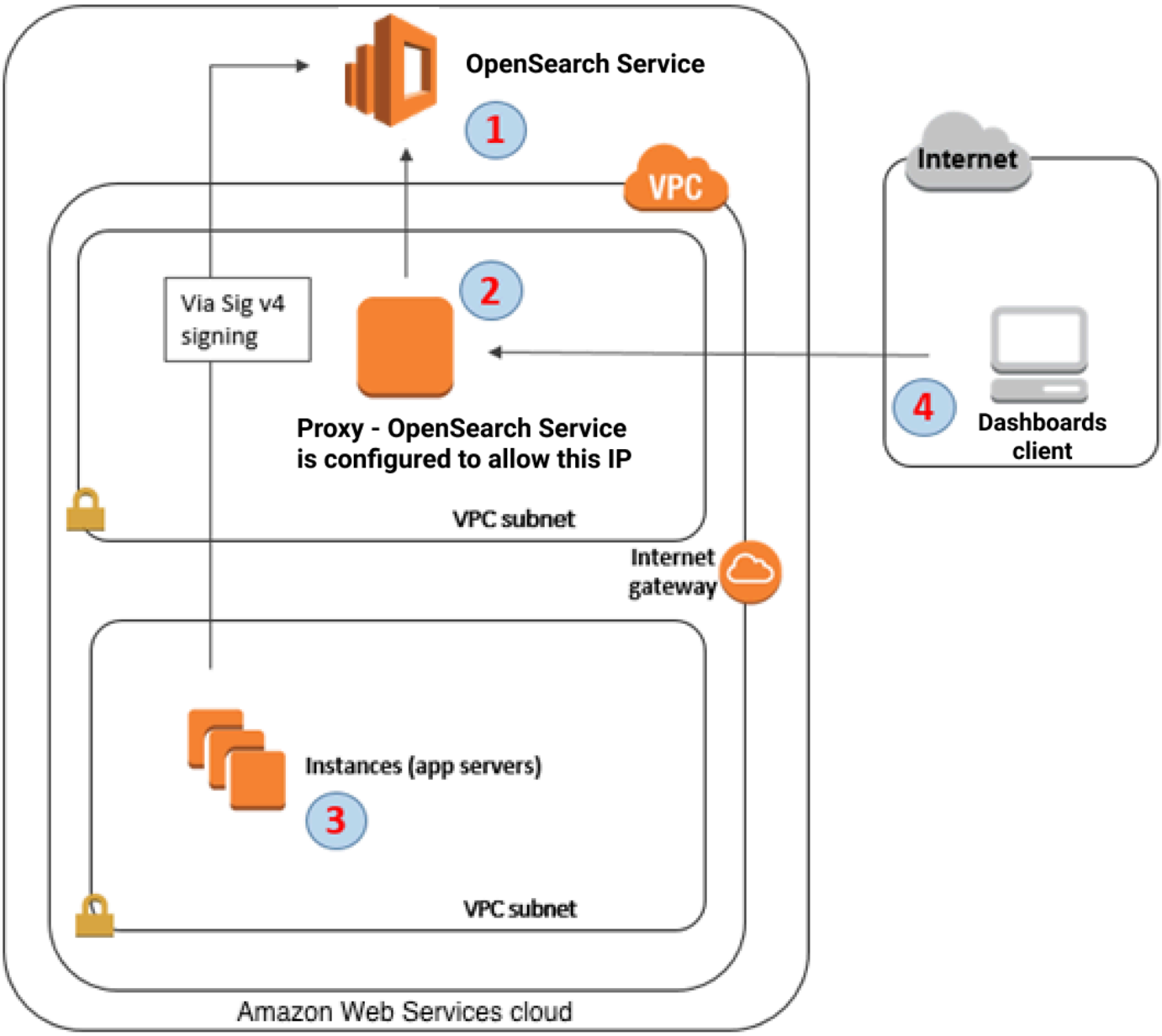
Dashboards unterstützt IAM-Benutzer und -Rollen nicht nativ, aber OpenSearch Service bietet mehrere Lösungen für die Steuerung des Zugriffs auf Dashboards:

- Aktivieren Sie die SAML-Authentifizierung für Dashboards.
- Verwenden Sie eine differenzierte Zugriffskontrolle mit HTTP-Basisauthentifizierung.
- Konfiguration Cognito-Authentifizierung für Dashboards.
- Konfigurieren Sie für öffentliche Zugriff-Domains eine IP-basierte Zugriffsrichtlinie, mit oder ohne Proxy-Server.
- Verwenden Sie für VPC-Zugriff-Domains eine offene Zugriffsrichtlinie mit oder ohne Proxyserver und Sicherheitsgruppen, um den Zugriff zu steuern. Weitere Informationen hierzu finden Sie unter the section called “Zugriffsrichtlinien für VPC-Domänen”.

Verwenden eines Proxys für den Zugriff auf den Service über Dashboards OpenSearch

> **Note**
>
> Dieses Verfahren ist nur anwendbar, wenn Ihre Domain einen öffentlichen Zugriff verwendet und Sie die Cognito-Authentifizierung nicht verwenden möchten. Siehe the section called “Steuern des Zugriffs auf Dashboards ”.

Da es sich bei Dashboards um eine JavaScript Anwendung handelt, stammen Anfragen von der IP-Adresse des Benutzers. Eine IP-basierte Zugriffskontrolle ist möglicherweise wegen der hohen Anzahl von IP-Adressen unpraktisch, die Sie erlaubt haben müssten, um jedem Benutzer Zugriff auf Dashboards zu gewähren. Eine Problemumgehung besteht darin, einen Proxyserver zwischen Dashboards und Service zu platzieren. OpenSearch Anschließend können Sie eine IP-basierte Zugriffsrichtlinie hinzufügen, mit der Anforderungen von nur einer IP-Adresse möglich sind: der Adresse des Proxys. In der folgenden Abbildung ist diese Konfiguration dargestellt.



1. Dies ist Ihre OpenSearch Service-Domain. IAM bietet autorisierten Zugriff auf diese Domain. Eine zusätzliche, IP-basierte Zugriffsrichtlinie bietet Zugriff auf den Proxy-Server.
2. Dies ist der Proxy-Server, der auf einer EC2 Amazon-Instance läuft.
3. Andere Anwendungen können den Signaturprozess von Signature Version 4 verwenden, um authentifizierte Anfragen an den OpenSearch Service zu senden.
4. Dashboard-Clients stellen über den Proxy eine Verbindung zu Ihrer OpenSearch Service-Domain her.

Wenn Sie diese Art von Konfiguration aktivieren möchten, benötigen Sie eine ressourcenbasierte Richtlinie, in der Rollen und IP-Adressen angegeben sind. Hier sehen Sie ein Beispiel für eine Richtlinie:

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Resource":"arn:aws:es:us-west-2:111111111111:domain/my-domain/*",
         "Principal":{
            "AWS":"arn:aws:iam::111111111111:role/allowedrole1"
         },
         "Action":[
            "es:ESHttpGet"
         ],
         "Effect":"Allow"
      },
      {
         "Effect":"Allow",
         "Principal":{
            "AWS":"*"
         },
         "Action":"es:*",
         "Condition":{
            "IpAddress":{
               "aws:SourceIp":[
                  "203.0.113.0/24",
                  "2001:DB8:1234:5678::/64"
               ]
            }
         },
         "Resource":"arn:aws:es:us-west-2:111111111111:domain/my-domain/*"
      }
   ]
}
```

Wir empfehlen, dass Sie die EC2 Instance, auf der der Proxy-Server ausgeführt wird, mit einer Elastic IP-Adresse konfigurieren. Auf diese Weise können Sie die Instance bei Bedarf ersetzen und weiterhin

dieselbe öffentliche IP-Adresse an sie anfügen. Weitere Informationen finden Sie unter Elastic IP Addresses im EC2 Amazon-Benutzerhandbuch.

Wenn Sie einen Proxy-Server und die Cognito-Authentifizierung, verwenden, müssen Sie möglicherweise Einstellungen für Dashboards und Amazon Cognito hinzufügen, um `redirect_mismatch`-Fehler zu vermeiden. Sehen Sie sich das folgende `nginx.conf`-Beispiel an:

```
server {
    listen 443;
    server_name $host;
    rewrite ^/$ https://$host/_plugin/_dashboards redirect;

    ssl_certificate           /etc/nginx/cert.crt;
    ssl_certificate_key       /etc/nginx/cert.key;

    ssl on;
    ssl_session_cache  builtin:1000  shared:SSL:10m;
    ssl_protocols  TLSv1 TLSv1.1 TLSv1.2;
    ssl_ciphers HIGH:!aNULL:!eNULL:!EXPORT:!CAMELLIA:!DES:!MD5:!PSK:!RC4;
    ssl_prefer_server_ciphers on;

    location /_plugin/_dashboards {
        # Forward requests to Dashboards
        proxy_pass https://$dashboards_host/_plugin/_dashboards;

        # Handle redirects to Cognito
        proxy_redirect https://$cognito_host https://$host;

        # Update cookie domain and path
        proxy_cookie_domain $dashboards_host $host;
        proxy_cookie_path / /_plugin/_dashboards/;

        # Response buffer settings
        proxy_buffer_size 128k;
        proxy_buffers 4 256k;
        proxy_busy_buffers_size 256k;
    }

    location ~ \/(log|sign|fav|forgot|change|saml|oauth2) {
        # Forward requests to Cognito
        proxy_pass https://$cognito_host;

        # Handle redirects to Dashboards
```

```
        proxy_redirect https://$dashboards_host https://$host;

        # Update cookie domain
        proxy_cookie_domain $cognito_host $host;
    }
}
```

> **Note**
>
> (Optional) Wenn Sie sich dafür entscheiden, einen dedizierten Koordinatorknoten bereitzustellen, beginnt dieser automatisch mit dem Hosten von OpenSearch Dashboards. Dadurch wird die Verfügbarkeit von Datenknotenressourcen wie CPU und Arbeitsspeicher erhöht. Diese erhöhte Verfügbarkeit von Datenknotenressourcen kann dazu beitragen, die allgemeine Ausfallsicherheit Ihrer Domain zu verbessern.

Konfiguration von Dashboards für die Verwendung eines WMS-Kartenservers

Die Standardinstallation von Dashboards for OpenSearch Service umfasst einen Kartenservice, mit Ausnahme von Domains in den Regionen Indien und China. Der Karten-Service unterstützt bis zu 10 Zoomstufen.

Unabhängig von Ihrer Region können Sie Dashboards so konfigurieren, dass ein anderer Web-Map-Server (WMS)-Server für Koordinatenkartenvisualisierungen verwendet wird. Regionskartenvisualisierungen unterstützen nur den Standardkarten-Service.

So konfigurieren Sie Dashboards für die Verwendung eines WMS-Map-Servers:

1. Öffnen von Dashboards
2. Klicken Sie auf Verwaltung von Stack.
3. Wählen Sie Advanced settings (Erweiterte Einstellungen) aus.
4. Suchen Sie Visualization:TileMap:. WMSdefaults
5. Ändern Sie `enabled` zu `true` und `url` zur URL eines gültigen WMS Map-Servers.

```
{
  "enabled": true,
  "url": "wms-server-url",
```

```
  "options": {
    "format": "image/png",
    "transparent": true
  }
}
```

6. Wählen Sie Änderungen speichern aus.

Um den neuen Standardwert auf Visualisierungen anzuwenden, müssen Sie möglicherweise Dashboards erneut laden. Wenn Sie Visualisierungen gespeichert haben, wählen Sie Options (Optionen), nachdem Sie die Visualisierung geöffnet haben. Stellen Sie sicher, dass der WMS Map Server aktiviert ist und die WMS-URL den bevorzugten Map-Server enthält, und wählen Sie dann Apply changes (Änderungen übernehmen) aus.

> **Note**
>
> Map-Services erheben häufig Lizenzgebühren oder schränken die Nutzung ein. Sie sind für all diese Aspekte des Map-Servers verantwortlich, den Sie angeben. Map-Services des U.S. Geological Survey (Geologisches Amt der USA) können zum Testen nützlich sein.

Einen lokalen Dashboards-Server mit dem Service verbinden OpenSearch

Wenn Sie bereits viel Zeit in die Konfiguration Ihrer eigenen Dashboards-Instanz investiert haben, können Sie diese anstelle der von Service bereitgestellten Standard-Dashboards-Instanz (oder zusätzlich zu) verwenden. OpenSearch Das folgende Verfahren funktioniert für Domains, die eine differenzierte Zugriffskontrolle mit einer offenen Zugriffsrichtlinie verwenden.

Um einen lokalen Dashboards-Server mit Service zu verbinden OpenSearch

1. Erstellen Sie in Ihrer OpenSearch Service-Domain einen Benutzer mit den entsprechenden Berechtigungen:

   a. Wechseln Sie in Dashboards zu Sicherheit, Interne Benutzer und wählen Sie Erstellen eines internen Benutzers aus.
   b. Geben Sie einen Benutzernamen und ein Passwort ein und wählen Sie Erstellen aus.
   c. Wechseln Sie zu Rollen und wählen Sie eine Rolle aus.

d. Wählen Sie Zugeordnete Benutzer aus, und wählen Sie Mapping verwalten aus.

e. Fügen Sie unter Benutzer Ihren Benutzernamen hinzu und wählen Sie Mapping aus.

2. Laden Sie die entsprechende Version des OpenSearch Sicherheits-Plug-ins herunter und installieren Sie sie auf Ihrer selbstverwalteten Dashboards OSS-Installation.

3. Öffnen Sie die `config/opensearch_dashboards.yml` Datei auf Ihrem lokalen Dashboards-Server und fügen Sie Ihren OpenSearch Service-Endpunkt mit dem zuvor erstellten Benutzernamen und Passwort hinzu:

```
opensearch.hosts: ['https://domain-endpoint']
opensearch.username: 'username'
opensearch.password: 'password'
```

Verwenden Sie die folgende `opensearch_dashboards.yml`-Beispieldatei:

```
server.host: '0.0.0.0'

opensearch.hosts: ['https://domain-endpoint']

opensearchDashboards.index: ".username"

opensearch.ssl.verificationMode: none # if not using HTTPS

opensearch_security.auth.type: basicauth
opensearch_security.auth.anonymous_auth_enabled: false
opensearch_security.cookie.secure: false # set to true when using HTTPS
opensearch_security.cookie.ttl: 3600000
opensearch_security.session.ttl: 3600000
opensearch_security.session.keepalive: false
opensearch_security.multitenancy.enabled: false
opensearch_security.readonly_mode.roles: ['opensearch_dashboards_read_only']
opensearch_security.auth.unauthenticated_routes: []
opensearch_security.basicauth.login.title: 'Please log in using your username and
 password'

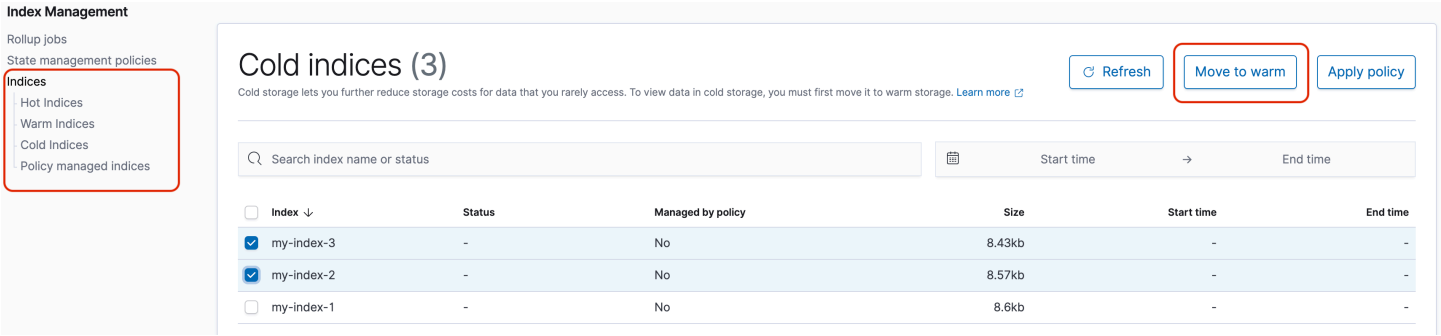
opensearch.username: 'username'
opensearch.password: 'password'
opensearch.requestHeadersWhitelist: [authorization, securitytenant,
 security_tenant]
```

Um Ihre OpenSearch Service-Indizes zu sehen, starten Sie Ihren lokalen Dashboards-Server, gehen Sie zu Dev Tools und führen Sie den folgenden Befehl aus:

```
GET _cat/indices
```

Indizes in Dashboards verwalten

Die Dashboards-Installation auf Ihrer OpenSearch Service-Domain bietet eine nützliche Benutzeroberfläche für die Verwaltung von Indizes in verschiedenen Speicherebenen Ihrer Domain. Wählen Sie im Hauptmenü der Dashboards die Option Indexverwaltung aus, UltraWarmum alle Indizes im Hot- und Cold-Storage sowie Indizes, die durch Index State Management (ISM) -Richtlinien verwaltet werden, anzuzeigen. Verwenden Sie die Indexverwaltung, um Indizes zwischen Warm- und Cold-Speicher zu verschieben und Migrationen zwischen den drei Ebenen zu überwachen.



Beachten Sie, dass die Indexoptionen „Heiß“, „Warm“ und „Kalter Speicher“ nicht angezeigt werden, es sei denn, Sie haben UltraWarm und/oder Kaltspeicher aktiviert.

Weitere Features

Die Standardinstallation von Dashboards auf jeder OpenSearch Service-Domain bietet einige zusätzliche Funktionen:

- Benutzeroberflächen für die verschiedenen Plugins OpenSearch
- Mandanten
- Berichte

  Verwenden Sie das Menü Berichterstellung, um CSV-Berichte on demand von der Entdecken-Seite und PDF- oder PNG-Berichte von Dashboards oder Visualisierungen zu generieren. CSV-Berichte haben eine Begrenzung von 10.000 Zeilen.

- Gantt-Diagramme
- Notebooks

Verwenden der OpenSearch Benutzeroberfläche in Amazon OpenSearch Service

OpenSearch UI (Benutzerschnittstelle) ist ein modernisiertes operatives Analyseerlebnis für Amazon OpenSearch Service, das Ihnen eine einheitliche Ansicht für die Interaktion mit Daten aus mehreren Quellen bietet. Im Gegensatz zu OpenSearch Dashboards, die nur mit der einen Domain oder Sammlung funktionieren, die sie hostet, wird die OpenSearch Benutzeroberfläche in der gehostet. AWS Cloud Auf diese Weise kann die OpenSearch Benutzeroberfläche eine hohe Verfügbarkeit erreichen und bei Cluster-Upgrades funktionsfähig bleiben. Außerdem kann eine native Verbindung mit mehreren Datenquellen hergestellt werden. Informationen zu OpenSearch Dashboards finden Sie unter. OpenSearch Dashboards

Im Folgenden sind die wichtigsten Funktionen der OpenSearch Benutzeroberfläche aufgeführt:

- Unterstützung mehrerer Datenquellen — Die OpenSearch Benutzeroberfläche kann eine Verbindung zu mehreren Datenquellen herstellen, um eine umfassende Ansicht zu erstellen. Dazu gehören OpenSearch Domains und serverlose Sammlungen sowie integrierte AWS Datenquellen wie Amazon CloudWatch, Amazon Security Lake und Amazon Simple Storage Service (Amazon S3).
- Keine Ausfallzeiten bei Upgrades — die OpenSearch Benutzeroberfläche wird im AWS Cloud gehostet. Dies bedeutet, dass es betriebsbereit OpenSearch bleibt und während Upgrade-Prozessen Daten aus Clustern abrufen kann.
- Arbeitsbereiche — Kuratierte Bereiche für die Zusammenarbeit im Team für verschiedene Workflows wie Observability, Security Analytics und Search. Du kannst die Datenschutzeinstellungen definieren und die Berechtigungen für Mitarbeiter in deinem Workspace verwalten.
- Single Sign-On — Die OpenSearch Benutzeroberfläche arbeitet mit SAML über AWS Identity and Access Management (IAM) AWS IAM Identity Center -Verbund zusammen, um die Integration mit deinen Identitätsanbietern zu ermöglichen und deinen Endbenutzern eine Single-Sign-On-Erfahrung zu bieten.
- GENAI-gestützte Analytik — Die OpenSearch Benutzeroberfläche unterstützt die Generierung von Abfragen in natürlicher Sprache, sodass Sie die richtigen Abfragen für Ihre Analyse generieren können. OpenSearch UI arbeitet auch mit Amazon Q Developer zusammen, um den Amazon Q-Chat bereitzustellen und bei der Generierung von Visualisierungen, Warnungszusammenfassungen, Erkenntnissen und empfohlenen Anomaliedetektoren zu helfen.

- Unterstützung mehrerer Abfragesprachen — Die OpenSearch Benutzeroberfläche unterstützt Piped Processing Language (PPL), SQL, Lucene und Dashboards Query Language (DQL).
- Regions- und kontenübergreifende Unterstützung — Die OpenSearch Benutzeroberfläche kann die clusterübergreifende Suchfunktion nutzen, um für aggregierte Analysen und Visualisierungen eine Verbindung zu OpenSearch Domains in verschiedenen Konten und Regionen herzustellen.

Folgen Sie den Anweisungen unter, um loszulegen und Ihre erste OpenSearch Benutzeroberfläche zu erstellen. the section called “Erste Schritte”

Informationen zu den neuesten Funktionen, die für die OpenSearch Benutzeroberfläche veröffentlicht wurden, finden Sie unterthe section called “Versionsverlauf”.

Themen

- Versionsverlauf der Amazon OpenSearch Service-Benutzeroberfläche
- Erste Schritte mit der OpenSearch Benutzeroberfläche in Amazon OpenSearch Service
- Aktivierung des SAML-Verbunds mit AWS Identity and Access Management
- Verwaltung von Datenquellenzuordnungen und Virtual Private Cloud-Zugriffsberechtigungen
- Amazon OpenSearch Service-Workspaces verwenden
- Regions- und kontoübergreifender Datenzugriff mit clusterübergreifender Suche
- Verwaltung des Zugriffs auf die OpenSearch Benutzeroberfläche von einem VPC-Endpunkt aus

Versionsverlauf der Amazon OpenSearch Service-Benutzeroberfläche

In der folgenden Tabelle sind alle Versionen des Amazon OpenSearch Service-Supports für OpenSearch UI sowie die Funktionen und Verbesserungen aufgeführt, die in jeder Version enthalten sind.

Änderung	Datum der Veröffentlichung	Beschreibung
Neues Feature	2025-04-16	OpenSearch Die Benutzeroberfläche funktioniert jetzt mit der clusterübergreifenden Suche. Auf diese Weise können Sie die OpenSearch Benutzeroberfläche in einer Region verwenden

Änderung	Datum der Veröffentlichung	Beschreibung
		AWS-Region , um auf Cluster in einer anderen Region zuzugreifen. Dazu wird es als Remote-Cluster konfiguriert, der mit einem Cluster in derselben Region verbunden ist. Weitere Informationen finden Sie unter the section called “Regions- und kontoübergreifender Datenzugriff mit clusterübergreifender Suche”.
Neues Feature	2025-03-31	Amazon Q Developer ist jetzt allgemein in Amazon OpenSearch Service verfügbar. Weitere Informationen finden Sie unter Amazon-Q-Unterstützung.
Neues Feature	05.02.2025	Der Verbund von Security Assertion Markup Language 2.0 (SAML) über AWS Identity and Access Management (IAM) funktioniert jetzt mit der Benutzeroberfläche. OpenSearch Auf diese Weise ist es möglich, ein vom Identitätsanbieter initiiert es Single Sign-On (SSO) -Erlebnis für Ihre Endbenutzer zu schaffen. Weitere Informationen finden Sie unter the section called “Aktivieren des SAML-Verbunds mit IAM”.
Neue Integration	2024-12-01	Die Zero-ETL-Integration mit Amazon CloudWatch vereinfacht die Analyse und Visualisierung von Protokolldaten und reduziert so den technischen Aufwand und die Betriebskosten. Weitere Informationen finden Sie im AWS News-Blog unter New Amazon CloudWatch and Amazon OpenSearch Service launchen ein integriertes Analyseerlebnis.
Neue Integration	2024-12-01	Die Zero-ETL-Integration mit Amazon Security Lake ermöglicht es Unternehmen, ihre Sicherheitsdaten effizient zu durchsuchen, zu analysieren und umsetzbare Erkenntnisse aus ihnen zu gewinnen. Weitere Informationen finden Sie im AWS News-Blog unter Einführung der Integration von Amazon OpenSearch Service und Amazon Security Lake zur Vereinfachung von Sicherheitsanalysen.

Änderung	Datum der Veröffentlichung	Beschreibung
Erstversion	2024-11-07	Die erste öffentliche Version von UI. OpenSearch Weitere Informationen finden Sie im AWS Big Data-Blog unter Amazon OpenSearch Service launcht die OpenSearch Benutzeroberfläche der nächsten Generation.

Erste Schritte mit der OpenSearch Benutzeroberfläche in Amazon OpenSearch Service

In Amazon OpenSearch Service ist eine Anwendung eine Instanz der OpenSearch Benutzeroberfläche (OpenSearch UI). Jede Anwendung kann mehreren Datenquellen zugeordnet werden, und eine einzelne Quelle kann mehreren Anwendungen zugeordnet werden. Sie können mehrere Anwendungen für verschiedene Administratoren mithilfe verschiedener unterstützter Authentifizierungsoptionen erstellen.

Verwenden Sie die Informationen in diesem Thema, um Sie durch den Prozess der Erstellung einer OpenSearch Benutzeroberflächenanwendung mit dem AWS Management Console oder dem zu führen AWS CLI.

Themen

- Erforderliche Berechtigungen für die Erstellung von Amazon OpenSearch Service-Anwendungen
- Eine OpenSearch UI-Anwendung erstellen
- Verwaltung von Anwendungsadministratoren

Erforderliche Berechtigungen für die Erstellung von Amazon OpenSearch Service-Anwendungen

Bevor Sie eine Anwendung erstellen, stellen Sie sicher, dass Ihnen die erforderlichen Berechtigungen für die Aufgabe erteilt wurden. Wenden Sie sich bei Bedarf an einen Kontoadministrator, um Unterstützung zu erhalten.

Allgemeine Berechtigungen

Um mit Anwendungen in OpenSearch Service arbeiten zu können, benötigen Sie die in der folgenden Richtlinie aufgeführten Berechtigungen. Die Berechtigungen dienen den folgenden Zwecken:

- Die fünf `es:*Application` Berechtigungen sind erforderlich, um eine Anwendung zu erstellen und zu verwalten.
- Die drei `es:*Tags` Berechtigungen sind erforderlich, um der Anwendung Tags hinzuzufügen, aufzulisten und zu entfernen.
- Die `es:GetDirectQueryDataSource` Berechtigungen `es:DescribeDomain` und sind erforderlich`aoss:BatchGetCollection`, um Datenquellen zuzuordnen.
- Die `opensearch:*DirectQuery*` Berechtigungen `aoss:APIAccessAlles:ESHttp*`, und 4 sind für den Zugriff auf Datenquellen erforderlich.
- Das `iam:CreateServiceLinkedRole` gibt Amazon OpenSearch Service die Erlaubnis, eine serviceverknüpfte Rolle (SLR) in Ihrem Konto zu erstellen. Diese Rolle wird verwendet und ermöglicht es der OpenSearch UI-Anwendung, CloudWatch Amazon-Metriken in Ihrem Konto zu veröffentlichen. Weitere Informationen finden Sie unter the section called “Berechtigungen” im Thema Verwenden von serviceverknüpften Rollen zur Erstellung von VPC-Domains und zur direkten Abfrage von Datenquellen.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "es:CreateApplication",
                "es:DeleteApplication",
                "es:GetApplication",
                "es:ListApplications",
                "es:UpdateApplication",
                "es:AddTags",
                "es:ListTags",
                "es:RemoveTags",
                "aoss:APIAccessAll",
```

```
                "es:ESHttp*",
                "opensearch:StartDirectQuery",
                "opensearch:GetDirectQuery",
                "opensearch:CancelDirectQuery",
                "opensearch:GetDirectQueryResult",
                "aoss:BatchGetCollection",
                "aoss:ListCollections",
                "es:DescribeDomain",
                "es:DescribeDomains",
                "es:ListDomainNames",
                "es:GetDirectQueryDataSource",
                "es:ListDirectQueryDataSources"
            ],
            "Resource": "*"
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/
opensearchservice.amazonaws.com/AWSServiceRoleForAmazonOpenSearchService"
        }
    ]
}
```

Berechtigungen zum Erstellen einer Anwendung, die die IAM Identity Center-Authentifizierung verwendet (optional)

Standardmäßig werden Dashboard-Anwendungen mithilfe von AWS Identity and Access Management (IAM) authentifiziert, um die Berechtigungen für AWS Ressourcenbenutzer zu verwalten. Sie können sich jedoch dafür entscheiden, ein Single Sign-On-Erlebnis bereitzustellen, indem Sie IAM Identity Center verwenden, sodass Sie Ihre vorhandenen Identitätsanbieter für die Anmeldung bei UI-Anwendungen verwenden können. OpenSearch In diesem Fall wählen Sie im Verfahren weiter unten in diesem Thema die Option Authentifizierung mit IAM Identity Center aus und gewähren dann IAM Identity Center-Benutzern die für den Zugriff auf die OpenSearch UI-Anwendung erforderlichen Berechtigungen.)

Um eine Anwendung zu erstellen, die die IAM Identity Center-Authentifizierung verwendet, benötigen Sie die folgenden Berechtigungen. Ersetzen Sie *`placeholder values`* durch Ihre Informationen. Wenden Sie sich bei Bedarf an einen Kontoadministrator, um Unterstützung zu erhalten.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "IDC_Permissions",
            "Effect": "Allow",
            "Action": [
                "es:CreateApplication",
                "es:DeleteApplication",
                "es:GetApplication",
                "es:ListApplications",
                "es:UpdateApplication",
                "es:AddTags",
                "es:ListTags",
                "es:RemoveTags",
                "aoss:BatchGetCollection",
                "aoss:ListCollections",
                "es:DescribeDomain",
                "es:DescribeDomains",
                "es:ListDomainNames",
                "es:GetDirectQueryDataSource",
                "es:ListDirectQueryDataSources",
                "sso:CreateApplication",
                "sso:DeleteApplication",
                "sso:PutApplicationGrant",
                "sso:PutApplicationAccessScope",
                "sso:PutApplicationAuthenticationMethod",
                "sso:ListInstances",
                "sso:DescribeApplicationAssignment",
                "sso:DescribeApplication",
                "sso:CreateApplicationAssignment",
                "sso:ListApplicationAssignments",
                "sso:DeleteApplicationAssignment",
                "sso-directory:SearchGroups",
                "sso-directory:SearchUsers",
                "sso:ListDirectoryAssociations",
                "identitystore:DescribeUser",
                "identitystore:DescribeGroup",
                "iam:ListRoles"
            ],
            "Resource": "*"
```

```
        },
        {
            "Sid": "SLR_Permission",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/
opensearchservice.amazonaws.com/AWSServiceRoleForAmazonOpenSearchService"
        },
        {
            "Sid": "PassRole_Permission",
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::account-id}:role/iam-role-for-identity-
center"
        }
    ]
}
```

Eine OpenSearch UI-Anwendung erstellen

Erstellen Sie mithilfe eines der folgenden Verfahren eine Anwendung, die einen Anwendungsnamen, eine Authentifizierungsmethode und Administratoren angibt.

Themen

- Erstellen einer OpenSearch UI-Anwendung, die die IAM-Authentifizierung in der Konsole verwendet
- Erstellen einer OpenSearch UI-Anwendung, die AWS IAM Identity Center Authentifizierung in der Konsole verwendet
- Erstellen einer OpenSearch UI-Anwendung, die AWS IAM Identity Center Authentifizierung mit dem verwendet AWS CLI

Erstellen einer OpenSearch UI-Anwendung, die die IAM-Authentifizierung in der Konsole verwendet

Um eine OpenSearch UI-Anwendung zu erstellen, die die IAM-Authentifizierung in der Konsole verwendet

1. Melden Sie sich zu https://console.aws.amazon.com/aos/Hause bei der Amazon OpenSearch Service-Konsole an.
2. Wählen Sie im linken Navigationsbereich OpenSearch UI (Dashboards) aus.
3. Wählen Sie Create application aus.
4. Geben Sie unter Anwendungsname einen Namen für die Anwendung ein.
5. Aktivieren Sie nicht das Kontrollkästchen Authentifizierung mit IAM Identity Center. Informationen zum Erstellen einer Anwendung mit Authentifizierung über finden Sie AWS IAM Identity Center weiter unten the section called “Erstellen einer OpenSearch UI-Anwendung, die AWS IAM Identity Center Authentifizierung in der Konsole verwendet” in diesem Thema.
6. (Optional) Sie werden automatisch als Administrator der Anwendung hinzugefügt, die Sie erstellen. Im Verwaltungsbereich für OpenSearch Anwendungsadministratoren können Sie anderen Benutzern Administratorrechte gewähren.

   > **Note**
   >
   > Die Administratorrolle für OpenSearch UI-Anwendungen gewährt Berechtigungen zum Bearbeiten und Löschen einer OpenSearch UI-Anwendung. Anwendungsadministratoren können auch Arbeitsbereiche in einer OpenSearch UI-Anwendung erstellen, bearbeiten und löschen.

   Um anderen Benutzern Administratorrechte zu gewähren, wählen Sie eine der folgenden Optionen:

   - Spezifischen Benutzern Administratorrechte gewähren — Wählen Sie im Feld OpenSearchAnwendungsadministratoren in der Popupliste „Eigenschaften“ die Option IAM-Benutzer oder

     AWS IAM Identity Center Benutzer und wählen Sie dann die einzelnen Benutzer aus, denen Administratorrechte erteilt werden sollen.

- Allen Benutzern Administratorrechte gewähren — Allen Benutzern in Ihrer Organisation oder Ihrem Konto werden Administratorrechte gewährt.

7. (Optional) Wenden Sie im Bereich „Tags“ ein oder mehrere name/value Tag-Schlüsselpaare auf die Anwendung an.

   Tags sind optionale Metadaten, die Sie einer Ressource zuweisen. Mithilfe von Tags können Sie eine Ressource unterschiedlich kategorisieren, beispielsweise nach Zweck, Besitzer oder Umgebung.

8. Wählen Sie Erstellen aus.

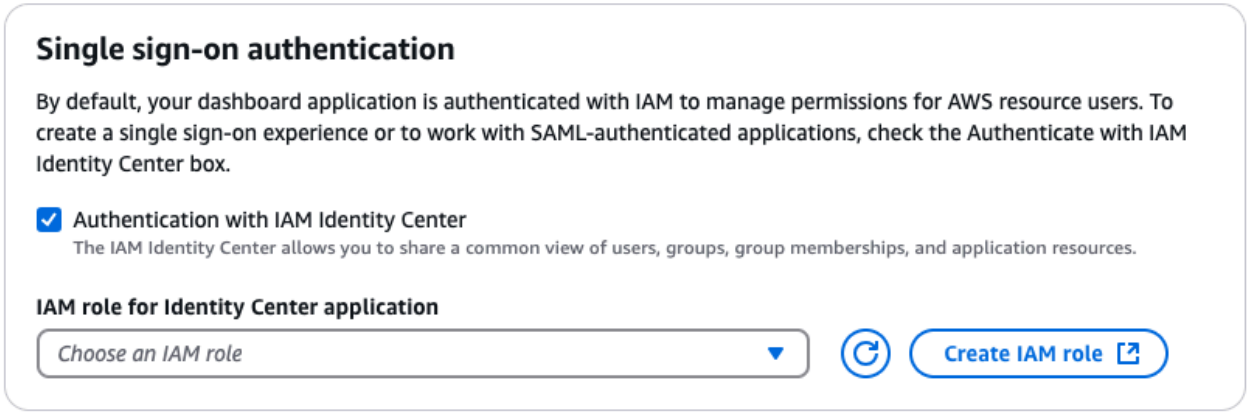
Erstellen einer OpenSearch UI-Anwendung, die AWS IAM Identity Center Authentifizierung in der Konsole verwendet

Um eine OpenSearch UI-Anwendung zu erstellen, die AWS IAM Identity Center Authentifizierung verwendet, benötigen Sie die weiter oben in diesem Thema unter beschriebenen IAM-Berechtigungen. the section called “Berechtigungen zum Erstellen einer Anwendung, die die IAM Identity Center-Authentifizierung verwendet (optional)”

So erstellen Sie eine OpenSearch UI-Anwendung, die AWS IAM Identity Center Authentifizierung in der Konsole verwendet

1. Melden Sie sich zu https://console.aws.amazon.com/aos/Hause bei der Amazon OpenSearch Service-Konsole an.
2. Wählen Sie im linken Navigationsbereich OpenSearch UI (Dashboards) aus.
3. Wählen Sie Create application aus.
4. Geben Sie unter Anwendungsname einen Namen für die Anwendung ein.
5. (Optional) Gehen Sie wie folgt vor, um Single Sign-On für Ihre Organisation oder Ihr Konto zu aktivieren:

   a. Aktivieren Sie das Kontrollkästchen Authentifizierung mit IAM Identity Center, wie in der folgenden Abbildung gezeigt:



b. Führen Sie eine der folgenden Aktionen aus:

- Wählen Sie in der Anwendungsliste „IAM-Rolle für Identity Center“ eine bestehende IAM-Rolle aus, die die erforderlichen Berechtigungen für den Zugriff auf die Benutzeroberfläche und die zugehörigen Datenquellen für IAM Identity Center bereitstellt. OpenSearch In den Richtlinien im nächsten Aufzählungszeichen finden Sie die Berechtigungen, über die die Rolle verfügen muss.
- Erstellen Sie eine neue Rolle mit den erforderlichen Berechtigungen. Verwenden Sie die folgenden Verfahren im IAM-Benutzerhandbuch mit den angegebenen Optionen, um eine neue Rolle und mit den erforderlichen Berechtigungsrichtlinien und Vertrauensrichtlinien zu erstellen.
  - Verfahren: IAM-Richtlinien erstellen (Konsole)

    Fügen Sie die folgenden Richtlinien in das JSON-Feld des Policy-Editors ein, während Sie die Schritte in diesem Verfahren ausführen:

    JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "IdentityStoreOpenSearchDomainConnectivity",
            "Effect": "Allow",
            "Action": [
                "identitystore:DescribeUser",
                "identitystore:ListGroupMembershipsForMember",
                "identitystore:DescribeGroup"
            ],
```

```
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:CalledViaLast": "es.amazonaws.com"
                }
            }
        },
        {
            "Sid": "OpenSearchDomain",
            "Effect": "Allow",
            "Action": [
                "es:ESHttp*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "OpenSearchServerless",
            "Effect": "Allow",
            "Action": [
                "aoss:APIAccessAll"
            ],
            "Resource": "*"
        }
    ]
}
```

- Verfahren: Erstellen Sie eine Rolle mithilfe benutzerdefinierter Vertrauensrichtlinien

  Wenn Sie die Schritte in diesem Verfahren ausführen, ersetzen Sie den Platzhalter JSON im Feld Benutzerdefinierte Vertrauensrichtlinie durch Folgendes:

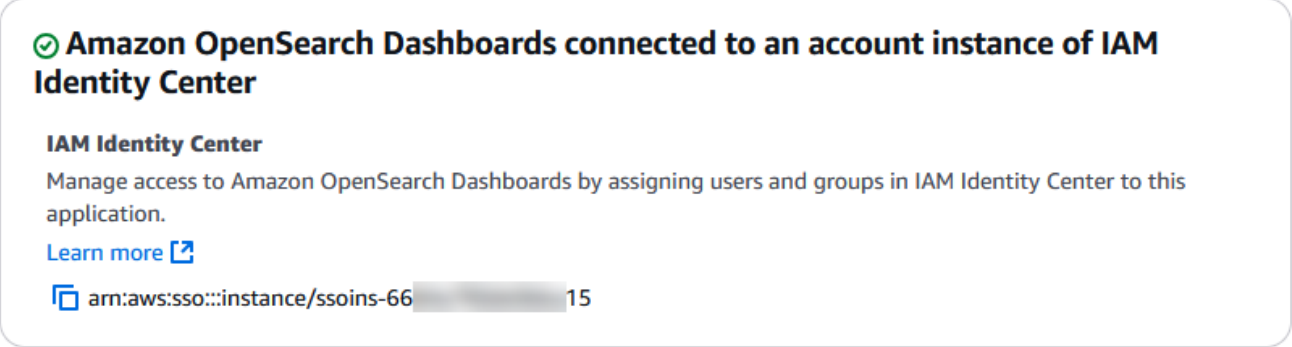
  > **Tip**
  >
  > Wenn Sie die Vertrauensrichtlinie zu einer vorhandenen Rolle hinzufügen, fügen Sie die Richtlinie auf der Registerkarte Vertrauensverhältnis der Rolle hinzu.

  JSON

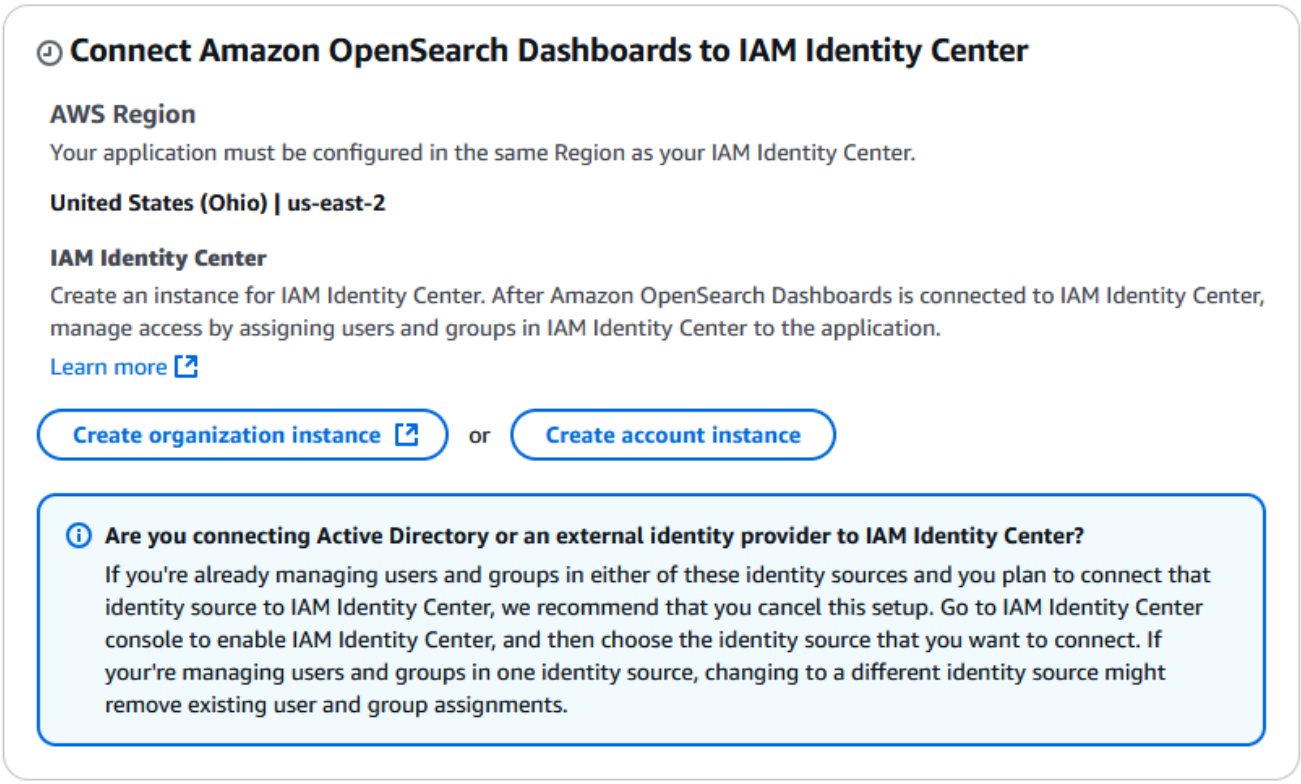
  ```
  {
      "Version": "2012-10-17",
      "Statement": [
  ```

```
        {
            "Effect": "Allow",
            "Principal": {
                "Service":
 "application.opensearchservice.amazonaws.com"
            },
            "Action": [
                "sts:AssumeRole",
                "sts:SetContext"
            ],
            "Condition": {
                "ForAllValues:ArnEquals": {
                    "sts:RequestContextProviders":
 "arn:aws:iam::aws:contextProvider/IdentityCenter"
                }
            }
        }
    ]
}
```

c. Wenn in Ihrer Organisation oder Ihrem Konto bereits eine IAM Identity Center-Instance erstellt wurde, meldet die Konsole, dass Amazon OpenSearch Dashboards bereits mit einer Organisationsinstanz von IAM Identity Center verbunden ist, wie in der folgenden Abbildung dargestellt.



Wenn IAM Identity Center in Ihrer Organisation oder Ihrem Konto noch nicht verfügbar ist, können Sie oder ein Administrator mit den erforderlichen Berechtigungen eine Organisations- oder Kontoinstanz erstellen. Der Bereich Amazon OpenSearch Dashboards mit IAM Identity Center Connect bietet Optionen für beide, wie in der folgenden Abbildung dargestellt:

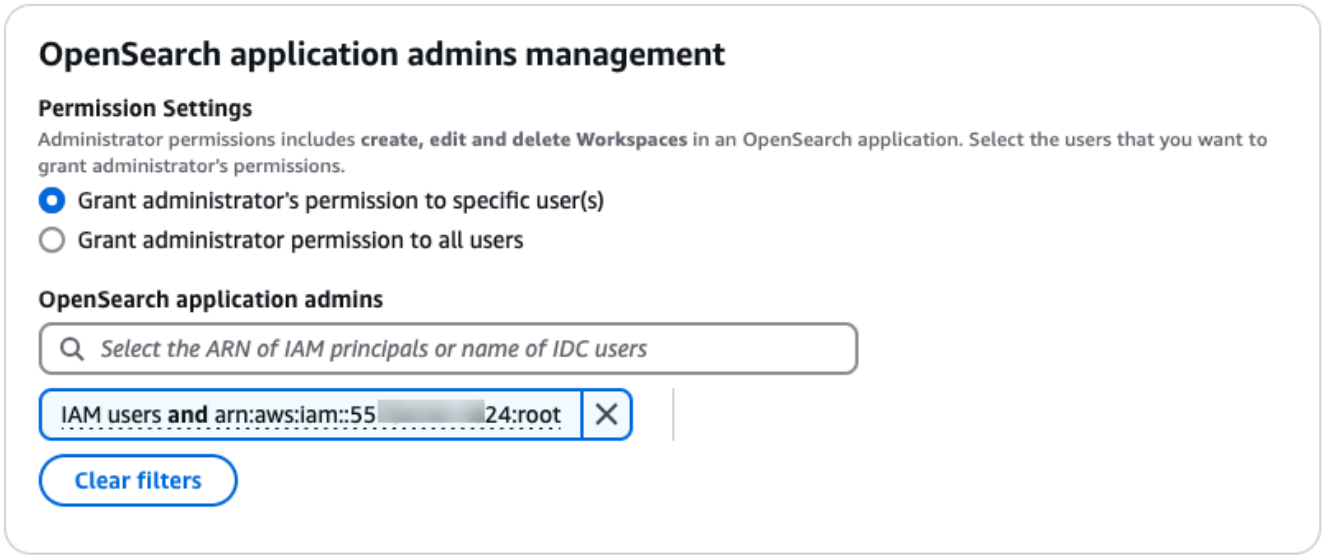


In diesem Fall können Sie zu Testzwecken eine Account-Instance in IAM Identity Center erstellen oder einen Administrator auffordern, eine Organisations-Instance im IAM Identity Center zu erstellen. Weitere Informationen finden Sie in folgenden Themen im AWS IAM Identity Center -Benutzerhandbuch:

> **Note**
>
> Derzeit können OpenSearch UI-Anwendungen nur in derselben AWS-Region IAM Identity Center-Organisationsinstanz erstellt werden. Informationen zum Zugriff auf Datenquellen in dieser Region, nachdem Sie die Anwendung erstellt haben, finden Sie unterthe section called “Regions- und kontoübergreifender Datenzugriff mit clusterübergreifender Suche”.

- Organisationsinstanzen von IAM Identity Center
- Kontoinstanzen von IAM Identity Center
- Aktivieren AWS IAM Identity Center

6. (Optional) Sie werden automatisch als Administrator der Anwendung hinzugefügt, die Sie erstellen. Im Verwaltungsbereich für OpenSearch Anwendungsadministratoren können Sie anderen Benutzern Administratorrechte gewähren, wie in der folgenden Abbildung dargestellt:



> **Note**
>
> Die Administratorrolle für OpenSearch UI-Anwendungen gewährt Berechtigungen zum Bearbeiten und Löschen einer OpenSearch UI-Anwendung. Anwendungsadministratoren können auch Arbeitsbereiche in einer OpenSearch UI-Anwendung erstellen, bearbeiten und löschen.

Um anderen Benutzern Administratorrechte zu gewähren, wählen Sie eine der folgenden Optionen:

- Spezifischen Benutzern Administratorrechte gewähren — Wählen Sie im Feld OpenSearchAnwendungsadministratoren in der Popupliste „Eigenschaften“ die Option IAM-Benutzer oder

  AWS IAM Identity Center Benutzer und wählen Sie dann die einzelnen Benutzer aus, denen Administratorrechte erteilt werden sollen.
- Allen Benutzern Administratorrechte gewähren — Allen Benutzern in Ihrer Organisation oder Ihrem Konto werden Administratorrechte gewährt.

7. (Optional) Wenden Sie im Bereich „Tags“ ein oder mehrere name/value Tag-Schlüsselpaare auf die Anwendung an.

   Tags sind optionale Metadaten, die Sie einer Ressource zuweisen. Mithilfe von Tags können Sie eine Ressource unterschiedlich kategorisieren, beispielsweise nach Zweck, Besitzer oder Umgebung.
8. Wählen Sie Erstellen aus.

Erstellen einer OpenSearch UI-Anwendung, die AWS IAM Identity Center Authentifizierung mit dem verwendet AWS CLI

Um eine OpenSearch UI-Anwendung zu erstellen, die AWS IAM Identity Center Authentifizierung mithilfe von verwendet AWS CLI, verwenden Sie den Befehl create-application mit den folgenden Optionen:

- `--name`— Der Name der Anwendung.
- `--iam-identity-center-options`— (Optional) Die IAM Identity Center-Instanz und die IAM-Rolle, die für die Authentifizierung und Zugriffskontrolle verwendet OpenSearch werden.

Ersetzen Sie *`placeholder values`* durch Ihre Informationen.

```
aws opensearch create-application \
    --name application-name \
    --iam-identity-center-options "
          {
          \"enabled\":true,
          \"iamIdentityCenterInstanceArn\":\"arn:aws:sso:::instance/sso-instance\",
          \"iamRoleForIdentityCenterApplicationArn\":\"arn:aws:iam::account-
id:role/role-name\"
          }
    "
```

Verwaltung von Anwendungsadministratoren

Ein OpenSearch UI-Anwendungsadministrator ist eine definierte Rolle mit der Berechtigung, eine OpenSearch UI-Anwendung zu bearbeiten und zu löschen.

Standardmäßig sind Sie als Ersteller einer OpenSearch UI-Anwendung der erste Administrator der OpenSearch UI-Anwendung.

Verwaltung von OpenSearch UI-Administratoren mithilfe der Konsole

Sie können einer OpenSearch UI-Anwendung zusätzliche Administratoren hinzufügen AWS Management Console, entweder während des Workflows zur Anwendungserstellung oder auf der Seite Bearbeiten, nachdem die Anwendung erstellt wurde.

Die Administratorrolle einer OpenSearch UI-Anwendung gewährt Berechtigungen zum Bearbeiten und Löschen einer OpenSearch UI-Anwendung. Anwendungsadministratoren können auch Arbeitsbereiche in einer OpenSearch UI-Anwendung erstellen, bearbeiten und löschen.

Auf einer Anwendungsdetailseite können Sie nach dem Amazon-Ressourcennamen (ARN) eines IAM-Prinzipals oder nach dem Namen eines IAM Identity Center-Benutzers suchen.

Um OpenSearch UI-Administratoren über die Konsole zu verwalten

1. Melden Sie sich zu https://console.aws.amazon.com/aos/Hause bei der Amazon OpenSearch Service-Konsole an.
2. Wählen Sie im linken Navigationsbereich OpenSearch UI (Dashboards) aus.
3. Wählen Sie im OpenSearch Anwendungsbereich den Namen einer vorhandenen Anwendung aus.
4. Wählen Sie Edit (Bearbeiten) aus.
5. Um anderen Benutzern Administratorrechte zu gewähren, wählen Sie eine der folgenden Optionen:

   - Spezifischen Benutzern Administratorrechte gewähren — Wählen Sie im Feld OpenSearchAnwendungsadministratoren in der Popupliste „Eigenschaften“ die Option IAM-Benutzer oder

     AWS IAM Identity Center Benutzer und wählen Sie dann die einzelnen Benutzer aus, denen Administratorrechte erteilt werden sollen.
   - Allen Benutzern Administratorrechte gewähren — Allen Benutzern in Ihrer Organisation oder Ihrem Konto werden Administratorrechte gewährt.
6. Wählen Sie Aktualisieren.

Sie können weitere Administratoren entfernen, aber jede OpenSearch UI-Anwendung muss mindestens einen Administrator behalten.

Verwaltung von OpenSearch UI-Administratoren mit dem AWS CLI

Sie können OpenSearch UI-Anwendungsadministratoren mit dem erstellen und aktualisieren AWS CLI.

Erstellen von OpenSearch Benutzeroberflächenadministratoren mit dem AWS CLI

Im Folgenden finden Sie Beispiele für das Hinzufügen von IAM-Prinzipalen und IAM Identity Center-Benutzern als Administratoren bei der Erstellung einer OpenSearch UI-Anwendung.

Beispiel 1: Erstellen Sie eine OpenSearch UI-Anwendung, die einen IAM-Benutzer als Administrator hinzufügt

Führen Sie den folgenden Befehl aus, um eine OpenSearch UI-Anwendung zu erstellen, die einen IAM-Benutzer als Administrator hinzufügt. Ersetzen Sie *placeholder values* durch Ihre Informationen.

```
aws opensearch create-application \
    --name application-name \
    --app-configs "
        {
        \"key\":\"opensearchDashboards.dashboardAdmin.users\",
        \"value\":\"arn:aws:iam::account-id:user/user-id\"
        }
    "
```

Beispiel 2: Erstellen Sie eine OpenSearch UI-Anwendung, die IAM Identity Center aktiviert und eine IAM Identity Center-Benutzer-ID als OpenSearch UI-Anwendungsadministrator hinzufügt

Führen Sie den folgenden Befehl aus, um eine OpenSearch UI-Anwendung zu erstellen, die IAM Identity Center aktiviert und eine IAM Identity Center-Benutzer-ID als UI-Anwendungsadministrator hinzufügt. OpenSearch Ersetzen Sie *placeholder values* durch Ihre Informationen.

`key`gibt das festzulegende Konfigurationselement an, z. B. die Administratorrolle für die OpenSearch UI-Anwendung. Gültige Werte sind `opensearchDashboards.dashboardAdmin.users` und `opensearchDashboards.dashboardAdmin.groups`.

*xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx*steht für den Wert, der dem Schlüssel zugewiesen wurde, z. B. den Amazon-Ressourcennamen (ARN) eines IAM-Benutzers.

```
aws opensearch create-application \
```

```
    --name myapplication \
    --iam-identity-center-options "
        {
        \"enabled\":true,
        \"iamIdentityCenterInstanceArn\":\"arn:aws:sso:::instance/ssoins-instance-id\",
        \"iamRoleForIdentityCenterApplicationArn\":\"arn:aws:iam::account-id:role/role-
name\"
        }
    " \
    --app-configs "
        {
        \"key\":\"opensearchDashboards.dashboardAdmin.users\",
        \"value\":\"xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx\"
        }
    "
```

Aktualisierung von OpenSearch UI-Administratoren mithilfe der AWS CLI

Im Folgenden finden Sie Beispiele für die Aktualisierung der IAM-Prinzipale und der IAM Identity Center-Benutzer, die einer vorhandenen Anwendung als Administratoren zugewiesen wurden. OpenSearch

Beispiel 1: Fügen Sie einen IAM-Benutzer als Administrator für eine bestehende Anwendung hinzu OpenSearch

Führen Sie den folgenden Befehl aus, um eine OpenSearch UI-Anwendung zu aktualisieren und einen IAM-Benutzer als Administrator hinzuzufügen. Ersetzen Sie *placeholder values* durch Ihre Informationen.

```
aws opensearch update-application \
    --id myapplication \
    --app-configs "
        {
        \"key\":\"opensearchDashboards.dashboardAdmin.users\",
        \"value\":\"arn:aws:iam::account-id:user/user-id\"
        }
    "
```

Beispiel 2: Aktualisieren Sie eine OpenSearch UI-Anwendung, um eine IAM Identity Center-Benutzer-ID als OpenSearch UI-Anwendungsadministrator hinzuzufügen

Führen Sie den folgenden Befehl aus, um eine OpenSearch UI-Anwendung zu aktualisieren und eine IAM Identity Center-Benutzer-ID als OpenSearch UI-Anwendungsadministrator hinzuzufügen. Ersetzen Sie *placeholder values* durch Ihre Informationen.

`key`gibt das festzulegende Konfigurationselement an, z. B. die Administratorrolle für die OpenSearch UI-Anwendung. Gültige Werte sind `opensearchDashboards.dashboardAdmin.users` und `opensearchDashboards.dashboardAdmin.groups`.

*xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx*steht für den Wert, der dem Schlüssel zugewiesen wurde, z. B. den Amazon-Ressourcennamen (ARN) eines IAM-Benutzers.

```
aws opensearch update-application \
    --id myapplication \
    --app-configs "
        {
        \"key\":\"opensearchDashboards.dashboardAdmin.users\",
        \"value\":\"xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx\"
        }
    "
```

Aktivierung des SAML-Verbunds mit AWS Identity and Access Management

OpenSearch Die Benutzeroberfläche unterstützt Security Assertion Markup Language 2.0 (SAML), einen offenen Standard, den viele Identitätsanbieter verwenden. Dies ermöglicht einen Identitätsverbund mit AWS Identity and Access Management (IAM). Mit dieser Unterstützung können Benutzer in Ihrem Konto oder Ihrer Organisation direkt auf die OpenSearch Benutzeroberfläche zugreifen, indem sie IAM-Rollen übernehmen. Sie können ein vom Identitätsanbieter initiiertes (IdP) Single Sign-On-Erlebnis für Ihre Endbenutzer einrichten, bei dem sie sich beim externen Identitätsanbieter authentifizieren und direkt zu Ihrer definierten Seite in der Benutzeroberfläche weitergeleitet werden können. OpenSearch Sie können auch eine differenzierte Zugriffskontrolle implementieren, indem Sie Ihre Endbenutzer oder Gruppen so konfigurieren, dass sie unterschiedliche IAM-Rollen mit unterschiedlichen Berechtigungen für den Zugriff auf die Benutzeroberfläche und die zugehörigen Datenquellen annehmen. OpenSearch

In diesem Thema step-by-step finden Sie Anweisungen zur Konfiguration der SAML-Verwendung mit der Benutzeroberfläche. OpenSearch In diesen Verfahren verwenden wir als Beispiel die Schritte zur Konfiguration der Okta-Anwendung für Identitäts- und Zugriffsverwaltung. Die Konfigurationsschritte für andere Identitätsanbieter wie Azure Active Directory und Ping sind ähnlich.

Themen

- Schritt 1: Richten Sie die Identitätsanbieter-Anwendung (Okta) ein
- Schritt 2: Richten Sie die AWS Konfiguration für Okta ein
- Schritt 3: Erstellen Sie die Amazon OpenSearch Service-Zugriffsrichtlinie in IAM
- Schritt 4: Überprüfen Sie das vom Identitätsanbieter initiierte Single Sign-On-Erlebnis mit SAML

Schritt 1: Richten Sie die Identitätsanbieter-Anwendung (Okta) ein

Um SAML mit OpenSearch UI zu verwenden, müssen Sie zunächst Ihren Identitätsanbieter einrichten.

Aufgabe 1: Okta-Benutzer erstellen

1. Melden Sie sich bei Ihrer Okta-Organisation unter https://login.okta.com/als Benutzer mit Administratorrechten an.
2. Wählen Sie in der Admin-Konsole im Navigationsbereich unter Verzeichnis die Option Personen aus.
3. Wählen Sie Person hinzufügen aus.
4. Geben Sie unter Vorname den Vornamen des Benutzers ein.
5. Geben Sie unter Nachname den Nachnamen des Benutzers ein.
6. Geben Sie unter Benutzername den Benutzernamen des Benutzers im E-Mail-Format ein.
7. Wählen Sie Ich werde ein Passwort festlegen und ein Passwort eingeben
8. (Optional) Deaktivieren Sie das Feld Benutzer muss das Passwort bei der ersten Anmeldung ändern, wenn Sie nicht möchten, dass der Benutzer das Passwort bei der ersten Anmeldung ändert.
9. Wählen Sie Speichern.

Aufgabe 2: Gruppen erstellen und zuweisen

1. Melden Sie sich bei Ihrer Okta-Organisation unter https://login.okta.com/als Benutzer mit Administratorrechten an.
2. Wählen Sie in der Admin-Konsole im Navigationsbereich unter Verzeichnis die Option Gruppen aus.
3. Wählen Sie Add Group (Gruppe hinzufügen) aus.
4. Geben Sie einen Gruppennamen ein und wählen Sie Speichern.
5. Wählen Sie die neu erstellte Gruppe aus und klicken Sie dann auf Personen zuweisen.
6. Wählen Sie das Pluszeichen (+) und dann „Fertig“.
7. (Optional) Wiederholen Sie die Schritte 1—6, um weitere Gruppen hinzuzufügen.

Aufgabe 3: Okta-Anwendungen erstellen

1. Melden Sie sich bei Ihrer Okta-Organisation unter https://login.okta.com/als Benutzer mit Administratorrechten an.
2. Wählen Sie in der Admin-Konsole im Navigationsbereich unter Anwendungen die Option Anwendungen aus.
3. Wählen Sie Create App Integration (App-Integration erstellen).
4. Wählen Sie SAML 2.0 als Anmeldemethode und klicken Sie dann auf Weiter.
5. Geben Sie einen Namen für Ihre App-Integration ein (z. B.**`OpenSearch_UI`**) und wählen Sie dann Weiter.
6. Geben Sie die folgenden Werte in die App ein. Sie müssen keine anderen Werte ändern:
    a. 1. Geben Sie für Single Sign On URL die kommerziellen AWS Regionen oder die **`https://signin.aws.amazon.com/saml`** für Ihre Region spezifische URL ein.
    b. 2. Geben Sie als Zielgruppen-URI (SP Entity ID) ein**`urn:amazon:webservices`**.
    c. 3. Geben Sie als Namens-ID-Format den Wert ein**`EmailAddress`**.
7. Wählen Sie Weiter aus.
8. Wählen Sie Ich bin ein Okta-Kunde, der eine interne App hinzufügt, und wählen Sie dann Dies ist eine interne App, die wir erstellt haben aus.
9. Wählen Sie Finish (Abschließen).
10. Wählen Sie „Aufgaben“ und dann „Zuweisen“.

11. Wählen Sie Zu Gruppen zuweisen und dann neben den Gruppen, die Sie hinzufügen möchten, die Option Zuweisen aus.
12. Wählen Sie Erledigt aus.

Aufgabe 4: Richten Sie die erweiterte Okta-Konfiguration ein

Nachdem Sie die benutzerdefinierte SAML-Anwendung erstellt haben, führen Sie die folgenden Schritte aus:

1. Melden Sie sich bei Ihrer Okta-Organisation unter https://login.okta.com/als Benutzer mit Administratorrechten an.

   Wählen Sie auf der Administratorkonsole im Bereich Allgemein unter SAML-Einstellungen die Option Bearbeiten aus.
2. Wählen Sie Weiter aus.
3. Stellen Sie den Standard-Relay-Status auf den OpenSearch UI-Endpunkt ein und verwenden Sie dabei das folgende Format:

   ```
   https://region.console.aws.amazon.com/aos/home?
   region=region#opensearch/applications/application-id/
   redirectToDashboardURL.
   ```

   Im Folgenden wird ein Beispiel gezeigt:

   ```
   https://us-east-2.console.aws.amazon.com/aos/home?region=us-
   east-2#opensearch/applications/abc123def4567EXAMPLE/
   redirectToDashboardURL
   ```
4. Fügen Sie unter Attributanweisungen (optional) die folgenden Eigenschaften hinzu:

   a. Geben Sie die IAM-Rolle und den Identitätsanbieter mithilfe des Role-Attributs in einem kommagetrennten Format an. Sie werden dieselbe IAM-Rolle und denselben Identitätsanbieter in einem späteren Schritt beim Einrichten der Konfiguration verwenden. AWS

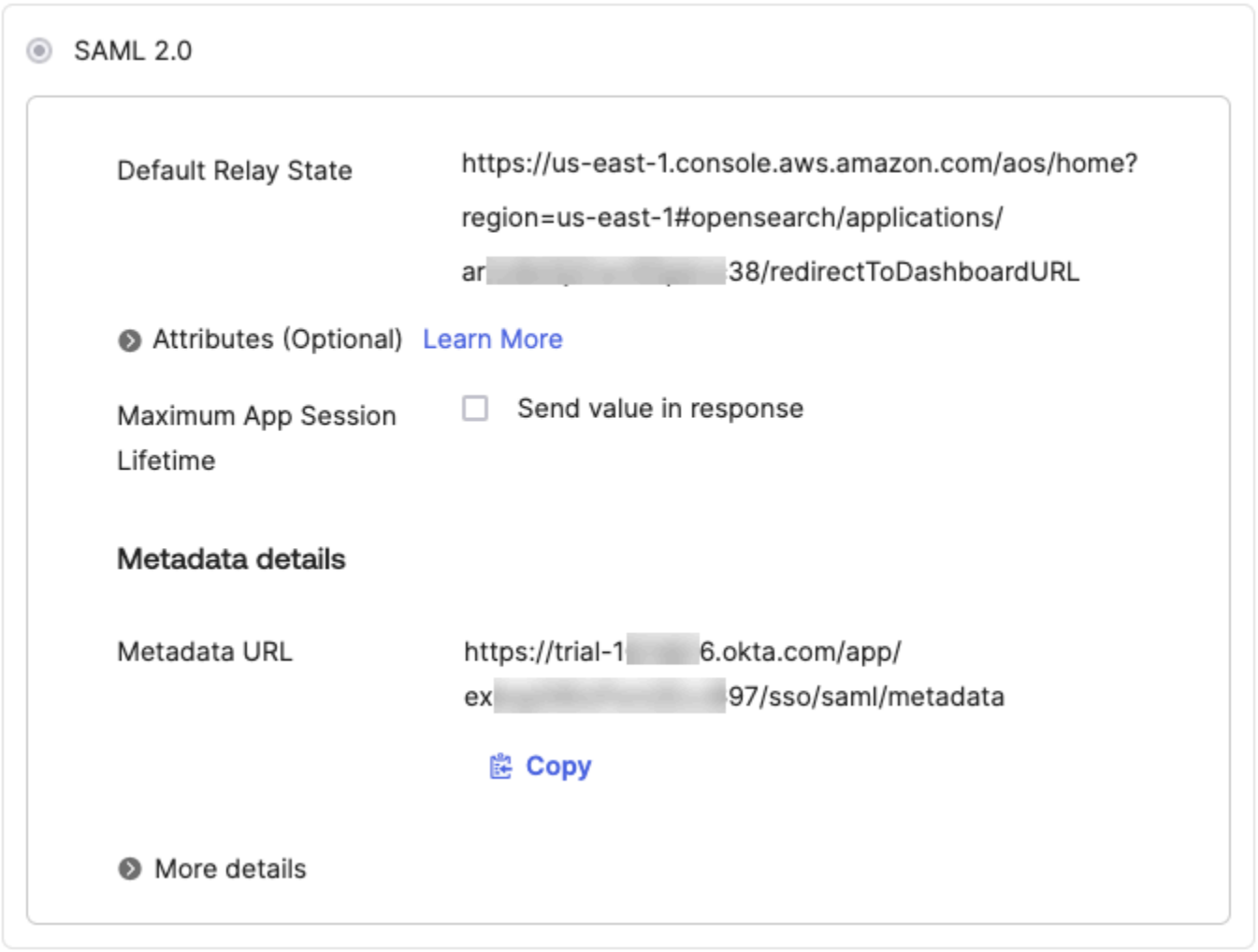
   b. Legen Sie user.login für fest. RoleSessionName Dies wird als Kennung für die temporären Anmeldeinformationen verwendet, die ausgestellt werden, wenn die Rolle übernommen wird.

Als Referenz:

Name	Format des Namens	Format	Beispiel
`https://aws.amazon.com/SAML/Attributes/Role`	Nicht spezifiziert	`arn:aws:iam:: aws-account-id :role/role-name,arn:aws:iam:: aws-account-id :saml-provider/ provider-name`	`arn:aws:iam::111222333444:role/oktarole,arn:aws:iam::111222333444:saml-provider/oktaidp`
`https://aws.amazon.com/SAML/Attributes/RoleSessionName`	Nicht spezifiziert	`user.login`	`user.login`

5. Nachdem Sie die Attributeigenschaften hinzugefügt haben, klicken Sie auf Weiter und anschließend auf Fertig stellen.

Ihre Attribute sollten ein ähnliches Format wie in der folgenden Abbildung haben. Der Standard-Relay-State-Wert ist die URL zur Definition der Landingpage für Endbenutzer in Ihrem Konto oder Ihrer Organisation, nachdem diese die Single Sign-On-Validierung von Okta abgeschlossen haben. Sie können es auf eine beliebige Seite in der OpenSearch Benutzeroberfläche festlegen und diese URL dann den vorgesehenen Endbenutzern zur Verfügung stellen.



Schritt 2: Richten Sie die AWS Konfiguration für Okta ein

Führen Sie die folgenden Aufgaben aus, um Ihre AWS Konfiguration für Okta einzurichten.

Aufgabe 1: Sammeln Sie Okta-Informationen

Für diesen Schritt müssen Sie Ihre Okta-Informationen sammeln, damit Sie sie später konfigurieren können. AWS

1. Melden Sie sich bei Ihrer Okta-Organisation unter https://login.okta.com/als Benutzer mit Administratorrechten an.
2. Wählen Sie auf der Registerkarte Anmelden in der unteren rechten Ecke der Seite die Option SAML-Setup-Anweisungen anzeigen aus.

3. Notieren Sie sich den Wert für die Single Sign-On-URL des Identity Providers. Sie können diese URL verwenden, wenn Sie eine Verbindung zu einem SQL-Client eines Drittanbieters wie SQL Workbench/J herstellen.
4. Verwenden Sie die Identitätsanbieter-Metadaten in Block 4 und speichern Sie dann die Metadatendatei im XML-Format (z. B.). `metadata.xml`

Aufgabe 2: Erstellen Sie den IAM-Anbieter

Gehen Sie wie folgt vor, um Ihren IAM-Anbieter zu erstellen:

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die IAM-Konsole unter. https://console.aws.amazon.com/iam/
2. Wählen Sie im Navigationsbereich unter Access Management die Option Identity Providers aus.
3. Wählen Sie Add provider (Anbieter hinzufügen) aus.
4. Wählen Sie als Anbietertyp die Option SAML aus.
5. Geben Sie für den Anbieternamen einen Namen ein.
6. Wählen Sie für Metadaten-Dokument die Option Datei auswählen und laden Sie die Metadatendatei (.xml) hoch, die Sie zuvor heruntergeladen haben.
7. Wählen Sie Add provider (Anbieter hinzufügen) aus.

Aufgabe 3: IAM-Rolle erstellen

Gehen Sie wie folgt vor, um Ihre AWS Identity and Access Management Rolle zu erstellen:

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich unter Zugriffsverwaltung die Option Rollen aus.
3. Wählen Sie Rolle erstellen aus.
4. Wählen Sie für Vertrauenswürdigen Entitätstyp die Option SAML 2.0-Verbund aus.
5. Wählen Sie für einen SAML 2.0-basierten Anbieter den Identitätsanbieter aus, den Sie zuvor erstellt haben.
6. Wählen Sie Programmatisch und Zugriff zulassen aus. AWS Management Console
7. Wählen Sie Weiter aus.
8. Aktivieren Sie in der Liste der Berechtigungsrichtlinien die Kontrollkästchen für die Richtlinie, die Sie zuvor erstellt haben, und für OpenSearchFullAccess.

9. Wählen Sie Weiter aus.
10. Geben Sie im Bereich Überprüfung in das Feld Rollenname den Namen Ihrer Rolle ein, zum Beispiel**`oktarole`**.
11. (Optional) Geben Sie unter Beschreibung eine kurze Beschreibung des Zwecks der Rolle ein.
12. Wählen Sie Rolle erstellen aus.
13. Navigieren Sie zu der Rolle, die Sie gerade erstellt haben, wählen Sie die Registerkarte Vertrauensbeziehungen und dann Vertrauensrichtlinie bearbeiten aus.
14. Wählen Sie im Bereich Aussage bearbeiten unter Aktionen für STS hinzufügen das Feld für aus TagSession.
15. Wählen Sie Richtlinie aktualisieren.

Schritt 3: Erstellen Sie die Amazon OpenSearch Service-Zugriffsrichtlinie in IAM

Dieses Thema enthält Informationen zur Konfiguration Ihrer IAM-Rollen mit Zugriff auf OpenSearch Dienste. Wir stellen Beispiele für zwei Gruppen zur Verfügung `Alice` und zeigen`Bob`, wie Sie mit Okta eine differenzierte Zugriffskontrolle für Ihre Benutzergruppen erreichen können.

Sample group: Alice

Anforderung:

```
GET _plugins/_security/api/roles/alice-group
```

Ergebnis:

```
{
  "alice-group": {
    "reserved": false,
    "hidden": false,
    "cluster_permissions": [
      "unlimited"
    ],
    "index_permissions": [
      {
        "index_patterns": [
          "alice*"
        ],
```

```
        "dls": "",
        "fls": [],
        "masked_fields": [],
        "allowed_actions": [
          "indices_all"
        ]
      }
    ],
    "tenant_permissions": [
      {
        "tenant_patterns": [
          "global_tenant"
        ],
        "allowed_actions": [
          "kibana_all_write"
        ]
      }
    ],
    "static": false
  }
}
```

Sample group: Bob

Anforderung:

```
GET _plugins/_security/api/roles/bob-group
```

Ergebnis:

```
{
  "bob-group": {
    "reserved": false,
    "hidden": false,
    "cluster_permissions": [
      "unlimited"
    ],
    "index_permissions": [
      {
        "index_patterns": [
          "bob*"
        ],
        "dls": "",
```

```
        "fls": [],
        "masked_fields": [],
        "allowed_actions": [
          "indices_all"
        ]
      }
    ],
    "tenant_permissions": [
      {
        "tenant_patterns": [
          "global_tenant"
        ],
        "allowed_actions": [
          "kibana_all_write"
        ]
      }
    ],
    "static": false
  }
}
```

Sie können die Amazon OpenSearch Service-Domänenrollen mithilfe der Backend-Rollenzuweisung IAM-Rollen zuordnen, wie im folgenden Beispiel gezeigt:

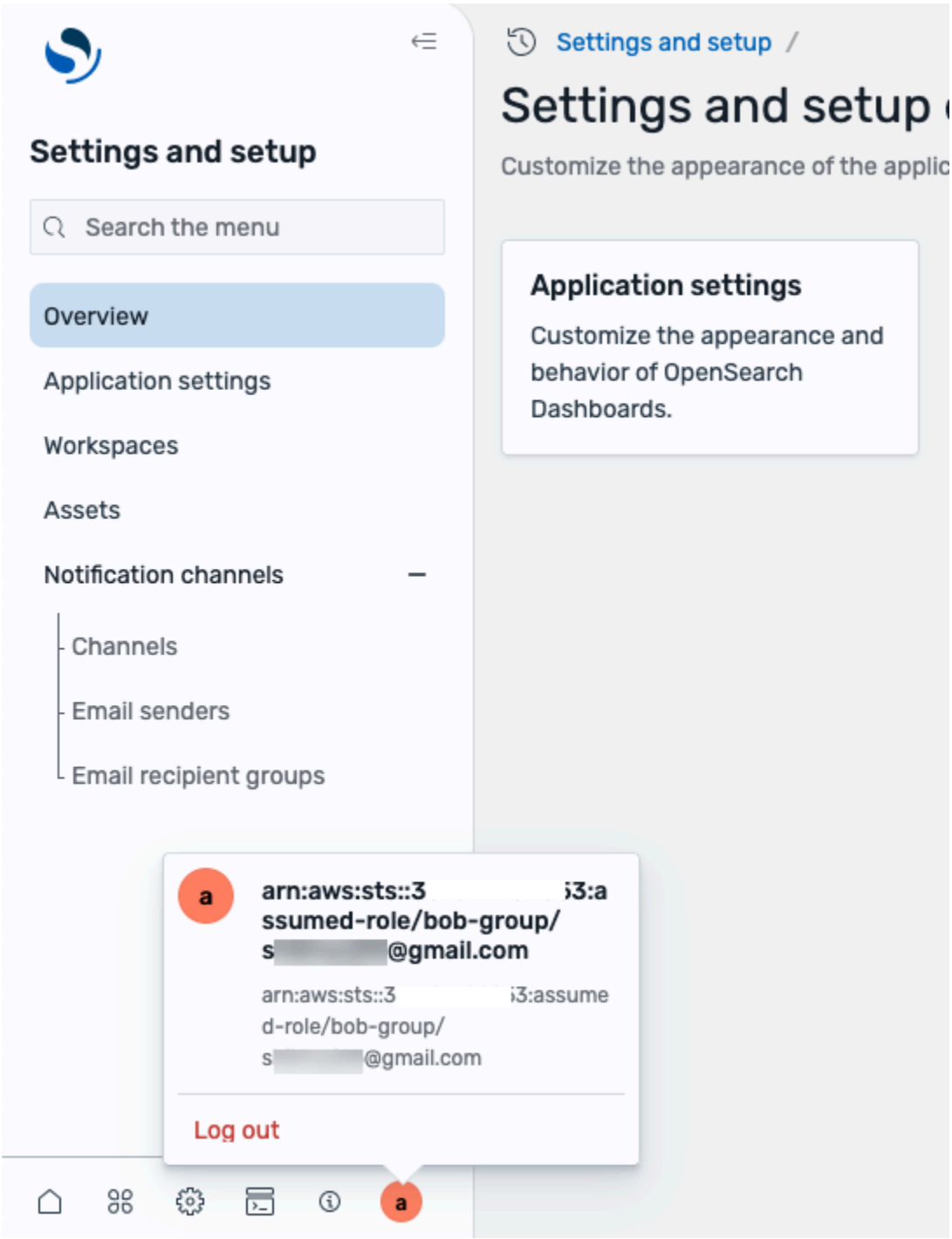
```
{
  "bob-group": {
    "hosts": [],
    "users": [],
    "reserved": false,
    "hidden": false,
    "backend_roles": [
      "arn:aws:iam::111222333444:role/bob-group"
    ],
    "and_backend_roles": []
  },
  "alice-group": {
    "hosts": [],
    "users": [],
    "reserved": false,
    "hidden": false,
    "backend_roles": [
      "arn:aws:iam::111222333444:role/alice-group"
```

```
    ],
    "and_backend_roles": []
  }
}
```

Schritt 4: Überprüfen Sie das vom Identitätsanbieter initiierte Single Sign-On-Erlebnis mit SAML

Öffnen Sie die URL für Default Relay State, um die Okta-Authentifizierungsseite zu öffnen. Geben Sie die Anmeldeinformationen eines Endbenutzers ein. Sie werden automatisch zur OpenSearch Benutzeroberfläche weitergeleitet.

Sie können Ihre aktuellen Anmeldeinformationen überprüfen, indem Sie auf das Benutzersymbol unten im Navigationsbereich klicken, wie in der folgenden Abbildung dargestellt:



Sie können die detaillierten Zugriffsberechtigungen für den Benutzer auch überprüfen, indem Sie unten im Navigationsbereich auf die Entwicklertools zugreifen und Abfragen in der Konsole ausführen. Im Folgenden finden Sie Beispielabfragen.

Example 1: Displays information about the current user

Anforderung:

```
GET _plugins/_security/api/account
```

Ergebnis:

```
{
  "user_name": "arn:aws:iam::XXXXXXXXXXXX:role/bob-group",
  "is_reserved": false,
  "is_hidden": false,
  "is_internal_user": false,
  "user_requested_tenant": null,
  "backend_roles": [
    "arn:aws:iam::XXXXXXXXXXXX:role/bob-group"
  ],
  "custom_attribute_names": [],
  "tenants": {
    "global_tenant": true,
    "arn:aws:iam::XXXXXXXXXXXX:role/bob-group": true
  },
  "roles": [
    "bob-group"
  ]
}
```

Example 2: Displays actions permitted for a user

Anforderung:

```
GET bob-test/_search
```

Ergebnis:

```
{
  "took": 390,
  "timed_out": false,
  "_shards": {
    "total": 5,
    "successful": 5,
    "skipped": 0,
    "failed": 0
  },
  "hits": {
    "total": {
```

```
      "value": 1,
      "relation": "eq"
    },
    "max_score": 1,
    "hits": [
      {
        "_index": "bob-test",
        "_id": "ui01N5UBCIHpjO8Jlvfy",
        "_score": 1,
        "_source": {
          "title": "Your Name",
          "year": "2016"
        }
      }
    ]
  }
}
```

Example 3: Displays actions not permitted for a user

Anforderung:

```
GET alice-test
```

Ergebnis:

```
{
  "error": {
    "root_cause": [
      {
        "type": "security_exception",
        "reason": "no permissions for [indices:admin/get]
 and User [name=arn:aws:iam::111222333444:role/bob-group,
 backend_roles=[arn:aws:iam::111222333444:role/bob-group], requestedTenant=null]"
      }
    ],
    "type": "security_exception",
    "reason": "no permissions for [indices:admin/get]
 and User [name=arn:aws:iam::111222333444:role/bob-group,
 backend_roles=[arn:aws:iam::111222333444:role/bob-group], requestedTenant=null]"
  },
  "status": 403
}
```

Verwaltung von Datenquellenzuordnungen und Virtual Private Cloud-Zugriffsberechtigungen

Verwenden Sie die Verfahren in diesem Abschnitt, um Datenquellenzuordnungen zu verwalten und alle erforderlichen Zugriffsberechtigungen für eine Virtual Private Cloud (VPC) zu konfigurieren.

Themen

- Zuordnen einer Datenquelle zu einer UI-Anwendung OpenSearch
- Verwaltung des Zugriffs auf Domänen in einer VPC
- Konfiguration des Zugriffs auf OpenSearch serverlose Sammlungen in einer VPC

Zuordnen einer Datenquelle zu einer UI-Anwendung OpenSearch

Nachdem Sie eine OpenSearch UI-Anwendung erstellt haben, können Sie die Konsole verwenden oder AWS CLI sie einer oder mehreren Datenquellen zuordnen. Danach können Endbenutzer Daten aus diesen Datenquellen abrufen, um sie zu durchsuchen, mit Dashboards zu arbeiten usw.

Ordnen Sie eine Datenquelle einer OpenSearch UI-Anwendung (Konsole) zu

So verknüpfen Sie mithilfe der Konsole eine Datenquelle mit einer OpenSearch UI-Anwendung

1. Melden Sie sich zu https://console.aws.amazon.com/aos/Hause bei der Amazon OpenSearch Service-Konsole an.
2. Wählen Sie OpenSearch UI (Dashboards) und dann den Namen einer OpenSearch UI-Anwendung.
3. Wählen Sie im Bereich Zugeordnete Datenquellen die Option Datenquellen verwalten aus.
4. Wählen Sie aus den OpenSearch Domänen und Sammlungen aus, die Sie der Anwendung zuordnen möchten.

> **Tip**
>
> Wenn Sie die Datenquellen, nach denen Sie suchen, nicht finden, wenden Sie sich an Ihre Administratoren, um Ihnen die erforderlichen Berechtigungen zu erteilen. Weitere Informationen finden Sie unter the section called “Berechtigungen zum Erstellen einer Anwendung, die die IAM Identity Center-Authentifizierung verwendet (optional)”.

5. Wählen Sie Weiter und dann Speichern aus.

Nachdem Sie der Anwendung eine Datenquelle zugeordnet haben, ist die Schaltfläche „Anwendung starten“ auf der Anwendungsdetailseite aktiviert. Sie können „Anwendung starten“ wählen, um die OpenSearch Seite Willkommen auf zu öffnen, auf der Sie Workspaces erstellen und verwalten können.

Informationen zum Arbeiten mit Workspaces finden Sie unter. the section called “Amazon OpenSearch Service-Workspaces verwenden”

Verwaltung des Zugriffs auf Domänen in einer VPC

Wenn der Anwendung eine OpenSearch Domain in einer VPC zugeordnet war, muss ein VPC-Administrator den Zugriff zwischen OpenSearch UI und VPC über die Konsole oder autorisieren. AWS CLI

Verwaltung des Zugriffs auf Domänen in einer VPC (Konsole)

Um den Zugriff auf eine VPC-Domain zu konfigurieren, verwenden Sie: AWS Management Console

1. Melden Sie sich zu https://console.aws.amazon.com/aos/Hause bei der Amazon OpenSearch Service-Konsole an.
2. Wählen Sie im linken Navigationsbereich Domains und anschließend den Namen der VPC-Domain aus.

   –oder–

   Wählen Sie Create Domain aus und konfigurieren Sie dann die Details für die Domain.
3. Wählen Sie die Registerkarte VPC-Endpoints und dann Principal autorisieren aus.
4. Wählen Sie im Dialogfeld Prinzipale autorisieren die Option Prinzipale aus anderen AWS Diensten autorisieren und wählen Sie dann OpenSearch Anwendungen (Dashboard) aus der Liste aus.
5. Klicken Sie auf Authorize.

Zugriff auf Domänen in einer VPC verwalten ()AWS CLI

Um eine VPC-Domain mit dem zu autorisieren AWS CLI

Führen Sie den folgenden Befehl aus AWS CLI, um die VPC-Domäne mit dem zu autorisieren. Ersetzen Sie *placeholder values* durch Ihre Informationen.

```
aws opensearch authorize-vpc-endpoint-access \
 --domain-name domain-name \
 --service application.opensearchservice.amazonaws.com \
 --region region-id
```

So widerrufen Sie eine VPC-Domänenzuweisung mithilfe der Konsole

Wenn eine Zuordnung nicht mehr benötigt wird, kann der VPC-Domaininhaber den Zugriff mithilfe des folgenden Verfahrens widerrufen.

1. Melden Sie sich zu https://console.aws.amazon.com/aos/Hause bei der Amazon OpenSearch Service-Konsole an.
2. Wählen Sie im linken Navigationsbereich Domains und anschließend den Namen der VPC-Domain aus.
3. Wählen Sie die Registerkarte VPC-Endpoints und dann die Schaltfläche für die OpenSearch Anwendungszeile (Dashboard).
4. Wählen Sie Zugriff widerrufen aus.

Um eine VPC-Domänenzuweisung zu widerrufen, verwenden Sie den AWS CLI

Führen Sie den folgenden Befehl aus, um eine VPC-Domänenzuweisung mit der OpenSearch UI-Anwendung zu widerrufen. Ersetzen Sie *placeholder values* durch Ihre Informationen.

```
aws opensearch revoke-vpc-endpoint-access \
    --domain-name domain-name \
    --service application.opensearchservice.amazonaws.com \
    --region region-id
```

Konfiguration des Zugriffs auf OpenSearch serverlose Sammlungen in einer VPC

Wenn eine Amazon OpenSearch Serverless-Sammlung in einer VPC mit der Anwendung verknüpft war, kann ein VPC-Administrator den Zugriff autorisieren, indem er eine neue Netzwerkrichtlinie erstellt und sie der Sammlung anhängt.

Konfiguration des Zugriffs auf OpenSearch serverlose Sammlungen in einer VPC (Konsole)

So konfigurieren Sie den Zugriff auf OpenSearch serverlose Sammlungen in einer VPC mithilfe der Konsole

1. Melden Sie sich zu https://console.aws.amazon.com/aos/Hause bei der Amazon OpenSearch Service-Konsole an.
2. Wählen Sie in der linken Navigationsleiste Netzwerkrichtlinien, wählen Sie den Namen der Netzwerkrichtlinie aus und klicken Sie dann auf Bearbeiten.

   –oder–

   Wählen Sie Netzwerkrichtlinie erstellen und konfigurieren Sie dann die Details für die Richtlinie.
3. Wählen Sie im Bereich Zugriffstyp die Option Privat (empfohlen) und dann privaten AWS Dienstzugriff aus.
4. Wählen Sie im Suchfeld Service und dann `ausapplication.opensearchservice.amazonaws.com`.
5. Wählen Sie im Bereich Ressourcentyp das Feld Zugriff auf OpenSearch Endpunkt aktivieren aus.
6. Wählen Sie unter Sammlung (en) durchsuchen oder bestimmte Präfixausdrücke in das Suchfeld die Option Sammlungsname und geben Sie dann den Namen der Sammlungen ein, die mit der Netzwerkrichtlinie verknüpft werden sollen, oder wählen Sie ihn aus.
7. Wählen Sie Erstellen für eine neue Netzwerkrichtlinie oder Aktualisieren für eine bestehende Netzwerkrichtlinie.

Konfiguration des Zugriffs auf OpenSearch serverlose Sammlungen in einer VPC ()AWS CLI

Um den Zugriff auf OpenSearch serverlose Sammlungen in einer VPC zu konfigurieren, verwenden Sie den AWS CLI

1. Erstellen Sie eine JSON-Datei, die der folgenden ähnelt. Ersetzen Sie *placeholder values* durch Ihre Informationen.

```
{
    "Description" : "policy-description",
```

```
    "Rules": [{
       "ResourceType" : "collection",
        "Resource" : ["collection/collection_name"]
     }],
    "SourceServices" : [
          "application.opensearchservice.amazonaws.com"
      ],
      "AllowFromPublic" : false
}
```

2. Erstellen oder aktualisieren Sie eine Netzwerkrichtlinie für eine Sammlung in einer VPC, damit sie mit OpenSearch UI-Anwendungen funktioniert.

   Create a network policy

   Führen Sie den folgenden Befehl aus. Ersetzen Sie *placeholder values* durch Ihre Informationen.

   ```
   aws opensearchserverless create-security-policy \
       --type network  \
       --region region \
       --endpoint-url endpoint-url \
       --name network-policy-name \
       --policy file:/path_to_network_policy_json_file
   ```

   Die vom System zurückgegebenen Informationen ähneln den Folgenden:

   ```
   {
       "securityPolicyDetail": {
           "createdDate": ******,
           "lastModifiedDate": ******,
           "name": "network-policy-name",
           "policy": [
               {
                   "SourceVPCEs": [],
                   "AllowFromPublic": false,
                   "Description": "",
                   "Rules": [
                       {
                           "Resource": [
                               "collection/network-policy-name"
                           ],
   ```

```
                        "ResourceType": "collection"
                    }
                ],
                "SourceServices": [
                    "application.opensearchservice.amazonaws.com"
                ]
            }
        ],
        "policyVersion": "******",
        "type": "network"
    }
}
```

Update a network policy

Führen Sie den folgenden Befehl aus. Ersetzen Sie *placeholder values* durch Ihre Informationen.

```
aws opensearchserverless update-security-policy \
    --type network  \
    --region region \
    --endpoint-url endpoint-url \
    --name network-policy-name \
    --policy-version "policy_version_from_output_of_network_policy_creation" \
    --policy file:/path_to_network_policy_json_file
```

Die vom System zurückgegebenen Informationen ähneln den Folgenden:

```
{
    "securityPolicyDetail": {
        "createdDate": ******,
        "lastModifiedDate": ******,
        "name": "network-policy-name",
        "policy": [
            {
                "SourceVPCEs": [],
                "AllowFromPublic": false,
                "Description": "",
                "Rules": [
                    {
                        "Resource": [
                            "collection/network-policy-name"
```

```
                        ],
                        "ResourceType": "collection"
                    }
                ],
                "SourceServices": [
                    "application.opensearchservice.amazonaws.com"
                ]
            }
        ],
        "policyVersion": "******",
        "type": "network"
    }
}
```

Amazon OpenSearch Service-Workspaces verwenden

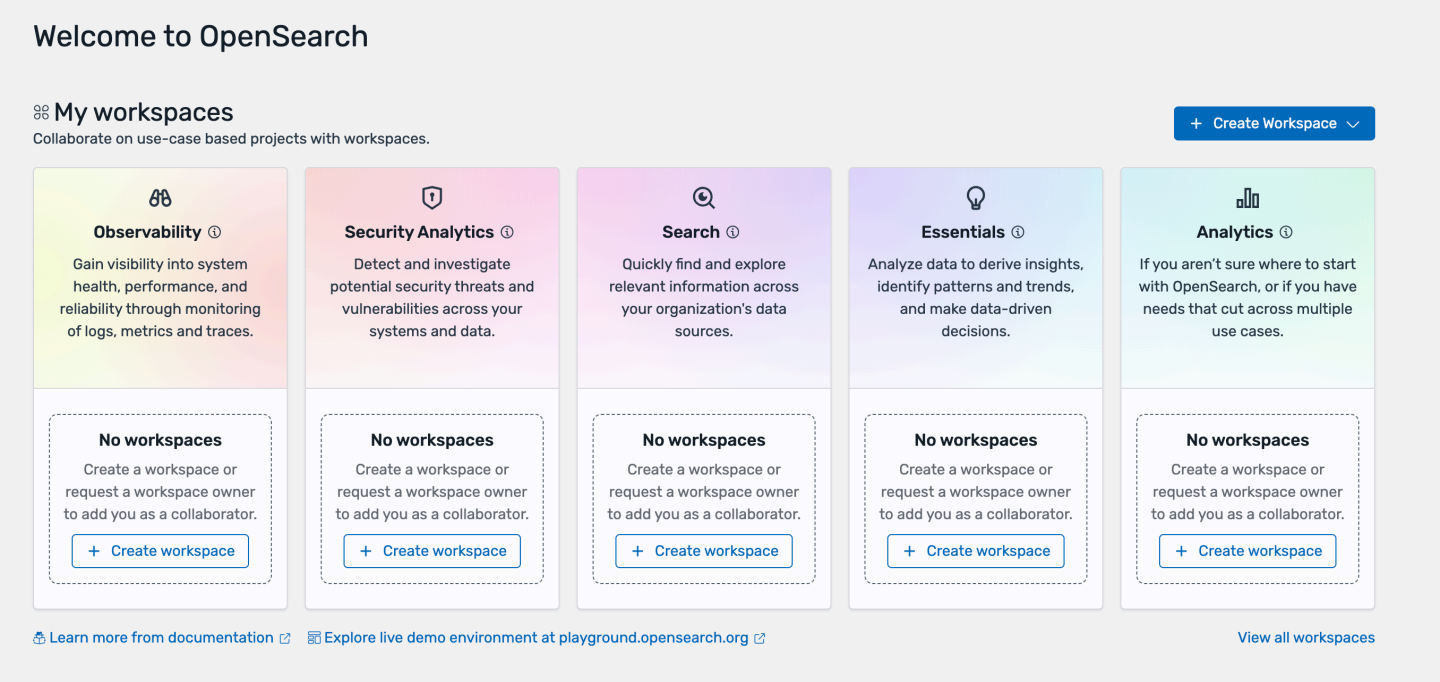
Amazon OpenSearch Service unterstützt die Erstellung mehrerer anwendungsfallspezifischer Arbeitsbereiche. Jeder Workspace bietet ein kuratiertes Erlebnis für beliebte Anwendungsfälle wie Observability, Security Analytics und Search. Workspace unterstützt auch die Verwaltung von Mitarbeitern, sodass du deinen Workspace nur mit deinen vorgesehenen Mitarbeitern teilen und die jeweiligen Berechtigungen verwalten kannst.

Arbeitsbereiche für OpenSearch UI-Anwendungen erstellen

Nachdem eine OpenSearch UI-Anwendung erstellt und mit Datenquellen verknüpft und Benutzerberechtigungen für die Anwendung konfiguriert wurden, können Sie die OpenSearch UI-Anwendung starten, um Arbeitsbereiche zu erstellen.

Um mit der Erstellung eines Arbeitsbereichs zu beginnen, können Sie auf der Detailseite der Anwendung auf die Schaltfläche Anwendung starten klicken oder die URL der OpenSearch UI-Anwendung verwenden, um die Startseite der OpenSearch UI-Anwendung in einem neuen Browserfenster zu öffnen.

Die OpenSearch UI-Anwendung bietet Optionen zum Erstellen von Arbeitsbereichen und listet alle vorhandenen Arbeitsbereiche auf der Startseite auf, sortiert nach Anwendungsfällen.



Weitere Informationen zu den unterstützten Arten von Arbeitsbereichen finden Sie unter. the section called “Typen von Arbeitsbereichen”

Datenschutz im Workspace und Mitarbeiter

Du kannst eine Datenschutzeinstellung für einen Workspace als Standardberechtigungsstufe für alle Benutzer definieren. Du kannst dies tun, während du einen Workspace erstellst oder einen bestehenden Workspace modifizierst (auf der Workspace-Registerkarte Mitarbeiter). Es stehen drei Datenschutzoptionen zur Auswahl:

- Privat für Mitwirkende — Nur Mitarbeiter, die du ausdrücklich zum Workspace hinzufügst, können auf den Workspace zugreifen. Du kannst für jeden Mitarbeiter Berechtigungsstufen definieren.
- Jeder kann sie ansehen — Jeder, der Zugriff auf die OpenSearch UI-Anwendung hat, kann auf den Workspace zugreifen und seine Assets einsehen, aber er kann keine Änderungen im Workspace vornehmen.
- Jeder kann bearbeiten — Jeder, der Zugriff auf die OpenSearch UI-Anwendung hat, kann auf den Workspace zugreifen, die darin enthaltenen Assets anzeigen und Änderungen an den Assets im Workspace vornehmen.

Auf der Workspace-Registerkarte Mitarbeiter können Sie IAM-Benutzer oder Rollen und AWS IAM Identity Center Benutzer als Mitarbeiter in einem Workspace hinzufügen. Es gibt drei Berechtigungsstufen, aus denen Mitarbeiter wählen können:

- Schreibgeschützt — Der Mitarbeiter kann nur die Assets im Workspace sehen. Diese Einstellung wird außer Kraft gesetzt, wenn der Workspace so konfiguriert ist, dass die Datenschutzeinstellung Jeder bearbeiten kann verwendet wird.
- Lesen und Schreiben — Der Mitarbeiter kann Assets im Workspace anzeigen und bearbeiten. Wenn der Workspace so konfiguriert ist, dass er die Datenschutzeinstellung Jeder kann einsehen verwendet, kann der Mitarbeiter trotzdem bearbeiten.
- Administrator — Der Mitarbeiter kann die Einstellungen aktualisieren und den Workspace löschen. Der Mitarbeiter kann auch die Datenschutzeinstellungen des Workspace ändern und Mitarbeiter verwalten. Der Benutzer, der den Workspace erstellt, wird automatisch zum Workspace-Administrator ernannt.

Typen von Arbeitsbereichen

Amazon OpenSearch Service bietet fünf Workspace-Typen mit jeweils unterschiedlichen Funktionen für die verschiedenen Anwendungsfälle:

- Der Observability-Arbeitsbereich wurde entwickelt, um durch die Überwachung von Protokollen, Metriken und Traces einen Überblick über den Zustand, die Leistung und Zuverlässigkeit des Systems zu erhalten.
- Der Arbeitsbereich Security Analytics dient der Erkennung und Untersuchung potenzieller Sicherheitsbedrohungen und Sicherheitslücken in Ihren Systemen und Daten.
- Der Arbeitsbereich Suchen dient dazu, relevante Informationen in den Datenquellen Ihres Unternehmens schnell zu finden und zu untersuchen.
- Der Arbeitsbereich Essentials wurde für OpenSearch Serverless als Datenquelle konzipiert und ermöglicht die Analyse von Daten, um Erkenntnisse zu gewinnen, Muster und Trends zu erkennen und schnell datengestützte Entscheidungen zu treffen. In einem Essentials-Arbeitsbereich können Sie relevante Informationen aus den Datenquellen Ihres Unternehmens suchen und untersuchen.
- Der Analytics-Arbeitsbereich (alle Funktionen) wurde für vielseitige Anwendungsfälle konzipiert und unterstützt alle in der OpenSearch Service-Benutzeroberfläche (Dashboards) verfügbaren Funktionen.

Regions- und kontoübergreifender Datenzugriff mit clusterübergreifender Suche

Mithilfe der clusterübergreifenden Suche in Amazon OpenSearch Serverless können Sie Abfragen und Aggregationen über mehrere verbundene Domains hinweg durchführen.

Die clusterübergreifende Suche in Amazon OpenSearch Serverless verwendet die Konzepte einer Quelldomäne und einer Zieldomäne. Eine clusterübergreifende Suchanfrage stammt von einer Quelldomäne. Die Zieldomäne kann sich in einer anderen AWS-Konto oder AWS-Region (oder beiden) befinden, von der aus die Quelldomäne abgefragt werden soll. Mithilfe der clusterübergreifenden Suche können Sie eine Quelldomäne so konfigurieren, dass sie mit Ihrer OpenSearch Benutzeroberfläche in demselben Konto verknüpft wird, und dann Verbindungen zu Zieldomänen herstellen. Daher können Sie die OpenSearch Benutzeroberfläche mit Daten aus den Zieldomänen verwenden, auch wenn sie sich in einem anderen Konto oder einer anderen Region befinden.

Sie zahlen die üblichen AWS Datenübertragungsgebühren für Daten, die innerhalb und außerhalb von Amazon OpenSearch Service übertragen werden. Für Datenübertragungen zwischen Knoten innerhalb Ihrer OpenSearch Service-Domain werden Ihnen keine Gebühren berechnet. Weitere Informationen zu Gebühren für eingehende und ausgehende Daten finden Sie unter Datenübertragung auf der Seite mit den EC2 Amazon-On-Demand-Preisen.

Sie können die clusterübergreifende Suche als Mechanismus verwenden, um Ihre OpenSearch Benutzeroberfläche mit Clustern in einem anderen Konto oder einer anderen Region zu verknüpfen. Die Anfragen zwischen Domänen werden bei der Übertragung standardmäßig als Teil der node-to-node Verschlüsselung verschlüsselt.

> **Note**
>
> Das OpenSearch Open-Source-Tool dokumentiert auch die clusterübergreifende Suche. Beachten Sie, dass sich die Einrichtung des Open-Source-Tools für Open-Source-Cluster im Vergleich zu verwalteten Amazon OpenSearch Serverless-Domains erheblich unterscheidet. Vor allem in Amazon OpenSearch Serverless konfigurieren Sie clusterübergreifende Verbindungen mithilfe von, AWS Management Console anstatt Anfragen zu verwenden`cURL`. Der verwaltete Service verwendet AWS Identity and Access Management (IAM) für die clusterübergreifende Authentifizierung zusätzlich zur detaillierten Zugriffskontrolle.

Wir empfehlen daher, anstelle der Open-Source-Dokumentation die Inhalte in diesem Thema zu verwenden, um die clusterübergreifende Suche für Ihre Domains zu konfigurieren. OpenSearch

Funktionale Unterschiede bei der Verwendung der clusterübergreifenden Suche

Im Vergleich zu regulären Domänen weisen Zieldomänen, die mithilfe der clusterübergreifenden Suche erstellt wurden, die folgenden funktionalen Unterschiede und Anforderungen auf:

- Sie können nicht in den Remote-Cluster schreiben oder PUT Befehle für ihn ausführen. Ihr Zugriff auf den Remote-Cluster ist schreibgeschützt.
- Sowohl die Quell- als auch die Zieldomäne müssen Domänen sein. OpenSearch Sie können keine Elasticsearch-Domain oder selbstverwaltete OpenSearch /Elasticsearch-Cluster für die Benutzeroberfläche verbinden. OpenSearch
- Eine Domain kann maximal 20 Verbindungen zu anderen Domains haben. Dies umfasst sowohl ausgehende als auch eingehende Verbindungen.
- Die Quelldomäne muss sich auf derselben oder einer höheren Version OpenSearch als die Zieldomäne befinden. Wenn Sie bidirektionale Verbindungen zwischen zwei Domänen einrichten möchten, sollten sich die beiden Domänen in derselben Version befinden. Wir empfehlen, beide Domains auf die neueste Version zu aktualisieren, bevor Sie die Verbindung herstellen. Wenn Sie Domänen aktualisieren müssen, nachdem Sie die bidirektionale Verbindung eingerichtet haben, müssen Sie zuerst die Verbindung löschen und anschließend neu erstellen.
- Sie können keine benutzerdefinierten Wörterbücher oder SQL mit den Remote-Clustern verwenden.
- Sie können es nicht verwenden, AWS CloudFormation um Domänen zu verbinden.
- Sie können die Cluster-übergreifende Suche auf M3- oder (T2 und T3) Burstable Instances nicht verwenden.
- Die clusterübergreifende Suche funktioniert nicht für Amazon OpenSearch Serverless-Sammlungen.

Voraussetzungen für die clusterübergreifende Suche für die Benutzeroberfläche OpenSearch

Bevor Sie die clusterübergreifende Suche mit zwei OpenSearch Domänen einrichten, stellen Sie sicher, dass Ihre Domänen die folgenden Anforderungen erfüllen:

- Für beide Domänen ist eine differenzierte Zugriffskontrolle aktiviert
- Node-to-node Die Verschlüsselung ist für beide Domänen aktiviert

Themen

- Einrichtung von Zugriffsberechtigungen für den region- und kontoübergreifenden Datenzugriff mit clusterübergreifender Suche
- Eine Verbindung zwischen Domänen herstellen
- Testen Sie Ihre Sicherheitseinstellungen für den region- und kontoübergreifenden Datenzugriff mit clusterübergreifender Suche
- Löschen einer Verbindung

Einrichtung von Zugriffsberechtigungen für den region- und kontoübergreifenden Datenzugriff mit clusterübergreifender Suche

Wenn Sie eine clusterübergreifende Suchanfrage an die Quelldomäne senden, bewertet die Domäne diese Anfrage anhand ihrer Domänenzugriffsrichtlinie. Eine clusterübergreifende Suche erfordert eine differenzierte Zugriffskontrolle. Im Folgenden finden Sie ein Beispiel mit einer Open-Access-Richtlinie für die Quelldomäne.

JSON

```
{
"Version": "2012-10-17",
"Statement": [
    {
        "Effect": "Allow",
        "Principal": {
          "AWS": [
            "*"
        ]
      },
      "Action": [
        "es:ESHttp*"
      ],
      "Resource": "arn:aws:es:region:111222333444:domain/src-domain/*"
    }
  ]
```

```
}
```

> **Note**
>
> Wenn Sie Remote-Indizes in den Pfad einbeziehen, müssen Sie den URI im Domänen-ARN URL-codieren.
> Verwenden Sie beispielsweise das folgende ARN-Format: `:arn:aws:es:us-east-1:111222333444:domain/my-domain/local_index,dst%3Aremote_index`
> Verwenden Sie nicht das folgende ARN-Format: `arn:aws:es:us-east-1:111222333444:domain/my-domain/local_index,dst:remote_index.`

Wenn Sie zusätzlich zur detaillierten Zugriffskontrolle eine restriktive Zugriffsrichtlinie verwenden möchten, muss Ihre Richtlinie mindestens den Zugriff auf zulassen. `es:ESHttpGet` Im Folgenden wird ein Beispiel gezeigt:

JSON

```
{
"Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::111222333444:user/john-doe"
        ]
      },
      "Action": "es:ESHttpGet",
      "Resource": "arn:aws:es:us-east-1:account:domain/my-domain/*"
    }
  ]
}
```

Eine differenzierte Zugriffskontrolle für die Quelldomäne bewertet die Anfrage, um festzustellen, ob sie mit gültigen IAM- oder HTTP-Basisanmeldedaten signiert ist. Ist dies der Fall, bewertet die feinkörnige Zugriffskontrolle als Nächstes, ob der Benutzer berechtigt ist, die Suche durchzuführen und auf die Daten zuzugreifen.

Im Folgenden sind die Berechtigungsanforderungen für Suchvorgänge aufgeführt:

- Wenn mit der Anfrage nur Daten in der Zieldomäne durchsucht werden (z. `dest-alias:dest-index/_search`) B. sind Berechtigungen nur für die Zieldomäne erforderlich).
- Wenn mit der Anfrage Daten in beiden Domänen durchsucht werden (z. `source-index,dest-alias:dest-index/_search`) B. sind Berechtigungen für beide Domänen erforderlich).
- Um eine differenzierte Zugriffskontrolle zu verwenden, `indices:admin/shards/search_shards` ist die Berechtigung zusätzlich zu den standardmäßigen Lese- oder Suchberechtigungen für die entsprechenden Indizes erforderlich.

Die Quelldomäne übergibt die Anforderung an die Zieldomäne. Die Zieldomäne wertet diese Anforderung anhand ihrer Domänenzugriffsrichtlinie aus. Um alle Funktionen der OpenSearch Benutzeroberfläche zu unterstützen, z. B. das Indizieren von Dokumenten und das Durchführen von Standardsuchen, müssen vollständige Berechtigungen festgelegt werden. Im Folgenden finden Sie ein Beispiel für unsere empfohlene Richtlinie für die Zieldomäne:

JSON

```
{
"Version": "2012-10-17",
 "Statement": [
    {
       "Effect": "Allow",
       "Principal": {
         "AWS": [
           "*"
        ]
      },
      "Action": [
        "es:ESHttp*"
      ],
      "Resource": "arn:aws:es:us-east-2:111222333444:domain/my-destination-
domain/*"
    },
```

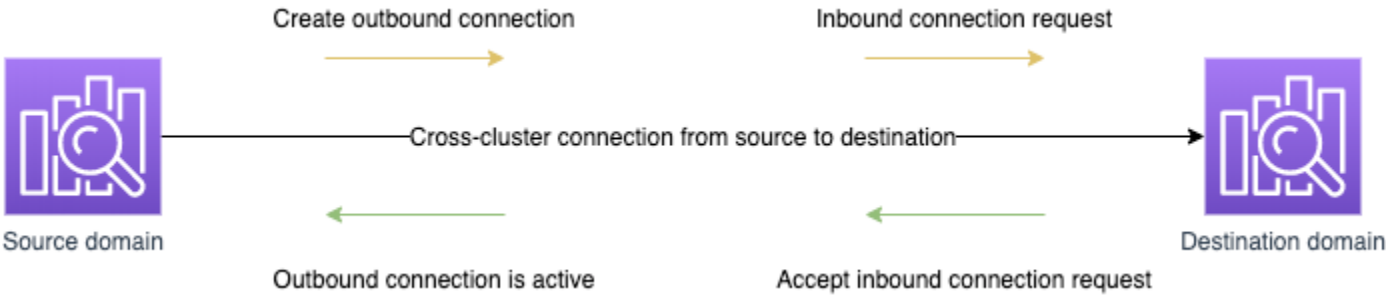
```
    {
    "Effect": "Allow",
        "Principal": {
    "AWS": "*"
      },
      "Action": "es:ESCrossClusterGet",
      "Resource": "arn:aws:es:us-east-2:111222333444:domain/"
    }
  ]
}
```

Wenn Sie nur einfache Suchen durchführen möchten, besteht die Richtlinienmindestanforderung darin, dass die `es:ESCrossClusterGet` Genehmigung für die Zieldomain ohne Unterstützung von Platzhaltern beantragt wird. In der vorherigen Richtlinie würden Sie beispielsweise den Domainnamen als */my-destination-domain* und nicht */my-destination-domain/** angeben.

In diesem Fall führt die Zieldomäne die Suche durch und gibt die Ergebnisse an die Quelldomäne zurück. Die Quelldomäne kombiniert ihre eigenen Ergebnisse (falls vorhanden) mit den Ergebnissen der Zieldomäne und gibt sie an Sie zurück.

Eine Verbindung zwischen Domänen herstellen

Eine clusterübergreifende Suchverbindung ist unidirektional von der Quelldomäne zur Zieldomäne. Das bedeutet, dass die Zieldomänen (in einem anderen Konto oder einer anderen Region) die Quelldomäne, die lokal auf der OpenSearch Benutzeroberfläche ist, nicht abfragen können. Die Quelldomäne stellt eine ausgehende Verbindung zur Zieldomäne her. Die Zieldomäne empfängt eine eingehende Verbindungsanfrage von der Quelldomäne.



Um eine Verbindung zwischen Domänen herzustellen

1. Melden Sie sich zu https://console.aws.amazon.com/aos/Hause bei der Amazon OpenSearch Service-Konsole an.

2. Wählen Sie in der linken Navigationsleiste Domains aus.
3. Wählen Sie den Namen einer Domain aus, die als Quelldomain dienen soll, und wählen Sie dann den Tab Verbindungen aus.
4. Wählen Sie im Bereich Ausgehende Verbindungen die Option Anfrage aus.
5. Geben Sie unter Verbindungs-Alias einen Namen für die Verbindung ein. Der Verbindungsalias wird in der OpenSearch Benutzeroberfläche für die Auswahl der Zieldomänen verwendet.
6. Wählen Sie für den Verbindungsmodus Direct für clusterübergreifende Suchen oder Replikation.
7. Um anzugeben, dass die Verbindung nicht verfügbare Cluster während einer Suche überspringen soll, aktivieren Sie das Feld Nicht verfügbare Cluster überspringen. Wenn Sie diese Option wählen, wird sichergestellt, dass Ihre clusterübergreifenden Abfragen unvollständige Ergebnisse zurückgeben, unabhängig von Ausfällen auf einem oder mehreren Remote-Clustern.
8. Wählen Sie für Zielcluster zwischen Connect einem Cluster in diesem verbinden AWS-Konto und Mit einem Cluster in einem anderen verbinden AWS-Konto.
9. Geben Sie für Remote Domain ARN den Amazon-Ressourcennamen (ARN) für den Cluster ein. Der Domain-ARN befindet sich im Bereich Allgemeine Informationen auf der Detailseite der Domain.

   Die Domain muss die folgenden Anforderungen erfüllen:

   - Der ARN muss das Format haben`arn:`*`partition`*`:es:`*`regionaccount-id`*`:`*`type`*`/`*`domain-id`*. Zum Beispiel:

     ```
     arn:aws:es:us-east-2:111222333444:domain/my-domain
     ```
   - Die Domain muss für die Verwendung von OpenSearch Version 1.0 (oder höher) oder Elasticsearch Version 6.7 (oder höher) konfiguriert sein.
   - Für die Domain muss eine detaillierte Zugriffskontrolle aktiviert sein.
   - Die Domain muss laufen. OpenSearch
10. Wählen Sie Request (Anfrage).

Die Cluster-übergreifende Suche überprüft zuerst die Verbindungsanforderung, um sicherzustellen, dass die Voraussetzungen erfüllt sind. Wenn die Domänen nicht kompatibel sind, wechselt die Verbindungsanforderung in den `Validation failed` Status.

Wenn die Verbindungsanforderung erfolgreich validiert wurde, wird sie an die Zieldomäne gesendet, wo sie genehmigt werden muss. Bis diese Genehmigung erteilt wird, bleibt die Verbindung in einem

`Pending acceptance` Zustand. Wenn die Verbindungsanforderung in der Zieldomäne akzeptiert wird, ändert sich der Status in `Active` und die Zieldomäne steht für Abfragen zur Verfügung.

Auf der Domänenseite werden die allgemeinen Domänenintegritäts- und Instance-Integritätsdetails Ihrer Zieldomäne angezeigt. Nur Domänenbesitzer haben die Flexibilität, Verbindungen zu oder von ihren Domänen zu erstellen, anzuzeigen, zu entfernen und zu überwachen.

Nachdem die Verbindung hergestellt wurde, wird jeder Datenverkehr, der zwischen den Knoten der verbundenen Domänen fließt, verschlüsselt. Wenn Sie eine VPC-Domäne mit einer Nicht-VPC-Domäne verbinden und die Nicht-VPC-Domäne ein öffentlicher Endpunkt ist, der Datenverkehr aus dem Internet empfangen kann, ist der clusterübergreifende Verkehr zwischen den Domänen weiterhin verschlüsselt und sicher.

Testen Sie Ihre Sicherheitseinstellungen für den region- und kontoübergreifenden Datenzugriff mit clusterübergreifender Suche

Nachdem Sie die Zugriffsberechtigungen für den region- und kontoübergreifenden Datenzugriff mit clusterübergreifender Suche eingerichtet haben, empfehlen wir, das Setup mit einer Drittanbieterplattform für die kollaborative PostmanAPI-Entwicklung zu testen.

Um Ihr Sicherheits-Setup einzurichten, verwenden Sie Postman

1. Indexieren Sie ein Dokument in der Zieldomäne. Im Folgenden finden Sie eine Beispielanforderung:

```
POST https://dst-domain.us-east-1.es.amazonaws.com/books/_doc/1
{
"Dracula": "Bram Stoker"
}
```

2. Wenn Sie diesen Index von der Quelldomäne abfragen möchten, fügen Sie den Verbindungsalias der Zieldomäne in die Abfrage ein. Sie finden den Verbindungsalias auf der Registerkarte Verbindungen in Ihrem Domänen-Dashboard. Im Folgenden finden Sie eine Beispielanforderung und eine gekürzte Antwort:

```
GET https://src-domain.us-east-1.es.amazonaws.com/connection_alias:books/_search
{
    ...
  "hits": [
    {
```

```
"_index": "source-destination:books",
      "_type": "_doc",
      "_id": "1",
      "_score": 1,
      "_source": {
"Dracula": "Bram Stoker"
      }
    }
  ]
}
```

3. (Optional) Sie können eine Konfiguration erstellen, die mehrere Domänen in einer einzigen Suche umfasst. Nehmen wir zum Beispiel an, Sie haben Folgendes eingerichtet:

   Eine Verbindung zwischen `domain-a` bis `domain-b` mit dem Namen des Verbindungsalias `cluster_b`

   Eine Verbindung zwischen `domain-a` bis`domain-c`, mit einem Verbindungsalias namens `cluster_c`

   In diesem Fall umfassen Ihre Suchanfragen den Inhalt `domain-a`, `domain-b`, und`domain-c`. Im Folgenden finden Sie ein Beispiel für eine Anfrage und eine Antwort:

   Anforderung

   ```
   GET https://src-domain.us-east-1.es.amazonaws.com/
   local_index,cluster_b:b_index,cluster_c:c_index/_search
   {
     "query": {
       "match": {
         "user": "domino"
       }
     }
   }
   ```

   Antwort:

   ```
   {
   "took": 150,
     "timed_out": false,
     "_shards": {
   "total": 3,
   ```

```
    "successful": 3,
    "failed": 0,
    "skipped": 0
  },
  "_clusters": {
"total": 3,
    "successful": 3,
    "skipped": 0
  },
  "hits": {
"total": 3,
    "max_score": 1,
    "hits": [
      {
"_index": "local_index",
        "_type": "_doc",
        "_id": "0",
        "_score": 1,
        "_source": {
"user": "domino",
          "message": "This is message 1",
          "likes": 0
        }
      },
      {
"_index": "cluster_b:b_index",
        "_type": "_doc",
        "_id": "0",
        "_score": 2,
        "_source": {
"user": "domino",
          "message": "This is message 2",
          "likes": 0
        }
      },
      {
"_index": "cluster_c:c_index",
        "_type": "_doc",
        "_id": "0",
        "_score": 3,
        "_source": {
"user": "domino",
          "message": "This is message 3",
          "likes": 0
```

```
        }
      }
    ]
  }
}
```

Wenn Sie in Ihrer Verbindungseinrichtung nicht ausgewählt haben, dass nicht verfügbare Cluster übersprungen werden sollen, müssen alle Zielcluster, die Sie durchsuchen, verfügbar sein, damit Ihre Suchanfrage erfolgreich ausgeführt werden kann. Andernfalls schlägt die gesamte Anforderung fehl, auch wenn eine der Domänen nicht verfügbar ist, werden keine Suchergebnisse zurückgegeben.

Löschen einer Verbindung

Durch das Löschen einer Verbindung werden alle clusterübergreifenden Suchvorgänge in der Zieldomäne beendet.

Sie können das folgende Verfahren entweder für die Quell- oder Zieldomäne ausführen, um die Verbindung zu entfernen. Nachdem Sie die Verbindung entfernt haben, bleibt sie mit einem Status von `Deleted` 15 Tagen sichtbar.

Sie können eine Domäne mit aktiven Cluster-übergreifenden Verbindungen nicht löschen. Um eine Domäne zu löschen, entfernen Sie zuerst alle eingehenden und ausgehenden Verbindungen aus dieser Domäne. Damit stellen Sie sicher, dass Sie die Benutzer der Cluster-übergreifenden Domäne berücksichtigen, bevor Sie die Domäne löschen.

So löschen Sie eine Verbindung

1. Melden Sie sich zu https://console.aws.amazon.com/aos/Hause bei der Amazon OpenSearch Service-Konsole an.
2. Wählen Sie in der linken Navigationsleiste Domains aus.
3. Wählen Sie den Namen einer zu löschenden Domain und anschließend den Tab Verbindungen aus.
4. Wählen Sie den Namen einer Verbindung aus, die gelöscht werden soll.
5. Wählen Sie Löschen und bestätigen Sie dann den Löschvorgang.

Verwaltung des Zugriffs auf die OpenSearch Benutzeroberfläche von einem VPC-Endpunkt aus

Mithilfe von können Sie eine private Verbindung zwischen Ihrer VPC und der OpenSearch Benutzeroberfläche herstellen AWS PrivateLink. Über diese Verbindung können Sie auf OpenSearch UI-Anwendungen zugreifen, als ob sie sich in derselben VPC befinden würden. Auf diese Weise müssen Sie kein Internet-Gateway, kein NAT-Gerät oder keine VPN-Verbindung konfigurieren oder AWS Direct Connect die Verbindung herstellen. Instances in Ihrer VPC benötigen keine öffentlichen IP-Adressen, um auf die OpenSearch Benutzeroberfläche zuzugreifen.

Um diese private Verbindung herzustellen, erstellen Sie zunächst einen Schnittstellenendpunkt, der von AWS PrivateLink betrieben wird. In jedem Subnetz, das Sie für den Schnittstellenendpunkt angeben, wird automatisch eine Endpunkt-Netzwerkschnittstelle erstellt. Dabei handelt es sich um vom Anforderer verwaltete Netzwerkschnittstellen, die als Einstiegspunkt für Datenverkehr dienen, der für UI-Anwendungen bestimmt ist. OpenSearch

Erstellen einer privaten Verbindung zwischen einer VPC und OpenSearch einer Benutzeroberfläche

Mit dem AWS Management Console oder AWS CLI können Sie eine private Verbindung für den Zugriff auf die OpenSearch Benutzeroberfläche von einer VPC aus herstellen.

Erstellen einer privaten Verbindung zwischen einer VPC und OpenSearch UI (Konsole)

So erstellen Sie mithilfe der Konsole eine private Verbindung zwischen einer VPC und der OpenSearch Benutzeroberfläche

1. Melden Sie sich zu https://console.aws.amazon.com/aos/Hause bei der Amazon OpenSearch Service-Konsole an.
2. Wählen Sie in der linken Navigationsleiste unter Serverless die Option VPC-Endpoints aus.
3. Wählen Sie Create VPC endpoint (VPC-Endpunkt) erstellen.
4. Geben Sie unter Name einen Namen für den Endpunkt ein.
5. Wählen Sie für VPC die VPC aus, von der aus Sie auf OpenSearch UI-Anwendungen zugreifen.
6. Wählen Sie für Subnetze ein Subnetz aus, von dem aus Sie auf UI-Anwendungen zugreifen OpenSearch möchten.

> **Note**
>
> Die IP-Adresse und der DNS-Typ eines Endpunkts basieren auf dem Subnetztyp:
>
> - Dual-Stack: Wenn alle Subnetze sowohl als auch Adressbereiche IPv4 haben. IPv6
> - IPv6: Wenn alle Subnetze nur Subnetze sind IPv6 .
> - IPv4: Wenn alle Subnetze Adressbereiche haben IPv4 .

7. Wählen Sie unter Sicherheitsgruppen eine oder mehrere Sicherheitsgruppen aus, die den Endpunkt-Netzwerkschnittstellen zugeordnet werden sollen.

> **Note**
>
> In diesem Schritt schränken Sie die Ports, Protokolle und Quellen für eingehenden Datenverkehr ein, den Sie für Ihren Endpunkt autorisieren. Stellen Sie sicher, dass die Sicherheitsgruppenregeln den Ressourcen, die den VPC-Endpunkt für die Kommunikation mit OpenSearch UI-Anwendungen verwenden, auch die Kommunikation mit der Endpunkt-Netzwerkschnittstelle ermöglichen.

8. 8. Wählen Sie Endpunkt erstellen aus.

Erstellen einer privaten Verbindung zwischen einer VPC und OpenSearch UI ()AWS CLI

Um eine private Verbindung zwischen einer VPC und der OpenSearch Benutzeroberfläche herzustellen, verwenden Sie den AWS CLI

Führen Sie den folgenden Befehl aus. Ersetzen Sie *placeholder values* durch Ihre Informationen.

```
aws opensearchserverless create-vpc-endpoint \
    --region region \
    --endpoint endpoint \
    --name vpc_endpoint_name \
    --vpc-id vpc_id \
    --subnet-ids subnet_ids
```

Aktualisierung der VPC-Endpunktrichtlinie, um den Zugriff auf die OpenSearch UI-Anwendung zu ermöglichen

Nachdem Sie die private Verbindung erstellt haben, aktualisieren Sie die VPC-Endpunktrichtlinie, um den Zugriff auf die OpenSearch UI-Anwendung in der VPC-Endpunktrichtlinie zu ermöglichen, indem Sie die Anwendungs-ID angeben.

Informationen zur Aktualisierung einer VPC-Endpunktrichtlinie finden Sie unter Aktualisieren einer VPC-Endpunktrichtlinie im AWS PrivateLink Handbuch.

Stellen Sie sicher, dass die VPC-Endpunktrichtlinie die folgende Aussage enthält. Ersetzen Sie *placeholder value* durch Ihre Informationen.

```
{
    "Statement": [{
        "Action": ["opensearch:*"],
        "Effect": "Allow",
        "Principal": "*",
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "opensearch:ApplicationId": ["opensearch-ui-application-id"]
            }
        }
    }]
}
```

Widerrufen des Zugriffs auf die OpenSearch Benutzeroberfläche in einer VPC-Endpunktrichtlinie

OpenSearch Für die Benutzeroberfläche ist eine ausdrückliche Genehmigung in der VPC-Endpunktrichtlinie erforderlich, damit Benutzer von der VPC aus auf die Anwendung zugreifen können. Wenn Sie nicht mehr möchten, dass Benutzer über die VPC auf die OpenSearch Benutzeroberfläche zugreifen, können Sie die Berechtigung in der Endpunktrichtlinie entfernen. Danach erhalten Benutzer eine `403 forbidden` Fehlermeldung, wenn sie versuchen, auf die OpenSearch Benutzeroberfläche zuzugreifen.

Informationen zur Aktualisierung einer VPC-Endpunktrichtlinie finden Sie unter Aktualisieren einer VPC-Endpunktrichtlinie im AWS PrivateLink Handbuch.

Im Folgenden finden Sie ein Beispiel für eine VPC-Endpunktrichtlinie, die den Zugriff auf die UI-Anwendungen von der VPC aus verweigert:

```
{
    "Statement": [{
        "Action": ["opensearch:*"],
        "Effect": "Allow",
        "Principal": "*",
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "opensearch:ApplicationId": [""]
            }
        }
    }]
}
```

Verwaltung von Indizes in Amazon Service OpenSearch

Nachdem Sie Daten zu Amazon OpenSearch Service hinzugefügt haben, müssen Sie diese Daten häufig neu indizieren, mit Index-Aliasnamen arbeiten, einen Index in einen kostengünstigeren Speicher verschieben oder ihn ganz löschen. Dieses Kapitel behandelt UltraWarm Speicher, Cold Storage und Index State Management. Informationen zum OpenSearch Index APIs finden Sie in der OpenSearch Dokumentation.

Themen

- UltraWarm Speicher für Amazon OpenSearch Service
- Cold-Speicher für Amazon OpenSearch Service
- OpenSearch optimierter Speicher für Amazon OpenSearch Service
- Verwaltung des Indexstatusmanagement in Amazon OpenSearch Service
- Zusammenfassen von Indizes in Amazon OpenSearch Service mit Index-Rollups
- Transformieren von Indizes im Amazon Service OpenSearch
- Clusterübergreifende Replikation für Amazon Service OpenSearch
- Migration von Amazon OpenSearch Service-Indizes mithilfe der Remote-Neuindizierung
- Zeitreihendaten in Amazon OpenSearch Service mit Datenströmen verwalten

UltraWarm Speicher für Amazon OpenSearch Service

UltraWarm bietet eine kostengünstige Möglichkeit, große Mengen schreibgeschützter Daten auf Amazon OpenSearch Service zu speichern. Standarddatenknoten verwenden „Hot“-Speicher, der in Form von Instance-Speichern oder Amazon EBS-Volumes an jeden Knoten angefügt ist. Hot Storage bietet die schnellstmögliche Leistung für die Indizierung und die Suche nach neuen Daten.

Anstelle angeschlossenen Speichers verwenden UltraWarm Knoten Amazon S3 und eine ausgeklügelte Caching-Lösung, um die Leistung zu verbessern. Für Indizes, in die Sie nicht aktiv schreiben, weniger häufig abfragen und für die Sie nicht die gleiche Leistung benötigen, UltraWarm bietet dies deutlich niedrigere Kosten pro GiB Daten. Da warme Indizes schreibgeschützt sind, es sei denn, Sie legen sie in den Hot-Speicher zurück, UltraWarm eignet sich das am besten für unveränderliche Daten, wie z. B. Protokolle.

In verhalten OpenSearch sich Warm-Indizes genau wie jeder andere Index. Sie können sie mit demselben abfragen APIs oder damit Visualisierungen in OpenSearch Dashboards erstellen.

Themen

- Voraussetzungen
- UltraWarm Speicheranforderungen und Leistungsüberlegungen
- UltraWarm Preisgestaltung
- Aktiviert UltraWarm
- Migration von Indizes auf Speicher UltraWarm
- Automatisieren von Migrationen
- Migrationsoptimierung
- Abbrechen von Migrationen
- Auflisten von Hot- und Warm-Indizes
- Warm-Indizes in den Hot Storage zurückbringen
- Wiederherstellen von Warm-Indizes aus Snapshots
- Manuelle Snapshots von Warm-Indizes
- Migration Warm-Indizes in Cold Storage
- Bewährte Methoden für KNN-Indizes
- Deaktivierung UltraWarm

Voraussetzungen

UltraWarm hat ein paar wichtige Voraussetzungen:

- UltraWarm erfordert OpenSearch oder Elasticsearch 6.8 oder höher.
- Um einen Warm-Speicher verwenden zu können, müssen Domains über dedizierte Hauptknoten verfügen.
- Bei Verwendung einer Multi-AZ mit Standby-Domain muss die Anzahl der warmen Knoten ein Vielfaches der Anzahl der verwendeten Availability Zones sein.
- Wenn Ihre Domäne einen T2- oder T3-Instance-Typ für Ihre Datenknoten verwendet, können Sie keinen Warm-Speicher verwenden.
- Wenn Ihr Index approximatives k-NN (`"index.knn":true`) verwendet, können Sie ihn von Version 2.17 und höher in einen warmen Speicher verschieben. Domains mit Versionen vor 2.17 können auf 2.17 aktualisiert werden, um diese Funktionalität zu nutzen, aber KNN-Indizes, die auf Versionen vor 2.x erstellt wurden, können nicht auf Version 2.x migriert werden. UltraWarm

- Wenn die Domäne eine differenzierte Zugriffskontrolle verwendet, müssen Benutzer der `ultrawarm_manager` Rolle in OpenSearch Dashboards zugeordnet werden, um API-Aufrufe zu tätigen. UltraWarm

> **Note**
>
> Die `ultrawarm_manager` Rolle ist möglicherweise in einigen bereits vorhandenen OpenSearch Dienstdomänen nicht definiert. Wenn die Rolle in Dashboards nicht angezeigt wird, müssen Sie sie manuell erstellen.

So konfigurieren Sie Berechtigungen

Wenn Sie die Aktivierung UltraWarm in einer bereits vorhandenen OpenSearch Dienstdomäne durchführen, ist die `ultrawarm_manager` Rolle möglicherweise nicht in der Domäne definiert. Benutzer ohne Administratorrechte müssen dieser Rolle zugeordnet werden, um Warm-Indizes in Domains mithilfe einer fein abgestuften Zugriffskontrolle zu verwalten. Führen Sie die folgenden Schritte aus, um die `ultrawarm_manager`-Rolle manuell zu erstellen:

1. Gehen Sie in OpenSearch Dashboards zu Sicherheit und wählen Sie Berechtigungen aus.
2. Wählen Sie Aktionsgruppe erstellen und konfigurieren Sie die folgenden Gruppen:

Group name (Gruppenname)	Berechtigungen
`ultrawarm_cluster`	• `cluster:admin/ultrawarm/migration/list` • `cluster:monitor/nodes/stats`
`ultrawarm_index_read`	• `indices:admin/ultrawarm/migration/get` • `indices:admin/get`
`ultrawarm_index_write`	• `indices:admin/ultrawarm/migration/warm` • `indices:admin/ultrawarm/migration/hot` • `indices:monitor/stats` • `indices:admin/ultrawarm/migration/cancel`

3. Wählen Sie Rollen und Rolle erstellen.

4. Benennen Sie die Rolle ultrawarm_manager.
5. Wählen Sie für Clusterberechtigungen `ultrawarm_cluster` und `cluster_monitor` aus.
6. Geben Sie für Index * ein.
7. Wählen Sie für Indexberechtigungen `ultrawarm_index_read`, `ultrawarm_index_write` und `indices_monitor` aus.
8. Wählen Sie Erstellen aus.
9. Nachdem Sie die Rolle erstellt haben, ordnen Sie sie einer beliebigen Benutzer- oder Backend-Rolle zu, die UltraWarm Indizes verwaltet.

UltraWarm Speicheranforderungen und Leistungsüberlegungen

Wie in erläutertthe section called “Berechnung der Speicheranforderungen”, verursachen Daten im Hot Storage einen erheblichen Overhead: Replikate, reservierter Linux-Speicherplatz und reservierter OpenSearch Dienstspeicher. Zum Beispiel benötigt ein primärer 20 GiB-Shard mit einem Replica-Shard etwa 58 GiB Hot Storage.

Da Amazon S3 verwendet wird, UltraWarm verursacht es keinen solchen Overhead. Bei der Berechnung des UltraWarm Speicherbedarfs berücksichtigen Sie nur die Größe der primären Shards. Durch die Dauerhaftigkeit der Daten in S3 entfällt die Notwendigkeit für Replicas und S3 macht alle Betriebssystem- oder Dienstüberlegungen überflüssig. Derselbe 20 GiB-Shard erfordert 20 GiB Warm-Speicher. Wenn Sie eine `ultrawarm1.large.search`-Instance bereitstellen, können Sie alle 20 TiB des maximalen Speichers für primäre Shards verwenden. Eine Zusammenfassung der Instance-Typen und Informationen zur maximalen Speicherkapazität, die jeder adressieren kann, finden Sie unter the section called “UltraWarm Speicherkontingente”.

Wir empfehlen weiterhin eine maximale Shard-Größe von 50 GiB. UltraWarm Die Anzahl der CPU-Kerne und die Menge an RAM, die jedem UltraWarm Instance-Typ zugewiesen ist, geben Ihnen eine Vorstellung davon, wie viele Shards gleichzeitig durchsucht werden können. Beachten Sie, dass während in S3 nur primäre Shards für den UltraWarm Speicher zählen, OpenSearch Dashboards die UltraWarm Indexgröße `_cat/indices` dennoch als Summe aller primären und Replikat-Shards melden.

Jede `ultrawarm1.medium.search`-Instance hat beispielsweise zwei CPU-Kerne und kann bis zu 1,5 TiB Speicher auf S3 adressieren. Zwei dieser Instances haben zusammen 3 TiB Speicher, was ungefähr 62 Shards ergibt, wenn jeder Shard 50 GiB groß ist. Wenn eine Anfrage an den Cluster nur vier dieser Shards durchsucht, kann die Leistung hervorragend sein. Wenn die Anfrage

breit gefächert ist und alle 62 durchsucht, können die vier CPU-Kerne Schwierigkeiten haben, den Vorgang auszuführen. Überwachen Sie die `WarmCPUUtilization` und `WarmJVMMemoryPressure` UltraWarm -Metriken, um zu verstehen, wie die Instances mit Ihren Workloads umgehen.

Wenn Sie viel oder häufig suchen, sollten Sie die Indizes im Hot Storage belassen. Wie bei jedem anderen OpenSearch Workload besteht der wichtigste Schritt zur Bestimmung, ob Ihre Anforderungen UltraWarm erfüllt werden, darin, repräsentative Client-Tests mit einem realistischen Datensatz durchzuführen.

UltraWarm Preisgestaltung

Bei Hot Storage zahlen Sie für das, was Sie bereitstellen. Einige Instances benötigen ein angefügtes Amazon-EBS-Volume, während andere einen Instance-Speicher enthalten. Unabhängig davon, ob dieser Speicher leer oder voll ist, zahlen Sie den gleichen Preis.

Bei UltraWarm Storage zahlen Sie nur für das, was Sie tatsächlich nutzen. Eine `ultrawarm1.large.search`-Instance kann bis zu 20 TiB Speicher auf S3 adressieren, aber wenn Sie nur 1 TiB Daten speichern, werden Ihnen nur 1 TiB Daten in Rechnung gestellt. Wie bei allen anderen Knotentypen zahlen Sie auch einen Stundensatz für jeden UltraWarm Knoten. Weitere Informationen finden Sie unter the section called “Preisgestaltung”.

Aktiviert UltraWarm

Die Konsole ist die einfachste Möglichkeit, eine Domain zu erstellen, die Warm-Speicher verwendet. Wählen Sie beim Erstellen der Domain Enable Warm data nodes (Warm-Datenknoten aktivieren) und die Anzahl der gewünschten Warm-Knoten aus. Derselbe grundlegende Prozess funktioniert auf vorhandenen Domains, sofern sie die Voraussetzungenerfüllen. Selbst nachdem der Domänenstatus von Processing (Verarbeitung) zu Active (Aktiv) geändert wurde, steht er UltraWarm möglicherweise mehrere Stunden lang nicht zur Verfügung.

Bei Verwendung einer Multi-AZ mit Standby-Domain muss die Anzahl der warmen Knoten ein Vielfaches der Anzahl der Availability Zones sein. Weitere Informationen finden Sie unter the section called “Multi-AZ mit Standby”.

Sie können auch die Konfigurations-API AWS CLIoder verwenden UltraWarm, um insbesondere die `WarmType` Optionen `WarmEnabled``WarmCount`, und in `ClusterConfig` zu aktivieren.

> **Note**
>
> Die Domains unterstützen eine maximale Anzahl von Warm-Knoten. Details hierzu finden Sie unter the section called “Kontingente”.

Beispiel für einen CLI-Befehl

Der folgende AWS CLI -Befehl erstellt eine Domäne mit drei Datenknoten, drei dedizierten Hauptknoten, sechs warmen Knoten und aktivierter feingranularer Zugriffskontrolle:

```
aws opensearch create-domain \
  --domain-name my-domain \
  --engine-version Opensearch_1.0 \
  --cluster-config
 InstanceCount=3,InstanceType=r6g.large.search,DedicatedMasterEnabled=true,DedicatedMasterType=
 \
  --ebs-options EBSEnabled=true,VolumeType=gp2,VolumeSize=11 \
  --node-to-node-encryption-options Enabled=true \
  --encryption-at-rest-options Enabled=true \
  --domain-endpoint-options EnforceHTTPS=true,TLSSecurityPolicy=Policy-Min-
TLS-1-2-2019-07 \
  --advanced-security-options
 Enabled=true,InternalUserDatabaseEnabled=true,MasterUserOptions='{MasterUserName=master-
user,MasterUserPassword=master-password}' \
  --access-policies '{"Version":"2012-10-17","Statement":
[{"Effect":"Allow","Principal":{"AWS":["123456789012"]},"Action":
["es:*"],"Resource":"arn:aws:es:us-west-1:123456789012:domain/my-domain/*"}]}' \
  --region us-east-1
```

Weitere Informationen finden Sie in der AWS CLI -Befehlsreferenz.

Beispiel für eine Konfigurations-API-Anforderung

Die folgende Anforderung an die Konfigurations-API erstellt eine Domain mit drei Datenknoten, drei dedizierten Hauptknoten und sechs Warm-Knoten mit differenzierter Zugriffskontrolle und einer restriktiven Zugriffsrichtlinie:

```
POST https://es.us-east-2.amazonaws.com/2021-01-01/opensearch/domain
{
  "ClusterConfig": {
    "InstanceCount": 3,
```

```
    "InstanceType": "r6g.large.search",
    "DedicatedMasterEnabled": true,
    "DedicatedMasterType": "r6g.large.search",
    "DedicatedMasterCount": 3,
    "ZoneAwarenessEnabled": true,
    "ZoneAwarenessConfig": {
      "AvailabilityZoneCount": 3
    },
    "WarmEnabled": true,
    "WarmCount": 6,
    "WarmType": "ultrawarm1.medium.search"
  },
  "EBSOptions": {
    "EBSEnabled": true,
    "VolumeType": "gp2",
    "VolumeSize": 11
  },
  "EncryptionAtRestOptions": {
    "Enabled": true
  },
  "NodeToNodeEncryptionOptions": {
    "Enabled": true
  },
  "DomainEndpointOptions": {
    "EnforceHTTPS": true,
    "TLSSecurityPolicy": "Policy-Min-TLS-1-2-2019-07"
  },
   "AdvancedSecurityOptions": {
    "Enabled": true,
    "InternalUserDatabaseEnabled": true,
    "MasterUserOptions": {
      "MasterUserName": "master-user",
      "MasterUserPassword": "master-password"
    }
  },
  "EngineVersion": "Opensearch_1.0",
  "DomainName": "my-domain",
  "AccessPolicies": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect\":\"Allow
\",\"Principal\":{\"AWS\":[\"123456789012\"]},\"Action\":[\"es:*\"],\"Resource\":
\"arn:aws:es:us-east-1:123456789012:domain/my-domain/*\"}]}"
}
```

Weitere Informationen finden Sie in der Amazon OpenSearch Service -API-Referenz.

Migration von Indizes auf Speicher UltraWarm

Wenn Sie das Schreiben in einen Index abgeschlossen haben und nicht mehr die schnellstmögliche Suchleistung benötigen, migrieren Sie ihn von Hot zu UltraWarm:

```
POST _ultrawarm/migration/my-index/_warm
```

Überprüfen Sie dann den Status der Migration:

```
GET _ultrawarm/migration/my-index/_status

{
  "migration_status": {
    "index": "my-index",
    "state": "RUNNING_SHARD_RELOCATION",
    "migration_type": "HOT_TO_WARM",
    "shard_level_status": {
      "running": 0,
      "total": 5,
      "pending": 3,
      "failed": 0,
      "succeeded": 2
    }
  }
}
```

Die Indexintegrität muss grün sein, um eine Migration durchzuführen. Wenn Sie mehrere Indizes schnell hintereinander migrieren, erhalten Sie eine Zusammenfassung aller Migrationen im Klartext, ähnlich der `_cat`-API:

```
GET _ultrawarm/migration/_status?v

index    migration_type state
my-index HOT_TO_WARM    RUNNING_SHARD_RELOCATION
```

OpenSearch Der Service migriert einen Index nach UltraWarm dem anderen im Sie können bis zu 200 Migrationen in der Warteschlange haben. Jede Anfrage, die das Limit überschreitet, wird abgelehnt. Um die aktuelle Anzahl von Migrationen in der Warteschlange zu überprüfen, überwachen Sie die `HotToWarmMigrationQueueSize`-Metrik. Indizes bleiben während des gesamten Migrationsprozesses verfügbar – keine Ausfallzeiten.

Der Migrationsprozess weist die folgenden Zustände auf:

```
PENDING_INCREMENTAL_SNAPSHOT
RUNNING_INCREMENTAL_SNAPSHOT
FAILED_INCREMENTAL_SNAPSHOT
PENDING_FORCE_MERGE
RUNNING_FORCE_MERGE
FAILED_FORCE_MERGE
PENDING_FULL_SNAPSHOT
RUNNING_FULL_SNAPSHOT
FAILED_FULL_SNAPSHOT
PENDING_SHARD_RELOCATION
RUNNING_SHARD_RELOCATION
FINISHED_SHARD_RELOCATION
```

Wie diese Zustände zeigen, können Migrationen während Snapshots, Shard-Verlagerungen oder erzwungenen Zusammenführungen fehlschlagen. Fehler bei Snapshots oder Shard-Verlagerungen sind in der Regel auf Knotenfehler oder S3-Konnektivitätsprobleme zurückzuführen. Ein Mangel an Speicherplatz ist in der Regel die zugrunde liegende Ursache für Fehler bei erzwungenen Zusammenführungen.

Nach Abschluss der Migration gibt dieselbe `_status`-Anforderung einen Fehler zurück. Wenn Sie den Index zu diesem Zeitpunkt überprüfen, können Sie einige Einstellungen sehen, die für Warm-Indizes eindeutig sind:

```
GET my-index/_settings

{
  "my-index": {
    "settings": {
      "index": {
        "refresh_interval": "-1",
        "auto_expand_replicas": "false",
        "provided_name": "my-index",
        "creation_date": "1599241458998",
        "unassigned": {
          "node_left": {
            "delayed_timeout": "5m"
          }
        },
        "number_of_replicas": "1",
        "uuid": "GswyCdR0RSq0SJYmzsIpiw",
```

```
        "version": {
          "created": "7070099"
        },
        "routing": {
          "allocation": {
            "require": {
              "box_type": "warm"
            }
          }
        },
        "number_of_shards": "5",
        "merge": {
          "policy": {
            "max_merge_at_once_explicit": "50"
          }
        }
      }
    }
  }
}
```

- `number_of_replicas` ist in diesem Fall die Anzahl der passiven Replicas, die keinen Speicherplatz verbrauchen.
- `routing.allocation.require.box_type` gibt an, dass der Index Warm-Knoten anstelle von Standarddatenknoten verwenden soll.
- `merge.policy.max_merge_at_once_explicit` gibt die Anzahl der Segmente an, die während der Migration gleichzeitig zusammengeführt werden sollen.

Indizes im Warm-Speicher sind schreibgeschützt, es sei denn, Sie legen sie in den Warm-Speicher zurück, wodurch sie UltraWarm am besten für unveränderliche Daten wie Protokolle geeignet ist. Sie können die Indizes abfragen und löschen, aber Sie können keine einzelnen Dokumente hinzufügen, aktualisieren oder löschen. Wenn Sie es versuchen, wird möglicherweise der folgende Fehler angezeigt:

```
{
  "error" : {
    "root_cause" : [
      {
        "type" : "cluster_block_exception",
```

```
        "reason" : "index [indexname] blocked by: [TOO_MANY_REQUESTS/12/disk usage
 exceeded flood-stage watermark, index has read-only-allow-delete block];"
      }
    ],
    "type" : "cluster_block_exception",
    "reason" : "index [indexname] blocked by: [TOO_MANY_REQUESTS/12/disk usage exceeded
 flood-stage watermark, index has read-only-allow-delete block];"
  },
  "status" : 429
}
```

Automatisieren von Migrationen

Wir empfehlen die Verwendung von the section called “Indexstatusmanagement” zur Automatisierung des Migrationsprozesses, nachdem ein Index ein bestimmtes Alter erreicht hat oder andere Bedingungen erfüllt. Sehen Sie sich die Beispielrichtlinie an, die diesen Workflow veranschaulicht.

Migrationsoptimierung

Indexmigrationen auf UltraWarm Speicher erfordern eine erzwungene Zusammenführung. Jeder OpenSearch Index besteht aus einer bestimmten Anzahl von Shards, und jeder Shard besteht aus einer bestimmten Anzahl von Lucene-Segmenten. Der Vorgang der erzwungenen Zusammenführung löscht Dokumente, die zum Löschen markiert wurden, und spart Speicherplatz. Führt Indizes standardmäßig zu einem Segment zusammen, mit Ausnahme von kNN-Indizes, bei denen der Standardwert 20 verwendet wird. UltraWarm

Sie können diesen Wert mit der `index.ultrawarm.migration.force_merge.max_num_segments`-Einstellung auf bis zu 1.000 Segmente ändern. Höhere Werte beschleunigen den Migrationsprozess, erhöhen jedoch die Abfragelatenz für den warmen Index nach Abschluss der Migration. Um die Einstellung zu ändern, stellen Sie die folgende Anfrage:

```
PUT my-index/_settings
{
  "index": {
    "ultrawarm": {
      "migration": {
        "force_merge": {
          "max_num_segments": 1
        }
```

```
      }
    }
  }
}
```

Um zu überprüfen, wie lange diese Phase des Migrationsprozesses dauert, überwachen Sie die `HotToWarmMigrationForceMergeLatency`-Metrik.

Abbrechen von Migrationen

UltraWarm verarbeitet Migrationen sequentiell in einer Warteschlange. Wenn sich eine Migration in der Warteschlange befindet, aber noch nicht gestartet wurde, können Sie sie mit der folgenden Anforderung aus der Warteschlange entfernen:

```
POST _ultrawarm/migration/_cancel/my-index
```

Wenn Ihre Domain eine differenzierte Zugriffskontrolle verwendet, müssen Sie die `indices:admin/ultrawarm/migration/cancel`-Berechtigung haben, um diese Anfrage zu stellen.

Auflisten von Hot- und Warm-Indizes

UltraWarm fügt zwei zusätzliche Optionen hinzu, ähnlich wie`_all`, um das Verwalten von Warm- und Hot-Indizes zu erleichtern. Für eine Auflistung aller Warm- oder Hot-Indizes, tätigen Sie folgende Anforderungen:

```
GET _warm
GET _hot
```

Sie können diese Optionen in anderen Anforderungen verwenden, die Indizes angeben, zum Beispiel:

```
_cat/indices/_warm
_cluster/state/_all/_hot
```

Warm-Indizes in den Hot Storage zurückbringen

Wenn Sie noch einmal in einen Index schreiben müssen, migrieren Sie ihn zurück in den Hot Storage:

```
POST _ultrawarm/migration/my-index/_hot
```

Sie können gleichzeitig bis zu 10 Migrationen vom Warm- zum Hot-Speicher durchführen. OpenSearch Der Service verarbeitet Migrationsanforderungen nacheinander in der Warteschlange. Überwachen Sie die `WarmToHotMigrationQueueSize`-Metrik, um die aktuelle Anzahl zu überprüfen.

Überprüfen Sie nach Abschluss der Migration die Indexeinstellungen, um sicherzustellen, dass sie Ihren Anforderungen entsprechen. Indizes werden mit einem Replikat im Hot Storage wiederhergestellt.

Wiederherstellen von Warm-Indizes aus Snapshots

Fügt zusätzlich zum Standard-Repository für automatisierte Snapshots ein zweites Repository für warme Indizes UltraWarm hinzu,. `cs-ultrawarm` Jeder Snapshot in diesem Repository enthält nur einen Index. Wenn Sie einen warmen Index löschen, bleibt sein Snapshot wie jeder andere automatisierte Snapshot 14 Tage lang im `cs-ultrawarm`-Repository.

Wenn Sie einen Snapshot aus `cs-ultrawarm` wiederherstellen, wird er im Warm Storage und nicht im Hot Storage wiederhergestellt. Snapshots in den Repositorys `cs-automated` und `cs-automated-enc` werden im Hot Storage wiederhergestellt.

Um einen UltraWarm Snapshot im Warmspeicher wiederherzustellen

1. Identifizieren Sie den neuesten Snapshot, der den Index enthält, den Sie wiederherstellen möchten:

```
GET _snapshot/cs-ultrawarm/_all?verbose=false

{
  "snapshots": [{
    "snapshot": "snapshot-name",
    "version": "1.0",
    "indices": [
      "my-index"
    ]
  }]
}
```

> **Note**
>
> Standardmäßig zeigt der `GET _snapshot/<repo>` Vorgang ausführliche Dateninformationen wie Startzeit, Endzeit und Dauer für jeden Snapshot innerhalb eines Repositorys an. Der `GET _snapshot/<repo>` Vorgang ruft Informationen aus den Dateien der einzelnen Snapshots ab, die in einem Repository enthalten sind. Wenn Sie die Startzeit, Endzeit und Dauer nicht benötigen und nur den Namen und die Indexinformationen eines Snapshots benötigen, empfehlen wir, den `verbose=false` Parameter beim Auflisten von Snapshots zu verwenden, um die Verarbeitungszeit zu minimieren und Zeitüberschreitungen zu vermeiden.

2. Wenn der Index bereits vorhanden ist, löschen Sie ihn:

```
DELETE my-index
```

   Wenn Sie den Index nicht löschen möchten, legen Sie ihn in den Hot Storage zurück und indizieren Sie ihn neu.

3. Stellen Sie den Snapshot wieder her:

```
POST _snapshot/cs-ultrawarm/snapshot-name/_restore
```

   UltraWarm ignoriert alle Indexeinstellungen, die Sie in dieser Wiederherstellungsanforderung angeben, aber Sie können Optionen wie `rename_pattern` und `rename_replacement` angeben. Eine Zusammenfassung der OpenSearch Snapshot-Wiederherstellungsoptionen finden Sie in der OpenSearch Dokumentation.

Manuelle Snapshots von Warm-Indizes

Sie können manuelle Snapshots von Warm-Indizes erstellen, dies wird jedoch nicht empfohlen. Das automatisierte `cs-ultrawarm`-Repository enthält bereits ohne Aufpreis einen Snapshot für jeden warmen Index, der während der Migration erstellt wurde.

Standardmäßig schließt OpenSearch Service keine warmen Indizes in manuelle Snapshots ein. Der folgende Aufruf enthält beispielsweise nur Hot-Indizes:

```
PUT _snapshot/my-repository/my-snapshot
```

Wenn Sie manuelle Snapshots von Warm-Indizes erstellen möchten, müssen mehrere wichtige Überlegungen angestellt werden.

- Sie können Hot- und Warm-Indizes nicht mischen. Die folgende Anfrage schlägt beispielsweise fehl:

  ```
  PUT _snapshot/my-repository/my-snapshot
  {
    "indices": "warm-index-1,hot-index-1",
    "include_global_state": false
  }
  ```

  Wenn sie eine Mischung aus Hot- und Warm-Indizes enthalten, schlagen auch Platzhalter (*)-Anweisungen fehl.

- Sie können nur einen warmen Index pro Snapshot einschließen. Die folgende Anfrage schlägt beispielsweise fehl:

  ```
  PUT _snapshot/my-repository/my-snapshot
  {
    "indices": "warm-index-1,warm-index-2,other-warm-indices-*",
    "include_global_state": false
  }
  ```

  Diese Anfrage ist erfolgreich:

  ```
  PUT _snapshot/my-repository/my-snapshot
  {
    "indices": "warm-index-1",
    "include_global_state": false
  }
  ```

- Manuelle Snapshots werden immer im Hot Storage wiederhergestellt, auch wenn sie ursprünglich einen warmen Index enthielten.

Migration Warm-Indizes in Cold Storage

Wenn Sie Daten haben, die Sie selten abfragen UltraWarm , sollten Sie in Erwägung ziehen, diese in einen Cold Storage zu migrieren. Cold Storage ist für Daten gedacht, auf die Sie nur gelegentlich zugreifen oder die nicht mehr aktiv genutzt werden. Sie können Cold-Indizes weder lesen noch in sie

schreiben, aber Sie können sie kostenlos zurück in den Warm-Speicher migrieren, wann immer Sie sie abfragen müssen. Anweisungen finden Sie unter Migrieren von Indizes in Cold Storage.

Bewährte Methoden für KNN-Indizes

- Die Stufe Ultrawarm/Cold ist für alle KNN-Index-Motortypen verfügbar. Wir empfehlen es für KNN-Indizes, die die Lucene-Engine und die festplattenoptimierte Vektorsuche verwenden, bei der die Grafikdaten nicht vollständig in den Off-Heap-Speicher geladen werden müssen. Bei der Verwendung mit systemeigenen In-Memory-Engines wie FAISS und NMSLIB müssen Sie die Größe des Shard-Diagramms berücksichtigen, nach dem aktiv gesucht wird, und die Instances, vorzugsweise des Instance-Typs, entsprechend bereitstellen. UltraWarm `uw.large` Wenn Kunden beispielsweise 2 `uw.large` Instances konfiguriert haben, verfügen sie jeweils über ungefähr `knn.memory.circuit_breaker.limit * 61` GiB verfügbaren Off-Heap-Speicher. Sie erzielen eine optimale Leistung, wenn all Ihre Warm-Abfragen auf Shards abzielen, deren kumulative Grafikgröße den verfügbaren Off-Heap-Speicher nicht überschreitet. Die Latenz wird beeinträchtigt, wenn der verfügbare Speicher aufgrund von Räumungen geringer ist als zum Laden des Diagramms erforderlich ist und darauf gewartet wird, dass Off-Heap-Speicher verfügbar wird. Aus diesem Grund empfehlen wir nicht, `uw.medium` Instances für Anwendungsfälle zu verwenden, in denen In-Memory-Engines verwendet werden, oder für Fälle mit höherem Suchdurchsatz, unabhängig von den Engines.
- KNN-Indizes, zu denen migriert UltraWarm wird, werden nicht zwangsweise zu einem einzigen Segment zusammengeführt. Dadurch werden Auswirkungen auf die heißen und warmen Knoten vermieden, bei denen OOM-Probleme auftreten, weil die Grafikgröße für In-Memory-Engines zu groß wird. Aufgrund der zunehmenden Anzahl von Segmenten pro Shard kann dies dazu führen, dass mehr lokaler Cache-Speicherplatz beansprucht wird und weniger Indizes auf die warme Ebene migriert werden können. Sie können festlegen, dass die Zusammenführung von Indizes zu einem einzelnen Segment erzwungen wird, indem Sie die vorhandene Einstellung verwenden und diese überschreiben, bevor Sie Indizes in die Warm-Tier migrieren. Weitere Informationen finden Sie unter the section called “Migrationsoptimierung”.
- Wenn Sie einen Anwendungsfall haben, in dem Indizes nur selten durchsucht werden und keine latenzempfindliche Arbeitslast abdecken, können Sie diese Indizes auf die Ebene migrieren. UltraWarm Auf diese Weise können Sie die Hot-Tier-Compute-Instances herunterskalieren und den UltraWarm Tier-Computing-Instanzen die Abfrage für Indizes mit niedriger Priorität überlassen. Dies kann auch dazu beitragen, die Ressourcen zu isolieren, die zwischen den Abfragen von Indizes mit niedriger und hoher Priorität verbraucht werden, sodass sie sich nicht gegenseitig beeinflussen.

Deaktivierung UltraWarm

Die Konsole ist die einfachste Möglichkeit, dies zu deaktivieren UltraWarm. Klicken Sie auf die Domain, wählen Sie Aktionen und Clusterkonfiguration bearbeiten. Deaktivieren Sie „Warm Data Nodes aktivieren“ und wählen Sie „Änderungen speichern“. Sie können die `WarmEnabled`-Option auch in der AWS CLI und der Konfigurations-API verwenden.

Bevor Sie das deaktivieren UltraWarm, müssen Sie entweder alle warmen Indizes löschen oder sie wieder in den Hot-Speicher migrieren. Nachdem der Warm-Speicher geleert wurde, warten Sie fünf Minuten, bevor Sie versuchen zu deaktivieren UltraWarm.

Cold-Speicher für Amazon OpenSearch Service

Mit dem Cold-Speicher können Sie beliebig viele selten aufgerufene oder historische Daten in Ihrer OpenSearch Amazon-Service-Domäne speichern und diese bei Bedarf analysieren, zu geringeren Kosten als andere Speicherebenen. Cold-Speicherung ist geeignet, wenn Sie regelmäßige Untersuchungen oder forensische Analysen an Ihren älteren Daten durchführen müssen. Praktische Beispiele für Daten, die für Cold-Speicher geeignet sind, sind selten aufgerufene Protokolle, Daten, die aufbewahrt werden müssen, um Compliance-Anforderungen zu erfüllen, oder Protokolle mit historischem Wert.

Ähnlich wie UltraWarmSpeicher wird der Cold-Speicher von Amazon S3 gesichert. Wenn Sie Cold-Daten abfragen müssen, können Sie diese selektiv an vorhandene UltraWarm Knoten anhängen. Sie können die Migration und den Lebenszyklus Ihrer Cold-Daten manuell oder mit Index-Statusmanagement-Verwaltungsrichtlinien verwalten.

Themen

- Voraussetzungen
- Cold-Speicheranforderungen und Leistungsüberlegungen
- Preise für Cold-Speicherung
- Aktivieren von Cold-Speicherung
- Verwaltung von Cold-Indizes in Dashboards OpenSearch
- Migration von Indizes auf Cold-Speicher
- Automatisierung von Migrationen zum Cold-Speicher
- Abbruch von Migrationen zum Cold-Speicher

- Auflisten der Cold-Indizes
- Migrieren von Cold-Indizes zum Warm-Speicher
- Wiederherstellen von Cold-Indizes aus Snapshots
- Abbruch von Migrationen von Cold- zu Warm-Speicher
- Cold-Index-Metadaten aktualisieren
- Cold-Indizes löschen
- Deaktivieren von Cold-Speicherung

Voraussetzungen

Cold-Speicherung hat die folgenden Voraussetzungen:

- Cold-Speicherung erfordert OpenSearch Elasticsearch Version 7.9 oder höher.
- Um den Cold-Speicher in einer OpenSearch Dienstdomäne zu aktivieren, müssen Sie auch den warmen Speicher in derselben Domäne aktivieren.
- Um einen Cold-Speicher verwenden zu können, müssen Domänen über dedizierte Hauptknoten verfügen.
- Wenn Ihre Domäne einen T2- oder T3-Instance-Typ für Ihre Datenknoten verwendet, können Sie keinen Cold-Speicher verwenden.
- Wenn Ihr Index approximatives k-NN (`"index.knn":true`) verwendet, können Sie ihn von Version 2.17 und höher in einen kühlen Speicher verschieben. Domains mit Versionen vor 2.17 können auf 2.17 aktualisiert werden, um diese Funktionalität zu nutzen, aber KNN-Indizes, die auf Versionen vor 2.x erstellt wurden, können nicht zu Cold migriert werden.
- Wenn die Domäne eine differenzierte Zugriffskontrolle verwendet, müssen Benutzer ohne Administratorrechte der `cold_manager` Rolle in OpenSearch Dashboards zugeordnet werden, um Cold-Indizes zu verwalten.

> **Note**
>
> Die `cold_manager` Rolle ist in einigen bereits vorhandenen OpenSearch Dienstdomänen möglicherweise nicht vorhanden. Wenn die Rolle in Dashboards nicht angezeigt wird, müssen Sie sie manuell erstellen.

So konfigurieren Sie Berechtigungen

Wenn Sie den Cold-Speicher in einer bereits vorhandenen OpenSearch Dienstdomäne aktivieren, ist die `cold_manager` Rolle möglicherweise nicht in der Domäne definiert. Wenn die Domäne eine differenzierte Zugriffskontrolle verwendet, müssen Benutzer ohne Administratorrechte der Rolle zugeordnet werden, um Cold-Indizes zu verwalten. Führen Sie die folgenden Schritte aus, um die `cold_manager`-Rolle manuell zu erstellen:

1. Gehen Sie in OpenSearch Dashboards zu Sicherheit und wählen Sie Berechtigungen aus.
2. Wählen Sie Aktionsgruppe erstellen und konfigurieren Sie die folgenden Gruppen:

Group name (Gruppenname)	Berechtigungen
`cold_cluster`	• `cluster:monitor/nodes/stats` • `cluster:admin/ultrawarm*` • `cluster:admin/cold/*`
`cold_index`	• `indices:monitor/stats` • `indices:data/read/minmax` • `indices:admin/ultrawarm/migration/get` • `indices:admin/ultrawarm/migration/cancel`

3. Wählen Sie Rollen und Rolle erstellen.
4. Benennen Sie die Rolle cold_manager.
5. Wählen Sie für Cluster-Berechtigungen die `cold_cluster`-Gruppe, die Sie erstellt haben.
6. Geben Sie für Index * ein.
7. Wählen Sie für Index-Berechtigungen die `cold_index`-Gruppe, die Sie erstellt haben.
8. Wählen Sie Erstellen aus.
9. Nachdem Sie die Rolle erstellt haben, ordnen Sie sie einer beliebigen Benutzer- oder Backend-Rolle zu, die Cold-Indizes verwaltet.

Cold-Speicheranforderungen und Leistungsüberlegungen

Da der Cold-Speicher Amazon S3 verwendet, entsteht kein Hot-Storage-Overhead, z. B. Replikate, reservierter Linux-Speicherplatz und reservierter Speicherplatz von OpenSearch Service. Cold-Speicher hat keine spezifischen Instance-Typen, da ihm keine Rechenkapazität zugeordnet ist. Sie können beliebig viele Daten im Cold-Speicher speichern. Überwachen Sie die `ColdStorageSpaceUtilization` Metrik in Amazon CloudWatch , um zu sehen, wie viel Speicherplatz Sie verwenden.

Preise für Cold-Speicherung

Ähnlich wie UltraWarm Speicher: mit Cold-Speicher zahlen Sie nur für die Datenspeicherung. Es fallen keine Rechenkosten für Cold-Daten an und Sie werden nicht in Rechnung gestellt, wenn keine Daten im Cold-Speicher vorhanden sind.

Beim Verschieben von Daten zwischen Cold- und Warm-Speicher fallen keine Transfergebühren an. Während Indizes zwischen Warm- und Cold-Speicher migriert werden, zahlen Sie weiterhin nur für eine Kopie des Indexes. Nach Abschluss der Migration wird der Index entsprechend der Speicherstufe in Rechnung gestellt, auf die er migriert wurde. Weitere Informationen zu den Preisen für Cold-Speicher finden Sie unter Preise OpenSearch für Amazon Service.

Aktivieren von Cold-Speicherung

Die Konsole ist die einfachste Möglichkeit, eine Domäne zu erstellen, die Cold-Speicher verwendet. Wählen Sie bei der Erstellung der Domain zunächst die Option Warm Data Nodes aktivieren, da Sie Warmspeicher auf derselben Domain aktivieren müssen. Wählen Sie dann Cold Storage aktivieren aus.

Derselbe Prozess funktioniert auf vorhandenen Domänen, sofern sie die Voraussetzungen erfüllen. Selbst nachdem der Domänenstatus von Processing (Verarbeitung) zu Active (Aktiv) geändert wurde, steht Cold-Speicher möglicherweise mehrere Stunden lang nicht zur Verfügung.

Sie können auch die AWS CLI oder Konfigurations-API verwenden, um die Cold-Speicherung zu aktivieren.

Beispiel für einen CLI-Befehl

Der folgende AWS CLI -Befehl erstellt eine Domäne mit drei Datenknoten, drei dedizierten Hauptknoten, aktiviertem Cold-Speicher und aktivierter feingranularer Zugriffskontrolle:

```
aws opensearch create-domain \
  --domain-name my-domain \
  --engine-version Opensearch_1.0 \
  --cluster-
config ColdStorageOptions={Enabled=true},WarmEnabled=true,WarmCount=4,WarmType=ultrawarm1.mediu
 \
  --ebs-options EBSEnabled=true,VolumeType=gp2,VolumeSize=11 \
  --node-to-node-encryption-options Enabled=true \
  --encryption-at-rest-options Enabled=true \
  --domain-endpoint-options EnforceHTTPS=true,TLSSecurityPolicy=Policy-Min-
TLS-1-2-2019-07 \
  --advanced-security-options
 Enabled=true,InternalUserDatabaseEnabled=true,MasterUserOptions='{MasterUserName=master-
user,MasterUserPassword=master-password}' \
  --region us-east-2
```

Weitere Informationen finden Sie in der AWS CLI -Befehlsreferenz.

Beispiel für eine Konfigurations-API-Anforderung

Die folgende Anfrage an die Konfigurations-API erstellt eine Domäne mit drei Datenknoten, drei dedizierten Hauptknoten, aktiviertem Cold-Speicher und aktivierter feingranularer Zugriffskontrolle:

```
POST https://es.us-east-2.amazonaws.com/2021-01-01/opensearch/domain
{
  "ClusterConfig": {
    "InstanceCount": 3,
    "InstanceType": "r6g.large.search",
    "DedicatedMasterEnabled": true,
    "DedicatedMasterType": "r6g.large.search",
    "DedicatedMasterCount": 3,
    "ZoneAwarenessEnabled": true,
    "ZoneAwarenessConfig": {
      "AvailabilityZoneCount": 3
     },
    "WarmEnabled": true,
    "WarmCount": 4,
    "WarmType": "ultrawarm1.medium.search",
    "ColdStorageOptions": {
       "Enabled": true
     }
  },
  "EBSOptions": {
```

```
    "EBSEnabled": true,
    "VolumeType": "gp2",
    "VolumeSize": 11
  },
  "EncryptionAtRestOptions": {
    "Enabled": true
  },
  "NodeToNodeEncryptionOptions": {
    "Enabled": true
  },
  "DomainEndpointOptions": {
    "EnforceHTTPS": true,
    "TLSSecurityPolicy": "Policy-Min-TLS-1-2-2019-07"
  },
   "AdvancedSecurityOptions": {
    "Enabled": true,
    "InternalUserDatabaseEnabled": true,
    "MasterUserOptions": {
      "MasterUserName": "master-user",
      "MasterUserPassword": "master-password"
    }
  },
  "EngineVersion": "Opensearch_1.0",
  "DomainName": "my-domain"
}
```

Weitere Informationen finden Sie in der OpenSearch Amazon-Service-API-Referenz.

Verwaltung von Cold-Indizes in Dashboards OpenSearch

Sie können Hot-, Warm- und Cold-Indizes mit der vorhandenen Dashboards-Oberfläche in Ihrer OpenSearch Service-Domäne verwalten. Mit Dashboards können Sie Indizes zwischen Warm- und Cold-Speicher migrieren und den Indexmigrationsstatus überwachen, ohne die CLI oder die Konfigurations-API zu verwenden. Weitere Informationen finden Sie unter Verwalten von Indizes in OpenSearch Dashboards.

Migration von Indizes auf Cold-Speicher

Wenn Sie Indizes in den Cold-Speicher migrieren, geben Sie einen Zeitbereich für die Daten an, um die Suche zu erleichtern. Sie können ein Zeitstempelfeld basierend auf den Daten in Ihrem Index auswählen, manuell einen Start- und Endzeitstempel angeben oder gar keinen angeben.

Parameter	Unterstützter Wert	Beschreibung
`timestamp_field`	Das Datum/Uhrzeitfeld aus dem Index-Mapping.	Die Minimal- und Maximalwerte des bereitgestellten Feldes werden berechnet und als `start_time` - und `end_time`-Metadaten für den Cold-Index gespeichert.
`start_time` und `end_time`	Eines der folgenden Formate: • strict_date_optional_time. Zum Beispiel `yyyy-MM-dd'T'HH:mm:ss.SSSZ` oder `yyyy-MM-dd` • Epochenzeit in Millisekunden	Die angegebenen Werte werden berechnet und als `start_time` - und `end_time`-Metadaten für den Cold-Index gespeichert.

Wenn Sie keinen Zeitstempel angeben möchten, fügen Sie stattdessen `?ignore=timestamp` zur Anfrage hinzu.

Die folgende Anforderung migriert einen Warm-Index in den Cold-Speicher und stellt Start- und Endzeiten für die Daten in diesem Index bereit:

```
POST _ultrawarm/migration/my-index/_cold
  {
    "start_time": "2020-03-09",
    "end_time": "2020-03-09T23:00:00Z"
  }
```

Überprüfen Sie dann den Status der Migration:

```
GET _ultrawarm/migration/my-index/_status

{
  "migration_status": {
    "index": "my-index",
    "state": "RUNNING_METADATA_RELOCATION",
```

```
    "migration_type": "WARM_TO_COLD"
  }
}
```

OpenSearch Der Service migriert jeweils einen Index in einen kühlen Speicher. Sie können bis zu 100 Migrationen in der Warteschlange haben. Jede Anfrage, die das Limit überschreitet, wird abgelehnt. Um die aktuelle Anzahl von Migrationen in der Warteschlange zu überprüfen, überwachen Sie die `WarmToColdMigrationQueueSize`-Metrik. Der Migrationsprozess weist die folgenden Zustände auf:

```
ACCEPTED_COLD_MIGRATION - Migration request is accepted and queued.
RUNNING_METADATA_MIGRATION - The migration request was selected for execution and
 metadata is migrating to cold storage.
FAILED_METADATA_MIGRATION - The attempt to add index metadata has failed and all
 retries are exhausted.
PENDING_INDEX_DETACH - Index metadata migration to cold storage is completed. Preparing
 to detach the warm index state from the local cluster.
RUNNING_INDEX_DETACH - Local warm index state from the cluster is being removed. Upon
 success, the migration request will be completed.
FAILED_INDEX_DETACH - The index detach process failed and all retries are exhausted.
```

Automatisierung von Migrationen zum Cold-Speicher

Sie können Index-Stausmanagement verwenden, um den Migrationsprozess zu automatisieren, nachdem ein Index ein bestimmtes Alter erreicht hat oder andere Bedingungen erfüllt. Sehen Sie sich die Beispielrichtlinie an, die zeigt, wie Indizes automatisch von Hot- UltraWarm zu Cold-Speicher migriert werden.

> **Note**
>
> Ein explizites `timestamp_field` ist erforderlich, um Indizes mithilfe einer Index-Statusmanagement-Richtlinie in den Cold-Speicher zu verlagern.

Abbruch von Migrationen zum Cold-Speicher

Wenn eine Migration zum Cold-Speicher in der Warteschlange oder in einem fehlgeschlagenen Zustand ist, können Sie die Migration mit der folgenden Anforderung abbrechen:

```
POST _ultrawarm/migration/_cancel/my-index
```

```
{
  "acknowledged" : true
}
```

Wenn Ihre Domäne differenzierte Zugriffskontrolle verwendet, benötigen Sie die `indices:admin/ultrawarm/migration/cancel`-Berechtigung, um diese Anfrage zu stellen.

Auflisten der Cold-Indizes

Vor dem Abfragen können Sie die Indizes im kühlen Speicher auflisten, um zu entscheiden, zu entscheiden, zu entscheiden, zu welchen UltraWarm für die weitere Analyse migriert werden soll. Die folgende Anforderung listet alle Cold-Indizes auf, sortiert nach Indexnamen:

```
GET _cold/indices/_search
```

Beispielantwort

```
{
  "pagination_id" : "je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY",
  "total_results" : 3,
  "indices" : [
    {
      "index" : "my-index-1",
      "index_cold_uuid" : "hjEoh26mRRCFxRIMdgvLmg",
      "size" : 10339,
      "creation_date" : "2021-06-28T20:23:31.206Z",
      "start_time" : "2020-03-09T00:00Z",
      "end_time" : "2020-03-09T23:00Z"
    },
    {
      "index" : "my-index-2",
      "index_cold_uuid" : "0vIS2n-oROmOWDFmwFIgdw",
      "size" : 6068,
      "creation_date" : "2021-07-15T19:41:18.046Z",
      "start_time" : "2020-03-09T00:00Z",
      "end_time" : "2020-03-09T23:00Z"
    },
    {
      "index" : "my-index-3",
      "index_cold_uuid" : "EaeXOBodTLiDYcivKsXVLQ",
      "size" : 32403,
```

```
      "creation_date" : "2021-07-08T00:12:01.523Z",
      "start_time" : "2020-03-09T00:00Z",
      "end_time" : "2020-03-09T23:00Z"
    }
  ]
}
```

Filtern

Sie können Cold-Indizes basierend auf einem Präfix-basierten Indexmuster und Zeitbereich-Offsets filtern.

Die folgende Anforderung listet Indizes auf, die mit dem Präfixmuster von `event-*` übereinstimmen:

```
GET _cold/indices/_search
 {
   "filters":{
      "index_pattern": "event-*"
   }
 }
```

Beispielantwort

```
{
  "pagination_id" : "je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY",
  "total_results" : 1,
  "indices" : [
    {
      "index" : "events-index",
      "index_cold_uuid" : "4eFiab7rRfSvp3slrIsIKA",
      "size" : 32263273,
      "creation_date" : "2021-08-18T18:25:31.845Z",
      "start_time" : "2020-03-09T00:00Z",
      "end_time" : "2020-03-09T23:00Z"
    }
  ]
}
```

Die folgende Anforderung gibt Indizes mit `start_time`- und `end_time`-Metadaten-Feldern zwischen `2019-03-01` und `2020-03-01` zurück:

```
GET _cold/indices/_search
```

```
{
  "filters": {
    "time_range": {
      "start_time": "2019-03-01",
      "end_time": "2020-03-01"
    }
  }
}
```

Beispielantwort

```
{
  "pagination_id" : "je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY",
  "total_results" : 1,
  "indices" : [
    {
      "index" : "my-index",
      "index_cold_uuid" : "4eFiab7rRfSvp3slrIsIKA",
      "size" : 32263273,
      "creation_date" : "2021-08-18T18:25:31.845Z",
      "start_time" : "2019-05-09T00:00Z",
      "end_time" : "2019-09-09T23:00Z"
    }
  ]
}
```

Sortieren

Sie können Cold-Indizes nach Metadatenfeldern wie Indexname oder Größe sortieren. Die folgende Abfrage listet alle Indizes nach Größe sortiert in absteigender Reihenfolge auf:

```
GET _cold/indices/_search
 {
 "sort_key": "size:desc"
 }
```

Beispielantwort

```
{
  "pagination_id" : "je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY",
  "total_results" : 5,
```

```
  "indices" : [
    {
      "index" : "my-index-6",
      "index_cold_uuid" : "4eFiab7rRfSvp3slrIsIKA",
      "size" : 32263273,
      "creation_date" : "2021-08-18T18:25:31.845Z",
      "start_time" : "2020-03-09T00:00Z",
      "end_time" : "2020-03-09T23:00Z"
    },
    {
      "index" : "my-index-9",
      "index_cold_uuid" : "mbD3ZRVDRI6ONqgEOsJyUA",
      "size" : 57922,
      "creation_date" : "2021-07-07T23:41:35.640Z",
      "start_time" : "2020-03-09T00:00Z",
      "end_time" : "2020-03-09T23:00Z"
    },
    {
      "index" : "my-index-5",
      "index_cold_uuid" : "EaeXOBodTLiDYcivKsXVLQ",
      "size" : 32403,
      "creation_date" : "2021-07-08T00:12:01.523Z",
      "start_time" : "2020-03-09T00:00Z",
      "end_time" : "2020-03-09T23:00Z"
    }
  ]
}
```

Andere gültige Sortierschlüssel sind `start_time:asc/desc`, `end_time:asc/desc` und `index_name:asc/desc`.

Paginierung

Sie können eine Liste von Cold-Indizes paginieren. Konfigurieren Sie die Anzahl der Indizes, die pro Seite zurückgegeben werden sollen, mit dem `page_size`-Parameter (der Standardwert ist 10). Jede `_search`-Anfrage auf Ihre Cold-Indizes gibt eine `pagination_id` zurück, die Sie für nachfolgende Aufrufe verwenden können.

Die folgende Anforderung paginiert die Ergebnisse einer `_search`-Anfrage Ihrer Cold-Indizes und zeigt die nächsten 100 Ergebnisse an:

```
GET _cold/indices/_search?page_size=100
```

```
{
"pagination_id": "je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY"
}
```

Migrieren von Cold-Indizes zum Warm-Speicher

Nachdem Sie die Liste der Cold-Indizes mit den Filterkriterien im vorherigen Abschnitt eingegrenzt haben, migrieren Sie sie zurück zu UltraWarm dem Ort, an dem Sie die Daten abfragen und sie zum Erstellen von Visualisierungen verwenden können.

Die folgende Anfrage migriert zwei Cold-Indizes zurück in den Warm-Speicher:

```
POST _cold/migration/_warm
 {
 "indices": "my-index1,my-index2"
 }


{
  "acknowledged" : true
}
```

Um den Status der Migration zu überprüfen und die Migrations-ID abzurufen, senden Sie die folgende Anforderung:

```
GET _cold/migration/_status
```

Beispielantwort

```
{
  "cold_to_warm_migration_status" : [
    {
      "migration_id" : "tyLjXCA-S76zPQbPVHkOKA",
      "indices" : [
        "my-index1,my-index2"
      ],
      "state" : "RUNNING_INDEX_CREATION"
    }
  ]
}
```

Um indexspezifische Migrationsinformationen abzurufen, geben Sie den Indexnamen ein:

```
GET _cold/migration/my-index/_status
```

Anstatt einen Index anzugeben, können Sie die Indizes nach ihrem aktuellen Migrationsstatus auflisten. Gültige Werte sind `_failed`, `_accepted` und `_all`.

Der folgende Befehl ruft den Status aller Indizes in einer einzelnen Migrationsanforderung ab:

```
GET _cold/migration/_status?migration_id=my-migration-id
```

Rufen Sie die Migrations-ID mit der Statusanforderung ab. Für detaillierte Migrationsinformationen fügen Sie `&verbose=true` hinzu.

Sie können Indizes aus dem kalten in den warmen Speicher in Batches von 10 oder weniger migrieren, wobei maximal 100 Indizes gleichzeitig migriert werden können. Jede Anfrage, die das Limit überschreitet, wird abgelehnt. Um die aktuelle Anzahl von Migrationen zu überprüfen, überwachen Sie die `ColdToWarmMigrationQueueSize`-Metrik. Der Migrationsprozess weist die folgenden Zustände auf:

```
ACCEPTED_MIGRATION_REQUEST - Migration request is accepted and queued.
RUNNING_INDEX_CREATION - Migration request is picked up for processing and will create
 warm indexes in the cluster.
PENDING_COLD_METADATA_CLEANUP - Warm index is created and the migration service will
 attempt to clean up cold metadata.
RUNNING_COLD_METADATA_CLEANUP - Cleaning up cold metadata from the indexes migrated to
 warm storage.
FAILED_COLD_METADATA_CLEANUP - Failed to clean up metadata in the cold tier.
FAILED_INDEX_CREATION - Failed to create an index in the warm tier.
```

Wiederherstellen von Cold-Indizes aus Snapshots

Wenn Sie einen gelöschten kalten Index wiederherstellen müssen, können Sie ihn wieder auf die warme Ebene zurücksetzen, indem Sie den Anweisungen unter folgen the section called “Wiederherstellen von Warm-Indizes aus Snapshots” und den Index dann wieder auf die kalte Ebene migrieren. Sie können einen gelöschten Cold-Index nicht direkt wieder auf die Cold-Ebene zurücksetzen. OpenSearch Der Service bewahrt Cold-Indizes 14 Tage lang nach dem Löschen auf.

Abbruch von Migrationen von Cold- zu Warm-Speicher

Wenn eine Indexmigration von Cold- zu Warm-Speicher in die Warteschlange gestellt wird oder sich in einem fehlgeschlagenen Zustand befindet, können Sie sie mit der folgenden Anforderung abbrechen:

```
POST _cold/migration/my-index/_cancel

{
  "acknowledged" : true
}
```

Um die Migration für einen Batch von Indizes abzubrechen (maximal 10 gleichzeitig), geben Sie die Migrations-ID an:

```
POST _cold/migration/_cancel?migration_id=my-migration-id

{
  "acknowledged" : true
}
```

Rufen Sie die Migrations-ID mit der Statusanforderung ab.

Cold-Index-Metadaten aktualisieren

Sie können die `start_time`- und `end_time`-Felder für einen Cold-Index aktualisieren:

```
PATCH _cold/my-index
 {
 "start_time": "2020-01-01",
 "end_time": "2020-02-01"
 }
```

Sie können nicht die `timestamp_field` eines Indexes im Cold-Speicher aktualiseiren.

> **Note**
>
> OpenSearch Dashboards unterstützen die PATCH-Methode nicht. Verwenden Sie curl, Postman oder eine andere Methode, um Cold-Metadaten zu aktualisieren.

Cold-Indizes löschen

Wenn Sie keine ISM-Richtlinie verwenden, können Sie Cold-Indizes manuell löschen. Die folgende Anforderung löscht einen Cold-Index:

```
DELETE _cold/my-index

{
  "acknowledged" : true
}
```

Deaktivieren von Cold-Speicherung

Die OpenSearch Service-Konsole ist die einfachste Möglichkeit, Cold-Speicherung zu deaktivieren. Wählen Sie die Domäne aus und wählen Sie Aktionen, Clusterkonfiguration bearbeiten und deaktivieren Sie dann Cold-Speicher aktivieren.

Um die AWS CLI oder die Konfigurations-API zu verwenden`ColdStorageOptions`, setzen Sie unter`"Enabled"="false"`.

Bevor Sie den Cold-Speicher deaktivieren, müssen Sie entweder alle Cold-Indizes löschen oder sie wieder in den Warm-Speicher migrieren. Andernfalls schlägt die Deaktivierungsaktion fehl.

OpenSearch optimierter Speicher für Amazon OpenSearch Service

Die OpenSearch optimierte Instance-Familie für Amazon OpenSearch Service ist eine kostengünstige Lösung für die Speicherung großer Datenmengen. Eine Domain mit OR1 Instances verwendet Amazon Elastic Block Store (Amazon EBS) `gp3` oder `io1` Volumes als Primärspeicher, wobei die Daten synchron nach Amazon S3 kopiert werden, sobald sie ankommen. Diese Speicherstruktur bietet einen erhöhten Indexierungsdurchsatz bei hoher Haltbarkeit. Die OpenSearch optimierte Instance-Familie unterstützt auch die automatische Datenwiederherstellung im Falle eines Fehlers. Informationen zu den Optionen für den OR1 Instanztyp finden Sie unterthe section called “Instance-Typen der aktuellen Generation”.

Wenn Sie umfangreiche Workloads für Betriebsanalysen wie Protokollanalysen, Observability oder Sicherheitsanalysen indizieren, können Sie von der verbesserten Leistung und Recheneffizienz der Instances profitieren. OR1 Darüber hinaus verbessert die automatische Datenwiederherstellung, die von OR1 Instances angeboten wird, die allgemeine Zuverlässigkeit Ihrer Domain.

OpenSearch Der Service sendet speicherbezogene OR1 Metriken an Amazon. CloudWatch Eine Liste der verfügbaren Metriken finden Sie unter ???.

OR1 Instances sind auf Abruf oder mit Reserved Instance-Preisen erhältlich, wobei ein Stundensatz für die in Amazon EBS und Amazon S3 bereitgestellten Instances und Speicher gilt.

Themen

- Einschränkungen
- Optimierung für einen besseren Aufnahmedurchsatz
- Wie sich OpenSearch optimierte Instances von anderen Instances unterscheiden
- Wie OR1 unterscheidet es sich vom UltraWarm Speicher
- Provisioning einer Domain mit Instanzen OR1

Einschränkungen

Beachten Sie die folgenden Einschränkungen, wenn Sie OR1 Instances für Ihre Domain verwenden.

- Neu erstellte Domains müssen OpenSearch Version 2.11 und höhere Versionen haben.
- Auf bestehenden Domains muss OpenSearch Version 2.15 oder höher ausgeführt werden.
- Für Ihre Domain muss die Verschlüsselung im Ruhezustand aktiviert sein. Weitere Informationen finden Sie unter ???.
- Wenn Ihre Domain dedizierte Master-Knoten verwendet, müssen diese Graviton-Instances verwenden. Weitere Informationen über dedizierte Master-Knoten finden Sie unter???.
- Das Aktualisierungsintervall für Indizes auf OR1 Instances muss mindestens 10 Sekunden betragen. Das standardmäßige Aktualisierungsintervall für OR1 Instances beträgt 10 Sekunden.

Optimierung für einen besseren Aufnahmedurchsatz

Um den besten Indexdurchsatz aus Ihren OR1 Instances zu erzielen, empfehlen wir außerdem Folgendes:

- Verwenden Sie große Mengen, um die Puffernutzung zu verbessern. Die empfohlene Größe ist 10 MB.
- Verwenden Sie mehrere Clients, um die Leistung der Parallelverarbeitung zu verbessern.

- Stellen Sie die Anzahl der aktiven primären Shards so ein, dass sie der Anzahl der Datenknoten entspricht, um die Ressourcennutzung zu maximieren.

Wie sich OpenSearch optimierte Instances von anderen Instances unterscheiden

OpenSearch optimierte Instanzen unterscheiden sich in folgenden Punkten von nicht optimierten Instanzen:

- Bei OpenSearch optimierten Instances wird die Indizierung nur für primäre Shards durchgeführt.
- Wenn OpenSearch optimierte Instances mit Replikaten konfiguriert sind, kann die Indexierungsrate niedriger erscheinen, als sie tatsächlich ist. Wenn es beispielsweise einen primären Shard und einen Replikat-Shard gibt, kann die Indexierungsrate eine Rate von 1000 anzeigen, obwohl die tatsächliche Indizierungsrate 2000 beträgt.
- OpenSearch optimierte Instances führen vor dem Senden an eine Remote-Quelle Pufferoperationen durch. Dies führt zu höheren Aufnahmelatenzen.

> **Note**
>
> Die `IndexingLatency` Metrik ist nicht betroffen, da sie keine Zeit für die Translog-Synchronisierung beinhaltet.

- Replikat-Shards können einige Sekunden hinter primären Shards zurückliegen. Sie können die Verzögerung mithilfe der `ReplicationLagMaxTime` CloudWatch Amazon-Metrik überwachen

Wie OR1 unterscheidet es sich vom UltraWarm Speicher

OpenSearch Service bietet UltraWarm Instanzen, die eine kostengünstige Möglichkeit bieten, große Mengen schreibgeschützter Daten zu speichern. OR1 Sowohl UltraWarm Instances als auch speichern Daten lokal in Amazon EBS und remote in Amazon S3. UltraWarm Instances unterscheiden sich jedoch in mehreren wichtigen Punkten: OR1

- OR1 Instanzen speichern eine Kopie der Daten sowohl in Ihrem lokalen als auch in Ihrem Remote-Speicher. In UltraWarm Instanzen werden Daten hauptsächlich im Remote-Speicher aufbewahrt, um die Speicherkosten zu senken. Abhängig von Ihren Nutzungsmustern können Daten in den lokalen Speicher verschoben werden.

- OR1 Instanzen sind aktiv und können Lese- und Schreibvorgänge akzeptieren, wohingegen die Daten auf UltraWarm Instanzen nur lesbar sind, bis Sie sie manuell zurück in den Hot-Storage verschieben.
- UltraWarm stützt sich aus Gründen der Datenbeständigkeit auf Index-Snapshots. OR1 Im Vergleich dazu führen Instanzen die Replikation und Wiederherstellung im Hintergrund durch. Im Falle eines roten Index stellen OR1 Instances fehlende Shards automatisch aus Ihrem Remotespeicher in Amazon S3 wieder her. Die Wiederherstellungsdauer variiert je nach zu wiederherstellender Datenmenge.

Weitere Hinweise zur UltraWarm Speicherung finden Sie unter???.

Provisioning einer Domain mit Instanzen OR1

Sie können OR1 Instanzen für Ihre Datenknoten auswählen, wenn Sie eine neue Domain mit dem AWS Management Console oder dem AWS Command Line Interface (AWS CLI) erstellen. Anschließend können Sie die Daten mit Ihren vorhandenen Tools indizieren und abfragen.

Konsole

1. Navigieren Sie zur Amazon OpenSearch Service-Konsole unterhttps://console.aws.amazon.com/aos/.
2. Wählen Sie im linken Navigationsbereich die Option Domains aus.
3. Wählen Sie Domain erstellen aus.
4. Erweitern Sie im Abschnitt Anzahl der Datenknoten das Menü Instance-Familie und wählen Sie OpenSearch optimiert aus.
5. Wählen Sie den Instanztyp und andere Speichereinstellungen aus.
6. Vergewissern Sie sich, dass im Abschnitt Verschlüsselung die Option Verschlüsselung ruhender Daten aktivieren ausgewählt ist.
7. Konfigurieren Sie den Rest Ihrer Domain und wählen Sie Erstellen.

AWS CLI

Um eine Domain bereitzustellen, die OR1 Speicher mithilfe von verwendet AWS CLI, müssen Sie den Wert der spezifischen OR1 Instanztypgröße in der angeben`InstanceType`.

Im folgenden Beispiel wird eine Domäne mit OR1 Instanzen der Größe A erstellt `2xlarge` und die Verschlüsselung im Ruhezustand aktiviert.

```
aws opensearch create-domain \
  --domain-name test-domain \
  --engine-version OpenSearch_2.11 \
  --cluster-config
 "InstanceType=or1.2xlarge.search,InstanceCount=3,DedicatedMasterEnabled=true,DedicatedMasterTy
 \
  --ebs-options "EBSEnabled=true,VolumeType=gp3,VolumeSize=200" \
  --encryption-at-rest-options Enabled=true \
  --advanced-security-options
 "Enabled=true,InternalUserDatabaseEnabled=true,MasterUserOptions={MasterUserName=test-
user,MasterUserPassword=test-password}" \
  --node-to-node-encryption-options Enabled=true \
  --domain-endpoint-options EnforceHTTPS=true \
  --access-policies '{"Version":"2012-10-17","Statement":
[{"Effect":"Allow","Principal":{"AWS":"*"},"Action":"es:*","Resource":"arn:aws:es:us-
east-1:account-id:domain/test-domain/*"}]}'
```

Verwaltung des Indexstatusmanagement in Amazon OpenSearch Service

Mit Indexstatusmanagement (ISM) in Amazon OpenSearch Service können Sie benutzerdefinierte Verwaltungsrichtlinien definieren, die Routineaufgaben automatisieren und sie auf Indizes und Indexmuster anwenden. Sie müssen keine externen Prozesse mehr einrichten und verwalten, um Ihre Indexvorgänge auszuführen.

Eine Richtlinie umfasst einen Standardzustand und eine Liste der Zustände, die der Index annehmen kann. Für jeden Zustand können Sie eine Liste der Aktionen definieren, die durchgeführt werden sollen, und welche Bedingungen den Zustandswechsel auslösen. Ein typischer Anwendungsfall besteht darin, alte Indizes regelmäßig nach Ablauf eines bestimmten Zeitraums zu löschen. Beispielsweise können Sie eine Richtlinie definieren, die den Index nach 30 Tagen in einen `read_only`-Status verschiebt und ihn dann nach 90 Tagen endgültig löscht.

NNachdem Sie eine Richtlinie an einen Index angefügt haben, erstellt ISM einen Auftrag, der alle 5 bis 8 Minuten (bzw. 30 bis 48 Minuten bei Clustern vor Version 1.3) ausgeführt wird, um Richtlinienaktionen durchzuführen, Bedingungen zu prüfen und den Index in verschiedene Zustände zu überführen. Die Basiszeit für die Ausführung dieses Auftrags beträgt alle 5 Minuten, außerdem wird ein zufälliger 0–60 %-Jitter hinzugefügt, um sicherzustellen, dass Ihnen nicht ein gleichzeitiger Anstieg der Aktivität von allen Ihren Indizes angezeigt wird. ISM führt keine Aufträge aus, wenn der Clusterstatus rot ist.

Für ISM ist eine Elasticsearch 6.8 oder höher erforderlich OpenSearch .

> **Note**
>
> Diese Dokumentation bietet einen kurzen Überblick über ISM und mehrere Beispielrichtlinien. Außerdem wird erklärt, wie sich ISM für Amazon OpenSearch Service-Domains von ISM auf selbstverwalteten OpenSearch Clustern unterscheidet. Eine vollständige Dokumentation von ISM, einschließlich einer umfassenden Parameterreferenz, Beschreibungen der einzelnen Einstellungen und einer API-Referenz, finden Sie in der OpenSearch Dokumentation unter Index State Management.

> **Important**
>
> Sie können keine Indexvorlagen mehr verwenden, um ISM-Richtlinien auf neu erstellte Indizes anzuwenden. Sie können neu erstellte Indizes weiterhin automatisch mit dem ISM-Vorlagenfeld verwalten. Dieses Update führt eine grundlegende Änderung ein, die sich auf vorhandene CloudFormation Vorlagen auswirkt, die diese Einstellung verwenden.

Erstellen einer ISM-Richtlinie

So beginnen Sie mit Indexstatusmanagement

1. Öffnen Sie die Amazon OpenSearch Service-Konsole zu https://console.aws.amazon.com/aos/Hause.
2. Wählen Sie die Domain aus, für die Sie eine ISM-Richtlinie erstellen möchten.
3. Navigieren Sie im Dashboard der Domain zur OpenSearch Dashboard-URL und melden Sie sich mit Ihrem Master-Benutzernamen und Passwort an. Die URL weist das folgende Format auf:

   ```
   domain-endpoint/_dashboards/
   ```

4. Öffnen Sie das linke Navigationsfenster in OpenSearch Dashboards und wählen Sie Index Management und dann Richtlinie erstellen.
5. Sie können den visuellen Editor oder JSON-Editor verwenden, um Richtlinien zu erstellen. Wir empfehlen die Verwendung des visuellen Editors, da er eine strukturiertere Methode zur

Definition von Richtlinien bietet. Hilfe beim Erstellen von Richtlinien finden Sie unten in den Beispielrichtlinien.

6. Nachdem Sie eine Richtlinie erstellt haben, fügen Sie sie einer oder mehreren Indizes an:

```
POST _plugins/_ism/add/my-index
{
  "policy_id": "my-policy-id"
}
```

> **Note**
>
> Wenn auf Ihrer Domain eine Legacy-Version von Elasticsearch ausgeführt wird, verwenden Sie `_opendistro`anstelle von `_plugins`.

Alternativ können Sie den Index in OpenSearch Dashboards auswählen und Richtlinie anwenden auswählen.

Beispielrichtlinien

Die folgenden Beispielrichtlinien veranschaulichen, wie allgemeine ISM-Anwendungsfälle automatisiert werden.

Hot- zu Warm- zu Cold Storage

Diese Beispielrichtlinie verschiebt einen Index vom Hot-Storage in und UltraWarmschließlich in kalter Speicher. Dann löscht es den Index.

Der Index befindet sich zunächst im `hot`-Zustand. Nach zehn Tagen versetzt ISM es in den `warm`-Zustand. 80 Tage später, nachdem der Index 90 Tage alt ist, versetzt ISM den Index in den `cold`-Zustand. Nach einem Jahr sendet der Service eine Benachrichtigung an einen Amazon-Chime-Raum, dass der Index gelöscht wird und löscht ihn dann endgültig.

Beachten Sie, dass Cold-Indizes die `cold_delete`-Operation erfordern, nicht die normale `delete`-Operation. Beachten Sie auch, dass in Ihren Daten ein explizites `timestamp_field` erforderlich ist, um Cold-Indizes mit ISM zu verwalten.

```
{
```

```
  "policy": {
    "description": "Demonstrate a hot-warm-cold-delete workflow.",
    "default_state": "hot",
    "schema_version": 1,
    "states": [{
        "name": "hot",
        "actions": [],
        "transitions": [{
          "state_name": "warm",
          "conditions": {
            "min_index_age": "10d"
          }
        }]
      },
      {
        "name": "warm",
        "actions": [{
          "warm_migration": {},
          "retry": {
            "count": 5,
            "delay": "1h"
          }
        }],
        "transitions": [{
          "state_name": "cold",
          "conditions": {
            "min_index_age": "90d"
          }
        }]
      },
      {
        "name": "cold",
        "actions": [{
            "cold_migration": {
              "timestamp_field": "<your timestamp field>"
            }
          }
        ],
        "transitions": [{
          "state_name": "delete",
          "conditions": {
             "min_index_age": "365d"
          }
        }]
```

```
      },
      {
        "name": "delete",
        "actions": [{
          "notification": {
            "destination": {
              "chime": {
                "url": "<URL>"
              }
            },
            "message_template": {
              "source": "The index {{ctx.index}} is being deleted."
            }
          }
        },
        {
          "cold_delete": {}
        }]
      }
    ]
  }
}
```

Reduzieren der Replikatanzahl

Diese Beispielrichtlinie reduziert die Replikatanzahl nach 7 Tagen auf 0, um Speicherplatz zu sparen, und löscht den Index nach 21 Tagen. Bei dieser Richtlinie wird davon ausgegangen, dass Ihr Index nicht kritisch ist und keine Schreibanforderungen mehr empfängt. Wenn keine Replikate vorhanden sind, birgt dies ein gewisses Risiko für Datenverluste.

```
{
  "policy": {
    "description": "Changes replica count and deletes.",
    "schema_version": 1,
    "default_state": "current",
    "states": [{
        "name": "current",
        "actions": [],
        "transitions": [{
          "state_name": "old",
          "conditions": {
            "min_index_age": "7d"
          }
```

```
        }]
      },
      {
        "name": "old",
        "actions": [{
          "replica_count": {
            "number_of_replicas": 0
          }
        }],
        "transitions": [{
          "state_name": "delete",
          "conditions": {
            "min_index_age": "21d"
          }
        }]
      },
      {
        "name": "delete",
        "actions": [{
          "delete": {}
        }],
        "transitions": []
      }
    ]
  }
}
```

Erstellen eines Index-Snapshots

Diese Beispielrichtlinie verwendet die `snapshot`-Operation, um eine Momentaufnahme eines Indexes zu erstellen, sobald er mindestens ein Dokument enthält. `repository` ist der Name des manuellen Snapshot-Repositorys, das Sie in Amazon S3 registriert haben. `snapshot` ist der Name des Snapshots. Informationen zu Snapshot-Voraussetzungen und Schritten zum Registrieren eines Repositorys finden Sie unter the section called “Erstellen von Index-Snapshots”.

```
{
  "policy": {
    "description": "Takes an index snapshot.",
    "schema_version": 1,
    "default_state": "empty",
    "states": [{
        "name": "empty",
        "actions": [],
```

```
        "transitions": [{
          "state_name": "occupied",
          "conditions": {
            "min_doc_count": 1
          }
        }]
      },
      {
        "name": "occupied",
        "actions": [{
          "snapshot": {
            "repository": "<my-repository>",
            "snapshot": "<my-snapshot>"
            }
          }],
          "transitions": []
      }
    ]
  }
}
```

ISM-Vorlagen

Sie können ein `ism_template`-Feld in einer Richtlinie einrichten, sodass beim Erstellen eines Index, der dem Vorlagenmuster entspricht, die Richtlinie automatisch an diesen Index angehängt wird. In diesem Beispiel wird jeder von Ihnen erstellte Index mit einem Namen, der mit „log“ beginnt, automatisch mit der ISM-Richtlinie `my-policy-id` abgeglichen:

```
PUT _plugins/_ism/policies/my-policy-id
{
  "policy": {
    "description": "Example policy.",
    "default_state": "...",
    "states": [...],
    "ism_template": {
      "index_patterns": ["log*"],
      "priority": 100
    }
  }
}
```

Ein ausführlicheres Beispiel finden Sie unter Beispielrichtlinie mit ISM-Vorlage für automatisches Rollover.

Unterschiede

Im Vergleich OpenSearch zu Elasticsearch weist ISM für Amazon OpenSearch Service mehrere Unterschiede auf.

ISM-Operationen

- OpenSearch Service unterstützt drei einzigartige ISM-Operationen: `warm_migration`cold_migration, und`cold_delete`:
  - Wenn Ihre Domain UltraWarmaktiviert ist, wird der Index durch diese `warm_migration` Aktion in den Warm-Storage übertragen.
  - Wenn in Ihrer Domain Cold Storage aktiviert ist, überträgt die `cold_migration`Aktion den Index in den Cold Storage und die `cold_delete`-Aktion löscht den Index aus dem Cold Storage.

  Auch wenn die -Aktion nicht innerhalb des festgelegten Timeout-Zeitraums abgeschlossen wird, wird die Migration zu Warm-Indizes dennoch fortgesetzt. Wenn Sie eine error_notification für eine der oben genannten Aktionen festlegen, werden Sie benachrichtigt, dass die Aktion fehlgeschlagen ist, wenn sie nicht innerhalb des Timeout-Zeitraums abgeschlossen wurde, aber die Benachrichtigung dient nur zu Ihrer eigenen Information. Der eigentliche Vorgang hat kein inhärentes Timeout und wird so lange ausgeführt, bis er schließlich erfolgreich ist oder fehlschlägt.
- Wenn Ihre Domain OpenSearch oder Elasticsearch 7.4 oder höher ausgeführt wird, unterstützt OpenSearch Service ISM `open` und ISM und ISM`close`.

- Wenn Ihre Domain OpenSearch oder Elasticsearch 7.7 oder höher ausgeführt wird, unterstützt OpenSearch Service die `snapshot` ISM-Operationen.

ISM-Vorgänge für Cold Storage

Für Cold-Indizes müssen Sie einen `?type=_cold` Parameter angeben, wenn Sie das folgende ISM APIs verwenden:

- Richtlinie hinzufügen
- Richtlinie entfernen

- Richtlinie aktualisieren
- Wiederholen fehlgeschlagener Index
- Index erklären

Diese APIs für Cold-Indizes weisen die folgenden zusätzlichen Unterschiede auf:

- Platzhalteroperatoren werden nur dann unterstützt, wenn Sie sie am Ende verwenden. Beispiel: `_plugins/_ism/<add, remove, change_policy, retry, explain>/logstash-*` wird unterstützt, `_plugins/_ism/<add, remove, change_policy, retry, explain>/iad-*-prod` jedoch nicht.
- Mehrzeilige Indexnamen und -muster werden nicht unterstützt. Beispiel: `_plugins/_ism/<add, remove, change_policy, retry, explain>/app-logs` wird unterstützt, `_plugins/_ism/<add, remove, change_policy, retry, explain>/app-logs,sample-data` jedoch nicht.

ISM-Einstellungen

OpenSearch und mit Elasticsearch können Sie alle verfügbaren ISM-Einstellungen über die `_cluster/settings` API ändern. Auf Amazon OpenSearch Service können Sie nur die folgenden ISM-Einstellungen ändern:

- Einstellungen auf Clusterebene:
  - `plugins.index_state_management.enabled`
  - `plugins.index_state_management.history.enabled`
- Einstellungen auf Index-Ebene:
  - `plugins.index_state_management.rollover_alias`

Tutorial: Automatisieren von Indexstatusmanagement-Prozessen

In diesem Tutorial wird erläutert, wie Sie eine ISM-Richtlinie implementieren, die routinemäßige Indexverwaltungsaufgaben automatisiert und sie auf Indizes und Indexmuster anwendet.

Mit Indexstatusmanagement (ISM) in Amazon OpenSearch Service können Sie wiederkehrende Indexverwaltungsaktivitäten automatisieren, sodass Sie keine zusätzlichen Tools zur Verwaltung von Indexlebenszyklen benötigen. Sie können eine Richtlinie erstellen, die diese Vorgänge basierend

auf Alter, Größe und anderen Bedingungen des Indexes automatisiert, und das alles innerhalb Ihrer OpenSearch Amazon-Service-Domain.

OpenSearch Der Service unterstützt drei Speicherebenen: den Standardstatus „Hot“ für aktives Schreiben und Analysen mit niedriger Latenz, UltraWarm für schreibgeschützte Daten bis zu drei Petabyte und Cold-Storage für unbegrenzte Langzeitarchivierung.

Dieses Tutorial stellt einen beispielhaften Anwendungsfall für den Umgang mit Zeitreihendaten in Tagesindizes vor. In diesem Tutorial richten Sie eine Richtlinie ein, die nach 24 Stunden einen automatischen Snapshot jedes angehängten Indexes erstellt. Anschließend wird der Index nach 60 Tagen vom standardmäßigen UltraWarm Hot-Storage in den Cold Storage migriert und nach 60 Tagen in den Cold Storage.

Voraussetzungen

- In Ihrer OpenSearch Service-Domain muss eine Elasticsearch-Version ab Version 6.8 laufen.
- Für Ihre Domain muss UltraWarmCold Storage aktiviert sein.
- Sie müssen ein manuelles Snapshot-Repository in Ihrer Domain registrieren.
- Ihre Benutzerrolle benötigt ausreichende Berechtigungen für den Zugriff auf die OpenSearch Service-Konsole. Validieren und konfigurieren Sie den Zugriff auf Ihre Domains, falls erforderlich.

Schritt 1: Konfigurieren der ISM-Richtlinie

Konfigurieren Sie zunächst eine ISM-Richtlinie in OpenSearch Dashboards.

1. Navigieren Sie vom Domain-Dashboard in der OpenSearch Service-Konsole aus zur OpenSearch Dashboard-URL und melden Sie sich mit Ihrem Master-Benutzernamen und -Passwort ein. Die URL weist folgendes Format auf: *`domain-endpoint`*`/_dashboards/`.
2. Wählen Sie in OpenSearch Dashboards Add sample data (Beispieldaten hinzufügen) aus und fügen Sie Ihrer Domain Beispielindizes hinzu.
3. Öffnen Sie das linke Navigationsfenster und wählen Sie Index Management (Indexverwaltung) und dann Create policy (Richtlinie erstellen).
4. Speichern Sie die Richtlinie unter dem Namen `ism-policy-example`.
5. Ersetzen Sie die Standardrichtlinie durch die folgende Richtlinie:

```
{
  "policy": {
```

```
    "description": "Move indexes between storage tiers",
    "default_state": "hot",
    "states": [
      {
        "name": "hot",
        "actions": [],
        "transitions": [
          {
            "state_name": "snapshot",
            "conditions": {
              "min_index_age": "24h"
            }
          }
        ]
      },
      {
        "name": "snapshot",
        "actions": [
          {
            "retry": {
              "count": 5,
              "backoff": "exponential",
              "delay": "30m"
            },
            "snapshot": {
              "repository": "snapshot-repo",
              "snapshot": "ism-snapshot"
            }
          }
        ],
        "transitions": [
          {
            "state_name": "warm",
            "conditions": {
              "min_index_age": "2d"
            }
          }
        ]
      },
      {
        "name": "warm",
        "actions": [
          {
            "retry": {
```

```
            "count": 5,
            "backoff": "exponential",
            "delay": "1h"
          },
          "warm_migration": {}
        }
      ],
      "transitions": [
        {
          "state_name": "cold",
          "conditions": {
            "min_index_age": "30d"
          }
        }
      ]
    },
    {
      "name": "cold",
      "actions": [
        {
          "retry": {
            "count": 5,
            "backoff": "exponential",
            "delay": "1h"
          },
          "cold_migration": {
            "start_time": null,
            "end_time": null,
            "timestamp_field": "@timestamp",
            "ignore": "none"
          }
        }
      ],
      "transitions": [
        {
          "state_name": "delete",
          "conditions": {
            "min_index_age": "60d"
          }
        }
      ]
    },
    {
      "name": "delete",
```

```
        "actions": [
          {
            "cold_delete": {}
          }
        ],
        "transitions": []
      }
    ],
    "ism_template": [
      {
        "index_patterns": [
          "index-*"
        ],
        "priority": 100
      }
    ]
  }
}
```

> **Note**
>
> Das Feld `ism_template` hängt die Richtlinie automatisch an jeden neu erstellten Index an, der einem der angegebenen `index_patterns` entspricht. In diesem Fall alle Indizes, die mit `index-` beginnen. Sie können dieses Feld so ändern, dass es einem Indexformat in Ihrer Umgebung entspricht. Weitere Informationen finden Sie unter ISM-Vorlagen.

6. Im Abschnitt `snapshot` der Richtlinie ersetzen Sie *`snapshot-repo`* durch den Namen des Snapshot-Repositorys, das Sie für Ihre Domain registriert haben. Optional können Sie auch *`ism-snapshot`* ersetzen, was der Name des Snapshots sein wird, wenn er erstellt wird.
7. Wählen Sie Erstellen aus. Die Richtlinie ist nun auf der Seite State management policies (Statusmanagementrichtlinien) sichtbar.

Schritt 2: Anfügen der Richtlinie an einen oder mehrere Indizes

Nachdem Sie Ihre Richtlinie erstellt haben, fügen Sie sie an einen oder mehrere Indizes in Ihrem Cluster an.

1. Öffnen Sie die Registerkarte Hot indicies (Hot-Indizes) auf und suchen Sie nach `opensearch_dashboards_sample`. Dadurch werden alle Beispielindizes aufgeführt, die Sie in Schritt 1 hinzugefügt haben.
2. Wählen Sie alle Indizes aus und klicken Sie auf Richtlinie anwenden. Wählen Sie dann die Richtlinie aus, die Sie ism-policy-examplegerade erstellt haben.
3. Wählen Sie Anwenden aus.

Auf der Seite Policy managed indices (Von der Richtlinie verwaltete Indizes) können Sie die Indizes überwachen, während sie die verschiedenen Zustände durchlaufen.

Zusammenfassen von Indizes in Amazon OpenSearch Service mit Index-Rollups

Mit Index-Rollups in Amazon OpenSearch Service können Sie Speicherkosten senken, indem Sie alte Daten regelmäßig in zusammengefasste Indizes zusammenrollen.

Sie wählen die Felder aus, die Sie interessieren, und verwenden ein Index-Rollup, um einen neuen Index zu erstellen, in dem nur diese Felder in gröberen Zeitbereichen zusammengefasst sind. Sie können Verlaufsdaten von Monaten oder Jahren zu einem Bruchteil der Kosten mit derselben Abfrageleistung speichern.

Für Index-Rollups ist Elasticsearch 7.9 OpenSearch oder höher erforderlich.

> **Note**
>
> Diese Dokumentation hilft Ihnen bei den ersten Schritten mit der Erstellung eines Index-Rollup-Jobs in Amazon OpenSearch Service. Eine umfassende Dokumentation, einschließlich einer Liste aller verfügbaren Einstellungen und einer vollständigen API-Referenz, finden Sie in der Dokumentation unter Index-Rollups. OpenSearch

Erstellen eines Index-Rollup-Auftrags

Um zu beginnen, wählen Sie „Indizes verwalten“ in OpenSearch Dashboards aus. Wählen Sie Rollup-Aufträge und Rollup-Aufträge erstellen aus.

Schritt 1: Indizes einrichten

Richten Sie die Quell- und die Zielindizes ein. Der Quellindex ist der, den Sie zusammenrollen möchten. Im Zielindex werden die Index-Rollup-Ergebnisse gespeichert.

Nachdem Sie einen Indizierungs-Rollup-Auftrag erstellt haben, können Sie Ihre Indizierungsauswahl nicht ändern.

Schritt 2: Aggregationen und Metriken definieren

Wählen Sie die Attribute mit den Aggregationen (Bedingungen und Histogramme) und Metriken (Mittelwert, Summe, Max, Min und Wertzahl) aus, die Sie zusammenfassen möchten. Stellen Sie sicher, dass Sie nicht viele stark differenzierte Attribute hinzufügen, da Sie sonst nicht viel Platz sparen.

Schritt 3: Zeitpläne festlegen

Geben Sie einen Zeitplan an, um die Indizes während der Erfassung zusammenzufassen. Standardmäßig ist der Indizierungs-Rollup-Auftrag aktiviert.

Schritt 4: Überprüfen und Erstellen

Überprüfen Sie Ihre Konfiguration und wählen Sie Erstellen aus.

Schritt 5: Den Zielindex suchen

Sie können die Standard-`_search`API verwenden, um den Zielindex zu durchsuchen. Sie können nicht auf die interne Struktur der Daten im Zielindex zugreifen, da das Plug-In die Abfrage automatisch im Hintergrund neu schreibt, um den Zielindex anzupassen. Dadurch wird sichergestellt, dass Sie für den Quell- und Zielindex dieselbe Abfrage verwenden können.

Um den Zielindex abzufragen, legen Sie `size` auf 0 fest:

```
GET target_index/_search
{
  "size": 0,
  "query": {
    "match_all": {}
  },
  "aggs": {
    "avg_cpu": {
```

```
      "avg": {
        "field": "cpu_usage"
      }
    }
  }
}
```

> **Note**
>
> OpenSearch Versionen 2.2 und höher unterstützen die Suche nach mehreren Rollup-Indizes in einer Anfrage. OpenSearch Versionen vor 2.2 und ältere Elasticsearch OSS-Versionen unterstützen nur einen Rollup-Index pro Suche.

Transformieren von Indizes im Amazon Service OpenSearch

Während Sie mit Indexrollup-Aufträgen die Datengranularität reduzieren können, indem Sie alte Daten in komprimierte Indizes zusammenfassen, können Sie mit Transformationsjobs eine andere, zusammengefasste Ansicht Ihrer Daten erstellen, die sich auf bestimmte Felder konzentriert, sodass Sie die Daten auf unterschiedliche Weise visualisieren oder analysieren können.

Indextransformationen verfügen über eine OpenSearch Dashboards-Benutzeroberfläche und eine REST-API. Das Feature erfordert OpenSearch 1.0 oder neuer.

> **Note**
>
> Diese Dokumentation bietet einen kurzen Überblick über Indextransformationen, um Ihnen den Einstieg in die Verwendung in einer Amazon OpenSearch Service-Domain zu erleichtern. Eine umfassende Dokumentation und eine REST-API-Referenz finden Sie unter Indextransformationen in der OpenSearch Open-Source-Dokumentation.

Erstellen eines Indextransformationsauftrags

Wenn Sie keine Daten in Ihrem Cluster haben, verwenden Sie die Beispielflugdaten in OpenSearch Dashboards, um Transformationsjobs auszuprobieren. Nachdem Sie die Daten hinzugefügt haben, starten Sie OpenSearch Dashboards. Wählen Sie dann Indexverwaltung, Transformationsaufträge und Transformationsauftrag erstellen.

Schritt 1: Indizes auswählen

Wählen Sie im Abschnitt Indizes den Quell- und Zielindex aus. Sie können entweder einen vorhandenen Zielindex auswählen oder einen neuen erstellen, indem Sie einen Namen dafür eingeben.

Wenn Sie nur eine Teilmenge Ihres Quellindex umwandeln möchten, wählen Sie Datenfilter hinzufügen und verwenden Sie die OpenSearch Abfrage-DSL, um eine Teilmenge Ihres Quellindexes anzugeben.

Schritt 2: Felder auswählen

Nachdem Sie Ihre Indizes ausgewählt haben, wählen Sie die Felder aus, die Sie in Ihrem Transformationsjob verwenden möchten, und legen Sie fest, ob Gruppierungen oder Aggregationen verwendet werden sollen.

- Sie können Gruppierungen verwenden, um Ihre Daten in separate Buckets in Ihrem transformierten Index zu platzieren. Wenn Sie beispielsweise alle Flughafenziele in den Beispielflugdaten gruppieren möchten, gruppieren Sie das `DestAirportID` Feld in ein Zielfeld von `DestAirportID_terms` field, und Sie können den gruppierten Flughafen IDs in Ihrem transformierten Index finden, nachdem der Transformationsauftrag abgeschlossen ist.
- Auf der anderen Seite können Sie mit Aggregationen einfache Berechnungen durchführen. Sie können beispielsweise eine Aggregation in Ihren Transformationsjob einschließen, um ein neues Feld von `sum_of_total_ticket_price` zu definieren, das die Summe aller Flugtickets berechnet. Anschließend können Sie die neuen Daten in Ihrem transformierten Index analysieren.

Schritt 3: Legen Sie einen Zeitplan fest

Transformationsjobs sind standardmäßig aktiviert und werden nach Zeitplänen ausgeführt. Geben Sie für den Ausführungsintervall der Transformation ein Intervall in Minuten, Stunden oder Tagen an.

Schritt 4: Überprüfen und überwachen

Überprüfen Sie Ihre Konfiguration und wählen Sie Erstellen aus. Überwachen Sie dann die Spalte Transformations-Auftragsstatus.

Schritt 5: Den Zielindex suchen

Nach Abschluss des Auftrags können Sie die Standard–`_search`API verwenden, um den Zielindex zu durchsuchen.

Nachdem Sie beispielsweise einen Transformationsjob ausgeführt haben, der die Flugdaten basierend auf dem `DestAirportID`-Feld umwandelt, können Sie die folgende Anforderung ausführen, um alle Felder mit dem Wert `SFO` zurückzugeben:

```
GET target_index/_search
{
  "query": {
    "match": {
      "DestAirportID_terms" : "SFO"
    }
  }
}
```

Clusterübergreifende Replikation für Amazon Service OpenSearch

Mit der clusterübergreifenden Replikation in Amazon OpenSearch Service können Sie Benutzerindizes, Zuordnungen und Metadaten von einer Service-Domain auf eine OpenSearch andere replizieren. Die clusterübergreifende Replikation trägt dazu bei, die Wiederherstellung im Falle eines Ausfalls sicherzustellen, und ermöglicht es Ihnen, Daten über geografisch weit entfernte Rechenzentren hinweg zu replizieren, um die Latenz zu verringern. Sie zahlen die Standardgebühren für die AWS Datenübertragung zwischen Domains.

Die clusterübergreifende Replikation folgt einem aktiv-passiven Replikationsmodell, bei dem der lokale Index oder der Follower-Index Daten aus dem Remote- oder Leader-Index abruft. Der Leader-Index bezieht sich auf die Datenquelle oder den Index, aus dem Sie Daten replizieren möchten. Der Follower-Index bezieht sich auf das Ziel für die Daten oder den Index, in den Sie Daten replizieren möchten.

Die clusterübergreifende Replikation ist auf Domains verfügbar, auf denen Elasticsearch 7.10 oder 1.1 oder höher ausgeführt wird. OpenSearch

> **Note**
>
> In dieser Dokumentation wird beschrieben, wie Sie die clusterübergreifende Replikation aus Sicht von Amazon OpenSearch Service einrichten. Dazu gehört die Verwendung von AWS Management Console , um clusterübergreifende Verbindungen einzurichten, was auf einem OpenSearch selbstverwalteten Cluster nicht möglich ist. Eine vollständige Dokumentation,

einschließlich einer Referenz zu Einstellungen und einer umfassenden API-Referenz, finden Sie in der Dokumentation unter Clusterübergreifende Replikation. OpenSearch

Themen

- Einschränkungen
- Voraussetzungen
- Berechtigungsanforderungen
- Einrichten einer clusterübergreifenden Verbindung
- So starten Sie eine Replikation
- Replikation bestätigen
- Replikation pausieren und Fortsetzen
- Replikation beenden
- Automatisches Folgen
- Aktualisierung verbundener Domänen

Einschränkungen

Clusterübergreifende Replikation weist folgende Einschränkungen auf:

- Sie können keine Daten zwischen Amazon OpenSearch Service-Domains und selbstverwalteten Clustern OpenSearch oder Elasticsearch-Clustern replizieren.
- Sie können einen Index nicht von einer Follower-Domain auf eine andere Follower-Domain replizieren. Wenn Sie einen Index auf mehrere Follower-Domains replizieren möchten, können Sie ihn nur von der Single-Leader-Domain aus replizieren.
- Eine Domain kann über eine Kombination aus ein- und ausgehenden Verbindungen mit maximal 20 anderen Domains verbunden werden.
- Wenn Sie anfänglich eine clusterübergreifende Verbindung einrichten, muss sich die Leader-Domain auf derselben oder einer höheren Version als die Follower-Domain befinden.
- Sie können es nicht AWS CloudFormation zum Verbinden von Domänen verwenden.
- Sie können die Cluster-übergreifende Replikation auf M3- oder (T2 und T3) Burstable Instances nicht verwenden.

- Sie können keine Daten zwischen UltraWarm oder kalten Indizes replizieren. Beide Indizes müssen sich im Hot Storage befinden.
- Wenn Sie einen Index aus der Leader-Domain löschen, wird der entsprechende Index in der Follower-Domain nicht automatisch gelöscht.

Voraussetzungen

Bevor Sie die Cluster-übergreifende Replikation einrichten, stellen Sie sicher, dass Ihre Domains die folgenden Anforderungen erfüllen:

- Elasticsearch 7.10 oder 1.1 oder höher OpenSearch
- Differenzierte Zugriffskontrolle aktiviert
- Node-to-node Verschlüsselung aktiviert

Berechtigungsanforderungen

Um die Replikation zu starten, müssen Sie die `es:ESCrossClusterGet`-Berechtigung für die Remote (Leader)-Domain einschließen. Wir empfehlen die folgende IAM-Richtlinie für die Remotedomäne. Mit dieser Richtlinie können Sie auch andere Operationen ausführen, z. B. das Indizieren von Dokumenten und das Durchführen von Standardsuchen:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "*"
        ]
      },
      "Action": [
        "es:ESHttp*"
      ],
      "Resource": "arn:aws:es:region:account:domain/leader-domain/*"
    },
```

```
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": "es:ESCrossClusterGet",
      "Resource": "arn:aws:es:region:account:domain/leader-domain"
    }
  ]
}
```

Stellen Sie sicher, dass die `es:ESCrossClusterGet`-Berechtigung auf `/leader-domain` und nicht `/leader-domain/*` angewendet wird.

Damit Nicht-Admin-Benutzer Replikationsaktivitäten ausführen können, müssen sie auch den entsprechenden Berechtigungen zugeordnet werden. Die meisten Berechtigungen entsprechen bestimmten REST-API-Operationen. Mit der Berechtigung `indices:admin/plugins/replication/index/_resume` können Sie beispielsweise die Replikation eines Index fortsetzen. Eine vollständige Liste der Berechtigungen finden Sie in der OpenSearch Dokumentation unter Replikationsberechtigungen.

> **Note**
>
> Die Befehle zum Starten der Replikation und zum Erstellen einer Replikationsregel sind Sonderfälle. Da sie Hintergrundprozesse in den Leader- und Follower-Domänen aufrufen, müssen Sie `follower_cluster_role` in der Anfrage ein `leader_cluster_role` UND übergeben. OpenSearch Der Service verwendet diese Rollen bei allen Backend-Replikationsaufgaben. Informationen zur Zuordnung und Verwendung dieser Rollen finden Sie in der Dokumentation unter Zuordnen der Leader- und Follower-Clusterrollen. OpenSearch

Einrichten einer clusterübergreifenden Verbindung

Um Indizes von einer Domain zu einer anderen zu replizieren, müssen Sie eine clusterübergreifende Verbindung zwischen den Domains einrichten. Der einfachste Weg, Domains zu verbinden, ist über die Registerkarte Verbindungen des Domain-Dashboards. Sie können auch die Konfigurations-API oder die AWS -CLI verwenden. Da die Cluster-übergreifende Replikation einem „Pull“-Modell folgt, initiieren Sie Verbindungen von der Follower-Domain.

> **Note**
>
> Wenn Sie zuvor zwei Domains verbunden haben, um clusterübergreifende Suchen durchzuführen, können Sie nicht dieselbe Verbindung für die Replikation verwenden. Die Verbindung ist in der Konsole mit `SEARCH_ONLY` gekennzeichnet. Um die Replikation zwischen zwei zuvor verbundenen Domains durchzuführen, müssen Sie die Verbindung löschen und neu erstellen. Wenn Sie dies getan haben, ist die Verbindung sowohl für die clusterübergreifende Suche als auch für die clusterübergreifende Replikation verfügbar.

So richten Sie eine Verbindung ein

1. Wählen Sie in der Amazon OpenSearch Service-Konsole die Follower-Domain aus, wechseln Sie zur Registerkarte Verbindungen und wählen Sie Anfrage aus.
2. Geben Sie unter Verbindungs-Alias einen Namen für die Verbindung ein.
3. Wählen Sie, ob Sie sich mit einer Domain in Ihrer AWS-Konto Region oder mit einem anderen Konto oder einer anderen Region verbinden möchten.
   - Um eine Verbindung zu einer Domain in Ihrer Region AWS-Konto und Ihrer Region herzustellen, wählen Sie die Domain aus und klicken Sie auf Anfrage.
   - Um eine Verbindung zu einer Domain in einer anderen Region AWS-Konto oder Region herzustellen, geben Sie den ARN der Remotedomäne an und wählen Sie Request.

OpenSearch Der Dienst validiert die Verbindungsanfrage. Wenn die Domains nicht kompatibel sind, schlägt die Verbindung fehl. Wenn die Validierung erfolgreich ist, wird sie zur Genehmigung an die Ziel-Domain gesendet. Wenn die ZielDomain die Anforderung genehmigt, können Sie mit der Replikation beginnen.

Die clusterübergreifende Replikation unterstützt die bidirektionale Replikation. Das bedeutet, dass Sie eine ausgehende Verbindung von Domäne A zu Domäne B und eine weitere ausgehende Verbindung von Domäne B zu Domäne A herstellen können. Anschließend können Sie die Replikation so einrichten, dass Domäne A einem Index in Domäne B und Domäne B einem Index in Domäne A folgt.

So starten Sie eine Replikation

Nachdem Sie eine clusterübergreifende Verbindung hergestellt haben, können Sie damit beginnen, Daten zu replizieren. Erstellen Sie zunächst einen Index für die zu replizierende Leader-Domain:

```
PUT leader-01
```

Um diesen Index zu replizieren, senden Sie diesen Befehl an die Follower-Domain:

```
PUT _plugins/_replication/follower-01/_start
{
   "leader_alias": "connection-alias",
   "leader_index": "leader-01",
   "use_roles":{
      "leader_cluster_role": "all_access",
      "follower_cluster_role": "all_access"
   }
}
```

Sie finden den Verbindungsalias auf der Registerkarte Verbindungen in Ihrem Domain-Dashboard.

In diesem Beispiel wird davon ausgegangen, dass ein Administrator die Anfrage ausgibt und der Einfachheit halber `all_access` für `leader_cluster_role` und `follower_cluster_role` verwendet. In Produktionsumgebungen empfehlen wir jedoch, dass Sie Replikationsbenutzer sowohl für den Leader- als auch für den Follower-Index anlegen und diese entsprechend zuweisen. Die Benutzernamen müssen identisch sein. Informationen zu diesen Rollen und zu deren Zuordnung finden Sie in der Dokumentation unter Zuordnen der Rollen des Leader- und Follower-Clusters. OpenSearch

Replikation bestätigen

Um zu bestätigen, dass die Replikation stattfindet, rufen Sie den Replikationsstatus ab:

```
GET _plugins/_replication/follower-01/_status

{
  "status" : "SYNCING",
  "reason" : "User initiated",
  "leader_alias" : "connection-alias",
  "leader_index" : "leader-01",
```

```
  "follower_index" : "follower-01",
  "syncing_details" : {
    "leader_checkpoint" : -5,
    "follower_checkpoint" : -5,
    "seq_no" : 0
  }
}
```

Die Checkpoint-Werte für Leader und Follower beginnen als negative Ganzzahlen und spiegeln die Anzahl der Shards wider, die Sie haben (-1 für einen Shard, -5 für fünf Shards usw.). Die Werte erhöhen sich bei jeder Änderung, die Sie vornehmen, zu positiven Ganzzahlen. Wenn die Werte identisch sind, bedeutet dies, dass die Indizes vollständig synchronisiert sind. Sie können diese Checkpoint-Werte verwenden, um die Replikationslatenz in Ihren Domains zu messen.

Um die Replikation weiter zu überprüfen, fügen Sie dem Führungslinien-Index ein Dokument hinzu:

```
PUT leader-01/_doc/1
{
   "Doctor Sleep":"Stephen King"
}
```

Und bestätige, dass es im Follower-Index angezeigt wird:

```
GET follower-01/_search

{
    ...
    "max_score" : 1.0,
    "hits" : [
      {
        "_index" : "follower-01",
        "_type" : "_doc",
        "_id" : "1",
        "_score" : 1.0,
        "_source" : {
          "Doctor Sleep" : "Stephen King"
        }
      }
    ]
  }
}
```

Replikation pausieren und Fortsetzen

Sie können die Replikation vorübergehend unterbrechen, wenn Sie Probleme beheben oder die Belastung der Leader-Domain reduzieren müssen. Senden Sie diese Anfrage an die Follower-Domain. Vergewissern Sie sich, einen leeren Anforderungstext einzubeziehen:

```
POST _plugins/_replication/follower-01/_pause
{}
```

Rufen Sie dann den Status ab, um sicherzustellen, dass die Replikation angehalten wurde:

```
GET _plugins/_replication/follower-01/_status

{
  "status" : "PAUSED",
  "reason" : "User initiated",
  "leader_alias" : "connection-alias",
  "leader_index" : "leader-01",
  "follower_index" : "follower-01"
}
```

Wenn Sie mit den Änderungen fertig sind, setzen Sie die Replikation fort. Senden Sie diese Anfrage an die Follower-Domain. Vergewissern Sie sich, einen leeren Anforderungstext einzubeziehen:

```
POST _plugins/_replication/follower-01/_resume
{}
```

Sie können die Replikation nicht fortsetzen, nachdem sie länger als 12 Stunden pausiert wurde. Sie müssen die Replikation beenden, den Follower-Index löschen und die Replikation des Leader neu starten.

Replikation beenden

Wenn Sie die Replikation vollständig einstellen, folgt der Follower-Index dem Leader-Index nicht mehr und wird zu einem Standard-Index. Sie können eine Replikation nicht neu starten, nachdem Sie sie gestoppt haben.

Beenden Sie die Replikation von der Follower-Domain. Vergewissern Sie sich, einen leeren Anforderungstext einzubeziehen:

```
POST _plugins/_replication/follower-01/_stop
{}
```

Automatisches Folgen

Sie können eine Reihe von Replikationsregeln für eine einzelne Führungs-Domain definieren, die automatisch Indizes replizieren, die einem bestimmten Muster entsprechen. Wenn ein Index auf der Leader-Domain einem der Muster entspricht (z. B.`books*`), wird ein entsprechender Follower-Index auf der Follower-Domain erstellt. OpenSearch Service repliziert alle vorhandenen Indizes, die dem Muster entsprechen, sowie neue Indizes, die Sie erstellen. Er repliziert keine Indizes, die bereits in der Follower-Domain vorhanden sind.

Um alle Indizes zu replizieren (mit Ausnahme von vom System erstellten Indizes und derjenigen, die bereits in der Follower-Domain vorhanden sind), verwenden Sie ein Platzhaltermuster (`*`).

Erstellen einer Replikationsrolle

Erstellen Sie eine Replikationsregel für die Follower-Domain und geben Sie den Namen der clusterübergreifenden Verbindung an:

```
POST _plugins/_replication/_autofollow
{
   "leader_alias" : "connection-alias",
   "name": "rule-name",
   "pattern": "books*",
   "use_roles":{
      "leader_cluster_role": "all_access",
      "follower_cluster_role": "all_access"
   }
}
```

Sie finden den Verbindungsalias auf der Registerkarte Verbindungen in Ihrem Domain-Dashboard.

In diesem Beispiel wird davon ausgegangen, dass ein Administrator die Anfrage stellt, und der Einfachheit halber werden `all_access` als Leader- und Follower-Domain-Rollen verwendet. In Produktionsumgebungen empfehlen wir jedoch, Replikationsbenutzer sowohl auf den Leader- als auch Follower-Indizes zu erstellen und diese entsprechend zuzuweisen. Die Benutzernamen müssen identisch sein. Informationen zu diesen Rollen und zu deren Zuordnung finden Sie in der Dokumentation unter Zuordnen der Rollen des Leader- und Follower-Clusters. OpenSearch

Um eine Liste vorhandener Replikationsregeln in einer Domain abzurufen, verwenden Sie den API-Vorgang für die automatische Verfolgung von Statistiken.

Um die Regel zu testen, erstellen Sie einen Index, der dem Muster in der Leader-Domain entspricht:

```
PUT books-are-fun
```

Und überprüfen Sie, ob das Replikat in der Follower-Domain angezeigt wird:

```
GET _cat/indices

health status index          uuid                   pri rep docs.count docs.deleted
 store.size pri.store.size
green  open   books-are-fun  ldfHO78xYYdxRMULuiTvSQ     1   1          0            0
     208b           208b
```

Löschen einer Replikationsrolle

Wenn Sie eine Replikationsregel löschen, beendet OpenSearch Service die Replikation neuer Indizes, die dem Muster entsprechen, setzt jedoch die bestehende Replikationsaktivität fort, bis Sie die Replikation dieser Indizes beenden.

Löschen Sie Replikationsregeln aus der Follower-Domain:

```
DELETE _plugins/_replication/_autofollow
{
   "leader_alias" : "connection-alias",
   "name": "rule-name"
}
```

Aktualisierung verbundener Domänen

Um die Engine-Version von zwei Domänen zu aktualisieren, die über eine clusterübergreifende Verbindung verfügen, aktualisieren Sie zuerst die Follower-Domain und dann die Leader-Domain. Löschen Sie nicht die Verbindung zwischen ihnen, da sonst die Replikation unterbrochen wird und Sie sie nicht fortsetzen können.

Migration von Amazon OpenSearch Service-Indizes mithilfe der Remote-Neuindizierung

Mit der Remote-Neuindizierung können Sie Indizes von einer Amazon OpenSearch Service-Domain in eine andere kopieren. Sie können Indizes aus beliebigen OpenSearch Service-Domains oder selbstverwalteten OpenSearch Clustern und Elasticsearch-Clustern migrieren.

Eine Remote-Domain und ein Index beziehen sich auf die Quelle der Daten oder die Domain und den Index, aus denen Sie Daten kopieren möchten. Eine lokale Domäne und ein lokaler Index beziehen sich auf das Ziel für die Daten oder auf die Domäne und den Index, in die Sie Daten kopieren möchten.

Für die Remote-Neuindizierung ist OpenSearch 1.0 oder höher oder Elasticsearch 6.7 oder höher für die lokale Domain erforderlich. Die Remote-Domain muss niedriger sein oder dieselbe Hauptversion wie die lokale Domain haben. Elasticsearch-Versionen gelten als ältere OpenSearch Versionen, was bedeutet, dass Sie Daten aus Elasticsearch-Domänen in Domains neu indizieren können. OpenSearch Innerhalb derselben Hauptversion kann es sich bei der Remote-Domain um eine beliebige Nebenversion handeln. Beispielsweise wird die Remote-Neuindizierung von Elasticsearch 7.10.x auf 7.9 unterstützt, aber OpenSearch 1.0 auf Elasticsearch 7.10.x wird nicht unterstützt.

> **Note**
>
> In dieser Dokumentation wird beschrieben, wie Daten zwischen Amazon OpenSearch Service-Domains neu indexiert werden. Die vollständige Dokumentation für diesen `reindex` Vorgang, einschließlich detaillierter Schritte und unterstützter Optionen, finden Sie im Dokument Reindex in der OpenSearch Dokumentation.

Themen

- Voraussetzungen
- Daten zwischen OpenSearch Service-Internetdomänen neu indizieren
- Daten zwischen OpenSearch Dienstdomänen neu indizieren, wenn sich die Fernbedienung in einer VPC befindet
- Indizieren Sie Daten zwischen OpenSearch Nicht-Servicedomänen neu
- Große Datensätze neu indizieren
- Remote-Neuindexierungseinstellungen

Voraussetzungen

Die Remote-Neuindexierung hat die folgenden Anforderungen:

- Auf die Remotedomäne muss von der lokalen Domäne aus zugegriffen werden können. Für eine Remotedomäne, die sich in einer VPC befindet, muss die lokale Domäne Zugriff auf die VPC haben. Dieser Prozess variiert je nach Netzwerkkonfiguration, beinhaltet aber wahrscheinlich eine Verbindung zu einem VPN oder einem verwalteten Netzwerk oder die Verwendung der nativen VPC-Endpunktverbindung. Weitere Informationen hierzu finden Sie unter the section called “VPC-Unterstützung”.
- Die Anfrage muss wie jede andere REST-Anfrage von der Remotedomäne autorisiert werden. Wenn für die Remotedomäne eine differenzierte Zugriffskontrolle aktiviert ist, benötigen Sie die Berechtigung, eine Neuindizierung der Remotedomäne durchzuführen und den Index in der lokalen Domäne zu lesen. Weitere Sicherheitsüberlegungen finden Sie unter the section called “Differenzierte Zugriffskontrolle”.
- Wir empfehlen Ihnen, einen Index mit der gewünschten Einstellung für Ihre lokale Domain zu erstellen, bevor Sie mit der Neuindizierung beginnen.
- Wenn Ihre Domain einen T2- oder T3-Instance-Typ für Ihre Datenknoten verwendet, können Sie die Remote-Neuindizierung nicht verwenden.

Daten zwischen OpenSearch Service-Internetdomänen neu indizieren

Das einfachste Szenario ist, dass sich der Remote-Index in derselben Domäne befindet AWS-Region wie Ihre lokale Domain mit einem öffentlich zugänglichen Endpunkt und Sie signierte IAM-Anmeldeinformationen haben.

Geben Sie in der Remotedomäne den Remote-Index an, von dem aus neu indexiert werden soll, und den lokalen Index, auf den neu indexiert werden soll:

```
POST _reindex
{
  "source": {
    "remote": {
      "host": "https://remote-domain-endpoint:443"
    },
    "index": "remote_index"
  },
  "dest": {
```

```
    "index": "local_index"
  }
}
```

Für eine Gültigkeitsprüfung müssen Sie am Ende des Endpunkts der Remote-Domäne 443 hinzufügen.

Um zu überprüfen, ob der Index in die lokale Domäne kopiert wurde, senden Sie diese Anfrage an die lokale Domäne:

```
GET local_index/_search
```

Wenn sich der Remote-Index in einer anderen Region als Ihrer lokalen Domain befindet, geben Sie den Namen der Region ein, wie in dieser Beispielanforderung:

```
POST _reindex
{
  "source": {
    "remote": {
      "host": "https://remote-domain-endpoint:443",
      "region": "eu-west-1"
    },
    "index": "remote_index"
  },
  "dest": {
    "index": "local_index"
  }
}
```

Bei isolierten Regionen wie AWS GovCloud (US) oder China ist der Endpunkt möglicherweise nicht zugänglich, da Ihr IAM-Benutzer in diesen Regionen nicht erkannt wird.

Wenn die Remote-Domain mit Standardauthentifizierung gesichert ist, geben Sie den Benutzernamen und das Passwort an:

```
POST _reindex
{
  "source": {
    "remote": {
      "host": "https://remote-domain-endpoint:443",
      "username": "username",
```

```
      "password": "password"
    },
    "index": "remote_index"
  },
  "dest": {
    "index": "local_index"
  }
}
```

Daten zwischen OpenSearch Dienstdomänen neu indizieren, wenn sich die Fernbedienung in einer VPC befindet

Jede OpenSearch Service-Domain besteht aus einer eigenen internen Virtual Private Cloud (VPC) - Infrastruktur. Wenn Sie eine neue Domain in einer vorhandenen OpenSearch Service-VPC erstellen, wird für jeden Datenknoten in der VPC eine elastic network interface erstellt.

Da der Remote-Neuindizierungsvorgang von der OpenSearch Remote-Servicedomäne aus und somit innerhalb einer eigenen privaten VPC ausgeführt wird, benötigen Sie eine Möglichkeit, auf die VPC der lokalen Domäne zuzugreifen. Sie können dazu entweder die integrierte VPC-Endpunktverbindungsfunktion verwenden, um eine Verbindung herzustellen AWS PrivateLink, oder indem Sie einen Proxy konfigurieren.

Wenn Ihre lokale Domain OpenSearch Version 1.0 oder höher verwendet, können Sie die Konsole oder die verwenden, AWS CLI um eine AWS PrivateLink Verbindung herzustellen. Eine AWS PrivateLink Verbindung ermöglicht es Ressourcen in der lokalen VPC, sich privat mit Ressourcen in der Remote-VPC innerhalb derselben zu verbinden. AWS-Region

Um eine VPC-Endpunktverbindung herzustellen, muss sich die Quelldomäne, die neu indexiert werden soll, in einer lokalen VPC befinden, und sowohl die Quell- als auch die Zieldomäne müssen sich in derselben befinden. AWS-Region

Indizieren Sie Daten neu mit dem AWS Management Console

Sie können die Remote-Neuindizierung mit der Konsole verwenden, um Indizes zwischen zwei Domänen zu kopieren, die sich eine VPC-Endpunktverbindung teilen.

1. Navigieren Sie zur Amazon OpenSearch Service-Konsole unterhttps://console.aws.amazon.com/aos/.
2. Wählen Sie im linken Navigationsbereich die Option Domains aus.

3. Wählen Sie die lokale Domain oder die Domain aus, in die Sie Daten kopieren möchten. Dadurch wird die Detailseite der Domain geöffnet. Wählen Sie unter den allgemeinen Informationen den Tab Verbindungen aus und klicken Sie auf Anfrage.
4. Wählen Sie auf der Seite Verbindung anfordern die Option VPC-Endpunktverbindung für Ihren Verbindungsmodus aus und geben Sie weitere relevante Details ein. Zu diesen Details gehört die Remote-Domain, also die Domain, von der Sie Daten kopieren möchten. Wählen Sie dann Request (Anfordern) aus.
5. Navigieren Sie zur Detailseite der Remotedomäne, wählen Sie die Registerkarte Verbindungen und suchen Sie die Tabelle Eingehende Verbindungen. Aktivieren Sie das Kontrollkästchen neben dem Namen der Domain, von der Sie gerade die Verbindung erstellt haben (die lokale Domain). Wählen Sie Approve (Genehmigen) aus.
6. Gehen Sie zurück zur lokalen Domain, wählen Sie die Registerkarte Connections (Verbindungen) aus und suchen Sie nach der Tabelle Outbound connections (Ausgehende Verbindungen). Nachdem die Verbindung zwischen den beiden Domains aktiviert wurde, wird in der Spalte Endpoint (Endpunkt) in der Tabelle ein Endpunkt verfügbar. Kopieren Sie den Endpunkt.
7. Öffnen Sie das Dashboard für die lokale Domain und wählen Sie in der linken Navigation Dev Tools aus. Führen Sie die folgende GET-Anfrage aus, um zu bestätigen, dass der Remote-Domänenindex in Ihrer lokalen Domain noch nicht existiert. *remote-domain-index-name*Ersetzen Sie es durch Ihren eigenen Indexnamen.

   ```
   GET remote-domain-index-name/_search
   {
      "query":{
         "match_all":{}
      }
   }
   ```

   In der Ausgabe sollte ein Fehler angezeigt werden, der darauf hinweist, dass der Index nicht gefunden wurde.
8. Erstellen Sie unter Ihrer GET-Anfrage eine POST-Anfrage und verwenden Sie Ihren Endpunkt wie folgt als Remote-Host.

   ```
   POST _reindex
   {
      "source":{
         "remote":{
   ```

```
            "host":"connection-endpoint",
            "username":"username",
            "password":"password"
         },
         "index":"remote-domain-index-name"
      },
      "dest":{
         "index":"local-domain-index-name"
      }
}
```

Führen Sie diese Anfrage aus.

9. Führen Sie die GET-Anfrage erneut aus. Die Ausgabe sollte nun anzeigen, dass der lokale Index existiert. Sie können diesen Index abfragen, um zu überprüfen, ob alle Daten aus dem Remote-Index OpenSearch kopiert wurden.

Indizieren Sie Daten mit OpenSearch Service-API-Vorgängen neu

Sie können die Remote-Neuindizierung mit der API verwenden, um Indizes zwischen zwei Domänen zu kopieren, die sich eine VPC-Endpunktverbindung teilen.

1. Verwenden Sie den CreateOutboundConnectionAPI-Vorgang, um eine neue Verbindung von Ihrer lokalen Domain zu Ihrer Remote-Domain anzufordern.

```
POST https://es.region.amazonaws.com/2021-01-01/opensearch/cc/outboundConnection

{
   "ConnectionAlias": "remote-reindex-example",
   "ConnectionMode": "VPC_ENDPOINT",
   "LocalDomainInfo": {
      "AWSDomainInformation": {
         "DomainName": "local-domain-name",
         "OwnerId": "aws-account-id",
         "Region": "region"
      }
   },
   "RemoteDomainInfo": {
      "AWSDomainInformation": {
         "DomainName": "remote-domain-name",
         "OwnerId": "aws-account-id",
         "Region": "region"
```

```
      }
   }
}
```

Sie erhalten `ConnectionId` in der Antwort eine. Speichern Sie diese ID, um sie im nächsten Schritt zu verwenden.

2. Verwenden Sie den AcceptInboundConnectionAPI-Vorgang mit Ihrer Verbindungs-ID, um die Anfrage von der lokalen Domain aus zu genehmigen.

```
PUT https://es.region.amazonaws.com/2021-01-01/opensearch/cc/
inboundConnection/ConnectionId/accept
```

3. Verwenden Sie den DescribeOutboundConnectionsAPI-Vorgang, um den Endpunkt für Ihre Remote-Domain abzurufen.

```
{
    "Connections": [
        {
            "ConnectionAlias": "remote-reindex-example",
            "ConnectionId": "connection-id",
            "ConnectionMode": "VPC_ENDPOINT",
            "ConnectionProperties": {
                "Endpoint": "connection-endpoint"
            },
            ...
        }
    ]
}
```

Speichern Sie das*connection-endpoint*, um es in Schritt 5 zu verwenden.

4. Führen Sie die folgende GET-Anfrage aus, um zu bestätigen, dass der Remote-Domänenindex in Ihrer lokalen Domain noch nicht existiert. *remote-domain-index-name*Ersetzen Sie es durch Ihren eigenen Indexnamen.

```
GET local-domain-endpoint/remote-domain-index-name/_search
{
   "query":{
      "match_all":{}
   }
}
```

In der Ausgabe sollte ein Fehler angezeigt werden, der darauf hinweist, dass der Index nicht gefunden wurde.

5. Erstellen Sie eine POST-Anfrage und verwenden Sie Ihren Endpunkt wie folgt als Remote-Host.

```
POST local-domain-endpoint/_reindex
{
   "source":{
      "remote":{
         "host":"connection-endpoint",
         "username":"username",
         "password":"password"
      },
      "index":"remote-domain-index-name"
   },
   "dest":{
      "index":"local-domain-index-name"
   }
}
```

Führen Sie diese Anfrage aus.

6. Führen Sie die GET-Anfrage erneut aus. Die Ausgabe sollte nun anzeigen, dass der lokale Index existiert. Sie können diesen Index abfragen, um zu überprüfen, ob alle Daten aus dem Remote-Index OpenSearch kopiert wurden.

Wenn die Remotedomäne in einer VPC gehostet wird und Sie die VPC-Endpunktverbindungsfunktion nicht verwenden möchten, müssen Sie einen Proxy mit einem öffentlich zugänglichen Endpunkt konfigurieren. In diesem Fall benötigt OpenSearch Service einen öffentlichen Endpunkt, da er keinen Datenverkehr an Ihre VPC senden kann.

Wenn Sie eine Domain im VPC-Modus ausführen, werden ein oder mehrere Endpoints in Ihrer VPC platziert. Diese Endpunkte sind jedoch nur für den Datenverkehr vorgesehen, der in die Domain innerhalb der VPC eingeht, und sie lassen keinen Datenverkehr in die VPC selbst zu.

Der Befehl remote reindex wird von der lokalen Domäne aus ausgeführt, sodass der ursprüngliche Datenverkehr diese Endpunkte nicht für den Zugriff auf die Remotedomäne verwenden kann. Aus diesem Grund ist in diesem Anwendungsfall ein Proxy erforderlich. Die Proxy-Domain muss über ein Zertifikat verfügen, das von einer öffentlichen Zertifizierungsstelle (CA) signiert wurde. Selbstsignierte oder private Zertifizierungsstellen-Zertifikate werden nicht unterstützt.

Indizieren Sie Daten zwischen OpenSearch Nicht-Servicedomänen neu

Wenn der Remote-Index außerhalb von OpenSearch Service gehostet wird, z. B. in einer selbstverwalteten EC2 Instanz, setzen Sie den `external` Parameter auf: `true`

```
POST _reindex
{
  "source": {
    "remote": {
      "host": "https://remote-domain-endpoint:443",
      "username": "username",
      "password": "password",
      "external": true
    },
    "index": "remote_index"
  },
  "dest": {
    "index": "local_index"
  }
}
```

In diesem Fall wird nur die Standardauthentifizierung mit einem Benutzernamen und einem Passwort unterstützt. Die Remotedomäne muss über einen öffentlich zugänglichen Endpunkt (auch wenn sie sich in derselben VPC wie die lokale OpenSearch Dienstdomäne befindet) und über ein von einer öffentlichen Zertifizierungsstelle signiertes Zertifikat verfügen. Selbstsignierte oder private, von einer Zertifizierungsstelle signierte Zertifikate werden nicht unterstützt.

Große Datensätze neu indizieren

Die Remote-Neuindizierung sendet eine Scroll-Anfrage mit den folgenden Standardwerten an die Remotedomäne:

- Suchkontext von 5 Minuten
- Socket-Timeout von 30 Sekunden
- Batch-Größe von 1.000

Wir empfehlen, diese Parameter an Ihre Daten anzupassen. Bei großen Dokumenten sollten Sie einen and/or längeren Timeout bei einer kleineren Batchgröße in Betracht ziehen. Weitere Informationen finden Sie unter Ergebnisse paginieren.

```
POST _reindex?pretty=true&scroll=10h&wait_for_completion=false
{
  "source": {
    "remote": {
      "host": "https://remote-domain-endpoint:443",
      "socket_timeout": "60m"
    },
    "size": 100,
    "index": "remote_index"
  },
  "dest": {
    "index": "local_index"
  }
}
```

Wir empfehlen außerdem, dem lokalen Index die folgenden Einstellungen hinzuzufügen, um die Leistung zu verbessern:

```
PUT local_index
{
  "settings": {
    "refresh_interval": -1,
    "number_of_replicas": 0
  }
}
```

Nachdem der Neuindizierungsprozess abgeschlossen ist, können Sie Ihre gewünschte Replikatanzahl festlegen und die Einstellung für das Aktualisierungsintervall entfernen.

Um nur eine Teilmenge der Dokumente, die Sie über eine Abfrage ausgewählt haben, neu zu indizieren, senden Sie diese Anfrage an die lokale Domäne:

```
POST _reindex
{
  "source": {
    "remote": {
      "host": "https://remote-domain-endpoint:443"
    },
    "index": "remote_index",
    "query": {
      "match": {
```

```
        "field_name": "text"
      }
    }
  },
  "dest": {
    "index": "local_index"
  }
}
```

Die Remote-Neuindexierung unterstützt keine Segmentierung, sodass Sie nicht mehrere Scroll-Vorgänge für dieselbe Anforderung parallel ausführen können.

Remote-Neuindexierungseinstellungen

Zusätzlich zu den Standardoptionen für die Neuindizierung unterstützt OpenSearch Service die folgenden Optionen:

Optionen	Zulässige Werte	Beschreibung	Erforderlich
Extern	Boolesch	Wenn es sich bei der Remotedomäne nicht um eine OpenSearch Dienstdomäne handelt oder wenn Sie zwischen zwei VPC-Domänen neu indizieren, geben Sie als an. `true`	Nein
Region	String	Wenn sich die Remotedomäne in einer anderen Region befindet, geben Sie den Namen der Region an.	Nein

Zeitreihendaten in Amazon OpenSearch Service mit Datenströmen verwalten

Ein typischer Workflow zum Verwalten von Zeitreihendaten umfasst mehrere Schritte, z. B. das Erstellen eines Rollover-Indexalias, das Definieren eines Schreibindexes und das Definieren allgemeiner Zuordnungen und Einstellungen für die Backing-Indizes.

Datenströme in Amazon OpenSearch Service vereinfachen diesen anfänglichen Einrichtungsprozess. Datenströme funktionieren sofort für zeitbasierte Daten wie Anwendungsprotokolle, die typischerweise nur Anhänge sind.

Es wird OpenSearch ab 1.0 erforderlich.

> **Note**
>
> Diese Dokumentation enthält grundlegende Schritte, die Ihnen den Einstieg in Datenstreams in einer Amazon OpenSearch Service-Domain erleichtern. Eine umfassende Dokumentation finden Sie unter Datenströme in der OpenSearch Dokumentation.

Erste Schritte mit Datenströmen

Ein Datenstrom besteht intern aus mehreren Backing-Indizes. Suchanforderungen werden an alle Backing-Indizes weitergeleitet, während Indizierungsanforderungen an den neuesten Schreibindex weitergeleitet werden.

Schritt 1: Erstellen einer Index-Vorlage

Um einen Datenstrom zu erstellen, müssen Sie zunächst eine Indexvorlage erstellen, die einen Satz von Indizes als Datenstrom konfiguriert. Das `data_stream`-Objekt zeigt an, dass es sich um einen Datenstrom und keine reguläre Indexvorlage handelt. Das Indexmuster stimmt mit dem Namen des Datenstroms überein:

```
PUT _index_template/logs-template
{
  "index_patterns": [
    "my-data-stream",
    "logs-*"
```

```
  ],
  "data_stream": {},
  "priority": 100
}
```

In diesem Fall muss jedes aufgenommene Dokument ein `@timestamp`-Feld haben. Sie können auch Ihr eigenes benutzerdefiniertes Zeitstempelfeld als Eigenschaft im `data_stream`-Objekt definieren:

```
PUT _index_template/logs-template
{
  "index_patterns": "my-data-stream",
  "data_stream": {
    "timestamp_field": {
      "name": "request_time"
    }
  }
}
```

Schritt 2: Erstellen eines Datenstroms

Nachdem Sie eine Indexvorlage erstellt haben, können Sie direkt mit der Erfassung von Daten beginnen, ohne einen Datenstrom zu erstellen.

Da wir eine übereinstimmende Indexvorlage mit einem `data_stream` Objekt haben, erstellt OpenSearch automatisch der Datenstrom:

```
POST logs-staging/_doc
{
  "message": "login attempt failed",
  "@timestamp": "2013-03-01T00:00:00"
}
```

Schritt 3: Daten in den Datenstrom aufnehmen

Um Daten in einen Datenstrom aufzunehmen, können Sie die reguläre APIs Indizierung verwenden. Stellen Sie sicher, dass jedes Dokument, das Sie indizieren, über ein Zeitstempelfeld verfügt. Wenn Sie versuchen, ein Dokument zu übernehmen, das kein Zeitstempelfeld enthält, erhalten Sie einen Fehler.

```
POST logs-redis/_doc
```

```
{
  "message": "login attempt",
  "@timestamp": "2013-03-01T00:00:00"
}
```

Schritt 4: Suchen eines Datenstroms

Sie können einen Datenstrom genauso durchsuchen, wie Sie einen regulären Index oder einen Indexalias durchsuchen. Der Suchvorgang gilt für alle Backing-Indizes (alle Daten, die im Stream vorhanden sind).

```
GET logs-redis/_search
{
  "query": {
    "match": {
      "message": "login"
    }
  }
}
```

Schritt 5: Rollover eines Datenstroms

Sie können eine Indexstatusmanagement (ISM)-Richtlinie einrichten, um den Rollover-Prozess für den Datenstrom zu automatisieren. Die ISM-Richtlinie wird zum Zeitpunkt ihrer Erstellung auf die Backing-Indizes angewendet. Wenn Sie eine Richtlinie einem Datenstrom zuordnen, wirkt sich dies nur auf die zukünftigen Sicherungsindizes dieses Datenstroms aus. Sie müssen auch die `rollover_alias`-Einstellung nicht angeben, da die ISM-Richtlinie diese Informationen aus dem Sicherungsindex ableitet.

> **Note**
>
> Wenn Sie einen Sicherungsindex auf Cold Storage übertragen, OpenSearch entfernt dieser Index aus dem Datenstrom. Auch wenn Sie den Index zurück auf verschieben UltraWarm, bleibt der Index unabhängig und nicht Teil des ursprünglichen Datenstroms. Nachdem ein Index aus dem Datenstream entfernt wurde, werden bei der Suche nach dem Stream keine Daten aus dem Index zurückgegeben.

> **Warning**
>
> Der Schreibindex für einen Datenstream kann nicht in einen Cold Storage migriert werden. Wenn Sie Daten in Ihrem Datenstrom in einen Cold Storage migrieren möchten, müssen Sie vor der Migration einen Rollover über den Datenstrom durchführen.

Schritt 6: Verwalten von Datenströmen in OpenSearch Dashboards

Um Datenströme von OpenSearch Dashboards aus zu verwalten, öffnen Sie OpenSearchDashboards, wählen Sie Indexverwaltung, dann Indizes oder Policy-verwaltete Indizes aus.

Schritt 7: Löschen eines Datenstroms

Der Löschvorgang löscht zuerst die Backing-Indizes eines Datenstroms und löscht dann den Datenstrom selbst.

So löschen Sie einen Datenstrom und alle versteckten Backing-Indizes:

```
DELETE _data_stream/name_of_data_stream
```

Überwachen von Daten in Amazon OpenSearch Service

Überwachen Sie Ihre Daten proaktiv in Amazon OpenSearch Service mit Warnungen und Anomalieerkennung. Richten Sie Warnungen ein, um Benachrichtigungen zu erhalten, wenn Ihre Daten bestimmte Schwellenwerte überschreiten. Die Anomalieerkennung verwendet Machine Learning, um Ausreißer in Ihren Streaming-Daten automatisch zu erkennen. Sie können die Anomalieerkennung mit Warnungen verbinden, damit Sie benachrichtigt werden, sobald eine Anomalie erkannt wird.

Themen

- Konfiguration von Benachrichtigungen in Amazon OpenSearch Service
- Erkennung von Anomalien in Amazon OpenSearch Service OpenSearch

Konfiguration von Benachrichtigungen in Amazon OpenSearch Service

Konfigurieren Sie Benachrichtigungen in Amazon OpenSearch Service, um benachrichtigt zu werden, wenn Daten aus einem oder mehreren Indizes bestimmte Bedingungen erfüllen. Sie möchten beispielsweise eine E-Mail erhalten, wenn Ihre Anwendung mehr als fünf HTTP-503-Fehler pro Stunde protokolliert, oder Sie möchten ggf. einen Entwickler benachrichtigen, wenn in den letzten 20 Minuten keine neuen Dokumente indiziert wurden.

Alerting erfordert Elasticsearch 6.2 OpenSearch oder höher.

> **Note**
>
> Diese Dokumentation bietet einen kurzen Überblick über Warnmeldungen und zeigt auf, wie sich Warnmeldungen auf einer Amazon OpenSearch Service-Domain von Warnmeldungen auf einem Open-Source-Cluster unterscheiden. OpenSearch Eine vollständige Dokumentation zu Warnmeldungen, einschließlich einer umfassenden API-Referenz, einer Liste verfügbarer Anforderungsfelder für zusammengesetzte Monitore und Beschreibungen der verfügbaren Auslöser- und Aktionsvariablen, finden Sie in der Dokumentation unter Alerting. OpenSearch

Themen

- Warnungsberechtigungen
- Erste Schritte mit Warnungen
- Benachrichtigungen
- Unterschiede

Warnungsberechtigungen

Warnungen unterstützen die differenzierte Zugriffskontrolle. Einzelheiten zum Kombinieren und Abgleichen von Berechtigungen für Ihren Anwendungsfall finden Sie in der Dokumentation unter Alerting security. OpenSearch

Um in OpenSearch Dashboards auf die Seite „Benachrichtigungen“ zugreifen zu können, müssen Sie mindestens der `alerting_read_access` vordefinierten Rolle zugeordnet sein oder Ihnen müssen entsprechende Berechtigungen erteilt werden. Diese Rolle gewährt Berechtigungen zum Anzeigen von Benachrichtigungen, Zielen und Monitoren, jedoch nicht zum Bestätigen von Warnungen oder zum Ändern von Zielen oder Monitoren.

Erste Schritte mit Warnungen

Um eine Warnung zu erstellen, konfigurieren Sie einen Monitor. Dabei handelt es sich um einen Job, der nach einem definierten Zeitplan ausgeführt wird und OpenSearch Indizes abfragt. Sie konfigurieren auch einen oder mehrere Auslöser, die die Bedingungen definieren, unter denen Ereignisse generiert werden. Abschließend konfigurieren Sie Aktionen, die nach dem Auslösen einer Warnung geschehen.

Erste Schritte mit Warnungen

1. Wählen Sie im Hauptmenü der OpenSearch Dashboards die Option Alerting und dann Monitor erstellen aus.
2. Erstellen Sie eine Überwachung pro Abfrage, pro Bucket, pro Cluster-Metriken oder pro Dokument. Anweisungen finden Sie unter Eine Überwachung erstellen.
3. Erstellen Sie für Triggers (Auslöser) einen oder mehrere Auslöser. Anweisungen finden Sie unter Auslöser erstellen.
4. Legen Sie für Actions (Aktionen) einen Benachrichtigungskanal für die Warnung fest. Wählen Sie zwischen Slack, Amazon Chime, einem benutzerdefinierten Webhook oder Amazon SNS. Wie Sie sich vorstellen können, erfordern Benachrichtigungen eine Verbindung zum Kanal. Um beispielsweise einen Slack-Channel zu benachrichtigen oder einen benutzerdefinierten Webhook

an einen Drittanbieter-Server zu senden, benötigt Ihre OpenSearch Service-Domain eine entsprechende Netzwerkkonnektivität. Der benutzerdefinierte Webhook muss eine öffentliche IP-Adresse haben, damit eine OpenSearch Service-Domain Benachrichtigungen an ihn senden kann.

> **Tip**
>
> Nachdem eine Aktion erfolgreich eine Nachricht gesendet hat, liegt die Zusicherung des Zugriffs auf diese Nachricht (z. B. den Zugriff auf einen Slack-Kanal) in Ihrer Verantwortung. Wenn Ihre Domain sensible Daten enthält, sollten Sie Auslöser ohne Aktionen verwenden und Dashboards regelmäßig auf Warnungen prüfen.

Benachrichtigungen

Alerting ist in Notifications integriert, ein einheitliches System für OpenSearch Benachrichtigungen. Mit Benachrichtigungen können Sie konfigurieren, welchen Kommunikationsservice Sie verwenden möchten, und relevante Statistiken und Informationen zur Fehlerbehebung anzeigen. Eine umfassende Dokumentation finden Sie in der OpenSearch Dokumentation unter Benachrichtigungen.

Auf Ihrer Domain muss OpenSearch Version 2.3 oder höher ausgeführt werden, um Benachrichtigungen verwenden zu können.

> **Note**
>
> OpenSearch Benachrichtigungen sind unabhängig von OpenSearch Dienstbenachrichtigungen, die Einzelheiten zu Service-Software-Updates, Auto-Tune-Verbesserungen und anderen wichtigen Informationen auf Domänenebene enthalten. OpenSearch Benachrichtigungen sind Plugin-spezifisch.

Benachrichtigungskanäle haben ab Version 2.0 die Benachrichtigungsziele ersetzt. OpenSearch Ziele wurden offiziell als veraltet eingestuft und alle Warnmeldungen werden künftig über Kanäle verwaltet.

Wenn Sie Ihre Domains auf Version 2.3 oder höher aktualisieren (da die OpenSearch Serviceunterstützung für 2.x mit 2.3 beginnt), werden Ihre vorhandenen Ziele automatisch auf Benachrichtigungskanäle migriert. Wenn ein Ziel nicht migriert werden kann, wird es vom Monitor

weiterhin verwendet, bis der Monitor zu einem Benachrichtigungskanal migriert wird. Weitere Informationen finden Sie in der Dokumentation unter Fragen zu Zielen. OpenSearch

Um mit Benachrichtigungen zu beginnen, melden Sie sich bei OpenSearch Dashboards an und wählen Sie Benachrichtigungen, Kanäle und Kanal erstellen aus.

Amazon Simple Notification Service (Amazon SNS) ist ein unterstützter Kanaltyp für Benachrichtigungen. Um Benutzer zu authentifizieren, müssen Sie dem Benutzer entweder vollen Zugriff auf Amazon SNS gewähren oder ihn eine IAM-Rolle übernehmen lassen, die Berechtigungen für den Zugriff auf Amazon SNS hat. Anweisungen finden Sie unter Amazon SNS als Kanaltyp.

Unterschiede

Im Vergleich zur Open-Source-Version von OpenSearch weist die Alarmierung in Amazon OpenSearch Service einige bemerkenswerte Unterschiede auf.

Warneinstellungen

OpenSearch Mit Service können Sie die folgenden Alarmeinstellungen ändern:

- `plugins.scheduled_jobs.enabled`
- `plugins.alerting.alert_history_enabled`
- `plugins.alerting.alert_history_max_age`
- `plugins.alerting.alert_history_max_docs`
- `plugins.alerting.alert_history_retention_period`
- `plugins.alerting.alert_history_rollover_period`
- `plugins.alerting.filter_by_backend_roles`

Alle anderen Einstellungen verwenden die Standardwerte, die Sie nicht ändern können.

Um Warnungen zu deaktivieren, senden Sie die folgende Anforderung:

```
PUT _cluster/settings
{
  "persistent" : {
    "plugins.scheduled_jobs.enabled" : false
  }
}
```

Mit der folgenden Anforderung werden Benachrichtigungen so konfiguriert, dass Verlaufsindizes automatisch nach sieben Tagen und nicht nach den standardmäßigen 30 Tagen gelöscht werden:

```
PUT _cluster/settings
{
  "persistent": {
    "plugins.alerting.alert_history_retention_period": "7d"
  }
}
```

Wenn Sie zuvor Monitore erstellt haben und die Erstellung von Indizes für tägliche Warnmeldungen beenden möchten, löschen Sie alle Indizes für den Warnungsverlauf:

```
DELETE .plugins-alerting-alert-history-*
```

Um die Anzahl der Shards für Verlaufsindizes zu reduzieren, erstellen Sie eine Indexvorlage. Die folgende Anforderung legt Verlaufsindizes für Warnungen auf einen Shard und ein Replikat fest:

```
PUT _index_template/template-name
{
  "index_patterns": [".opendistro-alerting-alert-history-*"],
  "template": {
    "settings": {
      "number_of_shards": 1,
      "number_of_replicas": 1
    }
  }
}
```

Abhängig von Ihrer Toleranz für Datenverlust können Sie sogar die Verwendung von Null-Replikaten in Erwägung ziehen. Weitere Informationen zum Erstellen und Verwalten von Indexvorlagen finden Sie in der OpenSearch Dokumentation unter Indexvorlagen.

Erkennung von Anomalien in Amazon OpenSearch Service OpenSearch

Die Funktion zur Anomalieerkennung in Amazon OpenSearch OpenSearch Service erkennt automatisch Anomalien in Ihren OpenSearch-Daten in Ihren OpenSearch OpenSearch-Daten in Ihren OpenSearch-Daten mithilfe des Anomalieerkennung (Random). RCF ist ein unüberwachter

Algorithmus für Machine Learning, der eine Skizze des eingehenden Datenstroms modelliert. Der Algorithmus berechnet einen `anomaly grade`- und `confidence score`-Wert für jeden eingehenden Datenpunkt. Die Funktion zur Anomalieerkennung verwendet diese Werte, um eine Anomalie von normalen Variationen in Ihren Daten zu unterscheiden.

Dieses Tutorial zeigt, wie Sie einen Anomaliedetektor in Amazon OpenSearch Service erstellen, um Detektoren zu erkennen.

Die Anomalieerkennung zeigt, wie Sie einen Anomaliedetektor in Amazon OpenSearch OpenSearch Service erstellen, um eine hohe CPU-Auslastung zu erkennen. Alle Instance-Typen unterstützen die Anomalieerkennung für `t2.micro` und `t2.small`.

> **Note**
>
> Diese Dokumentation bietet einen kurzen Überblick über die Erkennung von Anomalien im Kontext von Amazon OpenSearch Service. Eine umfassende Dokumentation, einschließlich detaillierter Schritte, einer API-Referenz, einer Referenz aller verfügbaren Einstellungen und Schritten zur Erstellung von Visualisierungen und Dashboards, finden Sie unter Anomalieerkennung in der Open-Source-Dokumentation. OpenSearch

Voraussetzungen

Für die Anomalieerkennung müssen die folgenden Voraussetzungen erfüllt sein:

- Die Anomalieerkennung erfordert OpenSearch OpenSearch oder Elasticsearch 7.4 oder höher.
- Die Anomalieerkennung erfordert nur eine differenzierte Zugriffskontrolle auf Elasticsearch 7.4 oder höher. OpenSearch Vor Elasticsearch 7.9 können nur Admin-Benutzer Detektoren erstellen, anzeigen und verwalten.
- Wenn Ihre Domain eine differenzierte Zugriffskontrolle verwendet, müssen Benutzer ohne Administratorrechte in OpenSearch OpenSearch-Dashboards der `anomaly_read_access` Rolle anomaly_access zugeordnet werden, um Detektoren zu erstellen und zu verwalten. `anomaly_full_access`

Erste Schritte mit der Anomalieerkennung

Wählen Sie Anomalieerkennung in OpenSearch OpenSearch Service

Schritt 1: Erstellen eines Detektors

Ein Detektor ist eine individuelle Anomalieerkennungsaufgabe. Sie können mehrere Detektoren erstellen, und alle Detektoren können gleichzeitig ausgeführt werden, wobei jeder Daten aus verschiedenen Quellen analysiert.

Schritt 2: Hinzufügen von Funktionen zu Ihrem Detektor

Eine Funktion ist das Feld in Ihrem Index, das Sie auf Anomalien überprüfen. Ein Detektor kann Anomalien in einer oder mehreren Funktionen entdecken. Sie müssen für jede Funktion eine der folgenden Aggregationen auswählen: `average()`, `sum()`, `count()`, `min()` oder `max()`.

> **Note**
>
> Die `count()` Anomalieerkennung ist nur in OpenSearch OpenSearch und Elasticsearch 7.4 oder höher verfügbar. Verwenden Sie für Elasticsearch 7.4 einen benutzerdefinierten Ausdruck wie den folgenden:
>
> ```
> {
>   "aggregation_name": {
>      "value_count": {
>         "field": "field_name"
>      }
>   }
> }
> ```

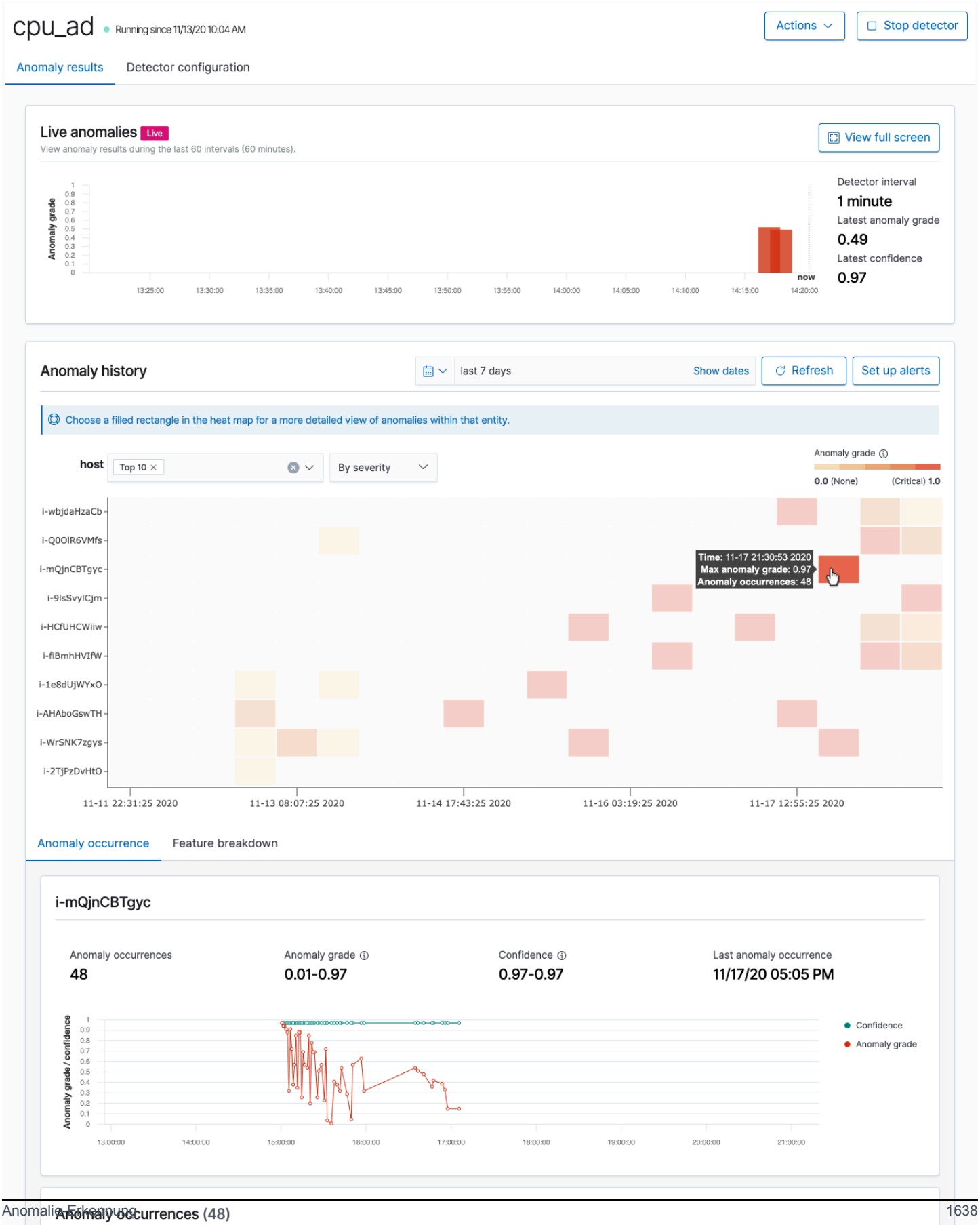
Die Aggregationsmethode legt fest, was eine Anomalie darstellt. Wenn Sie beispielsweise `min()` wählen, konzentriert sich der Detektor darauf, Anomalien basierend auf den Mindestwerten Ihrer Funktion zu finden. Wenn Sie `average()` wählen, findet der Detektor Anomalien basierend auf den Durchschnittswerten Ihrer Funktion. Sie können maximal fünf Funktionen pro Detektor hinzufügen.

Sie können die folgenden optionalen Einstellungen konfigurieren (verfügbar in Elasticsearch 7.7 und höher):

- Kategorie-Feld – Kategorisieren oder schneiden Sie Ihre Daten mit einer Dimension wie IP-Adresse, Produkt-ID, Ländercode usw.
- Größe des Fensters – Legen Sie die Anzahl der Aggregationsintervalle aus Ihrem Datenstrom fest, die in einem Erkennungsfenster berücksichtigt werden sollen.

Nachdem Sie die Funktionen eingerichtet haben, können Sie eine Vorschau von Beispielanomalien anzeigen und ggf. die Funktions-Einstellungen anpassen.

Schritt 3: Beobachten der Ergebnisse



- Live-Anomalien zeigt die Live-Anomalie-Ergebnisse für die letzten 60 Intervalle an. Wenn das Intervall beispielsweise auf 10 eingestellt ist, werden die Ergebnisse der letzten 600 Minuten angezeigt. Dieses Diagramm wird alle 30 Sekunden aktualisiert.
- Anomalieverlauf zeichnet die Anomalieklasse mit dem entsprechenden Konfidenzmaß.
- Funktionsaufschlüsselung – zeichnet die Funktionen basierend auf der Aggregationsmethode. Sie können den Datums-Uhrzeitbereich des Detektors variieren.
- Anomalie-Vorkommnisse – zeigen `Start time`, `End time`, `Data confidence` und `Anomaly grade` für jede erkannte Anomalie an.

  Wenn Sie das Kategoriefeld festlegen, sehen Sie ein zusätzliches Heatmap-Diagramm, das die Ergebnisse für anomale Elemente korreliert. Wählen Sie ein gefülltes Rechteck, um eine detailliertere Ansicht der Anomalie anzuzeigen.

Schritt 4: Einrichten von Warnungen

Um einen Monitor zu erstellen, der Ihnen Benachrichtigungen sendet, wenn Anomalien erkannt werden, wählen Sie Warnungen einrichten. Das Plug-In leitet Sie auf die Seite Monitor hinzufügen weiter, auf der Sie eine Warnung konfigurieren können.

Tutorial: Erkennen hoher CPU-Auslastung mit Anomalieerkennung

Dieses Tutorial zeigt, wie Sie einen Anomaliedetektor in Amazon OpenSearch OpenSearch Service erstellen, um eine hohe CPU-Auslastung zu erkennen. Dieses Tutorial zeigt OpenSearch , wie Ihre CPU-Auslastung einen bestimmten Schwellenwert definiert, wenn Ihre CPU-Auslastung einen bestimmten Schwellenwert überschreitet.

> **Note**
>
> Diese Schritte gelten für die neueste Version von OpenSearch OpenSearch und können bei früheren Versionen leicht abweichen.

Voraussetzungen

- Die OpenSearch Anomalieerkennung erfordert OpenSearch oder Elasticsearch 7.4 oder höher OpenSearch .

- Sie müssen Anwendungsprotokolldateien in Ihren Cluster aufnehmen, die CPU-Auslastungsdaten enthalten.

Schritt 1: Erstellen eines Detektors

Erstellen Sie zunächst einen Detektor, der Anomalien in Ihren CPU-Auslastungsdaten identifiziert.

1. Öffnen Sie das Menü im linken Bereich in OpenSearch und wählen Sie Anomalieerkennung OpenSearch und dann Create (Anomalieerkennung) und dann Create (Anomalieerkennung) aus.
2. Benennen Sie den Detektor **`high-cpu-usage`**.
3. Wählen Sie für Ihre Datenquelle Ihren Index aus, der Protokolldateien zur CPU-Auslastung enthält, in denen Sie Anomalien identifizieren möchten.
4. Wählen Sie das Feld Timestamp (Zeitstempel) in Ihren Daten aus. Optional können Sie einen Datenfilter hinzufügen. Dieser Datenfilter analysiert nur eine Teilmenge der Datenquelle und reduziert die Menge irrelevanter Daten.
5. Legen Sie den Wert für Detector interval (Detektorintervall) auf 2 Minuten fest. Dieses Intervall definiert die Zeit (in minütlichen Intervallen), die der Detektor benötigt, um die Daten zu sammeln.
6. Fügen Sie unter Window delay (Fensterverzögerung) eine Verzögerung von 1 Minute hinzu. Diese Verzögerung erhöht die Verarbeitungszeit, um sicherzustellen, dass alle Daten innerhalb des Fensters vorhanden sind.
7. Wählen Sie Weiter aus. Wählen Sie im Dashboard zur Erkennung von Anomalien unter dem Namen des Detektors Configure model (Modell konfigurieren).
8. Für Feature name (Feature-Namen) geben Sie **`max_cpu_usage`** ein. Für Feature state (Feature-Zustand) wählen Sie Enable feature (Feature aktivieren) aus.
9. Für Find anomalies based on (Anomalien finden anhand von) wählen Sie Field value (Feldwert).
10. Für Aggregation method (Aggregationsmethode) wählen Sie **`max()`** aus.
11. Für Field (Feld) wählen Sie das Feld in Ihren Daten aus, das auf Anomalien überprüft werden soll. Ein Beispiel wäre `cpu_usage_percentage`.
12. Behalten Sie alle anderen Einstellungen als Standardwerte bei und wählen Sie Next (Weiter) aus.
13. Ignorieren Sie die Einrichtung von Detektoraufträgen und klicken Sie auf Next (Weiter).
14. Wählen Sie im Popup-Fenster aus, wann der Detektor starten soll (automatisch oder manuell) und klicken Sie dann auf Confirm (Bestätigen).

Nachdem der Detektor konfiguriert ist, können Sie nach seiner Initialisierung Echtzeitergebnisse der CPU-Auslastung im Abschnitt Real-time results (Echtzeit-Ergebnisse) Ihres Detektorfensters ansehen. Der Abschnitt Live anomalies (Live-Anomalien) zeigt alle Anomalien an, die bei der Aufnahme von Daten in Echtzeit auftreten.

Schritt 2: Konfigurieren einer Warnung

Nachdem Sie einen Detektor erstellt haben, erstellen Sie eine Überwachung, die eine Warnung auslöst und eine Nachricht an Slack sendet, wenn eine CPU-Auslastung erkannt wird, die die in den Detektoreinstellungen angegebenen Bedingungen erfüllt. Sie erhalten Slack-Benachrichtigungen, wenn Daten aus einem oder mehreren Indizes die Bedingungen erfüllen, die die Warnung auslösen.

1. Öffnen Sie das Menü im linken Bereich in OpenSearch OpenSearch und wählen Sie Alerting (Anomalieerkennung) aus.
2. Geben Sie einen Namen für die Überwachung an.
3. Für Monitor type (Überwachungstyp) wählen Sie Per-query monitor (Überwachung pro Abfrage) aus. Eine abfragebasierte Überwachung führt eine angegebene Abfrage aus und definiert die Trigger.
4. Wählen Sie für Monitor defining method (Definierende Methode überwachen) Anomaly detector (Anomaliedetektor) aus. Wählen Sie dann den Detektor im Dropdown-Menü Detector (Detektor) aus, den Sie im vorherigen Abschnitt erstellt haben.
5. Wählen Sie für Schedule (Plan) aus, wie oft die Überwachung Daten erfassen soll und wie oft Sie alarmiert werden möchten. Legen Sie für die Zwecke dieses Tutorials die Ausführung alle 7 Minuten fest.
6. Wählen Sie im Bereich Triggers (Auslöser) Add trigger (Auslöser hinzufügen) aus. Für Trigger name (Auslösername) geben Sie **`High CPU usage`** ein. In diesem Tutorial wählen Sie für Severity level (Schweregrad) 1 aus. Das ist der höchste Schweregrad.
7. Für Anomaly grade threshold (Anomalieklassen-Schwellenwert) wählen Sie IS ABOVE (LIEGT ÜBER) aus. Wählen Sie im Menü darunter den anzuwendenden Klassen-Schwellenwert aus. Stellen Sie für dieses Tutorial die Anomaly grade (Anomalieklasse) zu 0.7.
8. Für Anomaly confidence threshold (Anomaliekonfidenz-Schwellenwert) wählen Sie IS ABOVE (LIEGT ÜBER) aus. Geben Sie im Menü darunter dieselbe Zahl wie für die Anomalieklasse an. Stellen Sie für dieses Tutorial den Anomaly confidence threshold (Anomaliekonfidenz-Schwellenwert) 0.7 ein.
9. Im Bereich Actions (Aktionen) wählen Sie Destination (Ziel) aus. Wählen Sie im Feld Name den Namen des Ziels aus. Wählen Sie im Menü Type (Typ) Slack aus. Im Feld Webhook URL

(Webhook-URL) geben seine Webhook-URL ein, an die Alarme gesendet werden sollen. Weitere Informationen finden Sie unter Sending messages using incoming webhooks (Senden von Nachrichten mit eingehenden Webhooks).

10. Wählen Sie Erstellen aus.

Zugehörige Ressourcen

- the section called “Warnfunktion”

- the section called “Anomalie-Erkennung”
- API zur Anomalieerkennung

Amazon Q Developer für Amazon OpenSearch Service

Amazon Q Developer ist ein generativer Assistent, der Ihnen helfen kann, wenn Sie ein Amazon-Q-Datenintegration benötigen. Amazon Q hilft AWS Kunden dabei, ihre laufenden Anwendungen zu codieren, zu testen, bereitzustellen, Fehler zu beheben und zu optimieren AWS.

Die Amazon Q-Integration mit Amazon OpenSearch Service bietet die folgenden generativen Funktionen:

- the section called “Generieren Sie Visualisierungen in natürlicher Sprache”
- the section called “Zusammenfassungen und Einblicke in Benachrichtigungen anzeigen”
- the section called “Sehen Sie sich die von Amazon Q generierten Zusammenfassungen der Abfrageergebnisse auf der Discover-Seite an”
- the section called “Anomaliedetektoren beschreiben beschreiben.”
- the section called “Greifen Sie auf den Amazon Q-Chat für OpenSearch Servicefragen zu”

Um auf die Funktionen von Amazon Q Developer in OpenSearch Service zuzugreifen, die für Ihre Aufgabe relevant sind, suchen Sie auf den Seiten Alerts, Discover und Create Visualization nach dem folgenden kontextbezogenen Symbol. Klicken Sie auf das Symbol, um Unterstützung anzufordern und die in diesem Abschnitt beschriebenen Funktionen zu nutzen.



Gehen Sie wie Amazon vor, um Ihre Rolle zu OpenSearch ändern. Amazon Q Chat unterstützt Antworten auf Fragen zu OpenSearch Servicemerkmalen und -funktionen.

> **Note**
>
> Amazon Q Chat kann nicht auf Ihre Daten zugreifen. Aus diesem Grund können Sie den Chatbot nicht in ein Gespräch über Ihre Daten einbeziehen.

Weitere Informationen zu Amazon Q finden Sie unter Was ist Amazon Q Developer? Amazon-Q-Datenintegration für das Amazon-Q-Benutzerhandbuch.

Unterstützt AWS-Regionen

Amazon Q-Support für OpenSearch Service ist in den folgenden Bereichen verfügbar AWS-Regionen:

- USA Ost (Nord-Virginia)
- USA West (Oregon)
- Asien-Pazifik (Mumbai)
- Asien-Pazifik (Sydney)
- Asien-Pazifik (Tokio)
- Canada (Central)
- Europa (Frankfurt)
- Europa (London)
- Europe (Paris)
- Südamerika (São Paulo)

Einrichten von Amazon Q Developer OpenSearch Service Service Service Service Service Service Service

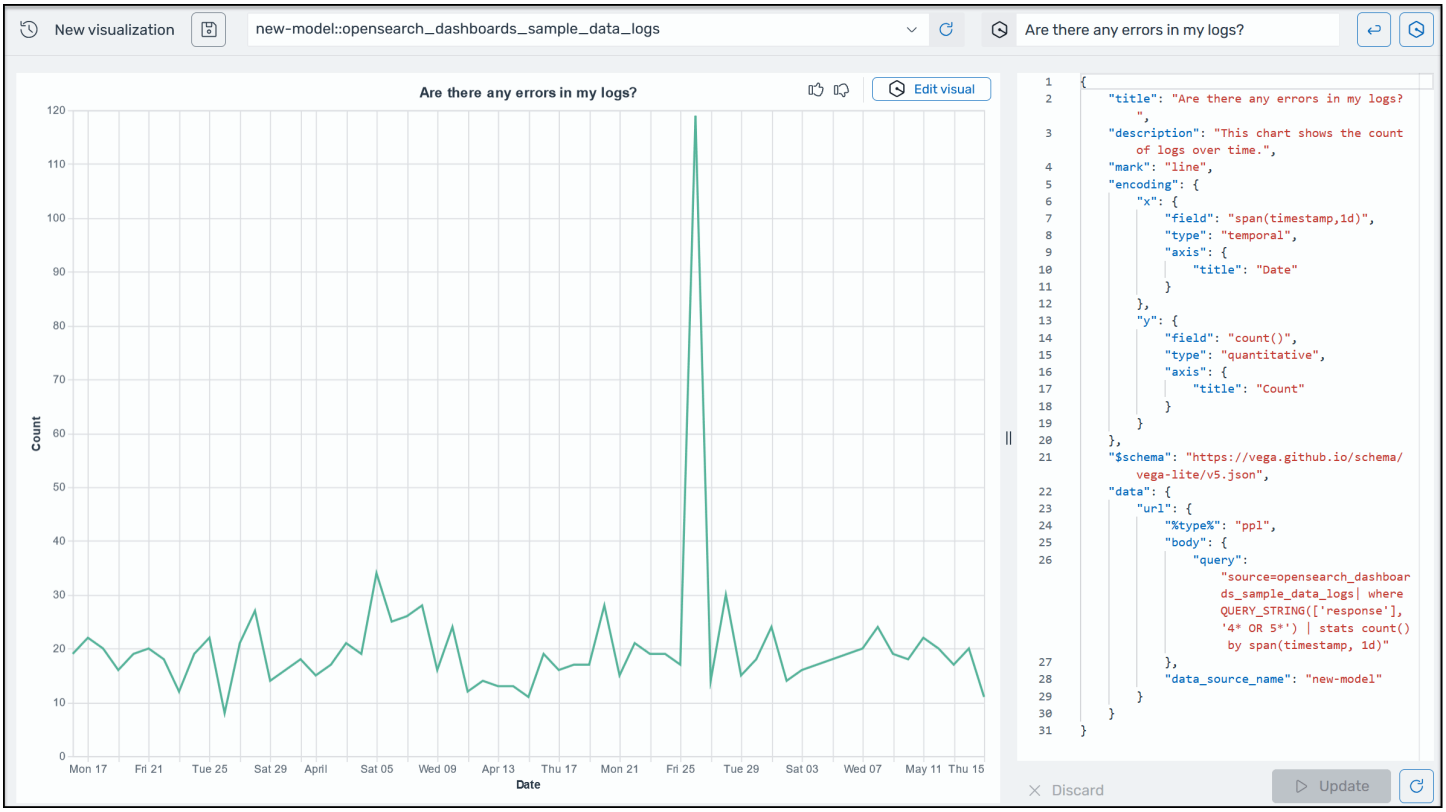
Gehen Sie wie folgt vor, um ein Amazon EMR Studio OpenSearch einzurichten.

1. Konfigurieren Sie die Zugriffskontrolle für OpenSearch eine differenzierte Zugriffskontrolle. Weitere Informationen finden Sie unter Feinkörnige Zugriffskontrolle in Amazon Service OpenSearch .
2. Stellen Sie sicher, dass Ihre Datenquelle OpenSearch Version 2.17 oder höher verwendet.
3. Stellen Sie sicher, dass Sie bei der Domainerstellung oder beim Bearbeiten der Clusterkonfiguration das Kontrollkästchen Generierung von Abfragen in natürlicher Sprache aktivieren im Abschnitt Künstliche Intelligenz (KI) und Machine Learning (ML) aktiviert haben.

> **Note**
>
> Die OpenSearch Funktionen von Amazon Q for Developer sind im Rahmen des kostenlosen Kontingents Q verfügbar. Weitere Informationen finden Sie unter Grundlegendes zu den Servicestufen im Amazon Q-Benutzerhandbuch.

Generieren Sie Visualisierungen in natürlicher Sprache

Um Ihnen zu helfen, weitere Einblicke in Ihre Betriebsdaten zu gewinnen, unterstützt Amazon Q Developer for OpenSearch Service die Verwendung von Eingabeaufforderungen in natürlicher Sprache zur Erstellung von Visualisierungen. Sie können Visualisierungen wie das folgende Beispiel in natürlicher Sprache auf der Visualisierungsseite oder der Discover-Seite generieren.



Visualisierungen können die Fehlerbehebung beschleunigen, indem sie die Fehleranalyse nach verschiedenen Dimensionen aufschlüsseln. Visualisierungen können Ihnen auch dabei helfen, Muster und Trends zu erkennen, die Entscheidungsfindung zu beschleunigen, Zusammenhänge aufzudecken und komplexe Daten zu vereinfachen.

Um eine Visualisierung in natürlicher Sprache zu generieren

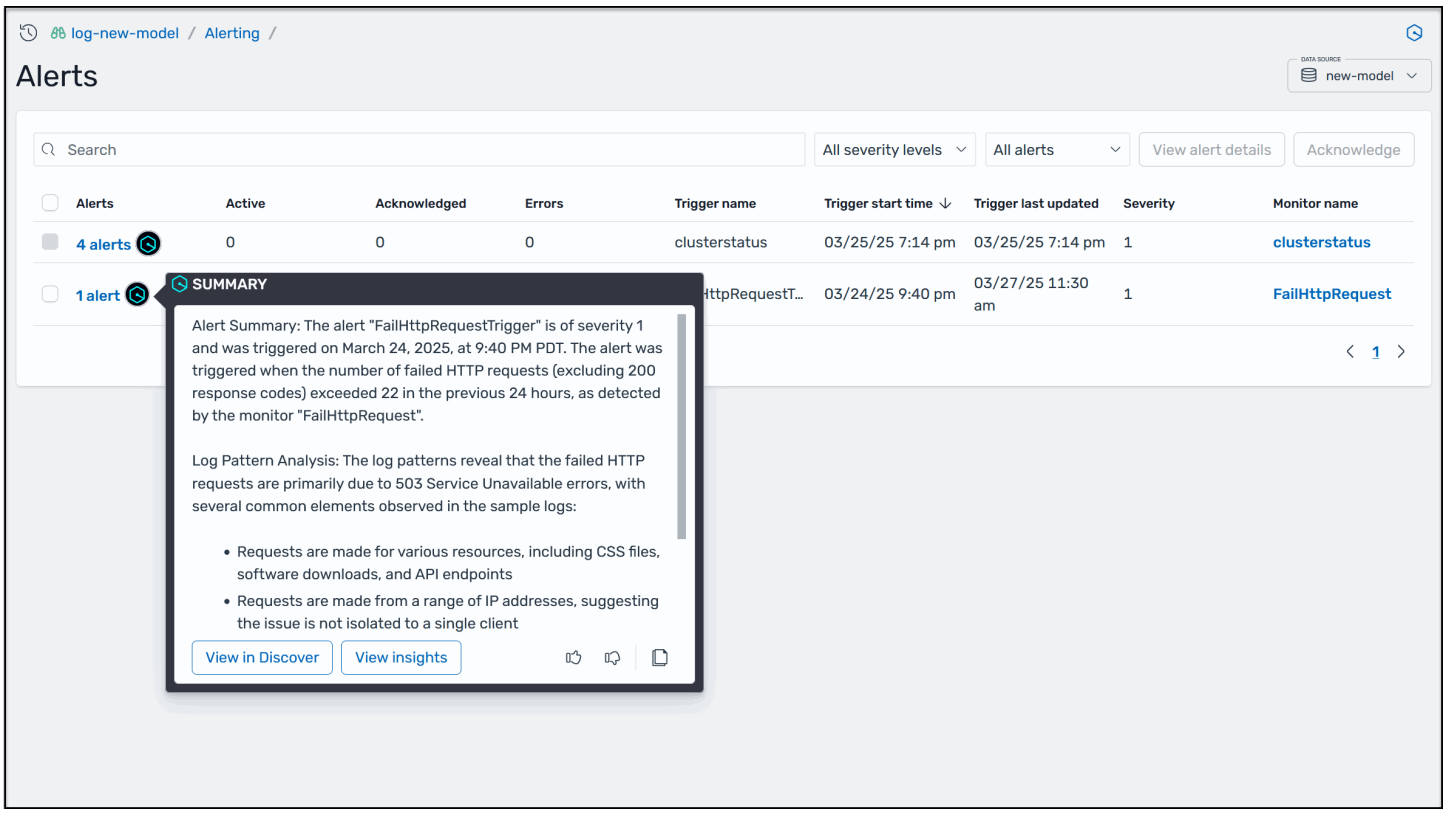
1. Stellen Sie sicher, dass Sie Amazon Q for OpenSearch Service eingerichtet haben.
2. Wählen Sie im Hauptmenü der OpenSearch Dashboards die Discover-Seite und wählen Sie dann eine Datenquelle aus.
3. Wählen Sie im Amazon Q-Menü die Option Visualisierung generieren, wie im folgenden Screenshot gezeigt.



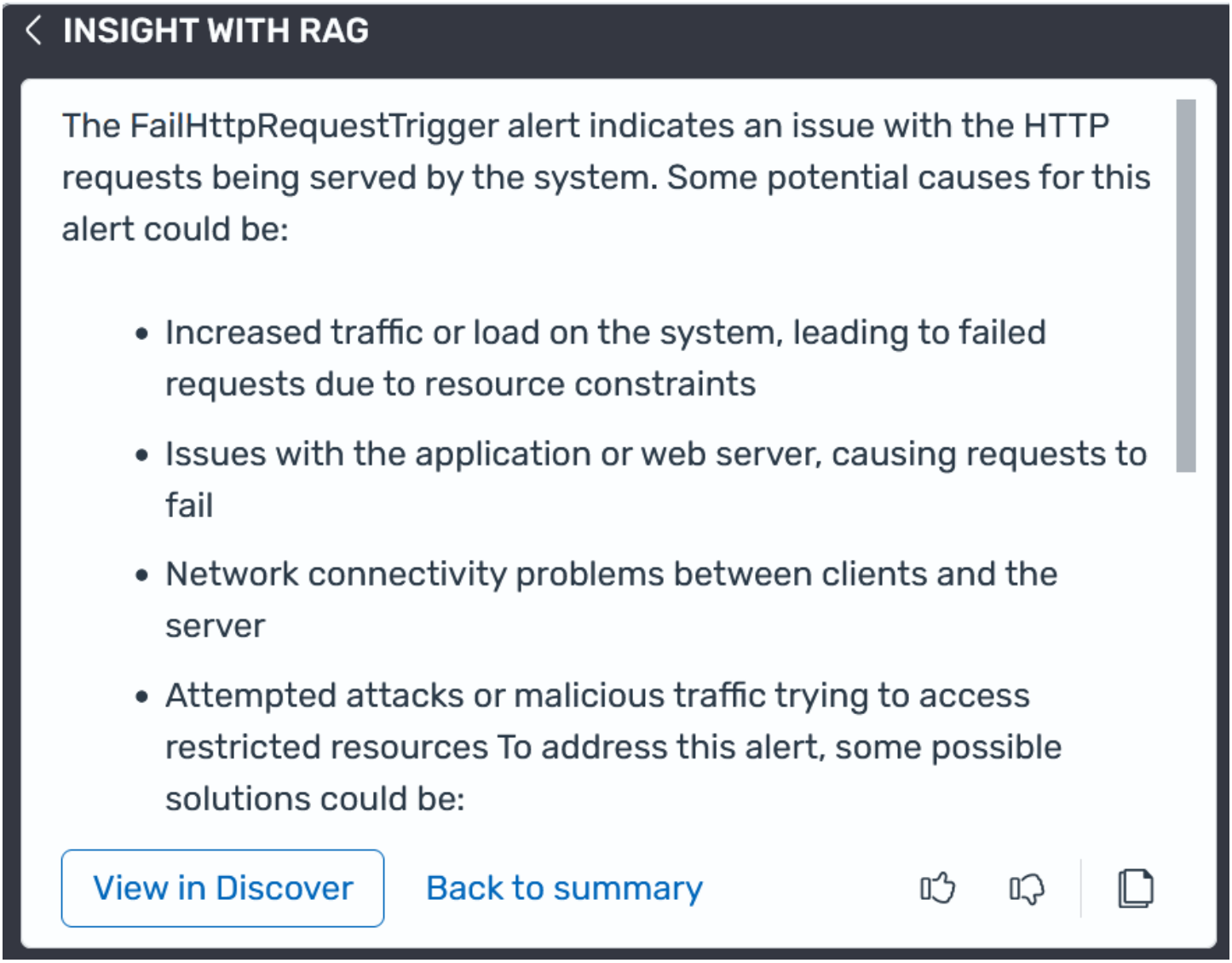
4. Wenn Sie auf der Discover-Seite eine Abfrage in natürlicher Sprache eingegeben haben, kopiert Amazon Q den Kontext, wenn eine auf dieser Abfrage basierende Visualisierung erstellt wird. Wenn Sie noch keine Abfrage in natürlicher Sprache eingegeben haben, geben Sie in das Amazon Q-Textfeld eine Aufforderung ein und klicken Sie dann auf die Schaltfläche neben dem Textfeld, um die Abfrage auszuführen. Amazon Abbilderstellung kann einige Sekunden dauern.
5. Wählen Sie das Suchfeld in der oberen rechten Ecke der oberen rechten Ecke des Themas aus. Geben Sie eine neue Aufforderung ein, z. B. „Das in ein Liniendiagramm ändern“, und wählen Sie dann Anwenden.

Zusammenfassungen und Einblicke in Benachrichtigungen anzeigen

Gehen Sie wie folgt OpenSearch vor, wenn Daten aus einem oder mehreren Sekunden dauern, wenn Daten aus einem oder mehreren Sekunden dauern. Um eine Warnung schnell zu verstehen und zu beheben, können Sie eine Warnungszusammenfassung anzeigen, indem Sie auf das Amazon Q Developer-Symbol neben einer Warnung klicken. Eine Zusammenfassung enthält Details zu dem zugrundeliegenden Problem, das die Warnung ausgelöst hat, und, sofern verfügbar, zusätzliche Analysen, die Ihnen helfen, die Ursache des Problems zu finden. Der folgende Screenshot zeigt ein Amazon-Q-Datenfeld.



Wenn Sie eine Wissensdatenbank verbinden, um zusätzlichen Kontext zu Ihrer Umgebung bereitzustellen, wie später in diesem Thema beschrieben, generiert Amazon Q Einblicke in eine Warnung. Insights bietet Details und Optionen zur Fehlerbehebung, die Ihnen helfen, die Ursache einer Warnung zu beheben. Für die zuvor angezeigte Warnung hat Amazon Q auch die folgenden Erkenntnisse gewonnen.



> **Note**
>
> Abhängig von der Art der Warnung und den verfügbaren Informationen kann Amazon Q Ihnen die Option bieten, die Warnungsdaten auf der Discover-Seite in den OpenSearch Dashboards einzusehen. Wenn Sie die Schaltfläche In Discover anzeigen am Ende einer Amazon Q-Warnmeldungsübersicht sehen, klicken Sie auf die Schaltfläche, um den entsprechenden Datensatz in Discover mit einem aktiven Filter für die Warnungsdaten zu öffnen.

Themen

- Bevor Sie beginnen

- Zusammenfassungen und Einblicke in Warnmeldungen anzeigen

Bevor Sie beginnen

Gehen Sie wie folgt vor, um eine Amazon Bedrock-Wissensdatenbank zu konfigurieren, sodass Amazon Q Einblicke für OpenSearch Service-Benachrichtigungen erstellen kann.

Schritt 1: Erstellen der LambdaInvokeOpenSearch MLCommons IAM-Rolle für die Aufgabenausführung.

Erstellen Sie eine neue Rolle mit dem Namen `LambdaInvokeOpenSearchMLCommonsRole` AWS Identity and Access Management (IAM). OpenSearch Der Service verwendet diese Rolle, um einen KI-Konnektor zu erstellen, der dabei hilft OpenSearch, Erkenntnisse auf der Grundlage konfigurierter Knowledgebase-Artikel zu gewinnen. Sie müssen diese Rolle der OpenSearch Servicerolle `ml_full_access` zuordnen, wie in Schritt 2 beschrieben.

Wenn Sie die neue Rolle erstellen, wählen Sie für den Entitätstyp Vertrauenswürdig die Option AWS Konto aus. Sie müssen keine Aufgabenplatzierungsstrategien angeben. Wählen Sie auf der Seite Add permissions (Berechtigungen hinzufügen) die Option Next (Weiter) aus. Weitere Informationen zum Erstellen einer Rolle für einen AWS-Service finden Sie unter Erstellen einer Rolle für einen AWS AWS-Service im IAM-Benutzerhandbuch.

Schritt 2: Ordnen Sie die LambdaInvokeOpenSearch MLCommons Rollenrolle der Rolle OpenSearch Service ml_full_access zu

Gehen Sie wie folgt vor, um die `LambdaInvokeOpenSearchMLCommonsRole` Rolle der Servicerolle zuzuordnen. OpenSearch `ml_full_access` Diese Zuordnung hilft OpenSearch Service auch dabei, den AI-Konnektor zu erstellen.

Um die erforderliche IAM-Rolle der OpenSearch Service-Rolle ml_full_access zuzuordnen

1. Öffnen Sie die Seite zur Verwaltung der Daten im OpenSearch Service Dashboard.
2. Wählen Sie unter Datenzugriff und Benutzer die Option Rollen aus.
3. Gehen Sie wie folgt vor, um die Rolle in Ihrer `ml_full_access` Rolle festzulegen.
4. Wählen Sie auf der Seite ml_full_access die Registerkarte Zugeordnete Benutzer aus.
5. Wählen Sie Benutzer zuordnen aus.
6. Fügen Sie im Feld Backend-Rollen den Amazon-Ressourcennamen (ARN) der `LambdaInvokeOpenSearchMLCommonsRole` Rolle ein und wählen Sie dann Map aus.

Schritt 3: Konfigurieren Sie eine OpenSearch Service-Wissensdatenbank mit AWS CloudFormation

Gehen Sie wie folgt vor, um eine OpenSearch Service-Wissensdatenbank AWS CloudFormation so zu konfigurieren, dass Amazon Q Erkenntnisse generieren kann.

Um eine Wissensdatenbank für Einblicke zu konfigurieren

1. Melden Sie sich auf der https://console.aws.amazon.com/aos/Startseite der Amazon OpenSearch Service-Konsole in einem unterstützten Bereich an AWS-Region. Weitere Informationen finden Sie unter Unterstützt AWS-Regionen.
2. Wählen Sie im Navigationsbereich Integrationen aus.
3. Wählen Sie im Abschnitt Integrationsvorlagen die Vorlage Mit der Wissensdatenbank über Amazon Bedrock integrieren aus. Gehen Sie wie folgt vor, um eine Antwort zu finden.
4. Wählen Sie auf der Kachel Mit der Wissensdatenbank über Amazon Bedrock integrieren die Option Domain konfigurieren und wählen Sie dann eine der verfügbaren Optionen aus. OpenSearch Der Service öffnet die AWS CloudFormation Stack-Vorlage, wobei die erforderlichen Felder bereits ausgefüllt sind. Der AWS CloudFormation Stack unterstützt die Integration für öffentliche Domains und VPC-Domains.
5. Wählen Sie Stack erstellen aus. Nachdem die Ressourcen AWS CloudFormation erstellt wurden, zeigt der Service den Amazon Bedrock-Agenten AgentIdConnectorId, und ModelIdan.

Falls zutreffend, erstellt Amazon Q jetzt Erkenntnisse für OpenSearch Servicewarnungen.

Zusammenfassungen und Einblicke in Warnmeldungen anzeigen

Gehen Sie wie folgt vor, um die OpenSearch Leistung eines Themas einzusehen.

Zusammenfassungen und Einblicke in Warnmeldungen anzeigen

1. Stellen Sie sicher, dass Sie Amazon Q for OpenSearch Service eingerichtet haben.
2. Stellen Sie sicher, dass Sie Benachrichtigungen für OpenSearch Service eingerichtet haben.
3. Wählen Sie im Hauptmenü der OpenSearch Dashboards die Option Alerting und dann Alerts aus.
4. Wählen Sie das Amazon Q-Symbol neben einer Warnung. Amazon kann bis zu 10 Minuten dauern.

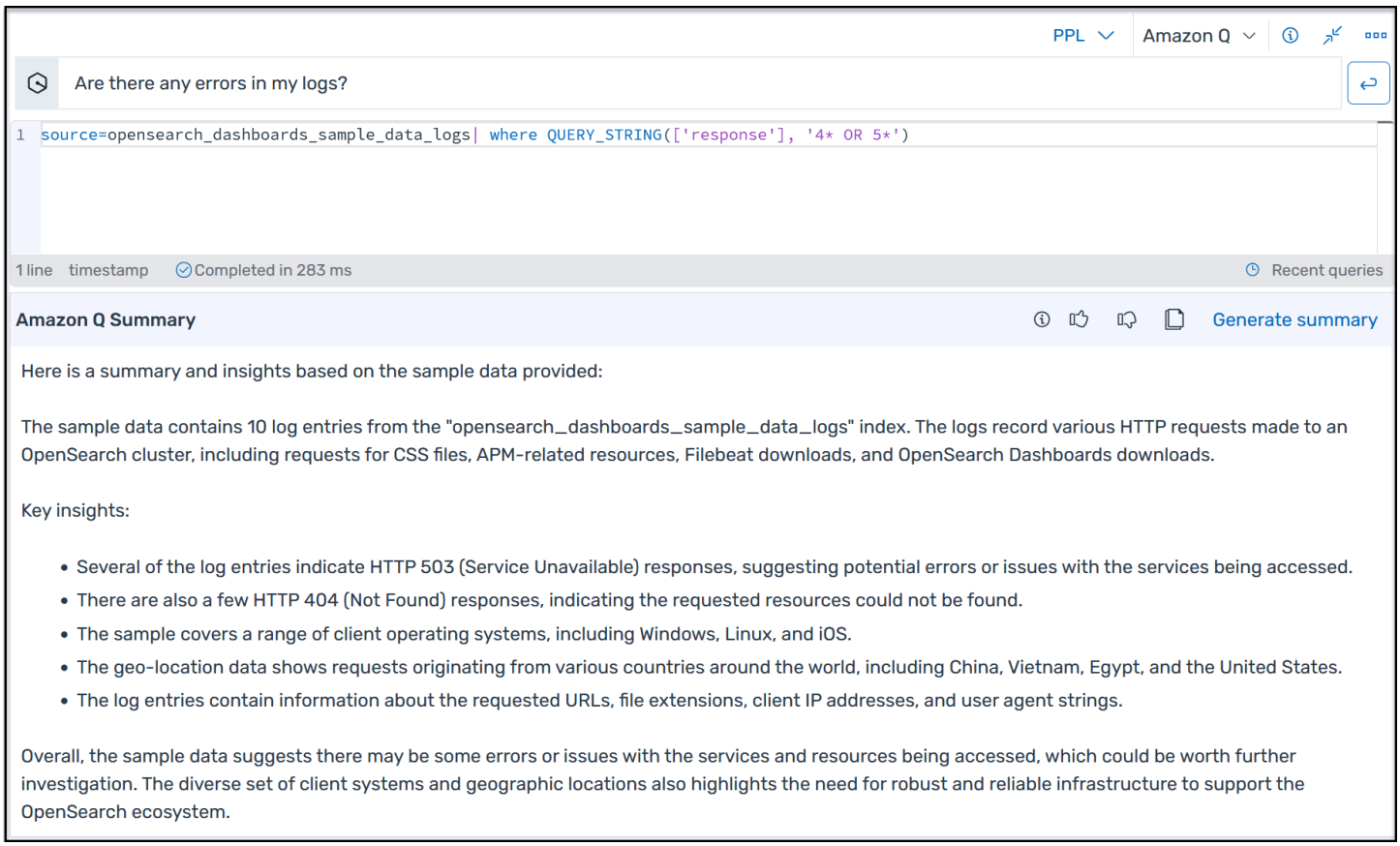
5. Falls in der Warnungszusammenfassung vorhanden, wählen Sie Einblicke anzeigen aus, um weitere Details zu der Warnung auf der Grundlage Ihrer konfigurierten Wissensdatenbank anzuzeigen.
6. Falls in der Warnungszusammenfassung vorhanden, wählen Sie In Discover anzeigen, um die Warnungsdaten auf der Discover-Seite in den OpenSearch Dashboards anzuzeigen.

Sehen Sie sich die von Amazon Q generierten Zusammenfassungen der Abfrageergebnisse auf der Discover-Seite an

OpenSearch Mit Service können Sie Ihre Daten mithilfe der Abfragesprache Piped Processing Language (PPL) auf der Discover-Seite mit Eingabeaufforderungen in natürlicher Sprache abfragen. Gehen Sie wie folgt vor:

- Gibt es Fehler in meinen Fehlerprotokollen?
- Wie groß ist die durchschnittliche Anzahl der Anfragen pro Woche?
- Wie viele Anfragen gab es letzte Woche, gruppiert nach Antwortcode?

Als Antwort generiert Amazon Q Zusammenfassungen Ihrer Abfrageergebnisse in natürlicher Sprache auf der Grundlage der ersten zehn Datensätze, wie die folgenden:



Die Kombination aus Generierung von Abfragen in natürlicher Sprache und Abfragezusammenfassungen kann bei der Behebung einer Warnung eine zusätzliche Abfrageebene hinzufügen oder eine benutzerfreundliche Möglichkeit bieten, Ihre Daten zu verstehen, ohne komplexe Abfragen schreiben zu müssen.

Um die von Amazon Q generierten Zusammenfassungen der Abfrageergebnisse auf der Discover-Seite anzuzeigen

1. Stellen Sie sicher, dass Sie Amazon Q for OpenSearch Service eingerichtet haben.
2. Wählen Sie im Hauptmenü der OpenSearch Dashboards die Option Discover aus.
3. Wählen Sie in der Dropdown-Liste die Verteilungs-ID aus.
4. Geben Sie im Amazon Q-Textfeld eine Aufforderung ein und klicken Sie dann auf die Schaltfläche neben dem Textfeld, um die Abfrage auszuführen. Amazon kann bis zu 10 Minuten dauern. Nach Ihrer ersten Anfrage müssen Sie Zusammenfassung generieren für nachfolgende Zusammenfassungen auswählen.

> **Note**
>
> Sie können die Generierung von Zusammenfassungen in der Amazon Q-Dropdown-Liste in Discover deaktivieren.

Anomaliedetektoren beschreiben beschreiben.

Die Funktion zur Anomalieerkennung in Amazon OpenSearch OpenSearch OpenSearch-Daten wird automatisch angezeigt. RCF ist ein unüberwachter Algorithmus für Machine Learning, der eine Skizze des eingehenden Datenstroms modelliert. Der Algorithmus berechnet einen `anomaly grade`- und `confidence score`-Wert für jeden eingehenden Datenpunkt. Die Funktion zur Anomalieerkennung verwendet diese Werte, um eine Anomalie von normalen Variationen in Ihren Daten zu unterscheiden.

Um den Prozess der Erstellung von Anomaliedetektoren zu vereinfachen, kann Amazon Q auf der Discover-Seite basierend auf Ihrer ausgewählten Datenquelle Meldervorschläge generieren. Amazon Q unterstützt empfohlene Anomaliedetektoren für jede Sprache.

Um die von Amazon Q empfohlenen Anomaliedetektoren anzuzeigen

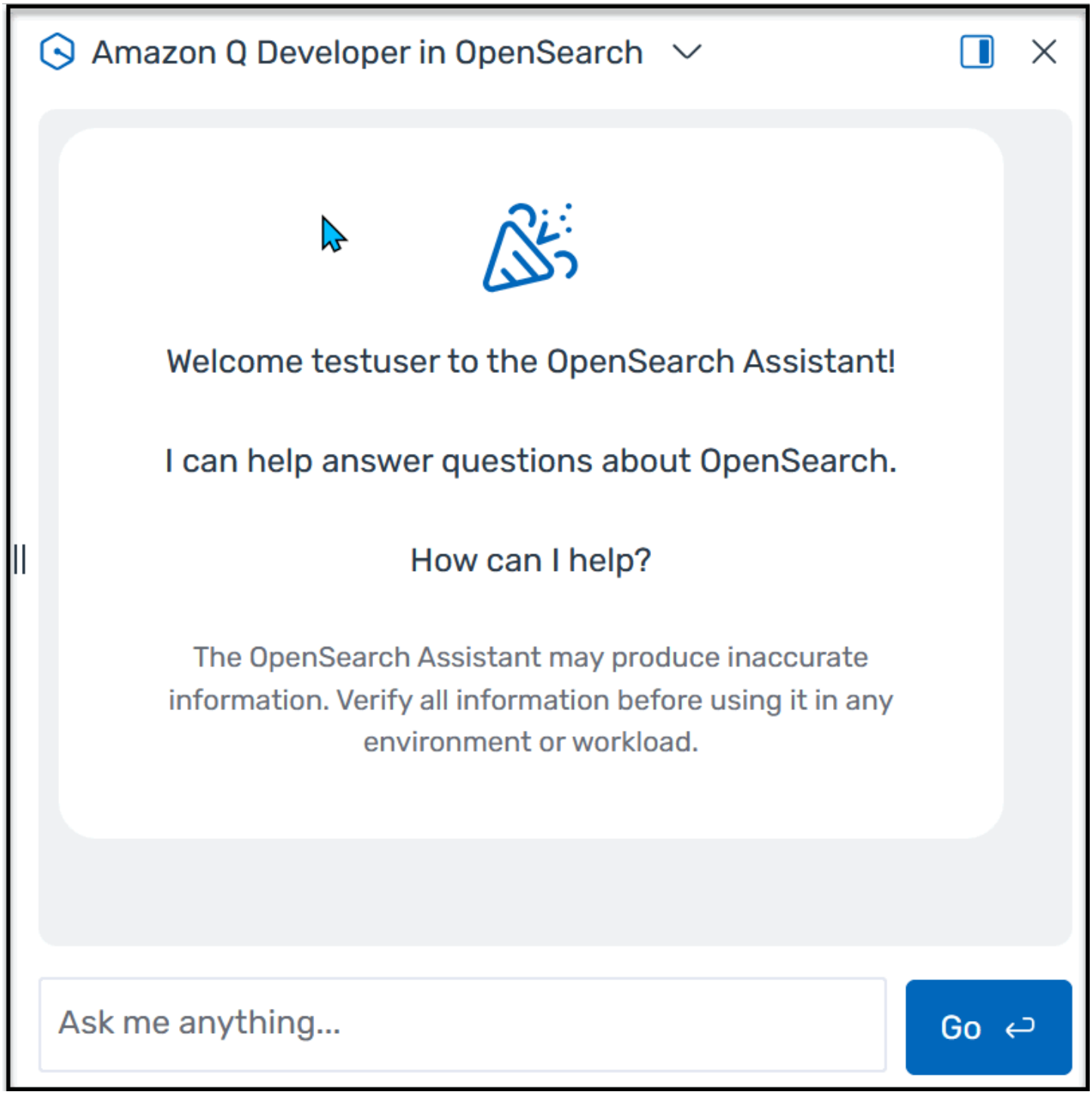
1. Stellen Sie sicher, dass Sie Amazon Q for OpenSearch Service eingerichtet haben.
2. Wählen Sie im Hauptmenü der OpenSearch Dashboards die Discover-Seite und wählen Sie dann eine Datenquelle aus.
3. Wählen Sie im Amazon Q-Menü die Option Anomaliedetektor vorschlagen aus, wie im folgenden Screenshot gezeigt.



   Amazon Q kann einige Sekunden benötigen, um die Funktionen für den Detektor zu generieren.
4. Wählen Sie Detektor erstellen.

Greifen Sie für OpenSearch verwandte Fragen auf den Amazon Q-Chat zu

Wenn Sie Fragen zu Amazon OpenSearch Service haben, einschließlich konzeptioneller oder verfahrenstechnischer Fragen zu OpenSearch Servicemerkmalen oder -funktionen, können Sie sich an Amazon Q Developer wenden, um weitere Informationen zu erhalten. Der Chatbot unterstützt einen Konversations-Chat, der den Kontext Ihrer Diskussion beibehält. Er speichert auch einen Verlauf Ihrer Konversationen, damit Sie später darauf zurückgreifen können. Um auf den Chatbot zuzugreifen, klicken Sie auf einer beliebigen OpenSearch Serviceseite oben rechts auf das Amazon Q-Symbol. Geben Sie eine Frage in das Textfeld ein und klicken Sie auf Los. Amazon kann bis zu 10 Minuten dauern.



Hier ist ein Beispiel für Amazon Antwort:

Can you suggest some node management best practices?

Based on your context of being in the OpenSearch Dashboard in the us-west-2 region, here are some node management best practices for Amazon OpenSearch Service: [1]

1. Implement Dedicated Manager Nodes:
    - Use dedicated manager nodes to improve cluster stability. [2]
    - Configure three dedicated manager nodes for optimal domain stability across three Availability Zones.
    - This offloads cluster management tasks from data nodes, enhancing overall performance.
2. Multi-AZ Deployment:
    - Deploy your domain across multiple Availability Zones for increased availability and resilience.
    - Consider using the Multi-AZ with Standby option for 99.99% availability and consistent performance.
3. Proper Sizing:

> **Note**
>
> Amazon Q Chat kann nicht auf Ihre Daten zugreifen. Aus diesem Grund können Sie den Chatbot nicht in ein Gespräch über Ihre Daten einbeziehen.

Maschinelles Lernen für Amazon OpenSearch Service

ML Commons ist ein OpenSearch Plugin, das eine Reihe gängiger Algorithmen für maschinelles Lernen (ML) durch Transport- und REST-API-Aufrufe bereitstellt. Diese Aufrufe wählen die richtigen Knoten und Ressourcen für jede ML-Anfrage aus und überwachen ML-Aufgaben, um die Verfügbarkeit sicherzustellen. Auf diese Weise können Sie bestehende Open-Source-ML-Algorithmen nutzen und den Aufwand für die Entwicklung neuer ML-Funktionen reduzieren. Weitere Informationen zum Plugin finden Sie in der OpenSearch Dokumentation unter Maschinelles Lernen. In diesem Kapitel wird beschrieben, wie Sie das Plugin mit Amazon OpenSearch Service verwenden.

Themen

- Amazon OpenSearch Service ML-Konnektoren für AWS-Services
- Amazon OpenSearch Service ML-Konnektoren für Plattformen von Drittanbietern
- Wird verwendet AWS CloudFormation , um Remote-Inferenz für die semantische Suche einzurichten
- ML Commons-Einstellungen werden nicht unterstützt
- OpenSearch Vorlagen für das Service Flow-Framework

Amazon OpenSearch Service ML-Konnektoren für AWS-Services

Wenn Sie Amazon OpenSearch Service Machine Learning (ML) Connectors mit einem anderen verwenden AWS-Service, müssen Sie eine IAM-Rolle einrichten, um Service sicher mit diesem OpenSearch Service zu verbinden. AWS-Services dass Sie einen Connector einrichten können, der Amazon SageMaker AI und Amazon Bedrock einschließt. In diesem Tutorial erfahren Sie, wie Sie einen Connector von OpenSearch Service zu SageMaker Runtime erstellen. Weitere Informationen zu Konnektoren finden Sie unter Unterstützte Konnektoren.

Themen

- Voraussetzungen
- Erstellen Sie einen OpenSearch Service-Connector

Voraussetzungen

Um einen Connector zu erstellen, benötigen Sie einen Amazon SageMaker AI-Domain-Endpunkt und eine IAM-Rolle, die OpenSearch Servicezugriff gewährt.

Richten Sie eine Amazon SageMaker AI-Domain ein

Informationen zur Bereitstellung Ihres Machine-Learning-Modells finden Sie unter Bereitstellen eines Modells in Amazon SageMaker AI im Amazon AI Developer Guide. SageMaker Notieren Sie sich die Endpunkt-URL für Ihr Modell, die Sie benötigen, um einen AI-Connector zu erstellen.

Erstellen einer IAM-Rolle

Richten Sie eine IAM-Rolle ein, um SageMaker Runtime-Berechtigungen an den Service zu OpenSearch delegieren. Informationen zum Erstellen einer neuen Rolle finden Sie unter Erstellen einer IAM-Rolle (Konsole) im IAM-Benutzerhandbuch. Optional können Sie eine bestehende Rolle verwenden, sofern sie über dieselben Rechte verfügt. Wenn Sie eine neue Rolle erstellen, anstatt eine AWS verwaltete Rolle zu verwenden, ersetzen Sie sie `opensearch-sagemaker-role` in diesem Tutorial durch den Namen Ihrer eigenen Rolle.

1. Fügen Sie Ihrer neuen Rolle die folgende verwaltete IAM-Richtlinie hinzu, damit OpenSearch Service auf Ihren SageMaker KI-Endpunkt zugreifen kann. Informationen zum Anhängen einer Richtlinie an eine Rolle finden Sie unter Hinzufügen von IAM-Identitätsberechtigungen.

   JSON

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

2. Folgen Sie den Anweisungen unter Vertrauensrichtlinie für Rollen ändern, um die Vertrauensstellung der Rolle zu bearbeiten. Sie müssen OpenSearch Service in der `Principal` Erklärung angeben:

   JSON

   ```
   {
   ```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "sts:AssumeRole"
            ],
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "opensearchservice.amazonaws.com"
                ]
            }
        }
    ]
}
```

Es wird empfohlen, die Bedingungsschlüssel `aws:SourceAccount` und die `aws:SourceArn` Bedingungsschlüssel zu verwenden, um den Zugriff auf eine bestimmte Domain zu beschränken. Das `SourceAccount` ist die AWS-Konto ID, die dem Besitzer der Domain gehört, und das `SourceArn` ist der ARN der Domain. Sie können der Vertrauensrichtlinie beispielsweise den folgenden Bedingungsblock hinzufügen:

```
"Condition": {
    "StringEquals": {
        "aws:SourceAccount": "account-id"
    },
    "ArnLike": {
        "aws:SourceArn": "arn:aws:es:region:account-id:domain/domain-name"
    }
}
```

Konfigurieren von Berechtigungen

Um den Connector zu erstellen, benötigen Sie die Erlaubnis, die IAM-Rolle an OpenSearch Service zu übergeben. Sie benötigen außerdem Zugriff auf die Aktion `es:ESHttpPost`. Um diese beiden Berechtigungen zu erteilen, fügen Sie die folgende Richtlinie an die IAM-Rolle an, deren Anmeldeinformationen zum Signieren der Anforderung verwendet werden:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::account-id:role/opensearch-sagemaker-role"
    },
    {
      "Effect": "Allow",
      "Action": "es:ESHttpPost",
      "Resource": "arn:aws:es:region:account-id:domain/domain-name/*"
    }
  ]
}
```

Wenn Ihr Benutzer oder Ihre Rolle nicht `iam:PassRole` berechtigt ist, Ihre Rolle weiterzugeben, kann es sein, dass beim Versuch, ein Repository im nächsten Schritt zu registrieren, ein Autorisierungsfehler auftritt.

Ordnen Sie die ML-Rolle in OpenSearch Dashboards zu (wenn Sie eine differenzierte Zugriffskontrolle verwenden)

Durch eine differenzierte Zugriffskontrolle wird beim Einrichten eines Konnektors ein zusätzlicher Schritt eingeführt. Auch wenn Sie die HTTP-Basisauthentifizierung für alle anderen Zwecke verwenden, müssen Sie die `ml_full_access`-Rolle Ihrer IAM-Rolle mit `iam:PassRole`-Berechtigungen zuordnen, um `opensearch-sagemaker-role` zu übergeben.

1. Navigieren Sie zum OpenSearch Dashboards-Plugin für Ihre OpenSearch Service-Domain. Sie finden den Dashboards-Endpunkt in Ihrem Domain-Dashboard in der OpenSearch Service-Konsole.
2. Wählen Sie im Hauptmenü Sicherheit, Rollen und dann die Rolle ml_full_access aus.
3. Wählen Sie Zugeordnete Benutzer, Mapping verwalten.
4. Fügen Sie unter Backend-Rollen den ARN der Rolle hinzu, die über Berechtigungen zur Weitergabe `opensearch-sagemaker-role` verfügt.

```
arn:aws:iam::account-id:role/role-name
```

5. Wählen Sie Zuordnen und bestätigen Sie, dass der Benutzer oder die Rolle unter Zugeordnete Benutzer angezeigt wird.

Erstellen Sie einen OpenSearch Service-Connector

Um einen Connector zu erstellen, senden Sie eine POST Anfrage an den Endpunkt der OpenSearch Service-Domäne. Sie können curl, den Python-Beispielclient, Postman oder eine andere Methode verwenden, um eine signierte Anfrage zu senden. Beachten Sie, dass Sie eine POST Anfrage in der Kibana-Konsole nicht verwenden können. Die Anfrage hat das folgende Format:

```
POST domain-endpoint/_plugins/_ml/connectors/_create
{
   "name": "sagemaker: embedding",
   "description": "Test connector for Sagemaker embedding model",
   "version": 1,
   "protocol": "aws_sigv4",
   "credential": {
      "roleArn": "arn:aws:iam::account-id:role/opensearch-sagemaker-role"
   },
   "parameters": {
      "region": "region",
      "service_name": "sagemaker"
   },
   "actions": [
      {
         "action_type": "predict",
         "method": "POST",
         "headers": {
            "content-type": "application/json"
         },
         "url": "https://runtime.sagemaker.region.amazonaws.com/endpoints/endpoint-id/
invocations",
         "request_body": "{ \"inputs\": { \"question\": \"${parameters.question}\",
 \"context\": \"${parameters.context}\" } }"
      }
   ]
}
```

Wenn sich Ihre Domain in einer Virtual Private Cloud (VPC) befindet, muss Ihr Computer mit der VPC verbunden sein, damit die Anfrage den AI-Connector erfolgreich erstellen kann. Der Zugriff auf eine VPC hängt von der Netzwerkkonfiguration ab, beinhaltet jedoch in der Regel eine Verbindung zu einem VPN- oder Unternehmensnetzwerk. Um zu überprüfen, ob Sie Ihre OpenSearch Service-Domain erreichen können, navigieren Sie `https://your-vpc-domain.region.es.amazonaws.com` in einem Webbrowser zu und überprüfen Sie, ob Sie die Standard-JSON-Antwort erhalten.

Beispiel für einen Python-Client

Der Python-Client ist einfacher zu automatisieren als eine HTTP-Anfrage und hat eine bessere Wiederverwendbarkeit. Um den AI-Konnektor mit dem Python-Client zu erstellen, speichern Sie den folgenden Beispielcode in einer Python-Datei. Der Client benötigt die `requests-aws4auth`Pakete AWS SDK für Python (Boto3)`requests`, und.

```
import boto3
import requests
from requests_aws4auth import AWS4Auth

host = 'domain-endpoint/'
region = 'region'
service = 'es'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
 session_token=credentials.token)

# Register repository
path = '_plugins/_ml/connectors/_create'
url = host + path

payload = {
   "name": "sagemaker: embedding",
   "description": "Test connector for Sagemaker embedding model",
   "version": 1,
   "protocol": "aws_sigv4",
   "credential": {
      "roleArn": "arn:aws:iam::account-id:role/opensearch-sagemaker-role"
   },
   "parameters": {
      "region": "region",
      "service_name": "sagemaker"
   },
```

```
   "actions": [
      {
         "action_type": "predict",
         "method": "POST",
         "headers": {
            "content-type": "application/json"
         },
         "url": "https://runtime.sagemaker.region.amazonaws.com/endpoints/endpoint-id/
invocations",
         "request_body": "{ \"inputs\": { \"question\": \"${parameters.question}\",
 \"context\": \"${parameters.context}\" } }"
      }
   ]
}
headers = {"Content-Type": "application/json"}

r = requests.post(url, auth=awsauth, json=payload, headers=headers)
print(r.status_code)
print(r.text)
```

Amazon OpenSearch Service ML-Konnektoren für Plattformen von Drittanbietern

In diesem Tutorial erfahren Sie, wie Sie einen Connector von OpenSearch Service zu Cohere erstellen. Weitere Informationen zu Konnektoren finden Sie unter Unterstützte Konnektoren.

Wenn Sie einen Amazon OpenSearch Service Machine Learning (ML) Connector mit einem externen Remote-Modell verwenden, müssen Sie Ihre spezifischen Autorisierungsdaten in speichern AWS Secrets Manager. Dies kann ein API-Schlüssel oder eine Kombination aus Benutzername und Passwort sein. Das bedeutet, dass Sie auch eine IAM-Rolle erstellen müssen, die es OpenSearch Service Access ermöglicht, aus Secrets Manager zu lesen.

Themen

- Voraussetzungen
- Erstellen Sie einen OpenSearch Service-Connector

Voraussetzungen

Um einen Connector für Cohere oder einen externen Anbieter mit OpenSearch Service zu erstellen, benötigen Sie eine IAM-Rolle, die dem OpenSearch Service Zugriff auf den Ort gewährt AWS Secrets Manager, an dem Sie Ihre Anmeldeinformationen speichern. Sie müssen Ihre Anmeldeinformationen auch in Secrets Manager speichern.

Erstellen einer IAM-Rolle

Richten Sie eine IAM-Rolle ein, um Secrets Manager Manager-Berechtigungen an den Service zu OpenSearch delegieren. Sie können auch die vorhandene `SecretManagerReadWrite` Rolle verwenden. Informationen zum Erstellen einer neuen Rolle finden Sie unter Erstellen einer IAM-Rolle (Konsole) im IAM-Benutzerhandbuch. Wenn Sie eine neue Rolle erstellen, anstatt eine AWS verwaltete Rolle zu verwenden, ersetzen Sie sie `opensearch-secretmanager-role` in diesem Tutorial durch den Namen Ihrer eigenen Rolle.

1. Fügen Sie Ihrer neuen Rolle die folgende verwaltete IAM-Richtlinie hinzu, damit OpenSearch Service auf Ihre Secrets Manager Manager-Werte zugreifen kann. Informationen zum Anhängen einer Richtlinie an eine Rolle finden Sie unter Hinzufügen von IAM-Identitätsberechtigungen.

   JSON

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

2. Folgen Sie den Anweisungen unter Vertrauensrichtlinie für Rollen ändern, um die Vertrauensstellung der Rolle zu bearbeiten. Sie müssen OpenSearch Service in der `Principal` Erklärung angeben:

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "sts:AssumeRole"
            ],
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "opensearchservice.amazonaws.com"
                ]
            }
        }
    ]
}
```

Es wird empfohlen, die Bedingungsschlüssel `aws:SourceAccount` und die `aws:SourceArn` Bedingungsschlüssel zu verwenden, um den Zugriff auf eine bestimmte Domäne zu beschränken. Das `SourceAccount` ist die AWS-Konto ID, die dem Besitzer der Domain gehört, und das `SourceArn` ist der ARN der Domain. Sie können der Vertrauensrichtlinie beispielsweise den folgenden Bedingungsblock hinzufügen:

```
"Condition": {
    "StringEquals": {
        "aws:SourceAccount": "account-id"
    },
    "ArnLike": {
        "aws:SourceArn": "arn:aws:es:region:account-id:domain/domain-name"
    }
}
```

Konfigurieren von Berechtigungen

Um den Connector zu erstellen, benötigen Sie die Erlaubnis, die IAM-Rolle an OpenSearch Service zu übergeben. Sie benötigen außerdem Zugriff auf die Aktion `es:ESHttpPost`. Um diese

beiden Berechtigungen zu erteilen, fügen Sie die folgende Richtlinie an die IAM-Rolle an, deren Anmeldeinformationen zum Signieren der Anforderung verwendet werden:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::account-id:role/opensearch-secretmanager-role"
    },
    {
      "Effect": "Allow",
      "Action": "es:ESHttpPost",
      "Resource": "arn:aws:es:region:account-id:domain/domain-name/*"
    }
  ]
}
```

Wenn Ihr Benutzer oder Ihre Rolle nicht `iam:PassRole` berechtigt ist, Ihre Rolle weiterzugeben, kann es sein, dass beim Versuch, ein Repository im nächsten Schritt zu registrieren, ein Autorisierungsfehler auftritt.

Richten Sie ein AWS Secrets Manager

Informationen zum Speichern Ihrer Autorisierungsdaten in Secrets Manager finden Sie unter Create an AWS Secrets Manager Secret im AWS Secrets Manager Benutzerhandbuch.

Nachdem Secrets Manager Ihr Schlüssel-Wert-Paar als Geheimnis akzeptiert hat, erhalten Sie einen ARN mit dem Format:. `arn:aws:secretsmanager:us-west-2:123456789012:secret:MySecret-a1b2c3` Notieren Sie sich diesen ARN, wie Sie ihn verwenden, und Ihren Schlüssel, wenn Sie im nächsten Schritt einen Connector erstellen.

Ordnen Sie die ML-Rolle in OpenSearch Dashboards zu (wenn Sie eine differenzierte Zugriffskontrolle verwenden)

Durch eine differenzierte Zugriffskontrolle wird beim Einrichten eines Konnektors ein zusätzlicher Schritt eingeführt. Auch wenn Sie die HTTP-Basisauthentifizierung für alle anderen Zwecke

verwenden, müssen Sie die `ml_full_access`-Rolle Ihrer IAM-Rolle mit `iam:PassRole`-Berechtigungen zuordnen, um `opensearch-sagemaker-role` zu übergeben.

1. Navigieren Sie zum OpenSearch Dashboards-Plugin für Ihre OpenSearch Service-Domain. Sie finden den Dashboards-Endpunkt in Ihrem Domain-Dashboard in der OpenSearch Service-Konsole.
2. Wählen Sie im Hauptmenü Sicherheit, Rollen und dann die Rolle ml_full_access aus.
3. Wählen Sie Zugeordnete Benutzer, Mapping verwalten.
4. Fügen Sie unter Backend-Rollen den ARN der Rolle hinzu, die über Berechtigungen zur Weitergabe `opensearch-sagemaker-role` verfügt.

   ```
   arn:aws:iam::account-id:role/role-name
   ```

5. Wählen Sie Zuordnen und bestätigen Sie, dass der Benutzer oder die Rolle unter Zugeordnete Benutzer angezeigt wird.

Erstellen Sie einen OpenSearch Service-Connector

Um einen Connector zu erstellen, senden Sie eine `POST` Anfrage an den Endpunkt der OpenSearch Service-Domäne. Sie können curl, den Python-Beispielclient, Postman oder eine andere Methode verwenden, um eine signierte Anfrage zu senden. Beachten Sie, dass Sie eine `POST` Anfrage in der Kibana-Konsole nicht verwenden können. Die Anfrage hat das folgende Format:

```
POST domain-endpoint/_plugins/_ml/connectors/_create
{
    "name": "Cohere Connector: embedding",
    "description": "The connector to cohere embedding model",
    "version": 1,
    "protocol": "http",
    "credential": {
        "secretArn": "arn:aws:secretsmanager:region:account-id:secret:cohere-key-id",
        "roleArn": "arn:aws:iam::account-id:role/opensearch-secretmanager-role"
    },
    "actions": [
        {
            "action_type": "predict",
            "method": "POST",
            "url": "https://api.cohere.ai/v1/embed",
            "headers": {
```

```
                "Authorization": "Bearer ${credential.secretArn.cohere-key-used-in-
secrets-manager}"
            },
            "request_body": "{ \"texts\": ${parameters.texts}, \"truncate\": \"END\" }"
        }
    ]
}
```

Der Anfragetext für diese Anfrage unterscheidet sich in zweierlei Hinsicht von dem einer Open-Source-Connector-Anfrage. Innerhalb des `credential` Felds übergeben Sie den ARN für die IAM-Rolle, die es OpenSearch Service ermöglicht, aus Secrets Manager zu lesen, zusammen mit dem ARN für welches Geheimnis. In `headers` diesem Feld verweisen Sie auf das Geheimnis, indem Sie den geheimen Schlüssel und die Tatsache verwenden, dass es aus einem ARN stammt.

Wenn sich Ihre Domain in einer Virtual Private Cloud (VPC) befindet, muss Ihr Computer mit der VPC verbunden sein, damit die Anfrage den AI-Connector erfolgreich erstellen kann. Der Zugriff auf eine VPC hängt von der Netzwerkkonfiguration ab, beinhaltet jedoch in der Regel eine Verbindung zu einem VPN- oder Unternehmensnetzwerk. Um zu überprüfen, ob Sie Ihre OpenSearch Service-Domain erreichen können, navigieren Sie `https://your-vpc-domain.region.es.amazonaws.com` in einem Webbrowser zu und überprüfen Sie, ob Sie die Standard-JSON-Antwort erhalten.

Beispiel für einen Python-Client

Der Python-Client ist einfacher zu automatisieren als eine HTTP-Anfrage und hat eine bessere Wiederverwendbarkeit. Um den AI-Konnektor mit dem Python-Client zu erstellen, speichern Sie den folgenden Beispielcode in einer Python-Datei. Der Client benötigt die `requests-aws4auth`Pakete AWS SDK für Python (Boto3)`requests`, und.

```
import boto3
import requests
from requests_aws4auth import AWS4Auth

host = 'domain-endpoint/'
region = 'region'
service = 'es'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
 session_token=credentials.token)
```

```
path = '_plugins/_ml/connectors/_create'
url = host + path

payload = {
    "name": "Cohere Connector: embedding",
    "description": "The connector to cohere embedding model",
    "version": 1,
    "protocol": "http",
    "credential": {
        "secretArn": "arn:aws:secretsmanager:region:account-id:secret:cohere-key-id",
        "roleArn": "arn:aws:iam::account-id:role/opensearch-secretmanager-role"
    },
    "actions": [
        {
            "action_type": "predict",
            "method": "POST",
            "url": "https://api.cohere.ai/v1/embed",
            "headers": {
                "Authorization": "Bearer ${credential.secretArn.cohere-key-used-in-
secrets-manager}"
            },
            "request_body": "{ \"texts\": ${parameters.texts}, \"truncate\": \"END\" }"
        }
    ]
}

headers = {"Content-Type": "application/json"}

r = requests.post(url, auth=awsauth, json=payload, headers=headers)
print(r.status_code)
print(r.text)
```

Wird verwendet AWS CloudFormation , um Remote-Inferenz für die semantische Suche einzurichten

Ab OpenSearch Version 2.9 können Sie Remote-Inferenz mit semantischer Suche verwenden, um Ihre eigenen Modelle für maschinelles Lernen (ML) zu hosten. Remote Inference verwendet das ML Commons-Plugin, damit Sie Ihre Modellinferenzen remote auf ML-Diensten wie Amazon BedRock hosten Amazon SageMaker AI und sie über ML-Konnektoren mit Amazon OpenSearch Service verbinden können.

Um die Einrichtung von Remote-Inferenzen zu vereinfachen, stellt Amazon OpenSearch Service eine AWS CloudFormationVorlage in der Konsole bereit. CloudFormation ist eine AWS-Service , mit der Sie Ressourcen von Drittanbietern modellieren, bereitstellen AWS und verwalten können, indem Sie Infrastruktur als Code behandeln.

Die OpenSearch CloudFormation Vorlage automatisiert den Prozess der Modellbereitstellung für Sie, sodass Sie auf einfache Weise ein Modell in Ihrer OpenSearch Service-Domain erstellen und dann die Modell-ID verwenden können, um Daten aufzunehmen und neuronale Suchabfragen auszuführen.

Wenn Sie neuronale Sparse-Encoder mit OpenSearch Service Version 2.12 und höher verwenden, empfehlen wir, das Tokenizer-Modell lokal zu verwenden, anstatt es remote bereitzustellen. Weitere Informationen finden Sie in der Dokumentation unter Sparse-Kodierungsmodelle. OpenSearch

Themen

- Voraussetzungen
- Amazon SageMaker AI Vorlagen
- Amazon Bedrock-Vorlagen

Voraussetzungen

Um eine CloudFormation Vorlage mit OpenSearch Service zu verwenden, müssen Sie die folgenden Voraussetzungen erfüllen.

Richten Sie eine OpenSearch Dienstdomäne ein

Bevor Sie eine CloudFormation Vorlage verwenden können, müssen Sie eine Amazon OpenSearch Service-Domain mit Version 2.9 oder höher und aktivierter detaillierter Zugriffskontrolle einrichten. Erstellen Sie eine OpenSearch Service-Backend-Rolle, um dem ML Commons-Plugin die Erlaubnis zu erteilen, Ihren Connector für Sie zu erstellen.

Die CloudFormation Vorlage erstellt für Sie eine Lambda-IAM-Rolle mit dem Standardnamen`LambdaInvokeOpenSearchMLCommonsRole`, den Sie überschreiben können, wenn Sie einen anderen Namen wählen möchten. Nachdem die Vorlage diese IAM-Rolle erstellt hat, müssen Sie der Lambda-Funktion die Erlaubnis erteilen, Ihre OpenSearch Service-Domain aufzurufen. Ordnen Sie dazu die benannte Rolle mit `ml_full_access` den folgenden Schritten Ihrer OpenSearch Service-Backend-Rolle zu:

1. Navigieren Sie zum OpenSearch Dashboards-Plugin für Ihre OpenSearch Service-Domain. Sie finden den Dashboards-Endpunkt in Ihrem Domain-Dashboard in der OpenSearch Service-Konsole.
2. Wählen Sie im Hauptmenü Sicherheit, Rollen und dann die Rolle ml_full_access aus.
3. Wählen Sie Zugeordnete Benutzer, Mapping verwalten.
4. Fügen Sie unter Backend-Rollen den ARN der Lambda-Rolle hinzu, für die eine Berechtigung zum Aufrufen Ihrer Domain erforderlich ist.

   ```
   arn:aws:iam::account-id:role/role-name
   ```

5. Wählen Sie Zuordnen und bestätigen Sie, dass der Benutzer oder die Rolle unter Zugeordnete Benutzer angezeigt wird.

Nachdem Sie die Rolle zugeordnet haben, navigieren Sie zur Sicherheitskonfiguration Ihrer Domain und fügen Sie die Lambda IAM-Rolle zu Ihrer OpenSearch Servicezugriffsrichtlinie hinzu.

Aktivieren Sie die Berechtigungen auf Ihrem AWS-Konto

Sie AWS-Konto müssen über die Zugriffsberechtigung CloudFormation und Lambda verfügen, zusammen mit dem, was AWS-Service Sie für Ihre Vorlage wählen — entweder SageMaker Runtime oder Amazon. BedRock

Wenn Sie Amazon Bedrock verwenden, müssen Sie auch Ihr Modell registrieren. Informationen zur Registrierung Ihres Modells finden Sie unter Modellzugriff im Amazon Bedrock-Benutzerhandbuch.

Wenn Sie Ihren eigenen Amazon S3 S3-Bucket verwenden, um Modellartefakte bereitzustellen, müssen Sie die CloudFormation IAM-Rolle zu Ihrer S3-Zugriffsrichtlinie hinzufügen. Informationen finden Sie im Abschnitt Hinzufügen und Entfernen von IAM-Identitätsberechtigungen im -IAM-Benutzerhandbuch.

Amazon SageMaker AI Vorlagen

Die Amazon SageMaker CloudFormation AI-Vorlagen definieren mehrere AWS Ressourcen, um das neuronale Plugin und die semantische Suche für Sie einzurichten.

Verwenden Sie zunächst die SageMaker Vorlage Integration mit Texteinbettungsmodellen über Amazon, um ein Texteinbettungsmodell in SageMaker Runtime als Server bereitzustellen. Wenn Sie keinen Modellendpunkt angeben, CloudFormation erstellt eine IAM-Rolle, die es SageMaker Runtime ermöglicht, Modellartefakte von Amazon S3 herunterzuladen und auf dem Server bereitzustellen.

Wenn Sie einen Endpunkt angeben, CloudFormation erstellt eine IAM-Rolle, die der Lambda-Funktion den Zugriff auf die OpenSearch Dienstdomäne ermöglicht oder, falls die Rolle bereits vorhanden ist, aktualisiert und wiederverwendet. Der Endpunkt dient dem Remote-Modell, das für den ML-Connector mit dem ML Commons-Plugin verwendet wird.

Verwenden Sie als Nächstes die Vorlage Integration with Sparse Encoders through Amazon Sagemaker, um eine Lambda-Funktion zu erstellen, mit der Ihre Domain Remote Inference Connectors einrichtet. Nachdem der Konnektor in OpenSearch Service erstellt wurde, kann die Remote-Inferenz mithilfe des Remote-Modells in Runtime eine semantische Suche ausführen. SageMaker Die Vorlage gibt Ihnen die Modell-ID in Ihrer Domain zurück, sodass Sie mit der Suche beginnen können.

Um die Amazon SageMaker CloudFormation AI-Vorlagen zu verwenden

1. Öffnen Sie die Amazon OpenSearch Service-Konsole zu https://console.aws.amazon.com/aos/Hause.
2. Wählen Sie in der linken Navigationsleiste Integrationen aus.
3. Wählen Sie unter jeder Amazon SageMaker AI-Vorlage die Optionen Domain konfigurieren, Public Domain konfigurieren aus.
4. Folgen Sie der Aufforderung in der CloudFormation Konsole, um Ihren Stack bereitzustellen und ein Modell einzurichten.

> **Note**
>
> OpenSearch Der Service bietet auch eine separate Vorlage zur Konfiguration der VPC-Domäne. Wenn Sie diese Vorlage verwenden, müssen Sie die VPC-ID für die Lambda-Funktion angeben.

Amazon Bedrock-Vorlagen

Ähnlich wie die Amazon SageMaker CloudFormation AI-Vorlagen stellt die Amazon CloudFormation Bedrock-Vorlage die AWS Ressourcen bereit, die zum Erstellen von Verbindungen zwischen OpenSearch Service und Amazon Bedrock benötigt werden.

Zunächst erstellt die Vorlage eine IAM-Rolle, die es der future Lambda-Funktion ermöglicht, auf Ihre OpenSearch Service-Domain zuzugreifen. Die Vorlage erstellt dann die Lambda-Funktion, bei der die

Domain mithilfe des ML Commons-Plugins einen Konnektor erstellt. Nachdem OpenSearch Service den Connector erstellt hat, ist die Einrichtung der Remote-Inferenz abgeschlossen und Sie können semantische Suchen mithilfe der Amazon Bedrock API-Operationen ausführen.

Beachten Sie, dass Sie kein Modell für SageMaker Runtime bereitstellen müssen, da Amazon Bedrock seine eigenen ML-Modelle hostet. Stattdessen verwendet die Vorlage einen vordefinierten Endpunkt für Amazon Bedrock und überspringt die Schritte zur Endpunktbereitstellung.

Um die Amazon CloudFormation Bedrock-Vorlage zu verwenden

1. Öffnen Sie die Amazon OpenSearch Service-Konsole zu https://console.aws.amazon.com/aos/Hause.
2. Wählen Sie in der linken Navigationsleiste Integrationen aus.
3. Wählen Sie unter Integrate with Amazon Titan Text Embeddings model through Amazon Bedrock die Optionen Domain konfigurieren, Public domain konfigurieren aus.
4. Folgen Sie der Aufforderung, um Ihr Modell einzurichten.

> **Note**
>
> OpenSearch Der Service bietet auch eine separate Vorlage zur Konfiguration der VPC-Domäne. Wenn Sie diese Vorlage verwenden, müssen Sie die VPC-ID für die Lambda-Funktion angeben.

Darüber hinaus bietet OpenSearch Service die folgenden Amazon Bedrock-Vorlagen für die Verbindung mit dem Cohere-Modell und dem multimodalen Einbettungsmodell von Amazon Titan:

- `Integration with Cohere Embed through Amazon Bedrock`
- `Integrate with Amazon Bedrock Titan Multi-modal`

ML Commons-Einstellungen werden nicht unterstützt

Amazon OpenSearch Service unterstützt die Verwendung der folgenden ML Commons-Einstellungen nicht:

- `plugins.ml_commons.allow_registering_model_via_url`
- `plugins.ml_commons.allow_registering_model_via_local_file`

> **Important**
>
> Deaktivieren Sie auf Produktionsclustern die Cluster-Einstellung nicht `plugins.ml_commons.only_run_on_ml_node` (setzen Sie sie nicht auf`false`). Die Option zur Deaktivierung dieses Schutzes dient der Erleichterung der Entwicklung, aber Produktionscluster sollten die Konnektoren verwenden. Weitere Informationen finden Sie unter the section called “Anschlüsse für AWS-Services”.

Weitere Informationen zu den ML Commons-Einstellungen finden Sie unter ML Commons-Cluster-Einstellungen.

OpenSearch Vorlagen für das Service Flow-Framework

Mit den Amazon OpenSearch Service Flow Framework-Vorlagen können Sie komplexe Aufgaben zur Einrichtung und Vorverarbeitung von OpenSearch Services automatisieren, indem sie Vorlagen für gängige Anwendungsfälle bereitstellen. Sie können beispielsweise Flow-Framework-Vorlagen verwenden, um Einrichtungsaufgaben für maschinelles Lernen zu automatisieren. Die Amazon OpenSearch Service Flow Framework-Vorlagen bieten eine kompakte Beschreibung des Einrichtungsprozesses in einem JSON- oder YAML-Dokument. Diese Vorlagen beschreiben automatisierte Workflow-Konfigurationen für Konversationschats oder die Generierung von Abfragen, KI-Konnektoren, Tools, Agenten und andere Komponenten, die den OpenSearch Service für die Backend-Nutzung für generative Modelle vorbereiten.

Die Vorlagen für das Amazon OpenSearch Service Flow Framework können an Ihre spezifischen Bedürfnisse angepasst werden. Ein Beispiel für eine benutzerdefinierte Flow-Framework-Vorlage finden Sie unter Flow-Framework. Vom OpenSearch Service bereitgestellte Vorlagen finden Sie unter Workflow-Vorlagen. Eine umfassende Dokumentation, einschließlich detaillierter Schritte, einer API-Referenz und einer Referenz aller verfügbaren Einstellungen, finden Sie in der Open-Source-Dokumentation unter Automatisieren der Konfiguration. OpenSearch

> **Note**
>
> Flow-Framework unterstützt keine Backend-Rollenfilterung für OpenSearch Service 2.17.

ML-Konnektoren im Service erstellen OpenSearch

Mit Amazon OpenSearch Service Flow Framework-Vorlagen können Sie ML-Konnektoren konfigurieren und installieren, indem Sie die in ml-commons angebotene Create Connector-API verwenden. Sie können ML-Konnektoren verwenden, um OpenSearch Service mit anderen AWS Diensten oder Plattformen von Drittanbietern zu verbinden. Weitere Informationen dazu finden Sie unter Connectors für ML-Plattformen von Drittanbietern erstellen. Die Amazon OpenSearch Service Flow Framework-API ermöglicht Ihnen die Automatisierung von Aufgaben zur Einrichtung und Vorverarbeitung von OpenSearch Services und kann zur Erstellung von ML-Konnektoren verwendet werden.

Bevor Sie einen Connector in OpenSearch Service erstellen können, müssen Sie Folgendes tun:

- Erstellen Sie eine Amazon SageMaker AI-Domain.
- Erstellen Sie eine IAM-Rolle.
- Konfigurieren Sie die Berechtigung zum Übergeben von Rollen.
- Ordnen Sie die Flow-Framework- und ML-Commons-Rollen in OpenSearch Dashboards zu.

Weitere Informationen zur Einrichtung von ML-Konnektoren für AWS Services finden Sie unter Amazon OpenSearch Service ML-Konnektoren für AWS Services. Weitere Informationen zur Verwendung von OpenSearch Service ML-Konnektoren mit Plattformen von Drittanbietern finden Sie unter Amazon OpenSearch Service ML-Konnektoren für Drittanbieterplattformen.

Einen Connector über einen Flow-Framework-Service erstellen

Um eine Flow-Framework-Vorlage mit Connector zu erstellen, müssen Sie eine `POST` Anfrage an Ihren OpenSearch Service-Domain-Endpunkt senden. Sie können cURL, einen Python-Beispielclient, Postman oder eine andere Methode verwenden, um eine signierte Anfrage zu senden. Die `POST` Anfrage hat das folgende Format:

```
POST /_plugins/_flow_framework/workflow
{
  "name": "Deploy Claude Model",
  "description": "Deploy a model using a connector to Claude",
  "use_case": "PROVISION",
  "version": {
    "template": "1.0.0",
    "compatibility": [
      "2.12.0",
```

```
      "3.0.0"
    ]
  },
  "workflows": {
    "provision": {
      "nodes": [
        {
          "id": "create_claude_connector",
          "type": "create_connector",
          "user_inputs": {
            "name": "Claude Instant Runtime Connector",
            "version": "1",
            "protocol": "aws_sigv4",
            "description": "The connector to BedRock service for Claude model",
            "actions": [
              {
                "headers": {
                  "x-amz-content-sha256": "required",
                  "content-type": "application/json"
                },
                "method": "POST",
                "request_body": "{ \"prompt\":\"${parameters.prompt}\",
 \"max_tokens_to_sample\":${parameters.max_tokens_to_sample},
 \"temperature\":${parameters.temperature},  \"anthropic_version\":
\"${parameters.anthropic_version}\" }",
                "action_type": "predict",
                "url": "https://bedrock-runtime.us-west-2.amazonaws.com/model/
anthropic.claude-instant-v1/invoke"
              }
            ],
            "credential": {
                "roleArn": "arn:aws:iam::account-id:role/opensearch-secretmanager-
role"
             },
            "parameters": {
              "endpoint": "bedrock-runtime.us-west-2.amazonaws.com",
              "content_type": "application/json",
              "auth": "Sig_V4",
              "max_tokens_to_sample": "8000",
              "service_name": "bedrock",
              "temperature": "0.0001",
              "response_filter": "$.completion",
              "region": "us-west-2",
              "anthropic_version": "bedrock-2023-05-31"
```

```
            }
          }
        }
      ]
    }
  }
}
```

Wenn sich Ihre Domain in einer Virtual Private Cloud (Amazon VPC) befindet, müssen Sie mit der Amazon VPC verbunden sein, damit die Anfrage den AI-Connector erfolgreich erstellen kann. Der Zugriff auf eine Amazon VPC hängt von der Netzwerkkonfiguration ab, beinhaltet jedoch in der Regel eine Verbindung zu einem VPN- oder Unternehmensnetzwerk. Um zu überprüfen, ob Sie Ihre OpenSearch Service-Domain erreichen können, navigieren Sie `https://`*`your-vpc-domain`*`.`*`region`*`.es.amazonaws.com` in einem Webbrowser zu und stellen Sie sicher, dass Sie die Standard-JSON-Antwort erhalten. (Ersetzen Sie die *`placeholder text`* durch Ihre eigenen Werte.

Beispiel für einen Python-Client

Der Python-Client ist einfacher zu automatisieren als eine HTTP Anfrage und hat eine bessere Wiederverwendbarkeit. Um den AI-Konnektor mit dem Python-Client zu erstellen, speichern Sie den folgenden Beispielcode in einer Python-Datei. Der Client benötigt das AWS SDK for Python (Boto3), die Pakete requests:Http for Humans und requests-aws4auth 1.2.3.

```
import boto3
import requests
from requests_aws4auth import AWS4Auth

host = 'domain-endpoint/'
region = 'region'
service = 'es'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
 session_token=credentials.token)

path = '_plugins/_flow_framework/workflow'
url = host + path

payload = {
  "name": "Deploy Claude Model",
  "description": "Deploy a model using a connector to Claude",
  "use_case": "PROVISION",
```

```
  "version": {
    "template": "1.0.0",
    "compatibility": [
      "2.12.0",
      "3.0.0"
    ]
  },
  "workflows": {
    "provision": {
      "nodes": [
        {
          "id": "create_claude_connector",
          "type": "create_connector",
          "user_inputs": {
            "name": "Claude Instant Runtime Connector",
            "version": "1",
            "protocol": "aws_sigv4",
            "description": "The connector to BedRock service for Claude model",
            "actions": [
              {
                "headers": {
                  "x-amz-content-sha256": "required",
                  "content-type": "application/json"
                },
                "method": "POST",
                "request_body": "{ \"prompt\":\"${parameters.prompt}\",
 \"max_tokens_to_sample\":${parameters.max_tokens_to_sample},
 \"temperature\":${parameters.temperature},  \"anthropic_version\":
\"${parameters.anthropic_version}\" }",
                "action_type": "predict",
                "url": "https://bedrock-runtime.us-west-2.amazonaws.com/model/
anthropic.claude-instant-v1/invoke"
              }
            ],
            "credential": {
                "roleArn": "arn:aws:iam::account-id:role/opensearch-secretmanager-
role"
             },
            "parameters": {
              "endpoint": "bedrock-runtime.us-west-2.amazonaws.com",
              "content_type": "application/json",
              "auth": "Sig_V4",
              "max_tokens_to_sample": "8000",
              "service_name": "bedrock",
```

```
              "temperature": "0.0001",
              "response_filter": "$.completion",
              "region": "us-west-2",
              "anthropic_version": "bedrock-2023-05-31"
            }
          }
        }
      ]
    }
  }
}

headers = {"Content-Type": "application/json"}

r = requests.post(url, auth=awsauth, json=payload, headers=headers)
print(r.status_code)
print(r.text)
```

Vordefinierte Workflow-Vorlagen

Amazon OpenSearch Service bietet mehrere Workflow-Vorlagen für einige gängige Anwendungsfälle des maschinellen Lernens (ML). Die Verwendung einer Vorlage vereinfacht komplexe Setups und bietet viele Standardwerte für Anwendungsfälle wie semantische Suche oder Konversationssuche. Sie können eine Workflow-Vorlage angeben, wenn Sie die Create Workflow API aufrufen.

- Um eine vom OpenSearch Service bereitgestellte Workflow-Vorlage zu verwenden, geben Sie den Anwendungsfall der Vorlage als `use_case` Abfrageparameter an.
- Um eine benutzerdefinierte Workflow-Vorlage zu verwenden, geben Sie die vollständige Vorlage im Anfragetext an. Ein Beispiel für eine benutzerdefinierte Vorlage finden Sie in einer JSON-Beispielvorlage oder einer YAML-Beispielvorlage.

Anwendungsfälle für Vorlagen

Diese Tabelle bietet einen Überblick über die verschiedenen verfügbaren Vorlagen, eine Beschreibung der Vorlagen und die erforderlichen Parameter.

Anwendungsfall für Vorlagen	Beschreibung	Erforderliche Parameter
`bedrock_titan_embedding_model_deploy`	Erstellt ein Amazon Bedrock-Einbettungsmodell und stellt es bereit (standardmäßig `titan-embed-text-v1`	`create_connector.credential.roleArn`
`bedrock_titan_embedding_model_deploy`	Erstellt und implementiert ein multimodales Einbettungsmodell von Amazon Bedrock (standardmäßig `titan-embed-text-v1`	`create_connector.credential.roleArn`
`cohere_embedding_model_deploy`	Erstellt ein Cohere-Einbettungsmodell und stellt es bereit (standardmäßig 3.0). embed-english-v	`create_connector.credential.roleArn` , `create_connector.credential.secretArn`
`cohere_chat_model_deploy`	Erstellt ein Cohere-Chat-Modell und stellt es bereit (standardmäßig Cohere Command).	`create_connector.credential.roleArn` , `create_connector.credential.secretArn`
`open_ai_embedding_model_deploy`	Erzeugt und implementiert ein OpenAI-Einbettungsmodell (standardmäßig -002). text-embedding-ada	`create_connector.credential.roleArn` , `create_connector.credential.secretArn`
`openai_chat_model_deploy`	Erzeugt und implementiert ein OpenAI-Chat-Modell (standardmäßig gpt-3.5-Turbo).	`create_connector.credential.roleArn` , `create_connector.credential.secretArn`
`semantic_search_with_cohere`	Konfiguriert die semantische Suche und stellt ein Cohere-Einbettungsmodell bereit. Sie müssen den API-	`create_connector.credential.roleArn` , `create_connector.credential.secretArn`

Anwendungsfall für Vorlagen	Beschreibung	Erforderliche Parameter
`_embedding`	Schlüssel für das Cohere-Modell angeben.	
`semantic_search_with_cohere_embedding_query_enricher`	Konfiguriert die semantische Suche und stellt ein Cohere-Einbettungsmodell bereit. Fügt einen query_enricher-Suchprozessor hinzu, der eine Standardmodell-ID für neuronale Abfragen festlegt. Sie müssen den API-Schlüssel für das Cohere-Modell angeben.	`create_connector.credential.roleArn` , `create_connector.credential.secretArn`
`multimodal_search_with_bedrock_titan`	Stellt ein multimodales Amazon Bedrock-Modell bereit und konfiguriert eine Aufnahme-Pipeline mit einem text_image_embedding-Prozessor und einem k-NN-Index für die multimodale Suche. Sie müssen Ihre Anmeldeinformationen angeben. AWS	`create_connector.credential.roleArn`

> **Note**
>
> Für alle Vorlagen, die einen geheimen ARN benötigen, wird das Geheimnis standardmäßig mit dem Schlüsselnamen „key“ in AWS Secrets Manager gespeichert.

Standardvorlagen mit vortrainierten Modellen

Amazon OpenSearch Service bietet zwei zusätzliche Standard-Workflow-Vorlagen, die im OpenSearch Open-Source-Service nicht verfügbar sind.

Anwendungsfall für Vorlagen	Beschreibung
`semantic_search_with_local_model`	Konfiguriert die semantische Suche und stellt ein vortrainiertes Modell bereit (). `msmarco-distilbert-base-tas-b` Fügt einen `neural_query_enricher` Suchprozessor hinzu, der eine Standardmodell-ID für neuronale Abfragen festlegt und einen verknüpften k-NN-Index namens " erstellt. my-nlp-index
`hybrid_search_with_local_model`	Konfiguriert die Hybridsuche und stellt ein vortrainiertes Modell bereit (). `msmarco-distilbert-base-tas-b` Fügt einen `neural_query_enricher` Suchprozessor hinzu, der eine Standardmodell-ID für neuronale Abfragen festlegt und einen verknüpften k-NN-Index namens " erstellt. my-nlp-index

Konfigurieren von Berechtigungen

Wenn Sie eine neue Domain mit Version 2.13 oder höher erstellen, sind die Berechtigungen bereits vorhanden. Wenn Sie Flow Framework auf einer bereits vorhandenen OpenSearch Service-Domain mit Version 2.11 oder früher aktivieren, die Sie dann auf Version 2.13 oder höher aktualisieren, müssen Sie die Rolle definieren. `flow_framework_manager` Benutzer ohne Administratorrechte müssen dieser Rolle zugeordnet werden, um Warm-Indizes in Domains mithilfe einer fein abgestuften Zugriffskontrolle zu verwalten. Führen Sie die folgenden Schritte aus, um die `flow_framework_manager`-Rolle manuell zu erstellen:

1. Gehen Sie in OpenSearch Dashboards zu Sicherheit und wählen Sie Berechtigungen aus.
2. Wählen Sie Aktionsgruppe erstellen und konfigurieren Sie die folgenden Gruppen:

Group name (Gruppenname)	Berechtigungen
`flow_framework_full_access`	• `cluster:admin/opensearch/flow_framework/*` • `cluster_monitor`
`flow_framework_read_accesss`	• `cluster:admin/opensearch/flow_framework/workflow/get` • `cluster:admin/opensearch/flow_framework/workflow/search` • `cluster:admin/opensearch/flow_framework/workflow_state/get` • `cluster:admin/opensearch/flow_framework/workflow_state/search`

3. Wählen Sie Rollen und Rolle erstellen.
4. Nennen Sie die Rolle flow_framework_manager.
5. Wählen Sie für Clusterberechtigungen `flow_framework_full_access` und `flow_framework_read_access` aus.
6. Geben Sie für Index * ein.
7. Wählen Sie für Indexberechtigungen `indices:admin/aliases/get`, `indices:admin/mappings/get` und `indices_monitor` aus.
8. Wählen Sie Erstellen aus.
9. Nachdem Sie die Rolle erstellt haben, ordnen Sie sie einer beliebigen Benutzer- oder Backend-Rolle zu, die die Flow-Framework-Indizes verwaltet.

Sicherheitsanalysen für Amazon OpenSearch Service

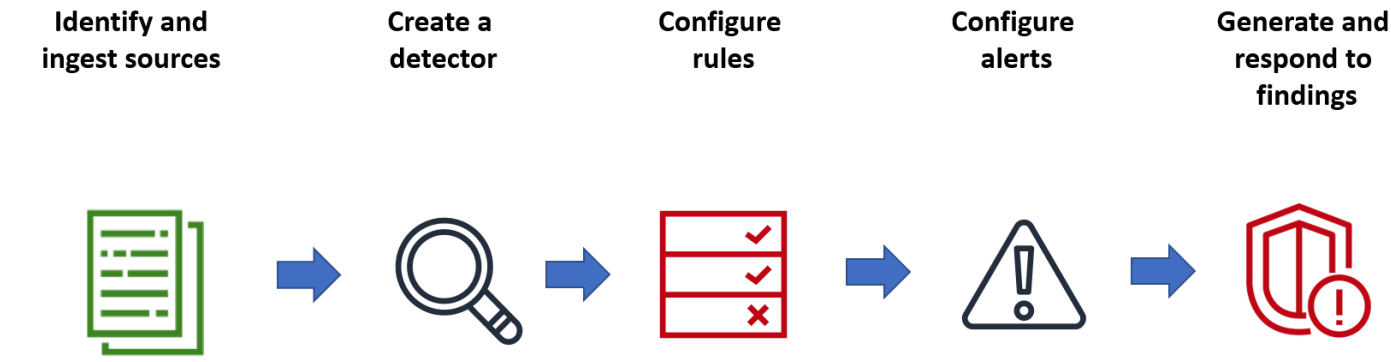
Security Analytics ist eine OpenSearch Lösung, die Einblick in die Infrastruktur Ihres Unternehmens bietet, ungewöhnliche Aktivitäten überwacht, potenzielle Sicherheitsbedrohungen in Echtzeit erkennt und Warnmeldungen an vorkonfigurierte Ziele auslöst. Sie können anhand Ihrer Sicherheitsereignisprotokolle nach böswilligen Aktivitäten Ausschau halten, indem Sie die Sicherheitsregeln kontinuierlich auswerten und die automatisch generierten Sicherheitsergebnisse überprüfen. Darüber hinaus kann Security Analytics automatische Warnmeldungen generieren und diese an einen bestimmten Benachrichtigungskanal wie Slack oder E-Mail senden.

Sie können das Security Analytics-Plugin verwenden, um häufig auftretende Bedrohungen zu erkennen out-of-the-box und wichtige Sicherheitsinformationen aus Ihren vorhandenen Sicherheitsereignisprotokollen wie Firewallprotokollen, Windows-Protokollen und Authentifizierungsprotokollen zu gewinnen. Um Security Analytics verwenden zu können, muss auf Ihrer Domain OpenSearch Version 2.5 oder höher ausgeführt werden.

> **Note**
>
> Diese Dokumentation bietet einen kurzen Überblick über Security Analytics for Amazon OpenSearch Service. Es definiert die wichtigsten Konzepte und enthält Schritte zur Konfiguration von Berechtigungen. Eine umfassende Dokumentation, einschließlich eines Einrichtungsleitfadens, einer API-Referenz und einer Referenz aller verfügbaren Einstellungen, finden Sie in der OpenSearch Dokumentation unter Security Analytics.

Komponenten und Konzepte der Sicherheitsanalyse

Eine Reihe von Tools und Funktionen bilden die Grundlage für den Betrieb von Security Analytics. Zu den Hauptkomponenten, aus denen das Plugin besteht, gehören Detektoren, Protokolltypen, Regeln, Ergebnisse und Warnungen.



Typen von Protokollen

OpenSearch unterstützt mehrere Arten von Protokollen und bietet out-of-the-box Zuordnungen für jeden Typ. Sie geben den Protokolltyp an und konfigurieren ein Zeitintervall, wenn Sie einen Detektor erstellen. Von dort aus aktiviert Security Analytics automatisch einen entsprechenden Regelsatz, der in diesem Intervall ausgeführt wird.

Detektoren

Detektoren identifizieren eine Reihe von Cybersicherheitsbedrohungen für einen Protokolltyp in Ihren Datenindizes. Sie konfigurieren Ihren Detektor so, dass er sowohl benutzerdefinierte Regeln als auch vorgefertigte Sigma-Regeln verwendet, die Ereignisse im System auswerten. Der Detektor generiert dann Sicherheitsergebnisse aus diesen Ereignissen. Weitere Informationen zu Meldern finden Sie in der OpenSearch Dokumentation unter Melder erstellen.

Regeln

Regeln zur Bedrohungserkennung definieren die Bedingungen, die Melder auf aufgenommene Protokolldaten anwenden, um ein Sicherheitsereignis zu identifizieren. Security Analytics unterstützt das Importieren, Erstellen und Anpassen von Regeln, um Ihre Anforderungen zu erfüllen, und bietet außerdem vorkonfigurierte Open-Source-Sigma-Regeln, mit denen Sie häufig auftretende Bedrohungen anhand Ihrer Protokolle erkennen können. Security Analytics ordnet viele Regeln einer ständig wachsenden Wissensbasis über gegnerische Taktiken und Techniken zu, die von der MITRE ATT&CK-Organisation verwaltet werden. Sie können beide OpenSearch Dashboards oder die verwenden, um Regeln zu erstellen und zu verwenden. APIs Weitere Informationen zum Erstellen von Regeln finden Sie in der Dokumentation zum Erstellen von Regeln in der OpenSearch Dokumentation zum Erstellen von Regeln.

Funde

Wenn ein Detektor eine Regel mit einem Protokollereignis abgleicht, generiert er einen Befund. Jedes Ergebnis umfasst eine eindeutige Kombination aus ausgewählten Regeln, einem Protokolltyp und einem Regelschweregrad. Die Ergebnisse deuten nicht unbedingt auf unmittelbare Bedrohungen innerhalb des Systems hin, aber sie isolieren immer ein interessierendes Ereignis. Weitere Informationen zu den Ergebnissen finden Sie in der OpenSearch Dokumentation unter Arbeiten mit Ergebnissen.

Benachrichtigungen

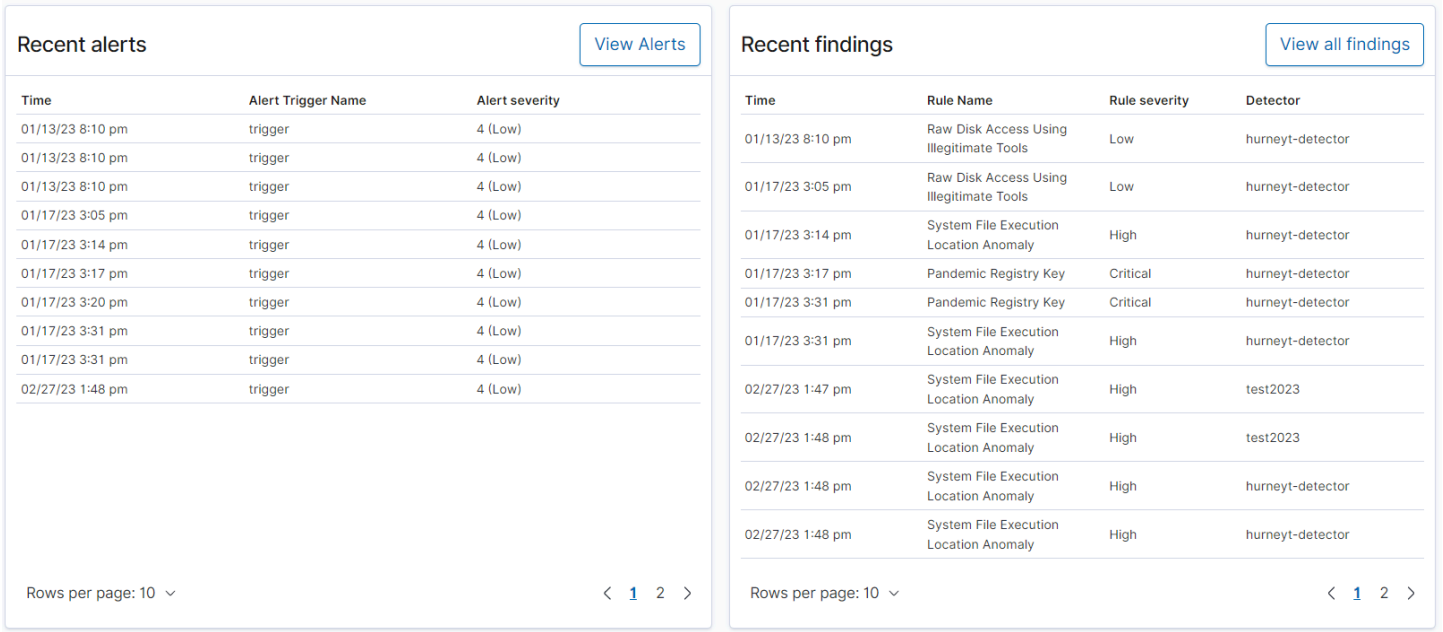
Wenn Sie einen Detector erstellen, können Sie eine oder mehrere Bedingungen angeben, die einen Alarm auslösen. Eine Warnung ist eine Benachrichtigung, die an einen bevorzugten Kanal wie Slack oder E-Mail gesendet wird. Sie legen fest, dass die Warnung ausgelöst wird, wenn der Detektor einer oder mehreren Regeln entspricht, und können die Benachrichtigungsnachricht anpassen. Weitere Informationen zu Warnmeldungen finden Sie in der OpenSearch Dokumentation unter Arbeiten mit Warnmeldungen.

Erkunden von Sicherheitsanalysen

Sie können OpenSearch Dashboards verwenden, um Ihr Security Analytics-Plugin zu visualisieren und Einblicke in dieses zu erhalten. Die Übersichtsansicht enthält Informationen wie Ergebnisse und Anzahl der Alarme, aktuelle Ergebnisse und Warnungen, Regeln für häufige Erkennungen und eine Liste Ihrer Melder. Sie können eine Übersichtsansicht sehen, die aus mehreren Visualisierungen besteht. Das folgende Diagramm zeigt beispielsweise den Trend der Ergebnisse und Warnmeldungen für verschiedene Protokolltypen über einen bestimmten Zeitraum.



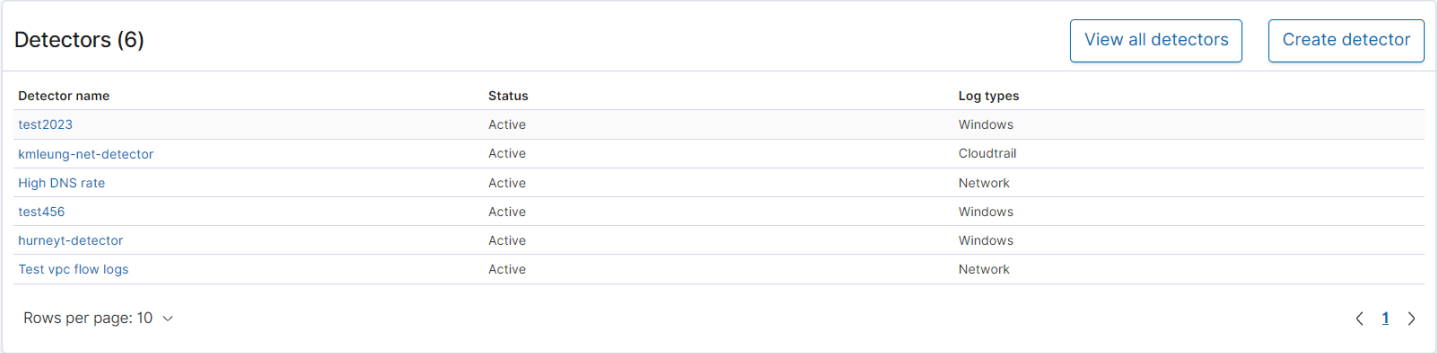
Weiter unten auf der Seite können Sie Ihre neuesten Ergebnisse und Warnungen überprüfen.



Darüber hinaus können Sie eine Verteilung der am häufigsten ausgelösten Regeln auf alle aktiven Melder sehen. Dies kann Ihnen helfen, verschiedene Arten von bösartigen Aktivitäten in den verschiedenen Protokolltypen zu erkennen und zu untersuchen.



Schließlich können Sie den Status der konfigurierten Melder anzeigen. Von diesem Fenster aus können Sie auch zum Erstellen von Detector-Workflows navigieren.



Um Ihr Security Analytics-Setup zu konfigurieren, erstellen Sie Regeln auf der Seite „Regeln“ und verwenden Sie diese Regeln, um Melder auf der Seite „Detektoren“ zu schreiben. Für eine genauere Ansicht Ihrer Security Analytics-Ergebnisse können Sie die Seiten Ergebnisse und Warnungen verwenden.

Konfigurieren von Berechtigungen

Wenn Sie Security Analytics in einer bereits vorhandenen OpenSearch Dienstdomäne aktivieren, ist die `security_analytics_manager` Rolle möglicherweise nicht in der Domäne definiert. Benutzer ohne Administratorrechte müssen dieser Rolle zugeordnet werden, um Warm-Indizes in Domains mithilfe einer fein abgestuften Zugriffskontrolle zu verwalten. Führen Sie die folgenden Schritte aus, um die `security_analytics_manager`-Rolle manuell zu erstellen:

1. Gehen Sie in OpenSearch Dashboards zu Sicherheit und wählen Sie Berechtigungen aus.
2. Wählen Sie Aktionsgruppe erstellen und konfigurieren Sie die folgenden Gruppen:

Group name (Gruppenname)	Berechtigungen
security_analytics_full_access	• cluster:admin/opensearch/securityanalytics/alerts/* • cluster:admin/opensearch/securityanalytics/detector/* • cluster:admin/opensearch/securityanalytics/findings/* • cluster:admin/opensearch/securityanalytics/mapping/* • cluster:admin/opensearch/securityanalytics/rule/*
security_analytics_read_access	• cluster:admin/opensearch/securityanalytics/alerts/get • cluster:admin/opensearch/securityanalytics/detector/get • cluster:admin/opensearch/securityanalytics/detector/search • cluster:admin/opensearch/securityanalytics/findings/get • cluster:admin/opensearch/securityanalytics/mapping/get • cluster:admin/opensearch/securityanalytics/mapping/view/get • cluster:admin/opensearch/securityanalytics/rule/get • cluster:admin/opensearch/securityanalytics/rule/search

3. Wählen Sie Rollen und Rolle erstellen.
4. Nennen Sie die Rolle security_analytics_manager.

5. Wählen Sie für Clusterberechtigungen `security_analytics_full_access` und `security_analytics_read_access` aus.
6. Geben Sie für Index * ein.
7. Wählen Sie für Indexberechtigungen die Option und aus. `indices:admin/mapping/put` `indices:admin/mappings/get`
8. Wählen Sie Erstellen aus.
9. Nachdem Sie die Rolle erstellt haben, ordnen Sie sie einer beliebigen Benutzer- oder Backend-Rolle zu, die Security Analyses-Indizes verwaltet.

Fehlerbehebung

Kein solcher Indexfehler

Wenn Sie keine Melder haben und das Security Analytics-Dashboard öffnen, sehen Sie möglicherweise unten rechts eine Benachrichtigung mit dem Hinweis`[index_not_found_exception] no such index [.opensearch-sap-detectors-config]`. Sie können diese Benachrichtigung ignorieren. Sie verschwindet innerhalb weniger Sekunden und erscheint nicht mehr, sobald Sie einen Detektor erstellt haben.

Sicherheit in Amazon Service OpenSearch

Die Standardinstallation von OpenSearch Dashboards für Amazon OpenSearch Service umfasst das Beobachtbarkeits-Plugin, mit dem Sie datengesteuerte Ereignisse mit Piped Processing Language (PPL) visualisieren können, um in gespeicherte Daten zu untersuchen, zu erkennen und abzufragen. OpenSearch Das Feature erfordert OpenSearch 1.2 oder höher.

Das Beobachtbarkeits-Plug-In bietet ein einheitliche Erlebnis zum Erfassen und Überwachen von Metriken, Protokollen und Traces aus gängigen Datenquellen. Die Datenerfassung und -überwachung an einem Ort ermöglicht eine Full-Stack- und end-to-end durchgängige Beobachtbarkeit Ihrer gesamten Infrastruktur.

> **Note**
>
> Diese Dokumentation bietet einen kurzen Überblick über Observability in Service. OpenSearch Eine umfassende Dokumentation des Observability-Plug-ins, einschließlich der Berechtigungen, finden Sie unter Observability.

Jeder Prozess zur Untersuchung von Daten ist anders. Wenn Sie noch nicht mit der Untersuchung von Daten und dem Erstellen von Visualisierungen arbeiten, empfehlen wir Ihnen, einen Workflow wie den folgenden auszuprobieren.

Erkunden Ihrer Daten mit Ereignisanalytik

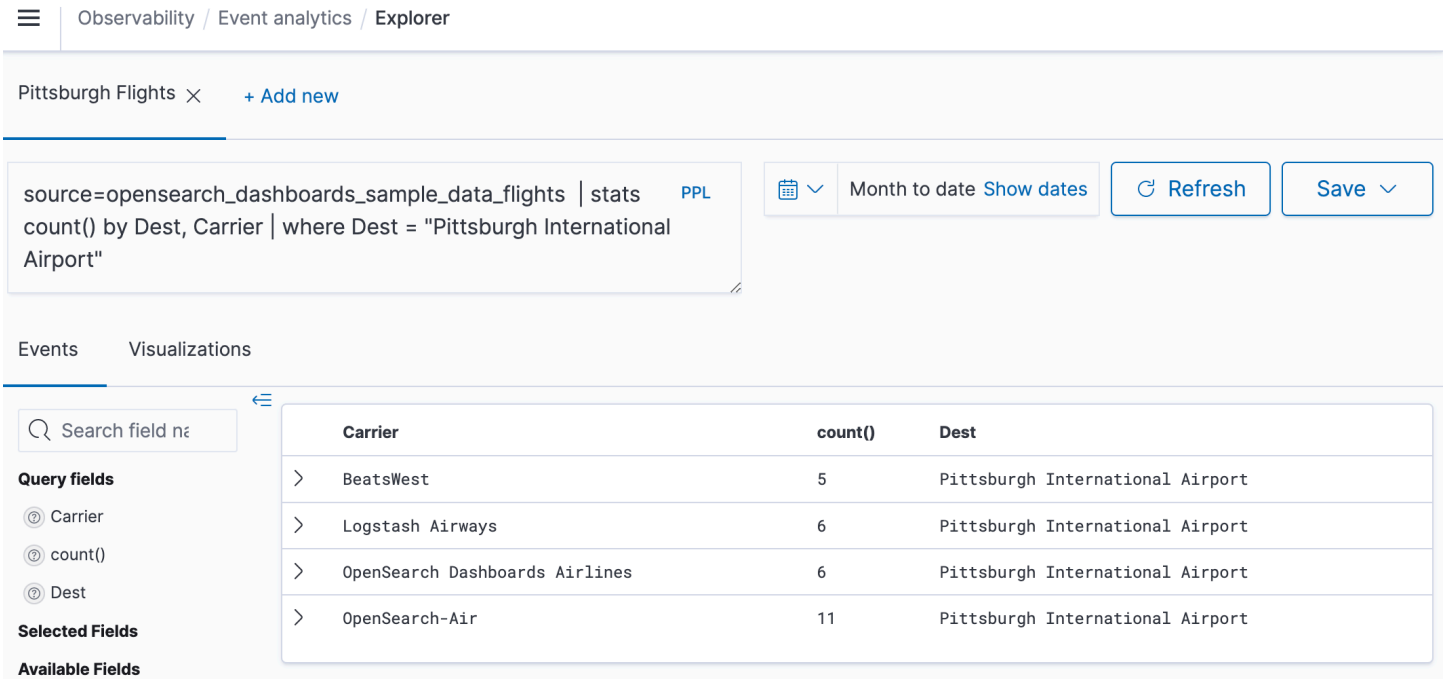
Nehmen wir an, dass Sie Flugdaten in Ihrer OpenSearch Domäne erfassen und herausfinden möchten, welche Fluggesellschaft im vergangenen Monat die meisten Flüge zum Pittsburgh International Airport hatte. Sie schreiben die folgende PPL-Abfrage:

```
source=opensearch_dashboards_sample_data_flights |
    stats count() by Dest, Carrier |
    where Dest = "Pittsburgh International Airport"
```

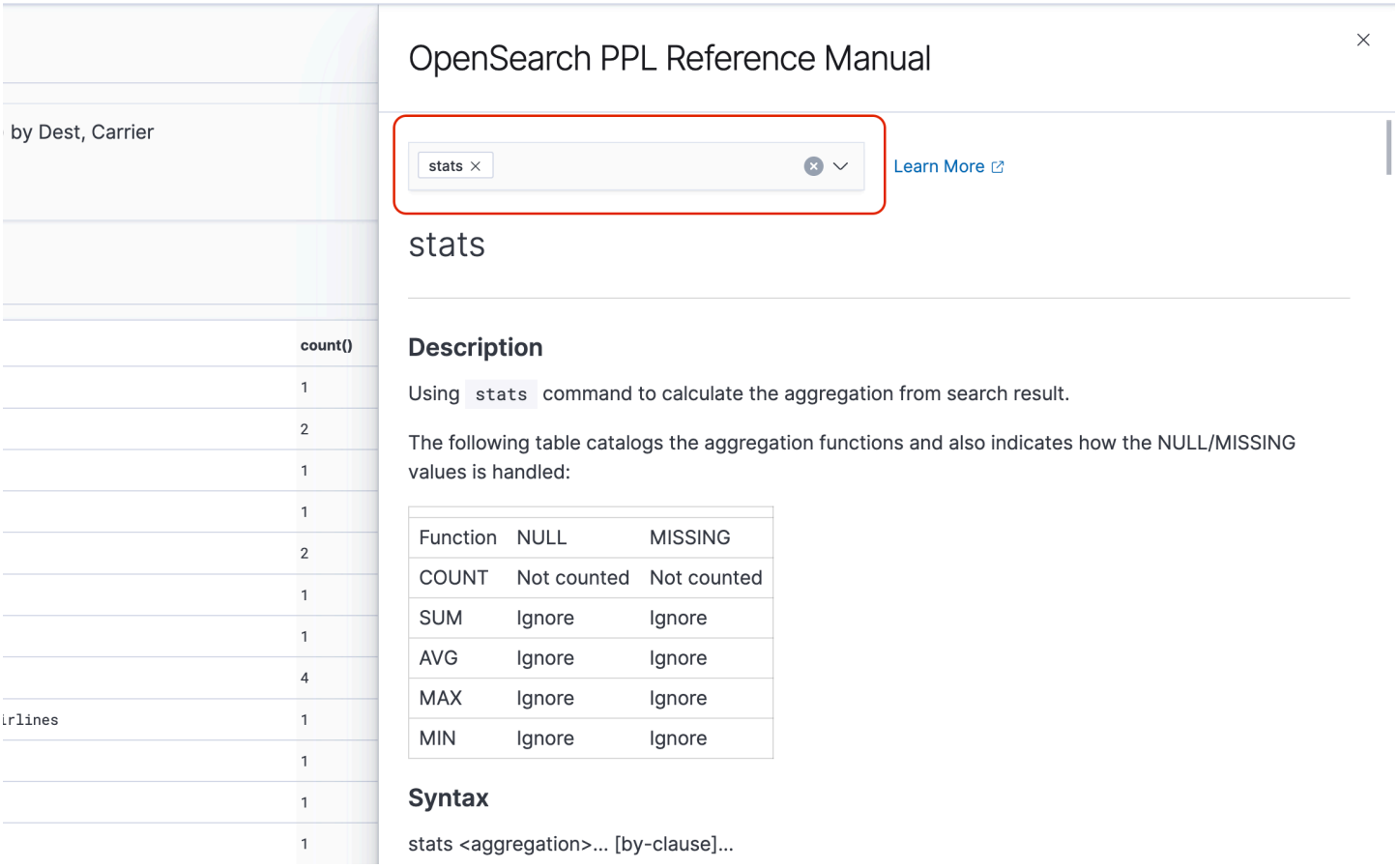
Diese Abfrage ruft Daten aus dem Index namens `opensearch_dashboards_sample_data_flights` ab. Sie nutzt dann den Befehl `stats`, um eine Gesamtzahl der Flüge zu erhalten und sie nach Zielflughafen und Fluggesellschaft zu

gruppieren. Schließlich benutzt sie die `where`-Klausel, um die Ergebnisse für Flüge zu filtern, die am Pittsburgh International Airport ankommen.

So sehen die Daten aus, wenn sie für den vergangenen Monat angezeigt werden:



Sie können die Schaltfläche PPL im Abfrage-Editor auswählen, um Nutzungsinformationen und Beispiele für jeden PPL-Befehl abzurufen:



Sehen wir uns ein komplexeres Beispiel an, das Informationen über Flugverspätungen abfragt:

```
source=opensearch_dashboards_sample_data_flights |
    where FlightDelayMin > 0 |
    stats sum(FlightDelayMin) as minimum_delay, count() as total_delayed by Carrier,
 Dest |
    eval avg_delay=minimum_delay / total_delayed |
    sort - avg_delay
```

Jeder Befehl in der Abfrage wirkt sich auf die endgültige Ausgabe aus:

- `source=opensearch_dashboards_sample_data_flights` ruft Daten aus demselben Index wie im vorherigen Beispiel ab.
- `where FlightDelayMin > 0` filtert die Daten nach Flügen, die verspätet waren.
- `stats sum(FlightDelayMin) as minimum_delay, count() as total_delayed by Carrier` ruft für jede Fluggesellschaft die gesamte minimale Verspätungszeit und die Gesamtzahl der verspäteten Flüge ab.

- `eval avg_delay=minimum_delay / total_delayed` berechnet die durchschnittliche Verspätungszeit für jede Fluggesellschaft durch Dividieren der minimalen Verspätungszeit durch die Gesamtzahl der verspäteten Flüge.
- `sort - avg_delay` sortiert die Ergebnisse nach durchschnittlicher Verzögerung in absteigender Reihenfolge.

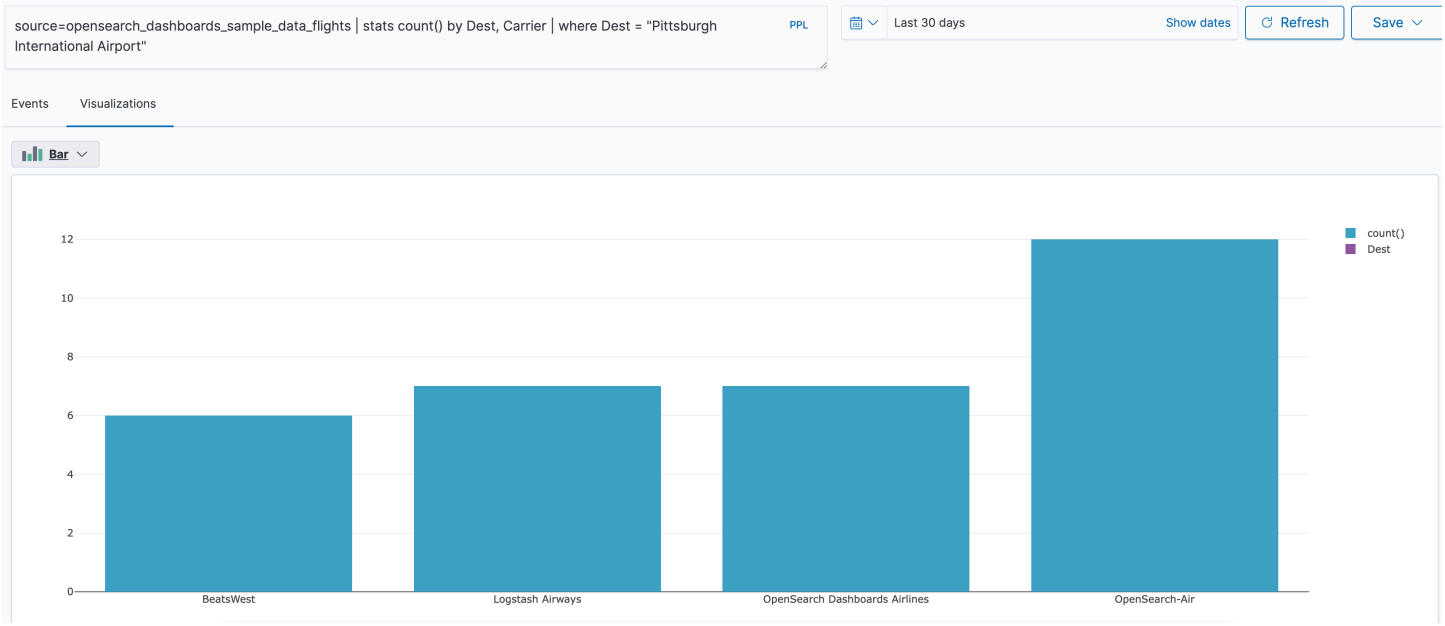
Mit dieser Abfrage können Sie feststellen, dass OpenSearch Dashboards Airlines im Durchschnitt weniger Verspätungen aufweist.

	avg_delay	Carrier	minimum_delay	total_delayed
>	212	Logstash Airways	4470	21
>	184	OpenSearch-Air	4245	23
>	155	BeatsWest	2025	13
>	153	OpenSearch Dashboards Airlines	4305	28

Weitere Beispiele für PPL-Abfragen finden Sie unter Abfragen und Visualisierungen auf der SeiteEreignisanalytik.

Erstellen von Visualisierungen

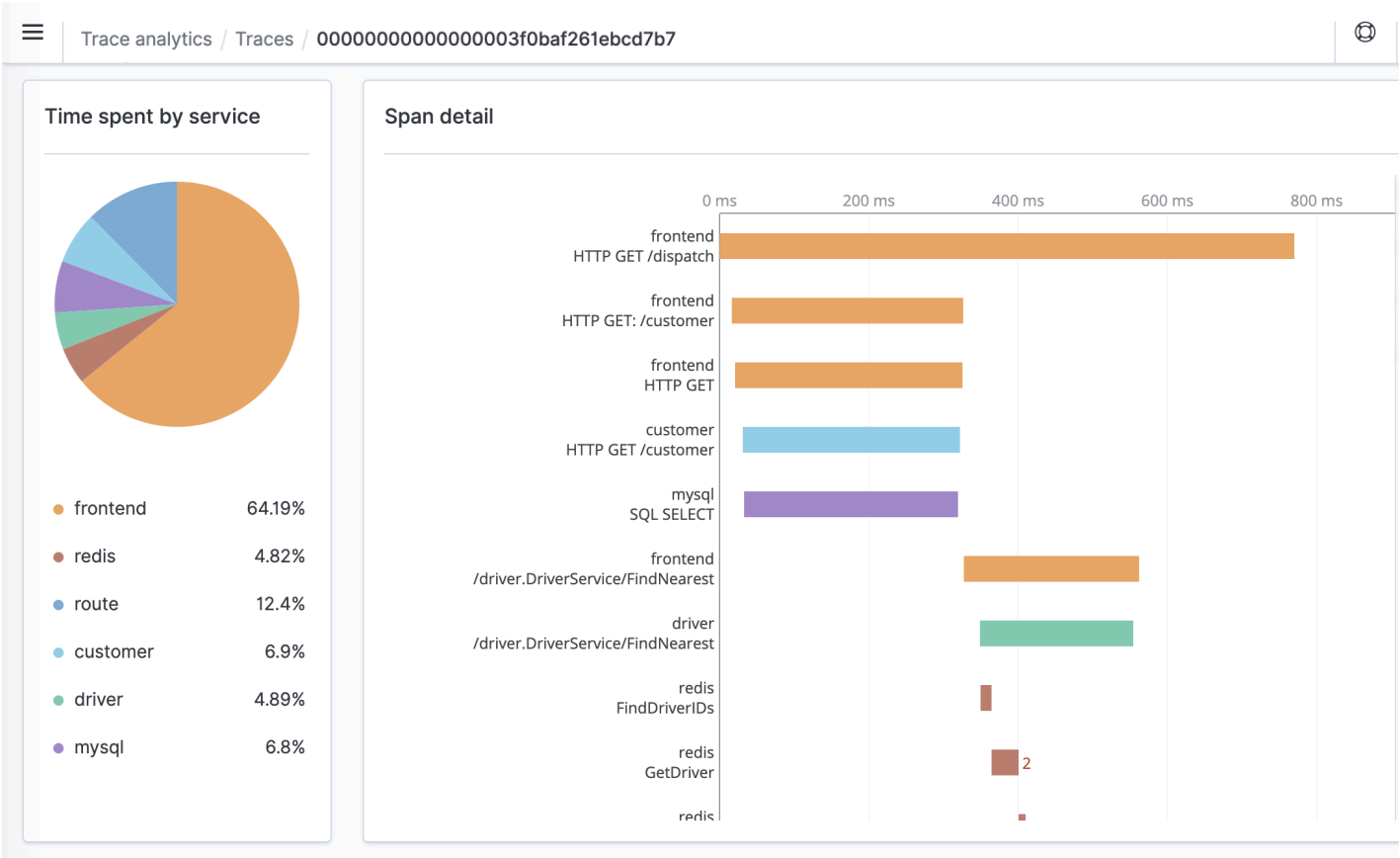
Sobald Sie die Daten, an denen Sie interessiert sind, korrekt abgefragt haben, können Sie diese Abfragen als Visualisierungen speichern:



Fügen Sie diese Visualisierungen dann Operative Bereiche hinzu, um verschiedene Daten zu vergleichen. Nutzen Sie Notebooks, um verschiedene Visualisierungen und Codeblöcke zu kombinieren, die Sie mit Teammitgliedern teilen können.

Detaillierter Einblick in Trace Analytics

Trace Analytics bietet eine Möglichkeit, den Ereignisfluss in Ihren OpenSearch Daten zu visualisieren, um Leistungsprobleme in verteilten Anwendungen zu identifizieren und zu beheben.



Spurenanalytik für Amazon OpenSearch Service

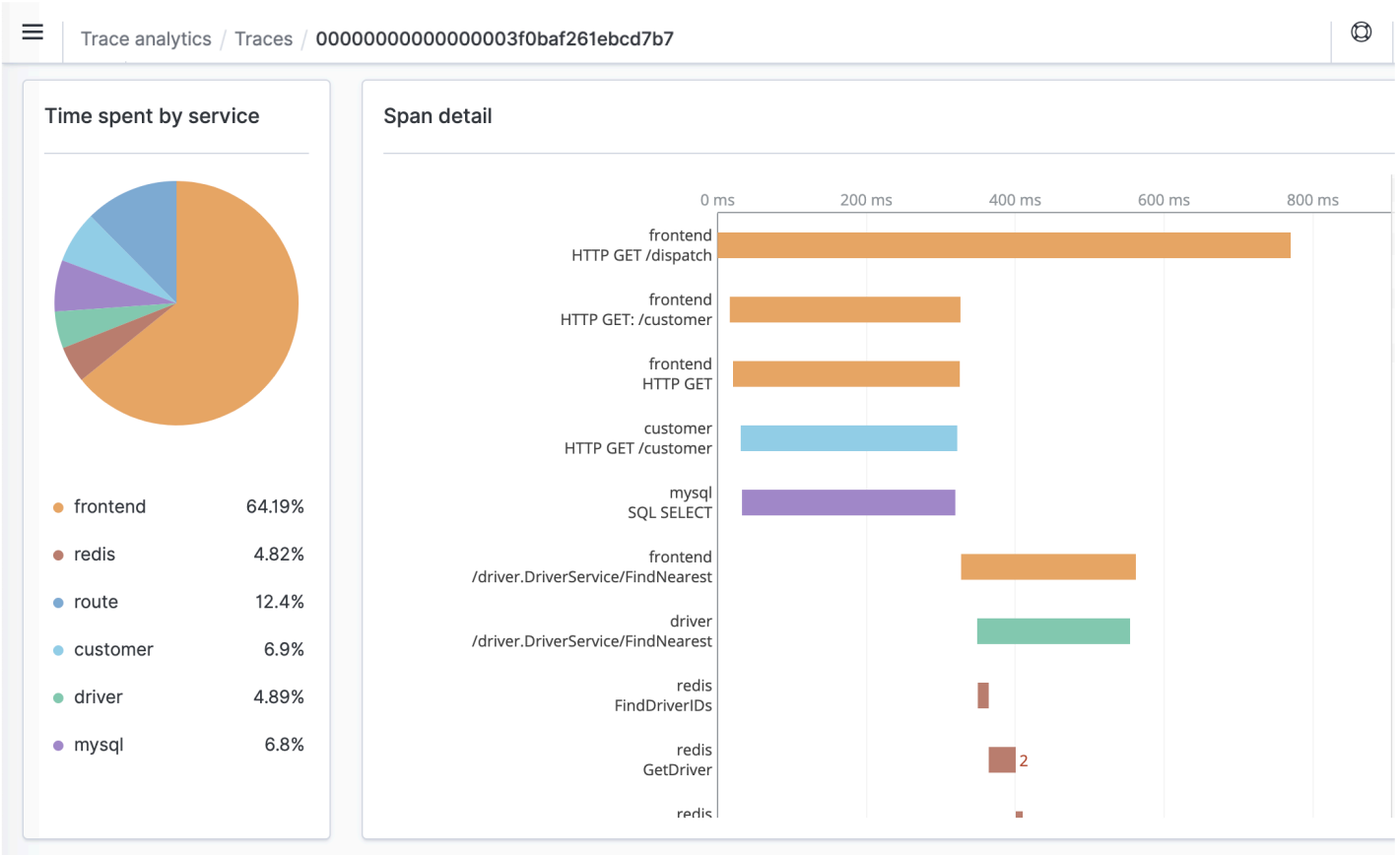
Sie können Trace Analytics, das Teil des OpenSearch Beobachtbarkeits-Plug-ins ist, verwenden, um Trace-Daten aus verteilten Anwendungen zu analysieren. Für Trace Analytics ist Elasticsearch 7.9 oder höher erforderlich OpenSearch .

In einer verteilten Anwendung kann ein einzelner Vorgang, z. B. das Klicken eines Benutzers auf eine Schaltfläche, eine erweiterte Reihe von Ereignissen auslösen. Das Anwendungs-Front-End kann beispielsweise einen Backend-Dienst aufrufen, der einen anderen Dienst aufruft, der eine Datenbank

abfragt, die Abfrage verarbeitet und ein Ergebnis zurückgibt. Dann sendet der erste Backend-Dienst eine Bestätigung an das Front-End, das die Benutzeroberfläche aktualisiert.

Sie können Spurenanalytik verwenden, um diesen Ereignisfluss zu visualisieren und Leistungsprobleme zu identifizieren.

> **Note**
>
> Diese Dokumentation bietet einen kurzen Überblick über Trace Analytics. Eine umfassende Dokumentation finden Sie unter Trace Analytics in der OpenSearch Open-Source-Dokumentation.



Voraussetzungen

Bei Trace Analytics müssen Sie Ihrer Anwendung Instrumentierung hinzufügen und Trace-Daten mithilfe einer OpenTelemetry unterstützten Bibliothek wie Jaeger oder Zipkin generieren. Dieser Schritt erfolgt vollständig außerhalb von OpenSearch Service. Die AWS OpenTelemetry

Dokumentation enthält Beispielanwendungen für viele Programmiersprachen, die Ihnen den Einstieg erleichtern, einschließlich Java, Python, Go und JavaScript.

Nachdem Sie Ihrer Anwendung Instrumentierung hinzugefügt haben, empfängt der OpenTelemetryCollector Daten von der Anwendung und formatiert sie in OpenTelemetry Daten. Die Liste der Empfänger finden Sie unter GitHub. AWS Distro for OpenTelemetry enthält einen Empfänger für. AWS X-Ray

Schließlich können Sie diese OpenTelemetry Daten für OpenSearch Einnahme durch Amazon die Verwendung mit OpenSearch formatieren.

OpenTelemetry Collector-Probenkonfiguration

Um den OpenTelemetry Collector mit zu verwenden OpenSearch Einnahme durch Amazon, versuchen Sie die folgende Beispielkonfiguration:

```
extensions:
  sigv4auth:
    region: "us-east-1"
    service: "osis"

receivers:
  jaeger:
    protocols:
      grpc:

exporters:
  otlphttp:
    traces_endpoint: "https://pipeline-endpoint.us-east-1.osis.amazonaws.com/
opentelemetry.proto.collector.trace.v1.TraceService/Export"
    auth:
      authenticator: sigv4auth
    compression: none

service:
  extensions: [sigv4auth]
  pipelines:
    traces:
      receivers: [jaeger]
      exporters: [otlphttp]
```

OpenSearch Beispielkonfiguration für die Aufnahme

Um Ablaufverfolgungsdaten an eine OpenSearch Dienstdomäne zu senden, versuchen Sie die folgende Beispielkonfiguration für OpenSearch Ingestion Pipelaufverfolgung. Anweisungen zum Erstellen einer Pipeline finden Sie unter. the section called “Pipelines erstellen”

```
version: "2"
otel-trace-pipeline:
  source:
    otel_trace_source:
      "/${pipelineName}/ingest"
  processor:
    - trace_peer_forwarder:
  sink:
    - pipeline:
        name: "trace_pipeline"
    - pipeline:
        name: "service_map_pipeline"
trace-pipeline:
  source:
    pipeline:
      name: "otel-trace-pipeline"
  processor:
    - otel_traces:
  sink:
    - opensearch:
        hosts: ["https://domain-endpoint"]
        index_type: trace-analytics-raw
        aws:
          # IAM role that OpenSearch Ingestion assumes to access the domain sink
          sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
          region: "us-east-1"

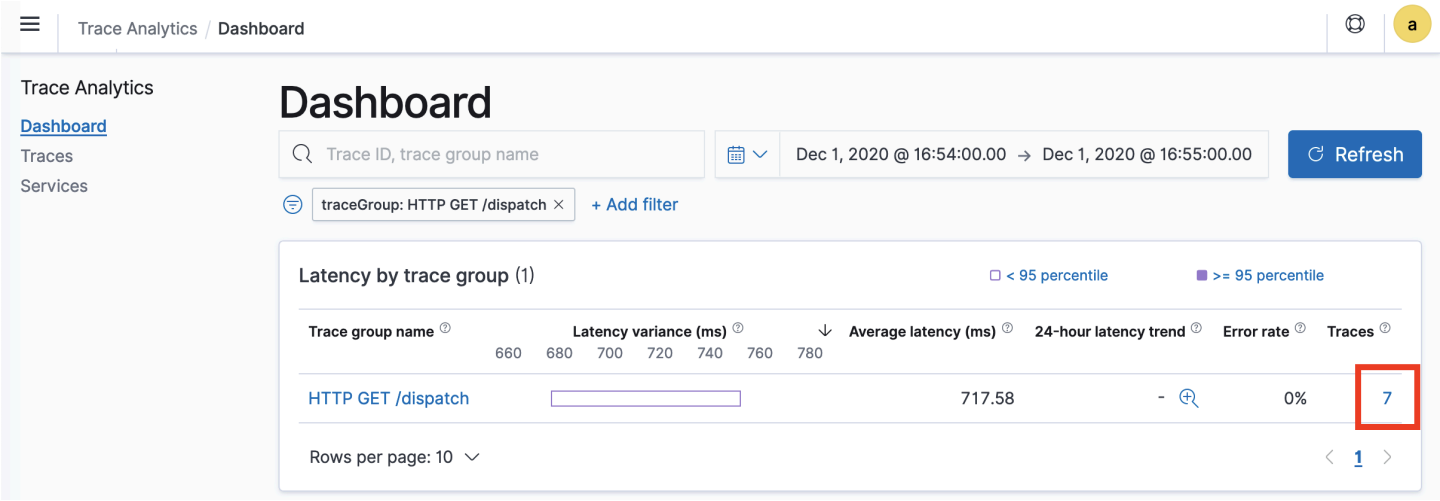
service-map-pipeline:
  source:
    pipeline:
      name: "otel-trace-pipeline"
  processor:
    - service_map:
  sink:
    - opensearch:
        hosts: ["https://domain-endpoint"]
        index_type: trace-analytics-service-map
```

```
    aws:
      # IAM role that the pipeline assumes to access the domain sink
      sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
      region: "us-east-1"
```

Die Pipelaufverfolgung, die Sie in der `sts_role_arn` Option angeben, muss über Schreibberechtigungen für die Senke verfügen. Anweisungen zum Konfigurieren von Berechtigungen für die Pipeline-Rolle finden Sie unterthe section called “Rollen und Benutzer einrichten”.

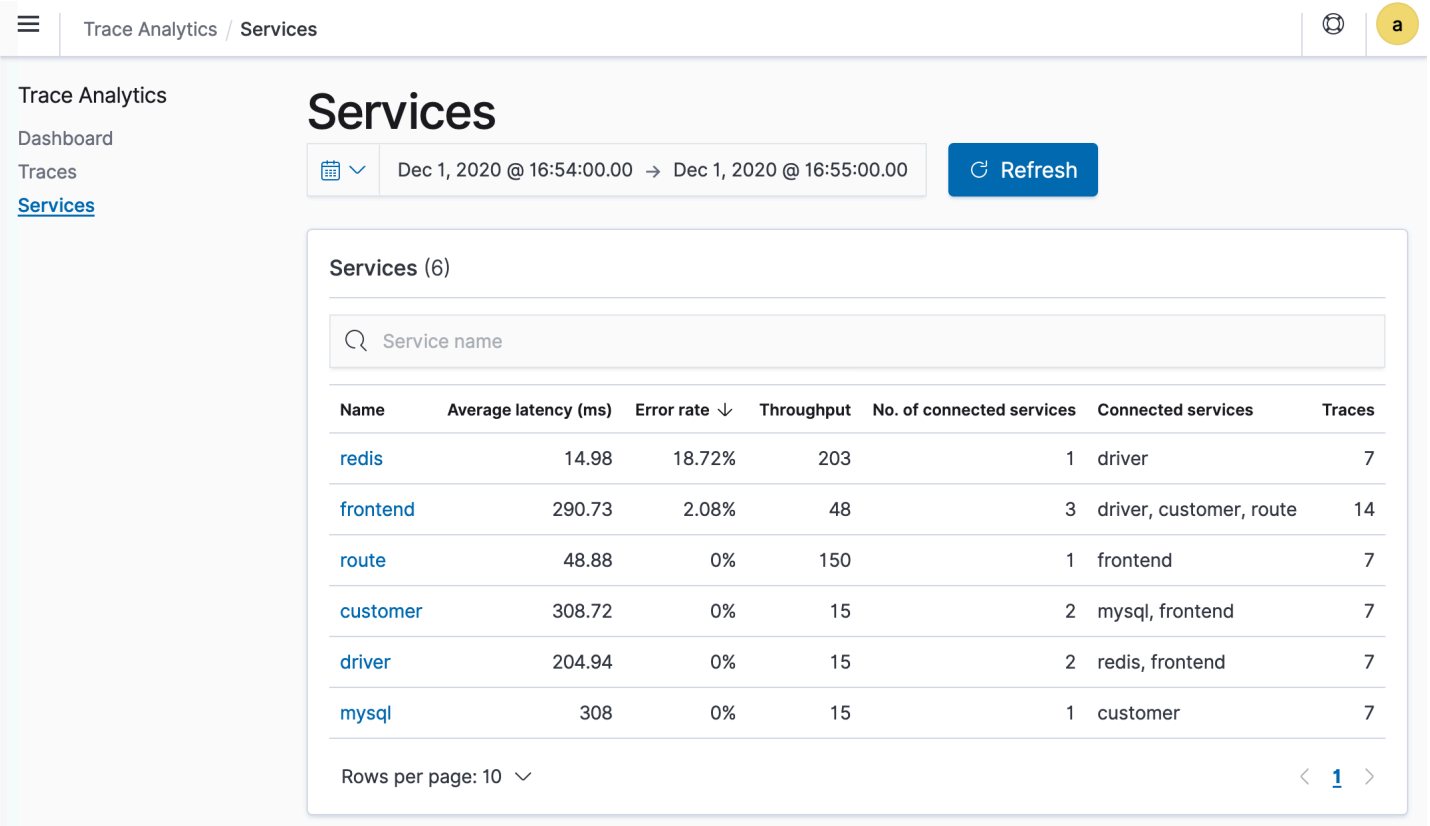
Spurendaten untersuchen

Die Dashboard-Ansicht gruppiert Spuren nach HTTP-Methode und -Pfad, sodass Sie die durchschnittliche Latenz, Fehlerrate und Trends im Zusammenhang mit einem bestimmten Vorgang sehen können. Versuchen Sie für eine fokussiertere Ansicht, nach Spurengruppennamen zu filtern.



Um einen Drilldown zu den Spuren durchzuführen, die eine Spuren-Gruppe bilden, wählen Sie die Anzahl der Spuren in der rechten Spalte. Wählen Sie dann eine einzelne Spur für eine detaillierte Zusammenfassung aus.

Die Ansicht Services listet alle Dienste in der Anwendung sowie eine interaktive Karte auf, die zeigt, wie die verschiedenen Dienste miteinander verbunden sind. Im Gegensatz zum Dashboard (das hilft, Probleme nach Betrieb zu identifizieren), hilft Ihnen die Service Map, Probleme nach Service zu identifizieren. Versuchen Sie, nach Fehlerrate oder Latenz zu sortieren, um ein Gefühl für potenzielle Problembereiche Ihrer Anwendung zu erhalten.



Abfragen von OpenSearch Amazon--Service-Daten mit Piped Processing Language

Piped Processing Language (PPL) ist eine Abfragesprache, mit der Sie die Pipe-Syntax (|) verwenden können, um in Amazon OpenSearch Service gespeicherte Daten abzufragen. Für PPL ist Elasticsearch 7.9 OpenSearch oder höher erforderlich.

> **Note**
>
> Diese Dokumentation bietet einen kurzen Überblick über PPL für Amazon OpenSearch Service. Ausführliche Schritte und eine vollständige Befehlsreferenz finden Sie unter PPL in der OpenSearch Open-Source-Dokumentation.

Die PPL-Syntax besteht aus Befehlen, die durch ein Pipe-Zeichen (|) begrenzt sind, wobei Daten von links nach rechts durch jede Pipeline fließen. Die PPL-Syntax, um die Anzahl der Hosts mit HTTP 403- oder 503-Fehlern zu ermitteln, sie pro Host zu aggregieren und sie in der Reihenfolge der Auswirkungen zu sortieren, lautet beispielsweise wie folgt:

```
source = dashboards_sample_data_logs | where response='403' or response='503' | stats
 count(request) as request_count by host, response | sort -request_count
```

Um zu beginnen, wählen Sie Abfrage-Workbench in OpenSearch Dashboards und wählen Sie PPL aus. Verwenden Sie die `bulk`-Operation, um einige Beispieldaten zu indizieren:

```
PUT accounts/_bulk?refresh
{"index":{"_id":"1"}}
{"account_number":1,"balance":39225,"firstname":"Amber","lastname":"Duke","age":32,"gender":"M"
 Holmes
 Lane","employer":"Pyrami","email":"amberduke@pyrami.com","city":"Brogan","state":"IL"}
{"index":{"_id":"6"}}
{"account_number":6,"balance":5686,"firstname":"Hattie","lastname":"Bond","age":36,"gender":"M"
 Bristol
 Street","employer":"Netagy","email":"hattiebond@netagy.com","city":"Dante","state":"TN"}
{"index":{"_id":"13"}}
{"account_number":13,"balance":32838,"firstname":"Nanette","lastname":"Bates","age":28,"gender"
 Mady Street","employer":"Quility","city":"Nogal","state":"VA"}
{"index":{"_id":"18"}}
{"account_number":18,"balance":4180,"firstname":"Dale","lastname":"Adams","age":33,"gender":"M"
 Hutchinson Court","email":"daleadams@boink.com","city":"Orick","state":"MD"}
```

Im folgenden Beispiel wird Folgendes zurückgegeben: `firstname`- und `lastname`-Felder für Dokumente in einem Kontenindex mit `age` größer als 18:

```
search source=accounts | where age > 18 | fields firstname, lastname
```

Beispielantwort

id	FirstName	LastName
0	Amber	Duke
1	Hattie	Bond
2	Nanette	Bates
3	Dale	Adams

Sie können einen kompletten Satz schreibgeschützter Befehle wie `search`, `where`, `fields`, `rename`, `dedup`, `stats`, `sort`, `eval`, `head`, `top` und `rare` verwenden. Das PPL-Plug-In unterstützt alle SQL-Funktionen, einschließlich mathematischer, trigonometrischer, Datum-Zeit-, Zeichenfolgen-, aggregierter und fortgeschrittener Operatoren und Ausdrücke. Weitere Informationen finden Sie im OpenSearch PPL-Referenzhandbuch.

Bewährte Betriebspraktiken für Amazon OpenSearch Service

Dieses Kapitel enthält bewährte Methoden für den Betrieb von Amazon OpenSearch Service-Domains und enthält allgemeine Richtlinien, die für viele Anwendungsfälle gelten. Jede Workload ist einzigartig und weist einzigartige Merkmale auf, sodass keine generische Empfehlung für jeden Anwendungsfall genau richtig ist. Die wichtigste bewährte Methode besteht darin, Ihre Domains in einem kontinuierlichen Zyklus bereitzustellen, zu testen und anzupassen, um die optimale Konfiguration, Stabilität und Kosten für Ihre Workload zu ermitteln.

Themen

- Überwachen und Warnen
- Shard-Strategie
- Stabilität
- Leistung
- Sicherheit
- Kostenoptimierung
- Dimensionierung von Amazon OpenSearch Service-Domains
- Petabyte-Größe im Amazon Service OpenSearch
- Dedizierte Koordinatorknoten in Amazon OpenSearch Service
- Dedizierte Masterknoten in Amazon OpenSearch Service

Überwachen und Warnen

Die folgenden bewährten Methoden gelten für die Überwachung Ihrer OpenSearch Service-Domains.

CloudWatch Alarme konfigurieren

OpenSearch Der Service sendet Leistungskennzahlen an Amazon CloudWatch. Überprüfen Sie regelmäßig Ihre Cluster- und Instance-Metriken und konfigurieren Sie empfohlene CloudWatch Alarme auf der Grundlage Ihrer Workload-Leistung.

Aktivieren der Protokollveröffentlichung

OpenSearch Der Service macht OpenSearch Fehlerprotokolle, Suchprotokolle, Indexierungsprotokolle und Auditprotokolle in Amazon CloudWatch Logs verfügbar. Protokolle für langsame Suchen, Protokolle für langsame Indizierung und Fehlerprotokolle sind für die Problembehandlung bei Leistungs- und Stabilitätsproblemen nützlich. Überwachungsprotokolle, die nur verfügbar sind, wenn Sie eine differenzierte Zugriffskontrolle aktivieren, verfolgen die Benutzeraktivität. Weitere Informationen finden Sie in der Dokumentation unter Logs. OpenSearch

Protokolle für langsame Suchen, Protokolle für langsame Indizierung sind ein wichtiges Tool, um die Leistung Ihrer Such- und Indizierungsvorgänge zu verstehen und Fehler zu beheben. Aktivieren Sie die Bereitstellung von Protokollen für langsame Suchen und Indizes für alle ProduktionsDomains. Sie müssen auch Schwellenwerte für die Protokollierung konfigurieren — andernfalls werden die Protokolle CloudWatch nicht erfasst.

Shard-Strategie

Shards verteilen Ihre Arbeitslast auf die Datenknoten in Ihrer OpenSearch Service-Domain. Richtig konfigurierte Indizes können dazu beitragen, die Gesamtleistung der Domain zu steigern.

Wenn Sie Daten an OpenSearch Service senden, senden Sie diese Daten an einen Index. Ein Index ist vergleichbar mit einer Datenbanktabelle, mit Dokumenten als Zeilen und Feldern als Spalten. Wenn Sie den Index erstellen, geben Sie an, OpenSearch wie viele primäre Shards Sie erstellen möchten. Die primären Shards sind unabhängige Partitionen des gesamten Datensatzes. OpenSearch Der Service verteilt Ihre Daten automatisch auf die primären Shards in einem Index. Sie können auch Replikate des Index konfigurieren. Jedes Replikat umfasst einen vollständigen Satz von Kopien der primären Shards für diesen Index.

OpenSearch Der Service ordnet die Shards für jeden Index den Datenknoten in Ihrem Cluster zu. Er stellt sicher, dass sich die Primär- und Replikat-Shards für den Index auf unterschiedlichen Datenknoten befinden. Das erste Replikat stellt sicher, dass Sie zwei Kopien der Daten im Index haben. Sie sollten immer mindestens ein Replikat verwenden. Zusätzliche Replikate bieten zusätzliche Redundanz und Lesekapazität.

OpenSearch sendet Indexierungsanfragen an alle Datenknoten, die Shards enthalten, die zum Index gehören. Indizierungsanforderungen werden zuerst an Datenknoten gesendet, die primäre Shards enthalten, und dann an Datenknoten, die Replikat-Shards enthalten. Suchanfragen werden vom Koordinationsknoten entweder an einen primären oder einen Replikat-Shard für alle zum Index gehörenden Shards weitergeleitet.

Bei einem Index mit fünf primären Shards und einem Replikat berührt beispielsweise jede Indizierungsanforderung 10 Shards. Im Gegensatz dazu werden Suchanfragen an n Shards gesendet, wobei n die Anzahl der primären Shards ist. Bei einem Index mit fünf primären Shards und einem Replikat berührt jede Suchanfrage fünf Shards (primär oder Replikat) aus diesem Index.

Ermitteln der Anzahl der Shards und Datenknoten

Verwenden Sie die folgenden bewährten Methoden, um die Anzahl der Shards und Datenknoten für Ihre Domain zu bestimmen.

Shard-Größe – Die Größe der Daten auf der Festplatte ist ein direktes Ergebnis der Größe Ihrer Quelldaten und ändert sich, wenn Sie mehr Daten indizieren. Das source-to-index Verhältnis kann stark variieren, von 1:10 bis 10:1 oder mehr, aber normalerweise liegt es bei etwa 1:1,10. Sie können dieses Verhältnis verwenden, um die Indexgröße auf der Festplatte vorherzusagen. Sie können auch einige Daten indizieren und die tatsächlichen Indexgrößen abrufen, um das Verhältnis für Ihre Workload zu bestimmen. Sobald Sie eine voraussichtliche Indexgröße haben, legen Sie eine Shard-Anzahl fest, sodass jeder Shard zwischen 10 und 30 GiB (für Such-Workloads) oder zwischen 30 und 50 GiB (für Protokoll-Workloads) liegt. 50 GiB sollten das Maximum sein; planen Sie auf jeden Fall einen Zuwachs ein.

Shard-Anzahl – Die Verteilung von Shards auf Datenknoten hat einen großen Einfluss auf die Leistung einer Domain. Wenn Sie Indizes mit mehreren Shards haben, versuchen Sie, dafür zu sorgen, dass der Shard ein Vielfaches der Anzahl der Datenknoten zählt. Dies sorgt dafür, dass Shards gleichmäßig über Datenknoten verteilt sind, und verhindert heiße Knoten. Wenn Sie beispielsweise 12 primäre Shards haben, sollte Ihre Datenknotenanzahl 2, 3, 4, 6 oder 12 betragen. Die Shard-Anzahl ist jedoch zweitrangig gegenüber der Shard-Größe; Wenn Sie über 5 GiB an Daten verfügen, sollten Sie dennoch einen einzelnen Shard verwenden.

Shards pro Datenknoten – Die Gesamtzahl der Shards, die ein Knoten verarbeiten kann, ist proportional zum Java Virtual Machine (JVM)-Speicher des Knotens. Streben Sie 25 Shards oder weniger pro GiB Heap-Speicher an. Beispielsweise sollte ein Knoten mit 32 GiB Heap-Speicher nicht mehr als 800 Shards verarbeiten. Obwohl die Shard-Verteilung je nach Ihren Workload-Mustern variieren kann, gibt es ein Limit von 1.000 Shards pro Node für Elasticsearch und von OpenSearch 1.1 bis 2.15 und 4.000 für 2.17 und höher. OpenSearch Die cat/allocation-API bietet einen schnellen Überblick über die Anzahl der Shards und den gesamten Shard-Speicher über Datenknoten hinweg.

Shard-zu-CPU-Verhältnis – Wenn ein Shard an einer Indexierungs- oder Suchanforderung beteiligt ist, verwendet es eine vCPU, um die Anforderung zu verarbeiten. Verwenden Sie als bewährte Methode einen anfänglichen Skalierungspunkt von 1,5 vCPU pro Shard. Wenn Ihr Instance-Typ 8 V

hatCPUs, legen Sie die Anzahl Ihrer Datenknoten so fest, dass jeder Knoten nicht mehr als sechs Shards hat. Beachten Sie, dass dies eine Annäherung ist. Testen Sie unbedingt Ihren Workload und skalieren Sie Ihren Cluster entsprechend.

Empfehlungen zu Speichervolumen, Shard-Größe und Instance-Typ finden Sie in den folgenden Ressourcen:

- the section called “Größenanpassung von Domains”
- the section called “Petabyte-Größe”

Vermeiden von Speicherversatz

Speicherversatz tritt auf, wenn ein oder mehrere Knoten innerhalb eines Clusters einen höheren Anteil an Speicher für einen oder mehrere Indizes halten als die anderen. Anzeichen für Speicherversatz sind ungleichmäßige CPU-Auslastung, intermittierende und ungleichmäßige Latenzzeiten und ungleichmäßige Warteschlangen auf den Datenknoten. Um festzustellen, ob Sie Probleme mit dem Versatz haben, lesen Sie die folgenden Abschnitte zur Fehlerbehebung:

- the section called “Knoten-Shard und Speicherversatz”
- the section called “Index-Shard und Speicherversatz”

Stabilität

Die folgenden bewährten Methoden gelten für die Aufrechterhaltung einer stabilen und fehlerfreien OpenSearch Service-Domain.

Bleiben Sie auf dem Laufenden mit OpenSearch

Service-Software-Updates

OpenSearch Service veröffentlicht regelmäßig Softwareupdates, die Funktionen hinzufügen oder Ihre Domains auf andere Weise verbessern. Updates ändern weder die Version noch die OpenSearch Version der Elasticsearch-Engine. Wir empfehlen, dass Sie einen wiederkehrenden Zeitpunkt für die Ausführung des DescribeDomainAPI-Vorgangs einplanen und gegebenenfalls ein Service-Software-Update einleiten. `UpdateStatus` `ELIGIBLE` Wenn Sie Ihre Domain nicht innerhalb eines bestimmten Zeitraums (normalerweise zwei Wochen) aktualisieren, führt der OpenSearch Service das Update automatisch durch.

OpenSearch Versions-Upgrades

OpenSearch Der Service bietet regelmäßig Unterstützung für von der Community verwaltete Versionen von. OpenSearch Führen Sie immer ein Upgrade auf die neuesten OpenSearch Versionen durch, wenn diese verfügbar sind.

OpenSearch Der Service aktualisiert gleichzeitig OpenSearch sowohl OpenSearch Dashboards als auch Dashboards (oder Elasticsearch und Kibana, wenn auf Ihrer Domain eine ältere Engine läuft). Wenn der Cluster über dedizierte Master-Knoten verfügt, werden Upgrades ohne Ausfallzeiten abgeschlossen. Andernfalls reagiert der Cluster nach dem Upgrade möglicherweise einige Sekunden lang nicht, während er einen Master-Knoten auswählt. OpenSearch Dashboards sind möglicherweise während eines Teils oder des gesamten Upgrades nicht verfügbar.

Es gibt zwei Möglichkeiten, eine Domain zu aktualisieren:

- Direktes Upgrade – Diese Option ist einfacher, da Sie denselben Cluster beibehalten.
- Snapshot-/Wiederherstellungs-Upgrade – Diese Option ist gut geeignet zum Testen neuer Versionen auf einem neuen Cluster oder zum Migrieren zwischen Clustern.

Unabhängig davon, welchen Upgradeprozess Sie verwenden, empfehlen wir, eine Domain zu verwalten, die ausschließlich zu Entwicklungs- und Testzwecken dient, und sie auf die neue Version zu aktualisieren, bevor Sie Ihre Produktion-Domain aktualisieren. Wählen Sie Development and testing (Entwicklung und Prüfung) als Bereitstellungstyp aus, wenn Sie die Test-Domain erstellen. Stellen Sie sicher, dass Sie alle Clients unmittelbar nach dem Domain-Upgrade auf kompatible Versionen aktualisieren.

Verbessern Sie die Snapshot-

Um zu verhindern, dass Ihr Snapshot bei der Verarbeitung hängen bleibt, sollte der Instance-Typ für den dedizierten Master-Knoten mit der Anzahl der Shards übereinstimmen. Weitere Informationen finden Sie unter the section called “Auswählen von Instance-Typen für dedizierte Hauptknoten”. Darüber hinaus sollte jeder Knoten nicht mehr als die empfohlenen 25 Shards pro GiB Java-Heap-Speicher haben. Weitere Informationen finden Sie unter the section called “Auswahl der Anzahl der Shards”.

Dedizierte Hauptknoten aktivieren

Dedizierte Hauptknoten erhöhen die Cluster-Stabilität. Ein dedizierter Hauptknoten führt Cluster-Verwaltungsaufgaben aus, enthält jedoch keine Indexdaten und antwortet nicht auf Client-

Anforderungen. Diese Auslagerung von Cluster-Verwaltungsaufgaben erhöht die Stabilität Ihrer Domain und ermöglicht es, einige Konfigurationsänderungen ohne Ausfallzeiten durchzuführen.

Aktivieren und verwenden Sie drei dedizierte Hauptknoten für optimale Domain-Stabilität in drei Availability Zones. Bei der Bereitstellung mit Multi-AZ mit Standby werden drei dedizierte Master-Knoten für Sie konfiguriert. Empfehlungen zu Instance-Typen finden Sie unter the section called "Auswählen von Instance-Typen für dedizierte Hauptknoten".

Bereitstellen über mehrere Availability Zones hinweg

Um Datenverlust zu vermeiden und die Ausfallzeit des Clusters im Falle einer Unterbrechung des Service zu minimieren, können Sie die Knoten auf zwei oder drei Availability Zones im selben AWS-Region verteilen. Eine bewährte Methode ist die Verwendung von Multi-AZ mit Standby, bei der drei Availability Zones konfiguriert werden, wobei zwei Zonen aktiv sind und eine als Standby-Zone fungiert, und mit zwei Replikat-Shards pro Index. Diese Konfiguration ermöglicht es dem OpenSearch Service, Replikat-Shards auf andere AZs als die entsprechenden primären Shards zu verteilen. Für die Cluster-Kommunikation zwischen Availability Zones fallen keine Availability-Zone-übergreifenden Datenübertragungsgebühren an.

Availability Zones sind isolierte Standorte innerhalb jeder -Region. Bei einer Konfiguration mit zwei Availability Zones bedeutet der Verlust einer Availability Zone, dass Sie die Hälfte der gesamten Domain-Kapazität verlieren. Durch die Umstellung auf drei Availability Zones werden die Auswirkungen des Verlusts einer einzelnen Availability Zone weiter reduziert.

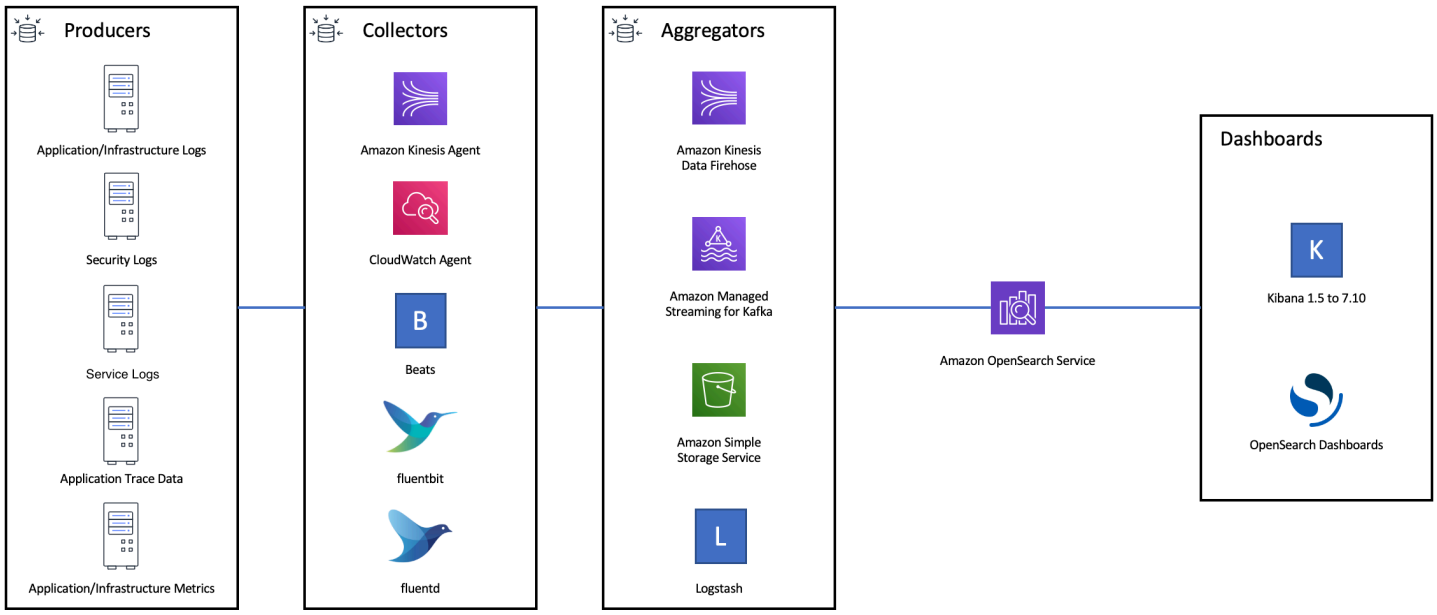
Steuern von Erfassungsablauf und Pufferung

Wir empfehlen, die Gesamtzahl der Anforderungen mithilfe des API-Vorgangs _bulk zu begrenzen. Es ist effizienter, eine `_bulk`-Anforderung zu senden, die 5 000 Dokumente enthält, als 5 000 Anforderungen zu senden, die jeweils ein Dokument enthalten.

Für eine optimale Betriebsstabilität ist es manchmal erforderlich, den Upstream-Ablauf von Indizierungsanforderungen zu begrenzen oder sogar anzuhalten. Die Begrenzung der Rate von Indexanforderungen ist ein wichtiger Mechanismus für den Umgang mit unerwarteten oder gelegentlichen Spitzen bei Anfragen, die andernfalls den Cluster überfordern könnten. Erwägen Sie, einen Mechanismus zur Ablaufkontrolle in Ihre Upstream-Architektur einzubauen.

Das folgende Diagramm zeigt mehrere Komponentenoptionen für eine Protokollerfassungsarchitektur. Konfigurieren Sie die Aggregationsebene so, dass ausreichend Platz

zum Puffern eingehender Daten für plötzliche Datenverkehrsspitzen und kurze Domain-Wartung vorhanden ist.



Erstellen von Zuordnungen für Such-Workloads

Erstellen Sie für Such-Workloads Zuordnungen, die definieren, wie Dokumente und ihre Felder OpenSearch gespeichert und indexiert werden. Setzen Sie `dynamic` auf `strict`, um ein versehentliches Hinzufügen neuer Felder zu verhindern:

```
PUT my-index
{
  "mappings": {
    "dynamic": "strict",
    "properties": {
      "title": { "type" : "text" },
      "author": { "type" : "integer" },
      "year": { "type" : "text" }
    }
  }
}
```

Verwenden von Indexvorlagen

Mithilfe einer Indexvorlage können Sie festlegen, wie ein Index konfiguriert wird, wenn er erstellt wird. OpenSearch Konfigurieren Sie Indexvorlagen, bevor Sie Indizes erstellen. Wenn Sie dann einen Index erstellen, erbt dieser die Einstellungen und Zuordnungen von der Vorlage. Sie können mehrere

Vorlage auf einen einzelnen Index anwenden, d. h. Sie können Einstellungen in einer Vorlage und Zuordnungen in einer anderen angeben. Diese Strategie ermöglicht eine Vorlage für allgemeine Einstellungen über mehrere Indizes hinweg und separate Vorlagen für spezifischere Einstellungen und Zuordnungen.

Die folgenden Einstellungen sind hilfreich bei der Konfiguration in Vorlagen:

- Anzahl der Primär- und Replikat-Shards
- Aktualisierungsintervall (wie oft der Index aktualisiert werden soll, damit die letzten Änderungen für die Suche verfügbar sind)
- Dynamische Zuordnungssteuerung
- Explizite Feldzuordnungen

Die folgende Beispielvorlage enthält jede dieser Einstellungen:

```
{
   "index_patterns":[
      "index-*"
   ],
   "order": 0,
   "settings": {
      "index": {
         "number_of_shards": 3,
         "number_of_replicas": 1,
         "refresh_interval": "60s"
      }
   },
   "mappings": {
      "dynamic": false,
      "properties": {
         "field_name1": {
            "type": "keyword"
         }
      }
   }
}
```

Auch wenn sie sich selten ändern, OpenSearch ist es einfacher, Einstellungen und Zuordnungen zentral zu definieren, als mehrere Upstream-Clients zu aktualisieren.

Indizes mit Indexstatusmanagement verwalten

Wenn Sie Protokolle oder Zeitreihendaten verwalten, empfehlen wir die Verwendung von Indexstatusmanagement (ISM). Mit ISM können Sie regelmäßige Aufgaben zur Verwaltung des Indexlebenszyklus automatisieren. Mit ISM können Sie Richtlinien erstellen, die Index-Alias-Rollover aufrufen, Index-Snapshots erstellen, Indizes zwischen Speicherebenen verschieben und alte Indizes löschen. Sie können den ISM-Rollover-Vorgang sogar als alternative Strategie für die Verwaltung des Datenlebenszyklus verwenden, um Shard-Versatz zu vermeiden.

Richten Sie zuerst eine ISM-Richtlinie ein. Ein Beispiel finden Sie unter the section called “Beispielrichtlinien”. Fügen Sie dann die Richtlinie einem oder mehreren Indizes zu. Wenn Sie ein ISM-Vorlagenfeld in die Richtlinie aufnehmen, wendet der OpenSearch Service die Richtlinie automatisch auf jeden Index an, der dem angegebenen Muster entspricht.

Entferne nicht verwendete Indizes

Überprüfen Sie regelmäßig die Indizes in Ihrem Cluster und identifizieren Sie alle, die nicht verwendet werden. Erstellen Sie einen Snapshot dieser Indizes, damit sie in S3 gespeichert werden, und löschen Sie sie dann. Wenn Sie nicht verwendete Indizes entfernen, reduzieren Sie die Anzahl der Shards und ermöglichen knotenübergreifend eine ausgewogenere Speicherverteilung und Ressourcenauslastung. Selbst im Leerlauf verbrauchen Indizes während der internen Indexwartung einige Ressourcen.

Anstatt ungenutzte Indizes manuell zu löschen, können Sie ISM verwenden, um automatisch einen Snapshot zu erstellen und Indizes nach einem bestimmten Zeitraum zu löschen.

Verwenden mehrerer Domains für hohe Verfügbarkeit

Um eine hohe Verfügbarkeit von über 99,9 % Betriebszeit in mehreren Regionen zu erreichen, sollten Sie die Verwendung von zwei Domains in Erwägung ziehen. Für kleine oder sich langsam ändernde Datensätze können Sie clusterübergreifende Replikation einrichten, um ein Aktiv-Passiv-Modell aufrechtzuerhalten. In diesem Modell wird nur in die Leader-Domain geschrieben, aber aus jeder Domain kann gelesen werden. Konfigurieren Sie für größere Datensätze und sich schnell ändernde Daten die duale Bereitstellung in Ihrer Aufnahmepipeline, sodass alle Daten in einem Aktiv-Aktiv-Modell unabhängig voneinander in beide Domains geschrieben werden.

Entwickeln Sie Ihre Upstream- und Downstream-Anwendungen unter Berücksichtigung von Failover. Stellen Sie sicher, dass Sie den Failover-Prozess zusammen mit anderen Notfallwiederherstellungsprozessen testen.

Leistung

Die folgenden bewährten Methoden gelten für die Abstimmung Ihrer Domains für eine optimale Leistung.

Größe und Komprimierung von Massenanfragen optimieren

Die Massengröße hängt von Ihren Daten, Ihrer Analyse und Ihrer Clusterkonfiguration ab, aber ein guter Ausgangspunkt sind 3–5 MiB pro Massenanforderung.

Senden Sie Anfragen und empfangen Sie Antworten von Ihren OpenSearch Domains, indem Sie die Gzip-Komprimierung verwenden, um die Nutzlast von Anfragen und Antworten zu reduzieren. Sie können die Gzip-Komprimierung mit dem OpenSearch Python-Client verwenden oder indem Sie die folgenden Header von der Clientseite aus einbeziehen:

- `'Accept-Encoding': 'gzip'`
- `'Content-Encoding': 'gzip'`

Zum Optimieren der Größe Ihrer Massenanforderungen beginnen Sie mit einer Massenanfragengröße von 3 MiB. Erhöhen Sie dann langsam die Anforderungsgröße, bis sich die Indizierungsleistung nicht mehr verbessert.

> **Note**
>
> Um die gzip-Komprimierung auf Domains zu aktivieren, auf denen Elasticsearch Version 6.x ausgeführt wird, müssen Sie `http_compression.enabled` auf Cluster-Ebene festlegen. Diese Einstellung ist standardmäßig in Elasticsearch-Versionen 7.x und allen Versionen von wahr. OpenSearch

Größe der Antworten auf Massenanfragen reduzieren

Um die Größe der OpenSearch Antworten zu reduzieren, schließen Sie unnötige Felder mit dem `filter_path` Parameter aus. Achten Sie darauf, keine Felder herauszufiltern, die zur Identifizierung oder Wiederholung fehlgeschlagener Anforderungen erforderlich sind. Weitere Informationen und Beispiele finden Sie unter the section called “Reduzierung der Antwortgröße”.

Aktualisierungsintervalle optimieren

OpenSearch Indizes weisen letztendlich Lesekonsistenz auf. Ein Aktualisierungsvorgang macht alle Aktualisierungen, die an einem Index durchgeführt werden, für die Suche verfügbar. Das standardmäßige Aktualisierungsintervall beträgt eine Sekunde, was bedeutet, dass OpenSearch jede Sekunde eine Aktualisierung durchgeführt wird, während in einen Index geschrieben wird.

Je seltener Sie einen Index aktualisieren (höheres Aktualisierungsintervall), desto besser ist die Indizierungsleistung insgesamt. Der Nachteil der Verlängerung des Aktualisierungsintervalls besteht darin, dass es eine längere Verzögerung zwischen einer Indexaktualisierung und dem Zeitpunkt gibt, zu dem die neuen Daten für die Suche verfügbar sind. Stellen Sie Ihr Aktualisierungsintervall so hoch wie möglich ein, um die Gesamtleistung zu verbessern.

Wir empfehlen, den `refresh_interval`-Parameter für alle Ihre Indizes auf 30 Sekunden oder mehr einzustellen.

Automatische Optimierung aktivieren

Auto-Tune verwendet Leistungs- und Nutzungsmetriken aus Ihrem OpenSearch Cluster, um Änderungen an den Warteschlangengrößen, Cachegrößen und den Einstellungen der Java Virtual Machine (JVM) auf Ihren Knoten vorzuschlagen. Diese optionalen Änderungen verbessern die Clustergeschwindigkeit und -stabilität. Sie können jederzeit zu den standardmäßigen OpenSearch Serviceeinstellungen zurückkehren. Automatische Optimierung ist bei neuen Domains standardmäßig aktiviert, es sei denn, Sie deaktivieren sie ausdrücklich.

Wir empfehlen, die automatische Optimierung für alle Domains zu aktivieren und entweder ein wiederkehrendes Wartungsfenster festzulegen oder die Empfehlungen regelmäßig zu überprüfen.

Sicherheit

Die folgenden bewährten Methoden gelten für die Sicherung Ihrer Domains.

Differenzierte Zugriffskontrolle aktivieren

Mit einer detaillierten Zugriffskontrolle können Sie steuern, wer auf bestimmte Daten innerhalb einer OpenSearch Dienstdomäne zugreifen kann. Im Vergleich zur allgemeinen Zugriffskontrolle gibt die differenzierte Zugriffssteuerung jedem Cluster, Index, Dokument und Feld eine eigene festgelegte Zugriffsrichtlinie. Zugriffskriterien können auf einer Reihe von Faktoren basieren, einschließlich der Rolle der Person, die den Zugriff anfordert, und der Aktion, die sie mit den Daten

durchführen möchte. Beispielsweise können Sie einem Benutzer Zugriff zum Schreiben in einen Index gewähren, während ein anderer nur Zugriff zum Lesen der Daten im Index erhält, ohne Änderungen vorzunehmen.

Durch die differenzierte Zugriffskontrolle können Daten mit unterschiedlichen Zugriffsanforderungen auf demselben Speicherplatz vorhanden sein, ohne dass Sicherheits- oder Compliance-Probleme auftreten.

Wir empfehlen, eine differenzierte Zugriffssteuerung für Ihre Domains zu aktivieren.

Bereitstellen von Domains innerhalb einer VPC

Wenn Sie Ihre OpenSearch Service-Domain in einer Virtual Private Cloud (VPC) platzieren, können Sie eine sichere Kommunikation zwischen dem OpenSearch Service und anderen Diensten innerhalb der VPC ermöglichen — ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains, die öffentliche Endpunkte nutzen, über eine zusätzliche Sicherheitsebene.

Wir empfehlen, dass Sie Ihre Domains innerhalb einer VPC erstellen.

Anwenden einer restriktiven Zugriffsrichtlinie

Selbst wenn Ihre Domain innerhalb einer VPC bereitgestellt wird, ist das Implementieren der Sicherheit in mehreren Schichten eine bewährte Methode. Stellen Sie sicher, dass Sie die Konfiguration Ihrer aktuellen Zugriffsrichtlinien überprüfen.

Wenden Sie eine restriktive, ressourcenbasierte Zugriffsrichtlinie auf Ihre Domains an und folgen Sie dem Prinzip der geringsten Rechte, wenn Sie Zugriff auf die Konfigurations-API und die OpenSearch API-Operationen gewähren. Vermeiden Sie in der Regel die Verwendung des anonymen Benutzerprinzipals `"Principal": {"AWS": "*" }` in Ihren Zugriffsrichtlinien.

In einigen Situationen ist es jedoch akzeptabel, eine offene Zugriffsrichtlinie zu verwenden, z. B. wenn Sie eine differenzierte Zugriffssteuerung aktivieren. Eine offene Zugriffsrichtlinie kann Ihnen den Zugriff auf die Domain in Fällen ermöglichen, in denen das Signieren von Anforderungen schwierig oder unmöglich ist, z. B. von bestimmten Clients und Tools.

Verschlüsselung im Ruhezustand aktivieren

OpenSearch Service-Domains bieten Verschlüsselung von Daten im Ruhezustand, um unbefugten Zugriff auf Ihre Daten zu verhindern. Encryption at Rest verwendet AWS Key Management Service

(AWS KMS) zum Speichern und Verwalten Ihrer Verschlüsselungsschlüssel und den Advanced Encryption Standard-Algorithmus mit 256-Bit-Schlüsseln (AES-256) zur Verschlüsselung.

Wenn Ihre Domain sensible Daten speichert, aktivieren Sie die Verschlüsselung der Daten im Ruhezustand.

Aktivieren Sie die Verschlüsselung node-to-node

Node-to-node Die Verschlüsselung bietet zusätzlich zu den Standardsicherheitsfunktionen des OpenSearch Dienstes eine zusätzliche Sicherheitsebene. Es implementiert Transport Layer Security (TLS) für die gesamte Kommunikation zwischen den Knoten, die innerhalb OpenSearch des Systems bereitgestellt werden. Node-to-nodeVerschlüsselung: Alle Daten, die über HTTPS an Ihre OpenSearch Service-Domain gesendet werden, bleiben während der Übertragung verschlüsselt, während sie zwischen den Knoten verteilt und repliziert werden.

Wenn Ihre Domain vertrauliche Daten speichert, aktivieren Sie die node-to-node Verschlüsselung.

Überwachen Sie mit AWS Security Hub

Überwachen Sie Ihre Nutzung des OpenSearch Dienstes in Bezug auf bewährte Sicherheitsverfahren, indem Sie AWS Security Hub Security Hub verwendet Sicherheitskontrollen für die Bewertung von Ressourcenkonfigurationen und Sicherheitsstandards, um Sie bei der Einhaltung verschiedener Compliance-Frameworks zu unterstützen. Weitere Informationen zur Verwendung von Security Hub zur Evaluierung von OpenSearch Serviceressourcen finden Sie unter Amazon OpenSearch Service Steuerelemente im AWS Security Hub Benutzerhandbuch.

Kostenoptimierung

Die folgenden bewährten Methoden gelten für die Optimierung und Einsparung Ihrer OpenSearch Servicekosten.

Instance-Typen der neuesten Generation verwenden

OpenSearch Der Service führt ständig neue EC2 Amazon-Instance-Typen ein, die eine bessere Leistung zu geringeren Kosten bieten. Wir empfehlen, immer die Instances der neuesten Generation zu verwenden.

Vermeiden Sie es, T2 oder `t3.small`-Instances für Produktion-Domains zu verwenden, da diese bei anhaltender hoher Last instabil werden können. `r6g.large`-Instances sind eine Option für kleine Produktion-Workloads (sowohl als Datenknoten als auch als dedizierte Hauptknoten).

Verwenden Sie die neuesten Amazon-EBS-gp3-Volumes

OpenSearch Datenknoten benötigen Speicher mit geringer Latenz und hohem Durchsatz, um eine schnelle Indizierung und Abfrage zu ermöglichen. Durch die Verwendung von Amazon-EBS-gp3-Volumes erhalten Sie eine höhere Basisleistung (IOPS und Durchsatz) zu 9,6 % niedrigeren Kosten als mit dem zuvor angebotenen Amazon-EBS-gp2-Volume-Typ. Mit gp3 können Sie unabhängig von der Volume-Größe zusätzliche IOPS und Durchsätze bereitstellen. Diese Volumes sind auch stabiler als Volumes der vorherigen Generation, da sie keine Burst-Gutschriften verwenden. Der GP3-Volumetyp verdoppelt außerdem die per-data-node Volumengrößenbeschränkungen des GP2-Volumetyps. Mit diesen größeren Volumina können Sie die Kosten für passive Daten senken, indem Sie die Speichermenge pro Datenknoten erhöhen.

Verwendung UltraWarm und Cold Storage für Zeitreihen-Protokolldaten

Wenn Sie sie OpenSearch für Protokollanalysen verwenden, verschieben Sie Ihre Daten in einen UltraWarm Kühlraum, um die Kosten zu senken. Verwenden Sie Indexstatusmanagement (ISM), um Daten zwischen Speicherebenen zu migrieren und die Datenaufbewahrung zu verwalten.

UltraWarmbietet eine kostengünstige Möglichkeit, große Mengen schreibgeschützter Daten im OpenSearch Service zu speichern. UltraWarm verwendet Amazon S3 für die Speicherung, was bedeutet, dass die Daten unveränderlich sind und nur eine Kopie benötigt wird. Sie zahlen nur für den Speicherplatz, der der Größe der primären Shards in Ihren Indizes entspricht. Die Latenzen für UltraWarm Abfragen steigen mit der Menge an S3-Daten, die für die Bearbeitung der Abfrage benötigt werden. Nachdem die Daten auf den Knoten zwischengespeichert wurden, verhalten sich Abfragen an UltraWarm Indizes ähnlich wie Abfragen an Hot-Indizes.

Cold Storage wird auch von S3 unterstützt. Wenn Sie kalte Daten abfragen müssen, können Sie sie selektiv an vorhandene Knoten anhängen. UltraWarm Für kalte Daten fallen dieselben verwalteten Speicherkosten an wie UltraWarm, aber Objekte im Cold Storage verbrauchen keine UltraWarm Knotenressourcen. Daher bietet Cold Storage eine beträchtliche Menge an Speicherkapazität, ohne die Größe oder Anzahl der UltraWarm Knoten zu beeinflussen.

UltraWarm wird kostengünstig, wenn Sie etwa 2,5 TiB an Daten aus dem Hot-Storage migrieren müssen. Überwachen Sie Ihre Füllrate und planen Sie, Indizes zu verschieben, UltraWarm bevor Sie dieses Datenvolumen erreichen.

Empfehlungen für Reserved Instances überprüfen

Erwägen Sie den Kauf von Reserved Instances (RIs), wenn Sie einen guten Basiswert für Ihre Leistung und Ihren Rechenverbrauch haben. Rabatte beginnen bei etwa 30 % für 1-Jahres-Reservierungen ohne Vorauszahlung und können bis zu 50 % für alle 3-Jahres-Verpflichtungen im Voraus erhöhen.

Wenn Sie einen stabilen Betrieb für mindestens 14 Tage beobachtet haben, lesen Sie im AWS Cost Management Benutzerhandbuch den Abschnitt Zugriff auf Reservierungsempfehlungen. In der Überschrift Amazon OpenSearch Service werden spezifische Kaufempfehlungen von RI und prognostizierte Einsparungen angezeigt.

Dimensionierung von Amazon OpenSearch Service-Domains

Es gibt keine perfekte Methode zur Dimensionierung von Amazon OpenSearch Service-Domains. Wenn Sie jedoch mit einem Verständnis Ihrer Speicheranforderungen, des Services und OpenSearch selbst beginnen, können Sie eine fundierte erste Schätzung Ihres Hardwarebedarfs vornehmen. Diese Schätzung kann als Ausgangspunkt für den wichtigsten Aspekt der Dimensionierung von Domains dienen: Tests mit repräsentativen Workloads und Überwachung ihrer Leistung.

Themen

- Berechnung der Speicheranforderungen
- Auswahl der Anzahl der Shards
- Auswählen von Instance-Typen und Tests

Berechnung der Speicheranforderungen

Die meisten OpenSearch Workloads lassen sich in eine von zwei großen Kategorien einteilen:

- Langlebiger Index: Sie schreiben Code, der Daten in einem oder mehreren Indizes verarbeitet und diese OpenSearch Indizes dann regelmäßig aktualisiert, wenn sich die Quelldaten ändern. Einige allgemeine Beispiele sind Suchen auf Websites, in Dokumenten und für e-Commerce-Zwecke.
- Rolling-Indizes: Daten fließen kontinuierlich in einen Satz temporärer Indizes mit einem Indizierungszeitraum und einem Aufbewahrungsfenster (z. B. einen Satz täglicher Indizes, der zwei Wochen lang aufbewahrt wird). Einige allgemeine Beispiele sind Protokollanalyse, Zeitreihenverarbeitung und Clickstream-Analyse.

Für langlebige Index-Workloads können Sie die Quelldaten auf dem Datenträger untersuchen und einfach bestimmen, wie viel Speicherplatz dafür benötigt wird. Wenn die Daten aus mehreren Quellen stammen, addieren Sie diese Quellen einfach.

Für Rolling-Indizes können Sie die während eines repräsentativen Zeitraums generierten Datenmenge mit dem Aufbewahrungszeitraum multiplizieren. Wenn Sie beispielsweise 200 MiB Protokolldaten pro Stunde generieren, sind das 4,7 GiB pro Tag, also 66 GiB Daten zu jedem Zeitpunkt, wenn Sie einen Aufbewahrungszeitraum von zwei Wochen verwenden.

Die Größe Ihrer Datenquelle ist jedoch nur ein Aspekt Ihrer Speicheranforderungen. Außerdem müssen Sie Folgendes berücksichtigen:

- Anzahl der Replikate: Jedes Replikat ist eine vollständige Kopie des primären Shards. Die Speichergröße des Indexes gibt die Größe an, die der Primär- und der Replikat-Shard einnehmen. Standardmäßig hat jeder OpenSearch Index ein Replikat. Wir empfehlen, mindestens eines zu verwenden, um sich gegen Datenverlust zu schützen. Replikate können auch die Suchleistung verbessern. Wenn Sie einen hohen Workload haben, können Sie in Betracht ziehen, mehrere zu erstellen. Verwenden Sie `PUT /my-index/_settings`, um die `number_of_replicas`-Einstellung für Ihren Index zu aktualisieren.
- OpenSearch Indizierungsaufwand: Die Größe eines Indexes auf der Festplatte variiert. Die Gesamtgröße der Quelldaten plus Index beträgt oft 110 % der Quelle, wobei der Index bis zu 10 % der Quelldaten ausmacht. Nachdem Sie Ihre Daten indiziert haben, können Sie die `_cat/indices?v`-API und den `pri.store.size`-Wert verwenden, um den genauen Zusatzaufwand zu berechnen. `_cat/allocation?v` bietet auch eine nützliche Zusammenfassung.
- Für das Betriebssystem reservierter Speicherplatz: Standardmäßig reserviert Linux 5 % des Dateisystems für den `root`-Benutzer für kritische Prozesse, zur Systemwiederherstellung und zum Schutz vor Problemen mit der Festplattenfragmentierung.
- OpenSearch Serviceaufwand: Der OpenSearch Service reserviert 20% des Speicherplatzes jeder Instanz (bis zu 20 GiB) für Segmentzusammenführungen, Protokolle und andere interne Operationen.

  Aufgrund dieses Höchstwerts von 20 GiB kann die Gesamtmenge an reserviertem Speicherplatz stark variieren und hängt von der Anzahl der Instances in Ihrer Domain ab. Beispiel: Eine Domain kann drei `m6g.xlarge.search`-Instances haben, mit jeweils 500 GiB Speicherplatz, also insgesamt 1,46 TiB. In diesem Fall beträgt der gesamte reservierte Speicherplatz nur 60 GiB. Eine andere Domain kann 10 `m3.medium.search`-Instances haben, mit jeweils 100 GiB Speicherplatz,

also insgesamt 0,98 TiB. Hier beträgt der gesamte reservierte Speicherplatz 200 GiB, auch wenn die erste Domain 50 % größer ist.

In der folgenden Formel wenden wir eine „Worst-Case“-Schätzung für den Zusatzaufwand an. Diese Schätzung beinhaltet zusätzlichen freien Speicherplatz, um die Auswirkungen von Knotenausfällen und Ausfällen der Availability Zone zu minimieren.

Wenn Sie insgesamt jederzeit 66 GiB Quelldaten haben und ein Replikat verwenden wollen, liegt Ihr minimaler Speicherbedarf nahe 66 * 2 * 1,1/0,95/0,8 = 191 GiB. Sie können diese Berechnung wie folgt verallgemeinern:

Quelldaten * (1 + Anzahl von Replikaten) * (1 + Indexierungsaufwand)/(1 — reservierter Linux-Speicherplatz)/(1 — OpenSearch Serviceaufwand) = Mindestspeicherbedarf

Sie können diese vereinfachte Version verwenden:

Quelldaten * (1 + Anzahl der Replikate) * 1,45 = Mindestspeicheranforderung

Unzureichender Speicherplatz ist eine der häufigsten Ursachen für Clusterinstabilität. Sie sollten also die Zahlen überprüfen, wenn Sie Instance-Typen, Instance-Anzahlen und Speicher-Volumes auswählen.

Es gibt weitere Überlegungen zum Speicher.

- Wenn Ihre Mindestspeicheranforderungen 1 PB überschreiten, lesen Sie nach unter the section called “Petabyte-Größe”.
- Wenn Sie Rolling-Indizes haben und eine Hot-Warm-Architektur verwenden wollen, lesen Sie the section called “UltraWarm Speicher”.

Auswahl der Anzahl der Shards

Nachdem Sie die Speicheranforderungen kennen, können Sie über Ihre Indizierungsstrategie nachdenken. Standardmäßig ist in OpenSearch Service jeder Index in fünf primäre Shards und ein Replikat (insgesamt 10 Shards) unterteilt. Dieses Verhalten unterscheidet sich von Open Source OpenSearch, bei dem standardmäßig ein primärer Shard und ein Replikat-Shard verwendet werden. Da Sie die Anzahl der primären Shards für einen vorhandenen Index nicht leicht ändern können, sollten Sie die Anzahl der Shards festlegen, bevor Sie Ihr erstes Dokument indizieren.

Das übergeordnete Ziel bei der Auswahl der Shard-Anzahl ist es, einen Index gleichmäßig über alle Knoten im Cluster zu verteilen. Diese Shards sollten jedoch nicht zu groß oder zu zahlreich sein. Als allgemeine Richtlinie gilt, dass die Shard-Größe bei Workloads, bei denen die Suchlatenz ein wichtiges Leistungsziel ist, zwischen 10 und 30 GiB und bei schreibintensiven Workloads wie der Protokollanalyse zwischen 30 und 50 GiB liegen sollte.

Große Shards können die Wiederherstellung OpenSearch nach einem Ausfall erschweren. Da jedoch jede Shard eine gewisse Menge an CPU und Arbeitsspeicher beansprucht, können zu viele kleine Shards zu Leistungsproblemen und Fehlern aufgrund unzureichender Speicherkapazität führen. Mit anderen Worten, Shards sollten klein genug sein, dass die zugrunde liegende OpenSearch Service-Instanz sie verarbeiten kann, aber nicht so klein, dass sie die Hardware unnötig belasten.

Angenommen, Sie haben 66 GiB Daten. Sie gehen nicht davon aus, dass diese Anzahl mit der Zeit zunimmt, und Sie möchten Ihre Shards mit je 30 GiB beibehalten. Die Anzahl der Shards sollte deshalb ca. 66 * 1,1/30 = 3 betragen. Sie können diese Berechnung wie folgt verallgemeinern:

(Datenquelle + Wachstumspotenzial) * (1 + Indizierungsaufwand)/Gewünschte Shard-Größe = Ungefähre Anzahl der primären Shards

Diese Gleichung hilft Daten-Wachstum im Laufe der Zeit auszugleichen. Wenn Sie davon ausgehen, dass sich dieselben 66 GiB Daten innerhalb des nächsten Jahres vervierfachen, ist die ungefähre Anzahl der Shards (66 + 198) * 1,1 / 30 = 10. Beachten Sie jedoch, dass Sie diese zusätzlichen 198 GiB Daten noch nicht haben. Stellen Sie sicher, dass diese Vorbereitung für die Zukunft nicht unnötig kleine Shards erzeugt, die aktuell sehr große Mengen an CPU-Leistung und Speicher verbrauchen. In diesem Fall sind 66 * 1,1/10 Shards = 7,26 GiB pro Shard, was zusätzliche Ressourcen verbraucht und unterhalb des empfohlenen Größenbereichs liegt. Sie könnten eher den middle-of-the-road Ansatz von sechs Shards in Betracht ziehen, sodass Sie heute 12-GiB-Shards und in future 48-GiB-Shards haben werden. Auch hier könnten Sie bevorzugen, mit drei Shards zu beginnen und Ihre Daten neu zu indizieren, wenn die Shards über 50 GiB zunehmen.

Ein weitaus weniger häufiges Problem ist die Begrenzung der Shard-Anzahl pro Knoten. Wenn Sie Ihre Shards entsprechend dimensionieren, geht Ihnen in der Regel schon lange vor Erreichen dieser Grenze der Datenträger-Speicherplatz aus. Beispielsweise verfügt eine `m6g.large.search`-Instance über eine maximale Datenträgergröße von 512 GiB. Wenn Sie unter 80 % der Datenträgernutzung bleiben und die Größe Ihrer Shards bei 20 GiB liegt, können ungefähr 20 Shards untergebracht werden. Elasticsearch 7. x und höher sowie alle Versionen OpenSearch bis 2.15 haben ein Limit von 1.000 Shards pro Knoten. Um die maximalen Shards pro Knoten anzupassen, konfigurieren Sie die `cluster.max_shards_per_node`-Einstellung. Für

OpenSearch 2.17 und höher unterstützt OpenSearch Service 1000 Shards pro 16 GB JVM-Heap-Speicher, bis zu einem Maximum von 4000 Shards pro Knoten. Ein Beispiel finden Sie unter Cluster-Einstellungen. Weitere Informationen zur Anzahl der Shards finden Sie unter. the section called “Anzahl der Kontingente”

Durch eine angemessene Dimensionierung der Shards bleiben Sie fast immer unter dieser Grenze, Sie können jedoch auch die Anzahl der Shards pro GiB des Java-Heaps prüfen. Auf einem vorgegebenen Knoten sollten Sie nicht mehr als 25 Shards pro GB des Java-Heaps haben. Eine `m5.large.search`-Instance verfügt bspw. über einen 4-GiB-Heap, sodass jeder Knoten nicht mehr als 100 Shards haben sollte. Bei dieser Anzahl an Shards ist jeder Shard etwa 5 GiB groß, was weit unter unserer Empfehlung liegt.

Auswählen von Instance-Typen und Tests

Nachdem Sie Ihre Speicheranforderungen berechnet und die Anzahl der benötigten Shards ausgewählt haben, können Sie Hardware-Entscheidungen treffen. Hardware-Anforderungen variieren je nach Workload erheblich. Wir können jedoch einige grundlegende Empfehlungen bieten.

Im Allgemeinen entsprechen die Speicherlimits für jeden Instance-Typ der CPU-Leistung und dem Speicher, die Sie gegebenenfalls für geringe Workloads benötigen. Angenommen, eine `m6g.large.search`-Instance hat eine maximale EBS-Volume-Größe von 512 GiB, 2 vCPU-Prozessorkerne und 8 GiB Arbeitsspeicher. Wenn Ihr Cluster viele Shards hat, aufwändige Aggregationen ausführt, Dokumente häufig aktualisiert oder eine große Anzahl von Abfragen verarbeitet, sind diese Ressourcen möglicherweise für Ihre Anforderungen nicht ausreichend. Wenn Ihr Cluster in eine dieser Kategorien fällt, versuchen Sie es zunächst mit einer Konfiguration von eher 2 vCPU-Prozessorkernen und 8 GiB Arbeitsspeicher für je 100 GiB Ihrer Speicheranforderung.

> **Tip**
>
> Eine Zusammenfassung der Hardwareressourcen, die jedem Instance-Typ zugewiesen sind, finden Sie unter Amazon OpenSearch Service-Preise.

Dennoch sind auch diese Ressourcen möglicherweise nicht ausreichend. Einige OpenSearch Benutzer berichten, dass sie ein Vielfaches dieser Ressourcen benötigen, um ihre Anforderungen zu erfüllen. Um die richtige Hardware für Ihre Workloads zu finden, müssen Sie eine fundierte erste Einschätzung vornehmen, mit repräsentativen Workloads testen, anpassen und erneut testen.

Schritt 1: Machen Sie einen ersten Schätzwert

Zu Beginn empfehlen wir mindestens drei Knoten, um mögliche OpenSearch Probleme zu vermeiden, wie z. B. einen Split-Brain-Status (wenn ein Kommunikationsausfall dazu führt, dass ein Cluster zwei Master-Knoten hat). Wenn Sie drei dedizierte Hauptknoten haben, empfehlen wir immer noch mindestens zwei Datenknoten für die Replikation.

Schritt 2: Berechnen Sie den Speicherbedarf pro Knoten

Wenn Sie eine Speicheranforderung von 184 GiB haben und die empfohlene Mindestanzahl von drei Knoten, verwenden Sie die Gleichung 184/3 = 61 GiB, um den Speicherplatz zu ermitteln, die jeder Knoten benötigt. In diesem Beispiel könnten Sie drei `m6g.large.search`-Instances auswählen, die jeweils ein EBS-Speicher-Volume mit 90 GiB verwenden, sodass Sie über eine Sicherheitsreserve verfügen und Wachstum im Laufe der Zeit unterstützen können. Diese Konfiguration bietet 6 vCPU-Kerne und 24 GiB Arbeitsspeicher, sodass sie für leichtere Workloads geeignet ist.

Als größer ausgelegtes Beispiel nehmen Sie etwa eine Speicheranforderung von 14 TiB (14.336 GiB) Speicher und einen hohen Workload an. In diesem Fall können Sie damit beginnen, Tests mit 2 * 144 = 288 vCPU-Prozessorkernen und 8 * 144 = 1152 GiB Arbeitsspeicher zu beginnen. Diese Zahlen funktionieren für etwa 18 `i3.4xlarge.search`-Instances. Wenn Sie keinen schnellen, lokalen Speicher benötigen, können Sie auch 18 `r6g.4xlarge.search`-Instances mit jeweils einem EBS-Speicher-Volume mit 1 TiB testen.

Informationen zu Clustern mit Hunderten von Terabytes an Daten finden Sie unter the section called “Petabyte-Größe”.

Schritt 3: Führen Sie repräsentative Tests durch

Nach der Konfiguration des Clusters können Sie Ihre Indizes anhand der zuvor berechneten Anzahl von Shards hinzufügen, einige repräsentative Client-Tests anhand eines realistischen Datensatzes durchführen und CloudWatch Metriken überwachen, um zu sehen, wie der Cluster mit der Arbeitslast umgeht.

Schritt 4: Erfolg oder Iterieren

Wenn die Leistung Ihren Anforderungen entspricht, die Tests erfolgreich sind und die CloudWatch Metriken normal sind, ist der Cluster einsatzbereit. Denken Sie daran, CloudWatch Alarme einzurichten, um eine ungesunde Ressourcennutzung zu erkennen.

Wenn die Leistung nicht akzeptabel ist, Tests fehlschlagen oder `CPUUtilization` oder `JVMMemoryPressure` hoch sind, müssen Sie möglicherweise einen anderen Instance-Typ wählen (oder Instances hinzufügen) und die Tests fortsetzen. Wenn Sie Instances hinzufügen, OpenSearch wird die Verteilung der Shards im Cluster automatisch ausgeglichen.

Da es einfacher ist, die überschüssige Kapazität in einem überlasteten Cluster als das Defizit in einem zu wenig ausgelasteten Cluster zu messen, empfehlen wir, mit einem Cluster zu beginnen, der größer ist als der, den Sie wahrscheinlich benötigen werden. Testen und skalieren Sie anschließend abwärts zu einem effizienten Cluster, der über die zusätzlichen Ressourcen verfügt, um einen stabilen Betrieb in Zeiten erhöhter Aktivität sicherzustellen.

Produktions-Cluster oder Cluster mit komplexen Zuständen profitieren von dedizierten Hauptknoten, die die Leistung und Cluster-Zuverlässigkeit verbessern.

Petabyte-Größe im Amazon Service OpenSearch

OpenSearch Amazon-Domänen bieten einen angeschlossenen Speicher von bis zu 10 PB. Sie können eine Domain mit 1000 `OR1.16xlarge.search` Instance-Typen mit jeweils 36 TB Speicher konfigurieren. Aufgrund des großen Unterschieds bei der Skalierung unterscheiden sich die Empfehlungen für Domänen dieser Größe von unseren allgemeinen Empfehlungen. In diesem Abschnitt werden Überlegungen bei der Erstellung von Domänen, Kosten, Speicher und Shard-Größe dargelegt.

In diesem Abschnitt wird zwar häufig auf die `i3.16xlarge.search` Instance-Typen verwiesen, Sie können jedoch auch mehrere andere Instance-Typen verwenden, um insgesamt 10 PB Domain-Speicher zu erreichen.

Domänen erstellen

> Domänen dieser Größe überschreiten das Standardlimit von 80 Instanzen pro Domain. Um eine Erhöhung der Serviceobergrenze von bis zu 1000 Instances pro Domäne anzufordern, erstellen Sie einen Fall im AWS -Support-Center.

Preisgestaltung

> Bevor Sie eine Domäne dieser Größe erstellen, lesen Sie auf der Seite Amazon OpenSearch Service — Preise nach, um sicherzustellen, dass die Kosten Ihren Erwartungen entsprechen. Überprüfen Sie the section called “UltraWarm Speicher” darauf, ob eine Hot-Warm-Architektur zu Ihrem Anwendungsfall passt.

Speicher

Die `i3` Instance-Typen sind so konzipiert, dass sie schnellen, lokalen, nichtflüchtigen Memory-Express-Speicher (NVMe) bereitstellen. Da dieser lokale Speicher häufig Leistungsvorteile im Vergleich zu Amazon Elastic Block Store aufweist, sind EBS-Volumes keine Option, wenn Sie diese Instance-Typen in OpenSearch Service auswählen. Wenn Sie lieber EBS-Speicher, verwenden Sie einen anderen Instance-Typ, z. B. `r6.12xlarge.search`.

Shard-Größe und -Anzahl

Ein üblicher OpenSearch Anhaltswert ist, 50 GB pro Shard nicht zu überschreiten. Aufgrund der Anzahl der Shards, die für große Domänen und die verfügbaren Ressourcen für `i3.16xlarge.search`-Instances erforderlich sind, empfehlen wir eine Shard-Größe von 100 GB.

Wenn Sie beispielsweise 450 TB Quelldaten haben und ein Replikat verwenden wollen, liegt Ihr minimaler Speicherbedarf nahe 450 TB * 2 * 1,1/0,95 = 1,04 PB. Eine Erklärung dieser Berechnung finden Sie unter the section called “Berechnung der Speicheranforderungen”. Obwohl 1.04 PB / 15 TB = 70 Instances ergibt, sollten Sie 90 oder mehr `i3.16xlarge.search` Instances wählen, damit Sie eine Sicherheitsreserve, einen Deal mit Knotenfehlern haben und Abweichungen in der Datenmenge im Laufe der Zeit berücksichtigt werden. Von jeder Instance werden weitere 20 GiB zu den Mindestspeicheranforderungen hinzugefügt, aber bei Datenträgern dieser Größe sind 20 GiB nahezu vernachlässigbar.

Das Steuern der Anzahl der Shards ist schwierig. OpenSearch Benutzer rotieren Indizes oft täglich und behalten Daten eine oder zwei Wochen lang bei. In diesem Fall finden Sie es möglicherweise nützlich, zwischen "aktiven" und "inaktiven" Shards zu unterscheiden. Aktive Shards werden aktiv gelesen oder geschrieben. Inaktive Shards können einige Leseanforderungen bedienen, sind aber größtenteils im Leerlauf. Im Allgemeinen gilt, die Anzahl der aktiven Shards unten ein paar Tausend zu halten. Wenn sich die Anzahl der aktiven Shards 10.000 nähert, ist dies mit erheblichen Leistungs- und Stabilitätsrisiken verbunden.

Zum Berechnen der Anzahl der primären Shards verwenden Sie die folgende Formel: 450.000 GB * 1,1/100 GB pro Shard = 4,950 Shards. Eine Verdoppelung dieser Anzahl zur Berücksichtigung von Replikaten ergibt 9.900 Shards. Wenn alle Shards aktiv sind, stellt dies ein großes Problem dar. Wenn Sie jedoch die Indizes rotieren und nur 1/7 oder 1/14 der Shards an einem bestimmten Tag aktiv sind (1 414 bzw. 707 Shards), kann der Cluster gut funktionieren. Wie immer besteht der wichtigste Schritt bei der Dimensionierung und Konfiguration Ihrer Domäne darin, repräsentative Client-Tests unter Verwendung einer realistischen Datenmenge auszuführen.

Dedizierte Koordinatorknoten in Amazon OpenSearch Service

Dedizierte Koordinatorknoten in Amazon OpenSearch Service sind spezialisierte Knoten, die Koordinationsaufgaben von Datenknoten auslagern. Zu diesen Aufgaben gehören die Verwaltung von Suchanfragen und das Hosten von OpenSearch Dashboards. Durch die Trennung dieser Funktionen reduzieren dedizierte Koordinatorknoten die Belastung der Datenknoten, sodass sie sich auf Datenspeicherung, Indexierung und Suchvorgänge konzentrieren können. Dies verbessert die Gesamtleistung des Clusters und die Ressourcennutzung.

Darüber hinaus tragen dedizierte Koordinatorknoten dazu bei, die Anzahl der für VPC-Konfigurationen erforderlichen privaten IP-Adressen zu reduzieren, was zu einem effizienteren Netzwerkmanagement führt. Diese Konfiguration kann je nach den Merkmalen der Arbeitslast zu einer Verbesserung des Indexdurchsatzes um bis zu 15% und einer um 20% besseren Abfrageleistung führen.

Wann sollten dedizierte Koordinatorknoten verwendet werden

Dedizierte Koordinatorknoten sind in den folgenden Szenarien am vorteilhaftesten.

- Große Cluster — In Umgebungen mit einem hohen Datenvolumen oder komplexen Abfragen kann die Verlagerung von Koordinationsaufgaben auf dedizierte Knoten die Clusterleistung verbessern.
- Häufige Abfragen — Workloads mit häufigen Suchanfragen oder Aggregationen, insbesondere solche mit komplexen Datumshistogrammen oder mehreren Aggregationen, profitieren von einer schnelleren Abfrageverarbeitung.
- Starke Nutzung von Dashboards — Dashboards können ressourcenintensiv sein. OpenSearch Die Übertragung dieser Verantwortung auf spezielle Koordinatorknoten reduziert die Belastung der Datenknoten.

Architektur und Verhalten

In einem OpenSearch Cluster übernehmen dedizierte Koordinatorknoten zwei Hauptaufgaben.

- Bearbeitung von Anfragen — Diese Knoten empfangen eingehende Suchanfragen und leiten sie an die entsprechenden Datenknoten weiter, die die entsprechenden Daten speichern. Anschließend konsolidieren sie die Ergebnisse mehrerer Datenknoten zu einer einzigen globalen Ergebnismenge, die an den Client zurückgegeben wird.

- Hosting von Dashboards — Coordinator-Knoten verwalten OpenSearch Dashboards, wodurch Datenknoten von der zusätzlichen Belastung durch das Hosten von OpenSearch Dashboards und die Bearbeitung des damit verbundenen Datenverkehrs entlastet werden.

In VPC-Domänen werden dedizierten Koordinatorknoten statt Datenknoten Elastic Network Interfaces (ENIs) zugewiesen. Diese Anordnung trägt dazu bei, die Anzahl der erforderlichen privaten IP-Adressen zu reduzieren VPCs, was die Netzwerkeffizienz verbessert. In der Regel machen dedizierte Koordinatorknoten etwa 10% der gesamten Datenknoten aus.

Anforderungen und Einschränkungen

Für dedizierte Koordinatorknoten gelten die folgenden Anforderungen und Einschränkungen.

- Dedizierte Koordinatorknoten werden in allen OpenSearch Versionen und den Elasticsearch-Versionen 6.8 bis 7.10 unterstützt.
- Um dedizierte Koordinatorknoten zu aktivieren, müssen für Ihre Domain dedizierte Master-Knoten aktiviert sein. Weitere Informationen finden Sie unter the section called “Dedizierte Hauptknoten”.
- Für die Bereitstellung von dedizierten Koordinatorknoten können zusätzliche Kosten anfallen. Die verbesserte Ressourceneffizienz und die verbesserte Leistung rechtfertigen jedoch die Investition, insbesondere für große oder komplexe Cluster.

Bereitstellung dedizierter Koordinatorknoten

Führen Sie die folgenden Schritte aus, um dedizierte Koordinatorknoten in einer vorhandenen Domäne bereitzustellen. Stellen Sie sicher, dass in Ihrer Domain dedizierte Master-Knoten aktiviert sind, bevor Sie Koordinatorknoten bereitstellen.

Konsole

Um dedizierte Koordinatorknoten im bereitzustellen AWS Management Console

1. Melden Sie sich zu https://console.aws.amazon.com/aos/Hause bei der Amazon OpenSearch Service-Konsole an.
2. Wählen Sie Domains und dann die Domain aus, die Sie ändern möchten.
3. Wählen Sie im Abschnitt Clusterkonfiguration die Option Bearbeiten aus.
4. Wählen Sie Dedizierte Koordinatorknoten aktivieren aus.
5. Wählen Sie den Instanztyp und die Anzahl der bereitzustellenden Koordinatorknoten aus.

6. Wählen Sie Änderungen speichern aus. Es kann mehrere Minuten dauern, bis die Domain aktualisiert ist.

AWS CLI

Verwenden Sie den update-domain-configBefehl AWS CLI, um mit dem dedizierte Koordinatorknoten bereitzustellen. Das folgende Beispiel stellt drei `r6g.large.search` Koordinatorknoten in einer Domäne bereit.

```
aws opensearch update-domain-config \
  --domain-name my-opensearch-domain \
  --cluster-config
 InstanceCount=3,InstanceType=r6g.large.search,DedicatedCoordinatorCount=3,ZoneAwarenessEnabled
```

Dieser Befehl aktiviert dedizierte Koordinatorknoten, legt den Instanztyp und die Anzahl der Koordinatorknoten fest und aktiviert die Zonenerkennung für eine höhere Verfügbarkeit.

Bewährte Methoden

Beachten Sie die folgenden bewährten Methoden, wenn Sie dedizierte Koordinatorknoten verwenden.

- Verwenden Sie für die meisten Anwendungsfälle Allzweckinstanzen. Sie bieten einen ausgewogenen Ansatz zwischen Kosten und Leistung. Speicheroptimierte Instances eignen sich ideal für Workloads, die umfangreiche Speicherressourcen benötigen, z. B. solche, die komplexe Aggregationen oder umfangreiche Suchen beinhalten.
- Ein guter Ausgangspunkt ist die Bereitstellung von 5 bis 10% Ihrer Datenknoten als dedizierte Koordinatorknoten. Wenn Ihre Domain beispielsweise 90 Datenknoten eines bestimmten Instanztyps hat, sollten Sie die Bereitstellung von 5 bis 9 Koordinatorknoten desselben Instanztyps in Betracht ziehen.

> **Note**
>
> Die Verfügbarkeit des Instanztyps variiert je nach Region. Stellen Sie bei der Auswahl von Instance-Typen für Koordinatorknoten sicher, dass der gewählte Instance-Typ in Ihrer Zielregion verfügbar ist. Sie können die Verfügbarkeit von Instanztypen in der OpenSearch Service-Konsole überprüfen, wenn Sie Ihre Domain erstellen oder ändern.

- Um das Risiko eines einzelnen Ausfallpunkts zu minimieren, sollten Sie mindestens zwei dedizierte Koordinatorknoten bereitstellen. Dadurch wird sichergestellt, dass Ihr Cluster auch dann betriebsbereit bleibt, wenn ein Knoten ausfällt.
- Wenn Sie die regionsübergreifende Suche verwenden, stellen Sie dedizierte Koordinatorknoten in den Zieldomänen bereit. Quelldomänen übernehmen normalerweise keine Koordinationsaufgaben.
- Für indizierungsintensive Umgebungen sollten Sie CPU-optimierte Instances in Betracht ziehen, die der Instanzgröße Ihrer Datenknoten entsprechen, um eine optimale Leistung zu erzielen.
- Verwenden Sie für speicherintensive Workloads einen etwas größeren Instance-Typ für Ihre dedizierten Koordinatorknoten, um den erhöhten Speicherbedarf zu bewältigen.
- Verfolgen Sie die `CoordinatorCPUUtilization` CloudWatch Amazon-Metrik. Wenn sie konstant über 80% liegt, kann dies darauf hindeuten, dass Sie größere oder zusätzliche Koordinatorknoten benötigen, um die Last zu bewältigen.

Knotenempfehlungen nach Clustergröße

Verwenden Sie die folgenden Richtlinien als Ausgangspunkt für die Bereitstellung von dedizierten Koordinatorknoten auf der Grundlage Ihrer Clustergröße. Passen Sie die Anzahl und den Typ der Knoten auf der Grundlage von Workload-Merkmalen und Leistungskennzahlen an.

Cluster-Größe	Empfohlene Koordinatorknoten	Instance-Typ
Klein (bis zu 50 Knoten)	3-5 Knoten	Allgemeine Zwecke
Mittel (50-100 Knoten)	5-9 Knoten	RAM-optimiert
Groß (über 100 Knoten)	10-15 Knoten	RAM-optimiert

Dedizierte Masterknoten in Amazon OpenSearch Service

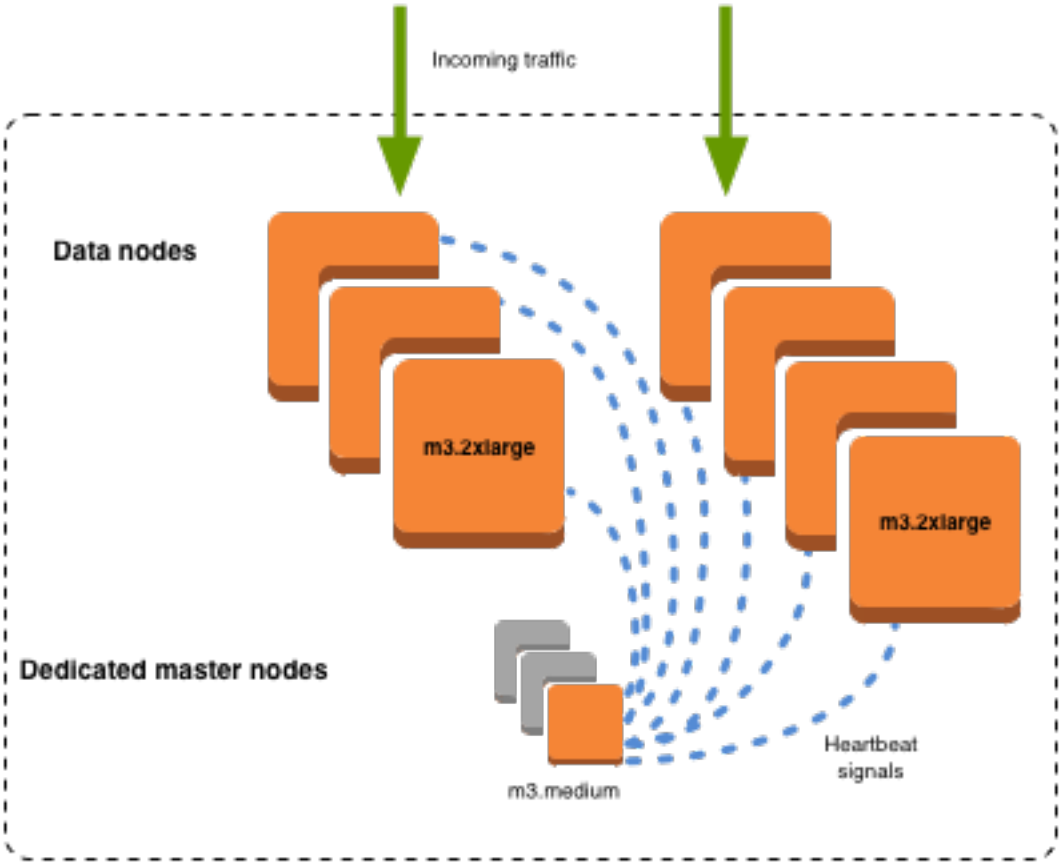
Amazon OpenSearch Service verwendet dedizierte Master-Knoten, um die Cluster-Stabilität zu erhöhen. Ein dedizierter Hauptknoten führt Cluster-Verwaltungsaufgaben aus, jedoch keine Daten hält oder auf Daten-Upload-Anforderungen reagiert. Diese Auslagerung von Cluster-

Verwaltungsaufgaben erhöht die Stabilität Ihrer Domain. Wie bei allen anderen Knotentypen zahlen Sie einen Stundensatz für jeden dedizierten Hauptknoten.

Dedizierte Hauptknoten führten die folgenden Cluster-Verwaltungsaufgaben aus:

- Nachverfolgung aller Knoten im Cluster
- Nachverfolgung der Indexanzahl im Cluster
- Nachverfolgung der Anzahl der Shards, die zu jedem Index gehören
- Pflege der Routing-Informationen für Knoten im Cluster
- Aktualisierung des Cluster-Status nach Statusänderungen, z. B. dem Erstellen eines Index und dem Hinzufügen oder Entfernen von Knoten im Cluster
- Replikation von Änderungen am Cluster-Status über alle Knoten im Cluster hinweg
- Überwachung der Integrität aller Cluster-Knoten, indem Funktionsmeldungen gesendet werden, also periodische Signale, die die Verfügbarkeit der Datenknoten im Cluster überwachen

Die folgende Abbildung zeigt eine OpenSearch Service-Domain mit 10 Instanzen. Sieben der Instances sind Datenknoten und drei sind dedizierte Hauptknoten. Nur einer der dedizierten Hauptknoten ist aktiv. Die beiden grauen dedizierte Hauptknoten sind als Sicherung vorgesehen, falls der aktive dedizierte Hauptknoten ausfällt. Alle Daten-Upload-Anforderungen werden von den sieben Datenknoten bedient und alle Cluster-Verwaltungsaufgaben werden vom aktiven dedizierten Hauptknoten übernommen.



Anzahl der dedizierten Hauptknoten auswählen

Wir empfehlen, Multi-AZ mit Standby zu verwenden, wodurch jeder OpenSearch Produktions-Servicedomäne drei dedizierte Masterknoten hinzugefügt werden. Wenn Sie mit Multi-AZ ohne Standby oder Single-AZ bereitstellen, empfehlen wir dennoch drei dedizierte Master-Knoten. Wählen Sie niemals eine gerade Anzahl an dedizierten Hauptknoten. Berücksichtigen Sie bei der Auswahl der Anzahl dedizierter Hauptknoten Folgendes:

- Ein dedizierter Master-Knoten ist vom OpenSearch Service ausdrücklich verboten, da Sie für den Fall eines Fehlers kein Backup haben. Sie erhalten eine Validierungsausnahme, wenn Sie versuchen, eine Domain mit nur einem dedizierten Hauptknoten zu erstellen.
- Wenn Sie zwei dedizierte Hauptknoten haben, verfügt Ihr Cluster nicht über das erforderliche Knoten-Quorum für die Wahl eines neuen Hauptknotens bei einem Ausfall.

  Ein Quorum ist die Anzahl der dedizierten Hauptknoten / 2 + 1 (abgerundet auf die nächste ganze Zahl). In diesem Fall: 2/2 + 1 = 2. Da ein dedizierter Hauptknoten ausgefallen ist und nur

ein Backup vorhanden ist, verfügt der Cluster nicht über ein Quorum und kann keinen neuen Hauptknoten wählen.

- Drei dedizierte Hauptknoten, die empfohlene Anzahl, bieten zwei Backup-Knoten für den Fall eines Hauptknotenausfalls, und das erforderliche Quorum (2) für die Wahl eines neuen Hauptknotens.
- Vier dedizierte Hauptknoten bieten gegenüber dreien keine Vorteile und können Probleme verursachen, wenn Sie mehrere Availability Zones verwenden.
  - Wenn ein Hauptknoten ausfällt, haben Sie das Quorum (3), um einen neuen Hauptknoten zu wählen. Wenn zwei Knoten ausfallen, verlieren Sie dieses Quorum, genau wie bei drei dedizierten Hauptknoten.
  - In einer Konfiguration mit drei Availability Zones AZs verfügen zwei über einen dedizierten Master-Knoten und eine AZ über zwei. Wenn es in dieser AZ zu einer Störung kommt, verfügen die verbleibenden beiden AZs nicht über das erforderliche Quorum (3), um einen neuen Master zu wählen.
- Fünf dedizierte Hauptknoten funktionieren ebenso wie drei und ermöglichen Ihnen, zwei Knoten zu verlieren und ein Quorum zu behalten. Da jedoch nur ein dedizierter Hauptknoten zu einem bestimmten Zeitpunkt aktiv ist, bedeutet diese Konfiguration, dass vier Leerlaufknoten bezahlt werden müssen. Nach Ansicht vieler Kunden ist ein derartiger Failover-Schutz übertrieben.

Wenn ein Cluster über eine gerade Anzahl von Knoten verfügt, die als Master in Frage kommen, OpenSearch und Elasticsearch-Versionen 7 sind. x und später ignorieren einen Knoten, sodass die Abstimmungskonfiguration immer eine ungerade Zahl ist. In diesem Fall sind vier dedizierte Hauptknoten im Wesentlichen mit drei (und zwei mit einem) äquivalent.

> **Note**
>
> Wenn Ihr Cluster nicht über das erforderliche Quorum für die Wahl eines neuen Hauptknotens verfügt, schlagen Schreib- und Leseanforderungen an den Cluster fehl. Dieses Verhalten unterscheidet sich von der OpenSearch Standardeinstellung.

Auswählen von Instance-Typen für dedizierte Hauptknoten

OpenSearch Kontingente für Dienstdomänen und Instanzen

Obwohl dedizierte Masterknoten keine Such- und Abfrageanfragen verarbeiten, korreliert ihre Größe stark mit der Instanzgröße und der Anzahl der Instanzen, Indizes und Shards, die sie verwalten

können. Für Produktionscluster empfehlen wir mindestens die folgenden Instance-Typen für dedizierte Master-Knoten.

Diese Empfehlungen basieren auf typischen Workloads und können je nach Ihren Anforderungen variieren. Cluster mit vielen Shards oder Feldzuordnungen profitieren von größeren Instance-Typen. Weitere Informationen finden Sie unter Empfohlene CloudWatch Alarme für Amazon OpenSearch Service, um festzustellen, ob Sie einen größeren Instance-Typ verwenden müssen.

RAM	Max Node-Unterstützung für Elasticsearch und OpenSearch Service 1.x bis 2.15	Max Shard-Unterstützung für Elasticsearch und OpenSearch Service 1.x bis 2.15	Max Node Support für OpenSearch Service 2.17 und höher	Max Shard Support für OpenSearch Service 2.17 und höher
2 GB	Nicht zutreffend	Nicht zutreffend	10	1 K
4 GB	Nicht zutreffend	Nicht zutreffend	10	5 K
8 GB	10	10 K	30	15 K
16 GB	30	30 K	60	30 K
32 GB	75	40 000	120	60 K
64 GB	125	75 K	240	120 K
128 GB	200	75 K	480	240 K
256 GB	Nicht zutreffend	Nicht zutreffend	1.002	500 K

Empfohlene CloudWatch Alarme für Amazon OpenSearch Service

CloudWatch Alarme führen eine Aktion aus, wenn eine CloudWatch Metrik für einen bestimmten Zeitraum einen bestimmten Wert überschreitet. Möglicherweise möchten Sie Ihnen eine E-Mail AWS senden, wenn Ihr Cluster-Integritätsstatus `red` länger als eine Minute andauert. Dieser Abschnitt enthält einige empfohlene Alarme für Amazon OpenSearch Service und wie Sie darauf reagieren können.

Sie können diese Alarme automatisch einrichten mit AWS CloudFormation. Einen Beispielstapel finden Sie im entsprechenden GitHubRepository.

> **Note**
>
> Wenn Sie den CloudFormation Stack bereitstellen, sind die `KMSKeyInaccessible` Alarme `KMSKeyError` und in einem bestimmten `Insufficient Data` Zustand vorhanden, da diese Metriken nur angezeigt werden, wenn bei einer Domain ein Problem mit ihrem Verschlüsselungsschlüssel auftritt.

Weitere Informationen zur Konfiguration von Alarmen finden Sie unter CloudWatchAmazon-Alarme erstellen im CloudWatch Amazon-Benutzerhandbuch.

Alarm	Problem
`ClusterStatus.red` Maximum ist >= 1 für 1 Minute, 1 Mal hintereinander	Mindestens ein primärer Shard und dessen Replikate sind keinem Knoten zugewiesen. Siehe the section called “Roter Cluster-Status”.
`ClusterStatus.yellow` Maximum ist >= 1 für 1 Minute, 5 Mal hintereinander	Mindestens ein Replikat-Shard ist nicht einem Knoten zugewiesen. Siehe the section called “Gelber Cluster-Status”.
`FreeStorageSpace` Minimum ist <= 20480 für 1 Minute, 1 Mal hintereinander	Ein Knoten in Ihrem Cluster hat nur noch 20 GiB freien Speicherplatz. Siehe the section called “Zu wenig verfügbarer Speicherplatz”. Dieser Wert wird in MiB angegeben, statt 20480 empfehlen wir deshalb eine Einstellung auf 25 % Ihres Speicherplatzes pro Knoten.
`ClusterIndexWritesBlocked` ist >= 1 für 5 Minuten, 1 Mal hintereinander	Ihr Cluster blockiert Schreibanforderungen. Siehe the section called “ClusterBlockException”.

Alarm	Problem
`Nodes` Minimum ist < x für 1 Tag, 1 Mal hintereinander	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. Siehe the section called “Fehlgeschlagene Cluster-Knoten”.

`AutomatedSnapshotFailure` Maximum ist >= 1 für 1 Minute, 1 Mal hintereinander	Ein automatisierter Snapshot ist fehlgeschlagen. Dieser Fehler ist häufig das Ergebnis eines roten Cluster-Integritätsstatus. Siehe the section called “Roter Cluster-Status”.
	
	Für eine Zusammenfassung aller automatischen Snapshots und einige Informationen zu Ausfällen können Sie auch einen der folgenden Schritte ausprobieren:
	
	`GET domain_endpoint /_snapshot/cs-automated/_all`
	`GET domain_endpoint /_snapshot/cs-automated-enc/_all`

`CPUUtilization` oder `WarmCPUUtilization` Maximum ist >= 80 % für 15 Minuten, 3 Mal hintereinander	Eine 100%ige CPU-Auslastung kann manchmal auftreten, aber eine anhaltend hohe Auslastung ist problematisch. Ziehen Sie die Verwendung von größeren Instance-Typen oder das Hinzufügen von Instances in Betracht.
`JVMMemoryPressure` Maximum ist >= 95 % für 1 Minute, 3 Mal hintereinander	Der Cluster könnte Fehler aufgrund von unzureichendem Speicherplatz erhalten, wenn die Nutzung zunimmt. Erwägen Sie eine vertikale Skalierung. OpenSearch Der Dienst verwendet die Hälfte des RAM einer Instanz 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 horizontale Skalierung durchführen, indem Sie Instances hinzufügen.
`OldGenJVMMemoryPressure` Maximum ist >= 80 % für 1 Minute, 3 Mal hintereinander	

Alarm	Problem
`MasterCPU Utilization` Maximum ist >= 50 % für 15 Minuten, 3 Mal hintereinander	Ziehen Sie die Verwendung von größeren Instance-Typen für Ihre dedizierten Hauptknoten in Betracht. Aufgrund ihrer Rolle für die Cluster-Stabilität und Blau/Grün-Bereitstellungen sollten dedizierte Hauptknoten eine geringere CPU-Nutzung als Datenknoten haben.
`MasterJVM MemoryPressure` Maximum ist >= 95 % für 1 Minute, 3 Mal hintereinander	
`MasterOld GenJVMMem oryPressure` Maximum ist >= 80 % für 1 Minute, 3 Mal hintereinander	
`KMSKeyError` ist >= 1 für 1 Minute, 1 Mal hintereinander	Der AWS KMS Verschlüsselungsschlüssel, der zum Verschlüsseln ruhender Daten in Ihrer Domain verwendet wird, ist deaktiviert. Reaktivie ren Sie es, um den normalen Betrieb wiederherzustellen. Weitere Informationen finden Sie unter the section called “Verschlüsselung im Ruhezustand”.
`KMSKeyIna ccessible` ist >= 1 für 1 Minute, 1 Mal hintereinander	Der AWS KMS Verschlüsselungsschlüssel, der zum Verschlüsseln von gespeicherten Daten in Ihrer Domain verwendet wird, wurde gelöscht oder der Service wurde nicht mehr gewährt. OpenSearch Für Domains, die sich in diesem Zustand befinden, ist die Wiederherstellung nicht möglich. Wenn Sie jedoch über einen manuellen Snapshot verfügen, können Sie diesen für die Migration zu einer neuen Domain verwenden . Weitere Informationen hierzu finden Sie unter the section called “Verschlüsselung im Ruhezustand”.

Alarm	Problem
`shards.active` ist >= 30000 für 1 Minute, 1 Mal hintereinander	Die Gesamtzahl der aktiven primären und Replikat-Shards ist größer als 30.000. Möglicherweise rotieren Sie Ihre Indizes zu häufig. Erwägen Sie, ISM zu verwenden, um Indizes zu entfernen, sobald sie ein bestimmtes Alter erreichen.
5*xx* Alarme >= 10 % von `OpenSearchRequests` .	Ein oder mehrere Datenknoten sind möglicherweise überlastet oder Anfragen können innerhalb des Zeitraums im Leerlauf nicht abgeschlossen werden. Erwägen Sie, zu größeren Instance-Typen zu wechseln oder dem Cluster weitere Knoten hinzuzufügen. Bestätigen Sie Bewährte Methoden für Shard- und Cluster-Architektur.
`MasterReachableFromNode` Der Höchstwert ist < 1 für 5 Minuten, 1 Mal hintereinander	Dieser Alarm zeigt an, dass der Hauptknoten angehalten wurde oder nicht erreichbar ist. Diese Ausfälle sind in der Regel auf ein Problem mit der Netzwerkkonnektivität oder auf ein AWS Abhängigkeitsproblem zurückzuführen.
`ThreadpoolWriteQueue` Durchschnitt ist >= 100 für 1 Minute, 1 Mal hintereinander	Der Cluster erlebt eine hohe Indexierungs-Parallelität. Überprüfen und steuern Sie Indexierungsanforderungen oder erhöhen Sie die Clusterressourcen.
`ThreadpoolSearchQueue` Durchschnitt ist >= 500 für 1 Minute, 1 Mal hintereinander	Der Cluster erlebt eine hohe Suchparallelität. Überlegen Sie, Ihren Cluster zu skalieren. Sie können auch die Größe der Suchwarteschlange erhöhen, aber eine übermäßige Erhöhung kann zu Fehlern außerhalb des Speichers führen.
`ThreadpoolSearchQueue` Maximum ist >= 5000 für 1 Minute, 1 Mal hintereinander	

Alarm	Problem
Die Erhöhung der `Threadpool SearchRejected` SUMME beträgt >=1 {mathematischer Ausdruck DIFF ()} für 1 Minute, 1 Mal hintereinander	Diese Alarme benachrichtigen Sie über Domain-Probleme, die sich auf Leistung und Stabilität auswirken können.
Die Erhöhung von `Threadpool WriteRejected` SUM beträgt >=1 {mathematischer Ausdruck DIFF ()} für 1 Minute, 1 Mal hintereinander	

> **Note**
>
> Wenn Sie nur Metriken anzeigen möchten, siehe the section called “Überwachen von Cluster-Metriken”.

Andere Alarme, die Sie in Betracht ziehen könnten

Erwägen Sie, je nachdem, welche OpenSearch Servicefunktionen Sie regelmäßig nutzen, die folgenden Alarme zu konfigurieren.

Alarm	Problem
`WarmFreeStorageSpace` ist >= 10%	Sie haben 10% Ihres gesamten freien Warmspeichers erreicht. `WarmFreeStorageSpace` misst die Summe Ihres freien warmen

Alarm	Problem
	Speicherplatzes in MiB. UltraWarm verwendet Amazon S3 anstelle von angeschlossenen Festplatten.
`HotToWarmMigrationQueueSize` ist >= 20 für 1 Minute, 3 Mal hintereinander	Eine große Anzahl von Indizes wird gleichzeitig vom Hot-in den Speicherbereich verschoben. UltraWarm Überlegen Sie, Ihren Cluster zu skalieren.
`HotToWarmMigrationSuccessLatency` ist >= 1 Tag, 1 Mal hintereinander	Konfigurieren Sie diesen Alarm so, dass Sie benachrichtigt werden, wenn die `HotToWarmMigrationSuccessCount` -x-Latenz mehr als 24 Stunden beträgt, wenn Sie versuchen, tägliche Indizes zu rollen.
`WarmJVMMemoryPressure` Maximum ist >= 95 % für 1 Minute, 3 Mal hintereinander	Der Cluster könnte Fehler aufgrund von unzureichendem Speicherplatz erhalten, wenn die Nutzung zunimmt. Ziehen Sie eine vertikale Skalierung in Betracht. OpenSearch Der Dienst verwendet die Hälfte des RAM einer Instanz 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 horizontale Skalierung durchführen, indem Sie Instances hinzufügen.
`WarmOldGenJVMMemoryPressure` Maximum ist >= 80 % für 1 Minute, 3 Mal hintereinander	
`WarmToColdMigrationQueueSize` ist >= 20 für 1 Minute, 3 Mal hintereinander	Eine große Anzahl von Indizes wird gleichzeitig vom UltraWarm Cold Storage in den Cold Storage verschoben. Überlegen Sie, Ihren Cluster zu skalieren.

Alarm	Problem
`HotToWarmMigrationFailureCount` ist >= 1 für 1 Minute, 1 Mal hintereinander	Migrationen können während Snapshots, Shard-Verlagerungen oder erzwungenen Zusammenführungen fehlschlagen. Fehler bei Snapshots oder Shard-Verlagerungen sind in der Regel auf Knotenfehler oder S3-Konnektivitätsprobleme zurückzuführen. Ein Mangel an Speicherplatz ist in der Regel die zugrunde liegende Ursache für Fehler bei erzwungenen Zusammenführungen.
`WarmToColdMigrationFailureCount` ist >= 1 für 1 Minute, 1 Mal hintereinander	Migrationen schlagen normalerweise fehl, wenn Versuche, Indexmetadaten auf Cold Storage zu migrieren, fehlschlagen. Fehler können auch auftreten, wenn der Warm-Indexcluster-Status entfernt wird.
`WarmToColdMigrationLatency` ist >= 1 Tag, 1 Mal hintereinander	Konfigurieren Sie diesen Alarm so, dass Sie benachrichtigt werden, wenn die `WarmToColdMigrationSuccessCount` -x-Latenz mehr als 24 Stunden beträgt, wenn Sie versuchen, tägliche Indizes zu rollen.
`AlertingDegraded` ist >= 1 für 1 Minute, 1 Mal hintereinander	Entweder ist der Warnungsindex rot, oder ein oder mehrere Knoten sind nicht im Zeitplan.
`ADPluginUnhealthy` ist >= 1 für 1 Minute, 1 Mal hintereinander	Das Plug-In zur Anomalieerkennung funktioniert nicht ordnungsgemäß, entweder aufgrund hoher Fehlerraten oder weil einer der verwendeten Indizes rot ist.
`AsynchronousSearchFailureRate` ist >= 1 für 1 Minute, 1 Mal hintereinander	Mindestens eine asynchrone Suche ist in letzter Minute fehlgeschlagen, was wahrscheinlich bedeutet, dass der Koordinatorknoten fehlgeschlagen ist. Der Lebenszyklus einer asynchronen Suchanfrage wird ausschließlich auf dem Koordinatorknoten verwaltet. Wenn der Koordinator ausfällt, schlägt die Anforderung fehl.

Alarm	Problem
`AsynchronousSearchStoreHealth` ist >= 1 für 1 Minute, 1 Mal hintereinander	Der Zustand des asynchronen Reaktionsspeichers für die asynchrone Suche im anhaltenden Index ist rot. Möglicherweise speichern Sie große asynchrone Antworten, die einen Cluster destabilisieren können. Versuchen Sie, Ihre asynchronen Suchantworten auf 10 MB oder weniger zu beschränken.
`SQLUnhealthy` ist >= 1 für 1 Minute, 3 Mal hintereinander	Das SQL-Plug-In gibt 5 Xx-Antwortcodes zurück oder übergibt eine ungültige DSL-Abfrage an. OpenSearch Beheben Sie Probleme mit den Anforderungen, die Ihre Clients an das Plug-in stellen.
`LTRStatus.red` ist >= 1 für 1 Minute, 1 Mal hintereinander	Mindestens einer der Indizes, die zum Ausführen des Plug-ins „Learning to Rank“ erforderlich sind, ist nicht funktionsfähig, da primäre Shards fehlen.

Allgemeine Referenz für Amazon OpenSearch Service

Amazon OpenSearch Service unterstützt eine Vielzahl von Instances, Vorgängen, Plugins und anderen Ressourcen.

Themen

- Unterstützte Instance-Typen in Amazon OpenSearch Service
- Funktionen nach Engine-Version in Amazon OpenSearch Service
- Plugins nach Engine-Version in Amazon OpenSearch Service
- Unterstützte Vorgänge in Amazon OpenSearch Service
- Amazon OpenSearch Service-Kontingente
- Reserved Instances in Amazon OpenSearch Service
- Andere unterstützte Ressourcen in Amazon OpenSearch Service

Unterstützte Instance-Typen in Amazon OpenSearch Service

Amazon OpenSearch Service unterstützt die folgenden Instance-Typen. Nicht alle Regionen unterstützen alle Instance-Typen. Einzelheiten zur Verfügbarkeit finden Sie unter Amazon OpenSearch Service-Preise.

Weitere Informationen darüber, welcher Instance-Typ für Ihren Anwendungsfall am besten geeignet ist, finden Sie unter the section called “Größenanpassung von Domains”, the section called “EBS-Volume-Größenkontigente” und the section called “Netzwerk-Kontingente”.

Instance-Typen der aktuellen Generation

Für eine optimale Leistung empfehlen wir, die folgenden Instance-Typen zu verwenden, wenn Sie neue OpenSearch Service-Domains erstellen.

Instance-Typ	Instances	Einschränkungen
i4i	i4i.large .search	Die i4i-Instance-Typen erfordern Elasticsearch 5.1 oder höher oder eine beliebige Version von und unterstützen EBS Volume Storage nicht. OpenSearch

Instance-Typ	Instances	Einschränkungen
	i4i.xlarge.search i4i.2xlarge.search i4i.4xlarge.search i4i.8xlarge.search i4i.12xlarge.search i4i.16xlarge.search i4i.24xlarge.search i4i.32xlarge.search	

Instance-Typ	Instances	Einschränkungen
i4g	i4g.large.search i4g.xlarge.search i4g.2xlarge.search i4g.4xlarge.search i4g.8xlarge.search i4g.16xlarge.search	Die i4G-Instance-Typen erfordern Elasticsearch 7.9 oder höher oder eine beliebige Version von und unterstützen keine EBS-Speichervolumes. OpenSearch

Instance-Typ	Instances	Einschränkungen
Graviton3	C7G.Large.Suche C7G.XLarge.Search C7G.2xLarge.Suche C7G.4XLarge.Suche C7G.8XLarge.Suche C7G.12XLarge.Suche C7G.16xLarge.Suche M7G.Large.Suche M7G.XLarge.Search M7G.2XLarge.Suche M7G.4XLarge.Suche M7G.8XLarge.Suche	Graviton3 unterstützt nur. GP3

Instance-Typ	Instances	Einschränkungen
	M7G.12XLarge.Suche	
	M7G.16xLarge.Suche	
	R7G.Medium.Search	
	R7G.Large.Search	
	R7G.XLarge.Search	
	R7G.2xLarge.Suche	
	R7G.4xLarge.Suche	
	R7G.8XLarge.Suche	
	R7G.12xLarge.Suche	
	R7G.16xLarge.Suche	
	R7GD.Large.Suche	

Instance-Typ	Instances	Einschränkungen
	R7GD.XLarge.Search R7GD.2xLarge.Suche R7GD.4xLarge.Suche R7GD.8XLarge.Suche R7GD.12xLarge.Suche R7GD.16xLarge.Suche	

Instance-Typ	Instances	Einschränkungen
OR1	or1.medium.search or1.large.search or1.xlarge.search or1.2xlarge.search or1.4xlarge.search or1.8xlarge.search or1.12xlarge.search or1.16xlarge.search	• Die OR1 Instanztypen erfordern OpenSearch 2.11 oder höher. • OR1 Instances sind nur mit Master-Knoten anderer Graviton-Instance-Typen (C6g, M6g, R6g) kompatibel.

Instance-Typ	Instances	Einschränkungen
OR2	or2.medium.search or2.large.search or2.xlarge.search or2.2xlarge.search or2.4xlarge.search or2.8xlarge.search or2.12xlarge.search or2.16xlarge.search	

Instance-Typ	Instances	Einschränkungen
OM2	om2.large.search om2.xlarge.search om2.2xlarge.search om2.4xlarge.search om2.8xlarge.search om2.12xlarge.search om2.16xlarge.search	

Instance-Typ	Instances	Einschränkungen

Im4gn	`im4gn.large.search`
	`im4gn.xlarge.search`
	`im4gn.2xlarge.search`
	`im4gn.4xlarge.search`
	`im4gn.8xlarge.search`
	`im4gn.16xlarge.search`
		• Die IM4GN-Instance-Typen erfordern Elasticsearch 7.9 oder höher oder eine beliebige Version von und unterstützen keine EBS-Speichervolumes. OpenSearch
		• iM4GN-Instances sind nur mit anderen Graviton-Instance-Typen (C6g, M6g, R6g, R6gd) kompatibel. Graviton- und Nicht-Graviton-Instances können nicht in demselben Cluster kombiniert werden.

Instance-Typ	Instances	Einschränkungen

C5	`c5.large.search`
	`c5.xlarge.search`
	`c5.2xlarge.search`
	`c5.4xlarge.search`
	`c5.9xlarge.search`
	`c5.18xlarge.search`
		Die C5-Instance-Typen erfordern Elasticsearch 5.1 oder höher oder eine beliebige Version von. OpenSearch

Instance-Typ	Instances	Einschränkungen

C6g	`c6g.large.search`
	`c6g.xlarge.search`
	`c6g.2xlarge.search`
	`c6g.4xlarge.search`
	`c6g.8xlarge.search`
	`c6g.12xlarge.search`
		• Die C6g-Instanztypen erfordern Elasticsearch 7.9 oder höher oder eine beliebige Version von. OpenSearch
		• C6g-Instances sind nur mit anderen Graviton-Instance-Typen (iM4GN, M6G, R6g, R6gd) kompatibel. Graviton- und Nicht-Graviton-Instances können nicht in demselben Cluster kombiniert werden.

Instance-Typ	Instances	Einschränkungen

I3	`i3.large.search`
	`i3.xlarge.search`
	`i3.2xlarge.search`
	`i3.4xlarge.search`
	`i3.8xlarge.search`
	`i3.16xlarge.search`	

M5	`m5.large.search`
	`m5.xlarge.search`
	`m5.2xlarge.search`
	`m5.4xlarge.search`
	`m5.12xlarge.search`
		Die M5-Instance-Typen erfordern Elasticsearch 5.1 oder höher oder eine beliebige Version von. OpenSearch

Instance-Typ	Instances	Einschränkungen

M6g	`m6g.large.search`
	`m6g.xlarge.search`
	`m6g.2xlarge.search`
	`m6g.4xlarge.search`
	`m6g.8xlarge.search`
	`m6g.12xlarge.search`
		• Die M6g-Instanztypen erfordern Elasticsearch 7.9 oder höher oder eine beliebige Version von. OpenSearch
		• M6g-Instances sind nur mit anderen Graviton-Instance-Typen (iM4GN, C6g, R6g, R6gd) kompatibel. Graviton- und Nicht-Graviton-Instances können nicht in demselben Cluster kombiniert werden.

Instance-Typ	Instances	Einschränkungen

R5	`r5.large.search`
	`r5.xlarge.search`
	`r5.2xlarge.search`
	`r5.4xlarge.search`
	`r5.12xlarge.search`
		Die R5-Instance-Typen erfordern Elasticsearch 5.1 oder höher oder eine beliebige Version von. OpenSearch

Instance-Typ	Instances	Einschränkungen

R6g	`r6g.large.search`
	`r6g.xlarge.search`
	`r6g.2xlarge.search`
	`r6g.4xlarge.search`
	`r6g.8xlarge.search`
	`r6g.12xlarge.search`
		• Die R6g-Instanztypen erfordern Elasticsearch 7.9 oder höher oder eine beliebige Version von. OpenSearch
		• R6g-Instances sind nur mit anderen Graviton-Instance-Typen (iM4GN, C6G, M6g, R6gd) kompatibel. Graviton- und Nicht-Graviton-Instances können nicht in demselben Cluster kombiniert werden.

Instance-Typ	Instances	Einschränkungen

R6gd	`r6gd.large.search`
	`r6gd.xlarge.search`
	`r6gd.2xlarge.search`
	`r6gd.4xlarge.search`
	`r6gd.8xlarge.search`
	`r6gd.12xlarge.search`
	`r6gd.16xlarge.search`
		• Die R6gd-Instance-Typen erfordern Elasticsearch 7.9 oder höher oder eine beliebige Version von und unterstützen keine EBS-Speichervolumes. OpenSearch
		• R6gd-Instances sind nur mit anderen Graviton-Instance-Typen (iM4gn, C6g, M6g, R6g) kompatibel. Graviton- und Nicht-Graviton-Instances können nicht in demselben Cluster kombiniert werden.

Instance-Typ	Instances	Einschränkungen
T3	`t3.small.search` `t3.medium.search`	• Die T3-Instance-Typen erfordern Elasticsearch 5.6 oder höher oder eine beliebige Version von. OpenSearch • Sie können T3-Instance-Typen nur verwenden, wenn Ihre Domain ohne Standby bereitgestellt wird. Weitere Informationen finden Sie unter the section called “Multi-AZ ohne Standby”. • Sie können T3-Instance-Typen nur verwenden, wenn die Anzahl der Instanzen für Ihre Domain 10 oder weniger beträgt. • Die T3-Instance-Typen unterstützen weder UltraWarm Storage, Cold Storage noch Auto-Tune.

c7i	`c7i.large.search`
	`c7i.xlarge.search`
	`c7i.2xlarge.search`
	`c7i.4xlarge.search`
	`c7i.8xlarge.search`
	`c7i.12xlarge.search`
	`c7i.16xlarge.search`
		• Die c7i-Instanz benötigt Elasticsearch 5.1 oder höher oder eine beliebige Version von und unterstützt nur OpenSearch Speichervolumes. GP3

Instance-Typ	Instances	Einschränkungen

m7i	`m7i.large.search`
	`m7i.xlarge.search`
	`m7i.2xlarge.search`
	`m7i.4xlarge.search`
	`m7i.8xlarge.search`
	`m7i.12xlarge.search`
	`m7i.16xlarge.search`
		• Die m7i-Instanz benötigt Elasticsearch 5.1 oder höher oder eine beliebige Version von und unterstützt nur OpenSearch Speichervolumes. GP3

Instance-Typ	Instances	Einschränkungen

r7i	`r7i.large.search`
	`r7i.xlarge.search`
	`r7i.2xlarge.search`
	`r7i.4xlarge.search`
	`r7i.8xlarge.search`
	`r7i.12xlarge.search`
	`r7i.16xlarge.search`
		• Die r7i-Instanz benötigt Elasticsearch 5.1 oder höher oder eine beliebige Version von und unterstützt nur OpenSearch Speichervolumes. GP3

Instance-Typen der vorherigen Generation

OpenSearch Der Service bietet Instance-Typen der vorherigen Generation für Benutzer, die ihre Anwendungen entsprechend optimiert haben und noch kein Upgrade durchgeführt haben. Wir raten dazu, Instance-Typen der aktuellen Generation zu verwenden, um von der besten Leistung zu profitieren, die folgenden Instance-Typen der vorherigen Generation werden aber weiterhin unterstützt.

Instance-Typ	Instances	Einschränkungen

C4	`c4.large.search`
	`c4.xlarge.search`
	`c4.2xlarge.search`
	`c4.4xlarge.search`
	`c4.8xlarge.search`	

I2	`i2.xlarge.search` `i2.2xlarge.search`	

M3	`m3.medium.search`
	`m3.large.search`
	`m3.xlarge.search`
	`m3.2xlarge.search`
		• Die M3-Instance-Typen unterstützen keine Verschlüsselung von Daten im Ruhezustand, differenzierte Zugriffskontrolle oder Cluster-übergreifende Suche.
		• Für die M3-Instance-Typen gelten je nach OpenSearch Version zusätzliche Einschränkungen. Weitere Informationen hierzu finden Sie unter the section called “Ungültiger M3-Instance-Typ”.

M4	`m4.large.search`	

Instance-Typ	Instances	Einschränkungen

	`m4.xlarge.search`
	`m4.2xlarge.search`
	`m4.4xlarge.search`
	`m4.10xlarge.search`	

R3	`r3.large.search`
	`r3.xlarge.search`
	`r3.2xlarge.search`
	`r3.4xlarge.search`
	`r3.8xlarge.search`
		Die R3-Instance-Typen unterstützen keine Verschlüsselung von Daten im Ruhezustand oder differenzierte Zugriffskontrolle.

Instance-Typ	Instances	Einschränkungen

R4	`r4.large.search`
	`r4.xlarge.search`
	`r4.2xlarge.search`
	`r4.4xlarge.search`
	`r4.8xlarge.search`
	`r4.16xlarge.search`	

T2	`t2.micro.search`
	`t2.small.search`
	`t2.medium.search`
		• Sie können die T2-Instance-Typen nur dann verwenden, wenn die Anzahl der Instances für Ihre Domain zehn oder weniger beträgt.
		• Der Instance-Typ `t2.micro.search` unterstützt nur Elasticsearch 1.5 und 2.3.
		• Die T2-Instance-Typen unterstützen keine Verschlüsselung von Daten im Ruhezustand, detaillierte Zugriffskontrolle, UltraWarm Speicherung, Cold Storage, clusterübergreifende Suche oder Auto-Tune.

> **Tip**
>
> Wir empfehlen oft verschiedene Instance-Typen für dedizierte Hauptknoten und Datenknoten.

Funktionen nach Engine-Version in Amazon OpenSearch Service

Für viele OpenSearch Servicefunktionen ist eine OpenSearch Mindestversion oder eine ältere Elasticsearch OSS-Version erforderlich. Wenn Sie die Mindestversion für eine Funktion erfüllen, die Funktion jedoch in Ihrer Domain nicht verfügbar ist, aktualisieren Sie die Service-Software.

Funktion	Erforderliche Mindestversion OpenSearch	Erforderliche Mindestversion von Elasticsearch
Benutzerdefinierte Plugins	2.15	Nicht enthalten
Dedizierter Koordinatorknoten	1,0	6.8
VPC-Unterstützung	1,0	1,0
HTTPS für den gesamten Datenverkehr zur Domain erforderlich		
Multi-AZ-Unterstützung		
Dedizierte Hauptknoten		

Funktion	Erforderliche Mindestversion OpenSearch	Erforderliche Mindestversion von Elasticsearch
Benutzerdefinierte Pakete		
Benutzerdefinierte Endpunkte		
Veröffentlichen von Slow-Protokollen		
Veröffentlichen von Fehler-Protokollen	1,0	5.1
Verschlüsselung gespeicherter Daten		
Cognito-Authentifizierung für Dashboards OpenSearch		
Direkte Upgrades		

Funktion	Erforderliche Mindestversion OpenSearch	Erforderliche Mindestversion von Elasticsearch
Kuratoren-Unterstützung	Nicht enthalten	5.1
Stündliche automatische Snapshots	1,0	5.3
Node-to-node Verschlüsselung	1,0	6.0
Java-Unterstützung für High-Level-REST-Clients		
HTTP-Anfragen und Antwort-Komprimierung		
Warnfunktion	1,0	6.2
SQL	1,0	6,5
Cluster-übergreifende Suche	1,0	6.7

Funktion	Erforderliche Mindestversion OpenSearch	Erforderliche Mindestversion von Elasticsearch
Differenzierte Zugriffskontrolle		
SAML-Authentifizierung für Dashboards OpenSearch		
Automatische Optimierung		
Remote-Neuindexierung		
UltraWarm	1,0	6.8
Indexstatusmanagement		
k-NN nach euklidischer Entfernung	1,0	7.1
Anomaliedetektion	1,0	7.4
k-NN nach Kosinus-Ähnlichkeit	1,0	7.7

Funktion	Erforderliche Mindestversion OpenSearch	Erforderliche Mindestversion von Elasticsearch
Learning to Rank		
Piped Processing Language	1,0	7.9
OpenSearch Dashboards, Berichte		
OpenSearch Dashboards Trace Analytics		
ARM-basierte Graviton-Instances		
Cold Storage		
Hamming-Distanz, L1-Norm-Distanz und Painless-Scripting für k-NN	1,0	7.10
Asynchrone Suche		

Funktion	Erforderliche Mindestversion OpenSearch	Erforderliche Mindestversion von Elasticsearch
Indextransformationen	1,0	Nicht enthalten
Cluster-übergreifende Replikation	1.1	7,10
ML Commons	1.3	Nicht enthalten
Benachrichtigungen	2.3	Nicht enthalten
Suche nach einem bestimmten Zeitpunkt	2.5	Nicht enthalten
Konnektoren für maschinelles Lernen	2.9	Nicht enthalten
Semantische Suche	2.9	Nicht enthalten
Multimodale semantische Suche	2.11	Nicht enthalten
Datenquellen direkt abfragen	2.11	Nicht enthalten

Funktion	Erforderliche Mindestversion OpenSearch	Erforderliche Mindestversion von Elasticsearch
Gleichzeitige Segmentsuche	2.13	Nicht enthalten
Generierung von Abfragen in natürlicher Sprache	2.13	Nicht enthalten
Amazon-Q-Unterstützung	2,17	Nicht enthalten

Weitere Informationen zu Plug-ins, die einige dieser Funktionen und zusätzliche Funktionalität ermöglichen, finden Sie unter the section called “Plug-ins nach Engine-Version”. Informationen zur OpenSearch -API für jede Version finden Sie unter the section called “Unterstützte Vorgänge”.

Plugins nach Engine-Version in Amazon OpenSearch Service

Amazon OpenSearch Service-Domains sind mit Plug-ins aus der OpenSearch Community vorkonfiguriert. Der Service stellt Plugins automatisch für Sie bereit und verwaltet sie. Je nachdem, welche Version OpenSearch oder welches Legacy-Elasticsearch-Betriebssystem Sie für Ihre Domain auswählen, werden jedoch unterschiedliche Plugins bereitgestellt.

In der folgenden Tabelle sind die Plugins nach OpenSearch Version sowie die kompatiblen Versionen der Legacy-Elasticsearch-Betriebssysteme aufgeführt. Sie enthält nur Plugins, mit denen Sie möglicherweise interagieren — sie ist nicht umfassend. OpenSearch Service verwendet zusätzliche Plug-ins, um die Kernfunktionen des Dienstes zu aktivieren, z. B. das S3 Repository-Plugin für Snapshots und das OpenSearchPerformance Analyzer-Plugin für Optimierung und Überwachung. Für eine vollständige Liste aller Plug-Ins, die auf Ihrer Domain ausgeführt werden, stellen Sie folgende Anfrage:

```
GET _cat/plugins?v
```

Plug-In	Erforderliche Mindestversion OpenSearch	Erforderliche Mindestversion von Elasticsearch
HanLP	2.11	Nicht unterstützt
Hebräische Analyse	2.11	Nicht unterstützt
Amazon Personalize Search Ranking	2.9	Nicht unterstützt
Neuronale Suche	2.9	Nicht unterstützt
Sicherheitsanalytik	2.5	Nicht unterstützt
OpenSearch notifications	2.3	Nicht unterstützt
ML Commons	1.3	Nicht unterstützt
Sudachi-Analyse (für Japanisch empfohlen)	1.3	Nicht unterstützt
STConvert	1.3	Nicht unterstützt
Pinyin-Analyse	1.3	Nicht unterstützt

Plug-In	Erforderliche Mindestversion OpenSearch	Erforderliche Mindestversion von Elasticsearch
Nori-Analyse	1.3	Nicht unterstützt
OpenSearch Beobachtbarkeit	1.2	Nicht unterstützt
OpenSearch Clusterübergreifende Replikation	1.1	7.10
OpenSearch asynchrone Suche	1,0	7.10
IK-Analyse (Chinesisch)	1,0	7.7
Vietnamesische Analyse		
Thai Analyse		
Learning to Rank		
OpenSearch Erkennung von Anomalien	1,0	7.4

Plug-In	Erforderliche Mindestversion OpenSearch	Erforderliche Mindestversion von Elasticsearch
OpenSearch k-NN	1,0	7.1
OpenSearch Indexstatusmanagement	1,0	6.8
OpenSearch Sicherheit	1,0	6.7
OpenSearch SQL	1,0	6,5
OpenSearch warnend	1,0	6.2
Ukrainische Analyse	1,0	5.3
Mapper Size	1,0	5.3
Mapper Murmur3	1,0	5.1
Ingest User Agent Processor	1,0	5.1
Ingest Attachment Processor	1,0	5.1

Plug-In	Erforderliche Mindestversion OpenSearch	Erforderliche Mindestversion von Elasticsearch
Stempel Polish Analysis	1,0	5.1
Smart Chinese Analysis	1,0	5.1
Seunjeon Korean Analysis	1,0	5.1
Phonetic Analysis	1,0	2.3
Japanese (kuromoji) Analysis	1,0	In allen Domains enthalten
ICU Analysis	1,0	In allen Domains enthalten

Optionale Plug-ins

Zusätzlich zu den vorinstallierten Standard-Plugins unterstützt Amazon OpenSearch Service mehrere optionale Sprachanalyse-Plugins. Sie können das AWS Management Console und verwenden AWS CLI , um ein Plugin einer Domain zuzuordnen, ein Plugin von einer Domain zu trennen und alle Plugins aufzulisten. Ein optionales Plugin-Paket ist mit einer bestimmten OpenSearch Version kompatibel und kann nur Domains mit dieser Version zugeordnet werden.

Beachten Sie, dass beim Sudachi-Plugin die erneute Zuordnung einer Wörterbuchdatei nicht sofort zur Domain beiträgt. Das Wörterbuch wird aktualisiert, wenn die nächste blue/green Bereitstellung im Rahmen einer Konfigurationsänderung oder eines anderen Updates auf der Domain ausgeführt wird. Alternativ können Sie ein neues Paket mit den aktualisierten Daten erstellen, mit diesem neuen Paket einen neuen Index erstellen, den vorhandenen Index erneut mit dem neuen Index indizieren

und dann den alten Index löschen. Wenn Sie den Ansatz der Neuindizierung bevorzugen, verwenden Sie einen Indexalias, damit Ihr Datenverkehr nicht unterbrochen wird.

Optionale Plugins verwenden den `ZIP-PLUGIN` Pakettyp. Weitere Hinweise zu optionalen Plugins finden Sie unterthe section called “Pakete”.

Unterstützte Vorgänge in Amazon OpenSearch Service

OpenSearch Der Service unterstützt viele Versionen OpenSearch und ältere Versionen von Elasticsearch OSS. In den folgenden Abschnitten werden die Operationen beschrieben, die OpenSearch Service für jede Version unterstützt.

Themen

- Erwähnenswerte API-Unterschiede

Erwähnenswerte API-Unterschiede

Neue Liste APIs

Um große Cluster mit einer großen Anzahl von Indizes und Shards zu unterstützen, haben wir eine neue Liste APIs mit Paginierungsunterstützung eingeführt, z. B. _. list/indices and _list/shards Die List-API ruft Statistiken über Indizes und Shards in einem paginierten Format ab. Dies vereinfacht die Verarbeitung von Antworten, die viele Indizes enthalten.

- `_list/indices`: _liste/indizes
- `_list/shards`: _liste/scherben

Änderungen an bestehenden APIs

Um große Cluster zu unterstützen, haben wir in der `_cluster/stats` API Unterstützung für das Hinzufügen zusätzlicher Metrikfilter hinzugefügt, sodass nur relevante Statistikantworten abgerufen werden können, zum Beispiel `_cluster/stats/<metric>/nodes/<node-filters>` und`_cluster/stats/<metric>/<index_metric>/nodes/<node-filters>`. Einzelheiten finden Sie unter _cluster/stats.

Wir haben in der `_cat/shards` API Unterstützung für das Abbrechen von Aufgaben durch Angabe eines Anforderungsparameters hinzugefügt. `cancel_after_time_interval` Einzelheiten finden Sie unter _cat/shards.

Begrenzung der Antwortgröße für die _cat-API

Um große Cluster mit einer Gesamtzahl von mehr als 200 Instanzen in Daten- und Warmknoten zu unterstützen, haben wir eine Obergrenze von 10.000 für die Anzahl der von der zurückgegebenen Indizes festgelegt. `_cat/segments API` Wenn die Anzahl der Indizes in der Antwort dieses Limit überschreitet, gibt die API einen 429-Fehler zurück. Um dies zu vermeiden, können Sie in Ihrer Abfrage einen Indexmusterfilter angeben, z. B. `_cat/segments/<index-pattern>`

Einstellungen und Statistiken

OpenSearch Der Service akzeptiert nur PUT-Anfragen an die `_cluster/settings` API, die das „flache“ Einstellungsformular verwenden. Es lehnt Anforderungen ab, die die ausgeschriebene Form der Einstellungen verwenden.

```
// Accepted
PUT _cluster/settings
{
  "persistent" : {
    "action.auto_create_index" : false
  }
}

// Rejected
PUT _cluster/settings
{
  "persistent": {
    "action": {
      "auto_create_index": false
    }
  }
}
```

Der High-Level-Java-REST-Client verwendet die ausgeschriebene Form. Wenn Sie also Einstellungsanforderungen senden müssen, verwenden Sie den Low-Level-Client.

Vor Elasticsearch 5.3 unterstützte die `_cluster/settings` API auf OpenSearch Service-Domains nur die `PUT` HTTP-Methode, nicht die `GET` Methode. OpenSearch und spätere Versionen von Elasticsearch unterstützen die `GET` Methode, wie im folgenden Beispiel gezeigt:

```
GET https://domain-name.region.es.amazonaws.com/_cluster/settings?pretty
```

Hier ist ein Rückgabebeispiel:

```
{
  "persistent": {
    "cluster": {
      "routing": {
        "allocation": {
          "cluster_concurrent_rebalance": "2",
          "node_concurrent_recoveries": "2",
          "disk": {
            "watermark": {
              "low": "1.35gb",
              "flood_stage": "0.45gb",
              "high": "0.9gb"
            }
          },
          "node_initial_primarirecoveries": "4"
        }
      }
    },
    "indices": {
      "recovery": {
        "max_bytper_sec": "40mb"
      }
    }
  }
}
```

Wenn Sie die Antworten eines OpenSearch Open-Source-Clusters und eines OpenSearch Dienstes für bestimmte Einstellungen und Statistiken vergleichen, stellen Sie möglicherweise fest APIs, dass Felder fehlen. OpenSearch Der Dienst unkennzeichnet bestimmte Informationen, die interne Daten des Dienstes offenlegen, z. B. den Datenpfad des Dateisystems von `_nodes/stats` oder den Namen und die Version des Betriebssystems. `_nodes`

Shrink

Die `_shrink`-API kann dazu führen, dass Upgrades, Konfigurationsänderungen und Domain-Löschvorgänge fehlschlagen. Wir empfehlen Ihnen nicht, sie auf Domains zu verwenden, die mit Elasticsearch Version 5.3 oder 5.1 ausführt werden. Diese Versionen beinhalten einen Fehler, der dazu führen kann, dass Snapshot-Wiederherstellungen von geschrumpften Indizes fehlschlagen.

Wenn Sie die `_shrink` API auf anderen Elasticsearch oder anderen OpenSearch Versionen verwenden, stellen Sie die folgende Anfrage, bevor Sie den Verkleinerungsvorgang starten:

```
PUT https://domain-name.region.es.amazonaws.com/source-index/_settings
{
  "settings": {
    "index.routing.allocation.require._name": "name-of-the-node-to-shrink-to",
    "index.blocks.read_only": true
  }
}
```

Nach dem Abschließen der Shrink-Operation senden Sie dann folgende Anforderungen:

```
PUT https://domain-name.region.es.amazonaws.com/source-index/_settings
{
  "settings": {
    "index.routing.allocation.require._name": null,
    "index.blocks.read_only": false
  }
}

PUT https://domain-name.region.es.amazonaws.com/shrunken-index/_settings
{
  "settings": {
    "index.routing.allocation.require._name": null,
    "index.blocks.read_only": false
  }
}
```

Neue Liste APIs

Um große Cluster mit einer großen Anzahl von Indizes und Shards zu unterstützen, haben wir eine neue Liste APIs mit Paginierungsunterstützung eingeführt, d. h. und. `_list/indices` `_list/shards` Die List-API ruft Statistiken über Indizes und Shards in einem paginierten Format ab. Dies vereinfacht die Verarbeitung von Antworten, die viele Indizes enthalten. Weitere Informationen dazu finden Sie unter `_list/indices` Indizes auflisten. Weitere Informationen dazu finden Sie `_list/shards` unter Shards auflisten.

Änderungen an bestehenden APIs

Um große Cluster zu unterstützen, haben wir Unterstützung in `_cluster/stats/<metric>/nodes/<node-filters>` und hinzugefügt`_cluster/stats/<metric>/<index_metric>/nodes/<node-filters>`. Weitere Informationen zu finden Sie `_cluster/stats` unter Cluster-Statistiken.

Begrenzung der Antwortgröße für _cat APIs

Um große Cluster mit einer Gesamtzahl von mehr als 200 Instanzen in Daten- und Warmknoten zu unterstützen, haben wir eine Obergrenze von 10.000 für die Anzahl der von der _cat/segments API zurückgegebenen Indizes festgelegt. Wenn die Anzahl der Indizes in der Antwort dieses Limit überschreitet, gibt die API einen Fehler zurück. `429` Um dies zu vermeiden, können Sie in Ihrer Abfrage einen Indexmusterfilter angeben (z. B.`_cat/segments/<index-pattern>`).

Darüber hinaus ist die Unterstützung für das Abbrechen von Aufgaben jetzt auch für die `_cat/shards` API zur Stornierung von Aufgaben durch Angabe eines `cancel_after_time_interval` Anforderungsparameters verfügbar. Weitere Informationen dazu finden Sie unter CAT-Shards.

Auswahl der Instance-Typen für dedizierte Master-Knoten

Die folgende Tabelle enthält Empfehlungen für die Auswahl der geeigneten Instance-Typen für dedizierte Master-Knoten:

RAM	Maximale Anzahl unterstützter Knoten	Maximal unterstützter Shard	
2 GB	10	1.000	
4 GB	10	5,000	
8 GB	30	15 000	
16 GB	60	30 000	
32 GB	120	60 000	
64 GB	240	120.000	

RAM	Maximale Anzahl unterstützter Knoten	Maximal unterstützter Shard
128 GB	480	240.000
256 GB	1.002	500 000

OpenSearch Versionen 2.18 und 2.19

Informationen zu den Vorgängen OpenSearch 2.18 und 2.19 finden Sie in der OpenSearch REST-API-Referenz oder in der API-Referenz für das jeweilige Plugin. Weitere Informationen zu den Änderungen in diesen Versionen finden Sie in den Versionshinweisen zu 2.18 und in den Versionshinweisen zu 2.19.

OpenSearch Version 2.17

Für OpenSearch 2.17 unterstützt OpenSearch Service die folgenden Operationen. Informationen zu den meisten Vorgängen finden Sie in der OpenSearch REST-API-Referenz oder in der API-Referenz für das jeweilige Plugin.

> **Note**
>
> Ab Version OpenSearch 2.17 kann die `cluster.max_shards_per_node` Einstellung nicht geändert werden. Für OpenSearch 2.17 und höher unterstützt OpenSearch Service 1000 Shards pro 16 GB JVM-Heap-Speicher, bis zu einem Maximum von 4000 Shards pro Knoten.

- Alle Operationen im Index-Pfad (bspw. */index-name* /_forcemerge , */index-name* /update/*id* und */index-name* /_close)
- /_alias
- /_aliases
- /_delete_by_query [1]
- /_explain
- /_field_caps
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_list
- /_refresh
- /_reindex [1]
- /_render
- /_resolve/index
- /_rollover
- /_scripts [3]
- /_search [2]

- /_all
- /_analyze
- /_bulk
- /_cat (außer /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings für mehrere Eigenschaften[4]:
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
  - cluster.search.request.slowlog.level
  - cluster.search.request.slowlog.threshold.warn
  - cluster.search.request.slowlog.threshold.info
  - cluster.search.request.slowlog.threshold.debug
- /_ltr
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_plugins/_asynchronous_search
- /_plugins/_alerting
- /_plugins/_anomaly_detection
- /_plugins/_ism
- /_plugins/_ml
- /_plugins/_notifications
- /_plugins/_ppl
- /_plugins/_security
- /_plugins/_security_analytics
- /_plugins/_sm
- /_plugins/_sql
- /_percolate
- /_rank_eval
- /_search/pipeline
- /_search/point_in_time
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

  - `cluster.search.request.slowlog.threshold.trace`
  - `search.phase_took_enabled`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_dashboards`

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des `/_tasks`-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für `/_search/scroll` mit einem Nachrichtentext müssen `"Content-Length"` im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in `scroll_id` Werten zu vermeiden, verwenden Sie den Anforderungstext und nicht die Abfragezeichenfolge, um Werte an Service zu übergeben. `scroll_id` OpenSearch
3. Überlegungen zur Verwendung von Skripts finden Sie unter the section called “Andere unterstützte Ressourcen”.
4. Beziehen Sie sich auf die `PUT` Methode. Weitere Information zur `GET`-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen OpenSearch Operationen, die der OpenSearch Service unterstützt, und umfasst keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM und andere.
5. Siehe the section called “Shrink”.

> **Note**
>
> Derzeit ist das Ändern der `cluster.max_shards_per_node` Einstellungsfunktion für Kunden mit Multi-AZ (Availability Zone) mit Standby nicht aktiviert.

OpenSearch Version 2.15

Für OpenSearch 2.15 unterstützt OpenSearch Service die folgenden Operationen. Informationen zu den meisten Vorgängen finden Sie in der OpenSearch REST-API-Referenz oder in der API-Referenz für das jeweilige Plugin.

- Alle Operationen im Index-Pfad (bspw. */index-name* /_forcemerge , */index-name* /update/*id* und */index-name* /_close)
- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (außer /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings für mehrere Eigenschaften[4]:
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
- /_delete_by_query [1]
- /_explain
- /_field_caps
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_ltr
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_plugins/_asynchronous_search
- /_plugins/_alerting
- /_plugins/_anomaly_detection
- /_plugins/_ism
- /_plugins/_ml
- /_plugins/_notifications
- /_plugins/_ppl
- /_plugins/_security
- /_refresh
- /_reindex [1]
- /_render
- /_resolve/index
- /_rollover
- /_scripts [3]
- /_search[2]
- /_search/pipeline
- /_search/point_in_time
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

  - indices.breaker.total.limit
  - cluster.max_shards_per_node
  - cluster.search.request.slowlog.level
  - cluster.search.request.slowlog.threshold.warn
  - cluster.search.request.slowlog.threshold.info
  - cluster.search.request.slowlog.threshold.debug
  - cluster.search.request.slowlog.threshold.trace
  - search.phase_took_enabled
- /_cluster/state
- /_cluster/stats
- /_count
- /_dashboards
- /_plugins/_security_analytics
- /_plugins/_sm
- /_plugins/_sql
- /_percolate
- /_rank_eval

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des `/_tasks`-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für `/_search/scroll` mit einem Nachrichtentext müssen "`Content-Length`" im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in `scroll_id` Werten zu vermeiden, verwenden Sie den Anforderungstext und nicht die Abfragezeichenfolge, um `scroll_id` Werte an OpenSearch Service zu übergeben.

3. Überlegungen zur Verwendung von Skripts finden Sie unter the section called “Andere unterstützte Ressourcen”.
4. Verweist auf die PUT-Methode. Weitere Information zur GET-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen OpenSearch Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.
5. Siehe the section called “Shrink”.

OpenSearch Version 2.13

Für OpenSearch 2.13 unterstützt OpenSearch Service die folgenden Operationen. Informationen zu den meisten Vorgängen finden Sie in der OpenSearch REST-API-Referenz oder in der API-Referenz für das jeweilige Plugin.

- Alle Operationen im Index-Pfad (bspw. `/index-name /_forcemerge`, `/index-name /update/id` und `/index-name /_close`)
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (außer `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` für mehrere Eigenschaften[4]:
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_ltr`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_plugins/_asynchronous_search`
- `/_plugins/_alerting`
- `/_plugins/_anomaly_detection`
- `/_plugins/_ism`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_resolve/index`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search/pipeline`
- `/_search/point_in_time`
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`

- action.auto_create_index
- action.search.shard_count.limit
- indices.breaker.fielddata.limit
- indices.breaker.request.limit
- indices.breaker.total.limit
- cluster.max_shards_per_node
- cluster.search.request.slowlog.level
- cluster.search.request.slowlog.threshold.warn
- cluster.search.request.slowlog.threshold.info
- cluster.search.request.slowlog.threshold.debug
- cluster.search.request.slowlog.threshold.trace
- search.phase_took_enabled

- /_cluster/state
- /_cluster/stats
- /_count
- /_dashboards
- /_plugins/_ml
- /_plugins/_notifications
- /_plugins/_ppl
- /_plugins/_security
- /_plugins/_security_analytics
- /_plugins/_sm
- /_plugins/_sql
- /_percolate
- /_rank_eval
- /_template
- /_update_by_query [1]
- /_validate

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des `/_tasks`-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für `/_search/scroll` mit einem Nachrichtentext müssen `"Content-Length"` im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in `scroll_id` Werten zu vermeiden, verwenden Sie den Anforderungstext und nicht die Abfragezeichenfolge, um `scroll_id` Werte an OpenSearch Service zu übergeben.
3. Überlegungen zur Verwendung von Skripts finden Sie unter the section called “Andere unterstützte Ressourcen”.
4. Verweist auf die PUT-Methode. Weitere Information zur GET-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen OpenSearch Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.
5. Siehe the section called “Shrink”.

OpenSearch Version 2.11

Für OpenSearch 2.11 unterstützt OpenSearch Service die folgenden Operationen. Informationen zu den meisten Vorgängen finden Sie in der OpenSearch REST-API-Referenz oder in der API-Referenz für das jeweilige Plugin.

- Alle Operationen im Index-Pfad (bspw. */index-name* / `_forcemerge` , */index-name* `/update/`*id* und */index-name* `/_close`)
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_ltr`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_resolve/index`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search/pipeline`
- `/_search/point_in_time`
- `/_search profile`

- /_cat (außer /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings für mehrere Eigenschaften[4]:
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
  - cluster.max_shards_per_node
- /_cluster/state
- /_cluster/stats
- /_count
- /_dashboards
- /_nodes
- /_plugins/_asynchronous_search
- /_plugins/_alerting
- /_plugins/_anomaly_detection
- /_plugins/_ism
- /_plugins/_ml
- /_plugins/_notifications
- /_plugins/_ppl
- /_plugins/_security
- /_plugins/_security_analytics
- /_plugins/_sm
- /_plugins/_sql
- /_percolate
- /_rank_eval
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des /_tasks-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für /_search/scroll mit einem Nachrichtentext müssen "Content-Length" im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in scroll_id Werten zu vermeiden, verwenden Sie den Anforderungstext und nicht die Abfragezeichenfolge, um scroll_id Werte an OpenSearch Service zu übergeben.

3. Überlegungen zur Verwendung von Skripts finden Sie unter the section called “Andere unterstützte Ressourcen”.
4. Verweist auf die PUT-Methode. Weitere Information zur GET-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen OpenSearch Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.
5. Siehe the section called “Shrink”.

OpenSearch Version 2.9

Für OpenSearch 2.9 unterstützt OpenSearch Service die folgenden Operationen. Informationen zu den meisten Vorgängen finden Sie in der OpenSearch REST-API-Referenz oder in der API-Referenz für das jeweilige Plugin.

- Alle Operationen im Index-Pfad (bspw. `/index-name /_forcemerge` , `/index-name /update/id` und `/index-name /_close`)
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (außer `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` für mehrere Eigenschaften[4]:
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_ltr`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_plugins/_asynchronous_search`
- `/_plugins/_alerting`
- `/_plugins/_anomaly_detection`
- `/_plugins/_ism`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_resolve/index`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search/pipeline`
- `/_search/point_in_time`
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`

- `action.auto_create_index`
- `action.search.shard_count.limit`
- `indices.breaker.fielddata.limit`
- `indices.breaker.request.limit`
- `indices.breaker.total.limit`
- `cluster.max_shards_per_node`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_dashboards`
- `/_plugins/_ml`
- `/_plugins/_notifications`
- `/_plugins/_ppl`
- `/_plugins/_security`
- `/_plugins/_security_analytics`
- `/_plugins/_sm`
- `/_plugins/_sql`
- `/_percolate`
- `/_rank_eval`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des `/_tasks`-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für `/_search/scroll` mit einem Nachrichtentext müssen `"Content-Length"` im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in `scroll_id` Werten zu vermeiden, verwenden Sie den Anforderungstext und nicht die Abfragezeichenfolge, um `scroll_id` Werte an OpenSearch Service zu übergeben.
3. Überlegungen zur Verwendung von Skripts finden Sie unter the section called “Andere unterstützte Ressourcen”.
4. Verweist auf die `PUT`-Methode. Weitere Information zur `GET`-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen OpenSearch Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.
5. Siehe the section called “Shrink”.

OpenSearch Version 2.7

Für OpenSearch 2.7 unterstützt OpenSearch Service die folgenden Operationen. Informationen zu den meisten Vorgängen finden Sie in der OpenSearch REST-API-Referenz oder in der API-Referenz für das jeweilige Plugin.

- Alle Operationen im Index-Pfad (bspw. */index-name* /_forcemerge , */index-name* /update/*id* und */index-name* /_close)
- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (außer /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings für mehrere Eigenschaften[4]:
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
- /_delete_by_query [1]
- /_explain
- /_field_caps
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_ltr
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_plugins/_asynchronous_search
- /_plugins/_alerting
- /_plugins/_anomaly_detection
- /_plugins/_ism
- /_plugins/_ml
- /_plugins/_notifications
- /_plugins/_ppl
- /_plugins/_security
- /_refresh
- /_reindex [1]
- /_render
- /_resolve/index
- /_rollover
- /_scripts [3]
- /_search[2]
- /_search/point_in_time
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

- indices.breaker.total.limit
- cluster.max_shards_per_node
- /_cluster/state
- /_cluster/stats
- /_count
- /_dashboards
- /_plugins/_security_analytics
- /_plugins/_sm
- /_plugins/_sql
- /_percolate
- /_rank_eval

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des /_tasks-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für /_search/scroll mit einem Nachrichtentext müssen "Content-Length" im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in scroll_id Werten zu vermeiden, verwenden Sie den Anforderungstext und nicht die Abfragezeichenfolge, um scroll_id Werte an OpenSearch Service zu übergeben.
3. Überlegungen zur Verwendung von Skripts finden Sie unter the section called “Andere unterstützte Ressourcen”.
4. Verweist auf die PUT-Methode. Weitere Information zur GET-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen OpenSearch Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.
5. Siehe the section called “Shrink”.

OpenSearch Version 2.5

Für OpenSearch 2.5 unterstützt OpenSearch Service die folgenden Operationen. Informationen zu den meisten Vorgängen finden Sie in der OpenSearch REST-API-Referenz oder in der API-Referenz für das jeweilige Plugin.

- Alle Operationen im Index-Pfad (bspw. /*index-name* /
- /_delete_by_query [1]
- /_explain
- /_refresh
- /_reindex [1]

_forcemerge , */index-name* /update/*id* und */index-name* /_close)

- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (außer /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings für mehrere Eigenschaften[4]:
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
  - cluster.max_shards_per_node
- /_cluster/state
- /_cluster/stats
- /_count
- /_dashboards
- /_field_caps
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_ltr
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_plugins/_asynchronous_search
- /_plugins/_alerting
- /_plugins/_anomaly_detection
- /_plugins/_ism
- /_plugins/_ml
- /_plugins/_notifications
- /_plugins/_ppl
- /_plugins/_security
- /_plugins/_security_analytics
- /_plugins/_sm
- /_plugins/_sql
- /_percolate
- /_rank_eval
- /_render
- /_resolve/index
- /_rollover
- /_scripts [3]
- /_search[2]
- /_search/point_in_time
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des `/_tasks`-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für `/_search/scroll` mit einem Nachrichtentext müssen `"Content-Length"` im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in `scroll_id` Werten zu vermeiden, verwenden Sie den Anforderungstext und nicht die Abfragezeichenfolge, um `scroll_id` Werte an OpenSearch Service zu übergeben.
3. Überlegungen zur Verwendung von Skripts finden Sie unter the section called “Andere unterstützte Ressourcen”.
4. Verweist auf die PUT-Methode. Weitere Information zur GET-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen OpenSearch Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.
5. Siehe the section called “Shrink”.

OpenSearch Version 2.3

Für OpenSearch 2.3 unterstützt OpenSearch Service die folgenden Operationen. Informationen zu den meisten Vorgängen finden Sie in der OpenSearch REST-API-Referenz oder in der API-Referenz für das jeweilige Plugin.

- Alle Operationen im Index-Pfad (bspw. */index-name* / `_forcemerge` , */index-name* `/update/`*id* und */index-name* `/_close`)
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_ltr`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_resolve/index`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`

- /_cat (außer /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings für mehrere Eigenschaften[4]:
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
  - cluster.max_shards_per_node
- /_cluster/state
- /_cluster/stats
- /_count
- /_dashboards
- /_nodes
- /_plugins/_asynchronous_search
- /_plugins/_alerting
- /_plugins/_anomaly_detection
- /_plugins/_ism
- /_plugins/_ml
- _plugins/_notifications
- /_plugins/_ppl
- /_plugins/_security
- /_plugins/_sql
- /_percolate
- /_rank_eval
- /_split
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des /_tasks-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für /_search/scroll mit einem Nachrichtentext müssen "Content-Length" im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in scroll_id Werten zu vermeiden, verwenden Sie den Anforderungstext und nicht die Abfragezeichenfolge, um scroll_id Werte an OpenSearch Service zu übergeben.

3. Überlegungen zur Verwendung von Skripts finden Sie unter the section called “Andere unterstützte Ressourcen”.
4. Verweist auf die PUT-Methode. Weitere Information zur GET-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen OpenSearch Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.
5. Siehe the section called “Shrink”.

OpenSearch Version 1.3

Für OpenSearch 1.3 unterstützt OpenSearch Service die folgenden Operationen. Informationen zu den meisten Vorgängen finden Sie in der OpenSearch REST-API-Referenz oder in der API-Referenz für das jeweilige Plugin.

- Alle Operationen im Index-Pfad (bspw. `/index-name /_forcemerge` , `/index-name /update/id` und `/index-name /_close`)
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (außer `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` für mehrere Eigenschaften[4]:
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_ltr`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_plugins/_asynchronous_search`
- `/_plugins/_alerting`
- `/_plugins/_anomaly_detection`
- `/_plugins/_ism`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_resolve/index`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
  - cluster.max_shards_per_node
- /_cluster/state
- /_cluster/stats
- /_count
- /_dashboards
- /_plugins/_ml
- /_plugins/_ppl
- /_plugins/_security
- /_plugins/_sql
- /_percolate
- /_rank_eval

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des `/_tasks`-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für `/_search/scroll` mit einem Nachrichtentext müssen `"Content-Length"` im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in `scroll_id` Werten zu vermeiden, verwenden Sie den Anforderungstext und nicht die Abfragezeichenfolge, um `scroll_id` Werte an OpenSearch Service zu übergeben.
3. Überlegungen zur Verwendung von Skripts finden Sie unter the section called “Andere unterstützte Ressourcen”.
4. Verweist auf die PUT-Methode. Weitere Information zur GET-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen OpenSearch Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.
5. Siehe the section called “Shrink”.

OpenSearch Version 1.2

Für OpenSearch 1.2 unterstützt OpenSearch Service die folgenden Operationen. Informationen zu den meisten Vorgängen finden Sie in der OpenSearch REST-API-Referenz oder in der API-Referenz für das jeweilige Plugin.

- Alle Operationen im Index-Pfad (bspw. `/index-name /_forcemerge` , `/index-name /update/id` und `/index-name /_close`)
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (außer `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` für mehrere Eigenschaften[4]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_ltr`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_plugins/_asynchronous_search`
- `/_plugins/_alerting`
- `/_plugins/_anomaly_detection`
- `/_plugins/_ism`
- `/_plugins/_ppl`
- `/_plugins/_security`
- `/_plugins/_sql`
- `/_percolate`
- `/_rank_eval`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_resolve/index`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

  - indices.breaker.total.limit
  - cluster.max_shards_per_node
- /_cluster/state
- /_cluster/stats
- /_count
- /_dashboards

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des /_tasks-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für /_search/scroll mit einem Nachrichtentext müssen "Content-Length" im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in scroll_id Werten zu vermeiden, verwenden Sie den Anforderungstext und nicht die Abfragezeichenfolge, um scroll_id Werte an OpenSearch Service zu übergeben.
3. Überlegungen zur Verwendung von Skripts finden Sie unter the section called “Andere unterstützte Ressourcen”.
4. Verweist auf die PUT-Methode. Weitere Information zur GET-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen OpenSearch Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.
5. Siehe the section called “Shrink”.

OpenSearch Version 1.1

Für OpenSearch 1.1 unterstützt OpenSearch Service die folgenden Operationen. Informationen zu den meisten Vorgängen finden Sie in der OpenSearch REST-API-Referenz oder in der API-Referenz für das jeweilige Plugin.

- Alle Operationen im Index-Pfad (bspw. */index-name /*
- /_delete_by_query [1]
- /_explain
- /_refresh
- /_reindex [1]

_forcemerge , */index-name* /update/*id* und */index-name* /_close)

- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (außer /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings für mehrere Eigenschaften[4]:
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
  - cluster.max_shards_per_node
- /_cluster/state
- /_cluster/stats
- /_count
- /_dashboards
- /_field_caps
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_ltr
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_plugins/_asynchronous_search
- /_plugins/_alerting
- /_plugins/_anomaly_detection
- /_plugins/_ism
- /_plugins/_ppl
- /_plugins/_security
- /_plugins/_sql
- /_plugins/_transforms
- /_percolate
- /_rank_eval
- /_render
- /_resolve/index
- /_rollover
- /_scripts [3]
- /_search[2]
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des `/_tasks`-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für `/_search/scroll` mit einem Nachrichtentext müssen `"Content-Length"` im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in `scroll_id` Werten zu vermeiden, verwenden Sie den Anforderungstext und nicht die Abfragezeichenfolge, um `scroll_id` Werte an OpenSearch Service zu übergeben.
3. Überlegungen zur Verwendung von Skripts finden Sie unter the section called “Andere unterstützte Ressourcen”.
4. Verweist auf die PUT-Methode. Weitere Information zur GET-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen OpenSearch Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.
5. Siehe the section called “Shrink”.

OpenSearch Version 1.0

Für OpenSearch 1.0 unterstützt OpenSearch Service die folgenden Operationen. Informationen zu den meisten Vorgängen finden Sie in der OpenSearch REST-API-Referenz oder in der API-Referenz für das jeweilige Plugin.

- Alle Operationen im Index-Pfad (bspw. */index-name* */_forcemerge* , */index-name* */update/id* und */index-name* */_close*)
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (außer `/_cat/nodeattrs`)
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_ltr`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_resolve/index`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`

- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` für mehrere Eigenschaften[4]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
  - `indices.breaker.total.limit`
  - `cluster.max_shards_per_node`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_dashboards`
- `/_nodes`
- `/_plugins/_asynchronous_search`
- `/_plugins/_alerting`
- `/_plugins/_anomaly_detection`
- `/_plugins/_ism`
- `/_plugins/_ppl`
- `/_plugins/_security`
- `/_plugins/_sql`
- `/_plugins/_transforms`
- `/_percolate`
- `/_rank_eval`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des `/_tasks`-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für `/_search/scroll` mit einem Nachrichtentext müssen `"Content-Length"` im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in `scroll_id` Werten zu vermeiden, verwenden Sie den Anforderungstext und nicht die Abfragezeichenfolge, um `scroll_id` Werte an OpenSearch Service zu übergeben.
3. Überlegungen zur Verwendung von Skripts finden Sie unter the section called “Andere unterstützte Ressourcen”.

4. Verweist auf die PUT-Methode. Weitere Information zur GET-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen OpenSearch Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.
5. Siehe the section called “Shrink”.

Elasticsearch Version 7.10

Für Elasticsearch 7.10 unterstützt OpenSearch Service die folgenden Operationen.

- Alle Operationen im Index-Pfad (bspw. */index-name* /_forcemerge , */index-name* /update/*id* und */index-name* /_close)
- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (außer /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings für mehrere Eigenschaften[4]:
  - action.auto_create_index
  - action.search.shard_count.limit
- /_delete_by_query [1]
- /_explain
- /_field_caps
- /_field_stats
- /_flush
- /_index_template [6]
- /_ingest/pipeline
- /_index_template
- /_ltr
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_opendistro/_alerting
- /_opendistro/_asynchronous_search
- /_opendistro/_anomaly_detection
- /_opendistro/_ism
- /_opendistro/_ppl
- /_refresh
- /_reindex [1]
- /_render
- /_resolve/index
- /_rollover
- /_scripts [3]
- /_search[2]
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template [6]
- /_update_by_query [1]
- /_validate

- indices.breaker.fielddata.limit
- indices.breaker.request.limit
- indices.breaker.total.limit
- cluster.max_shards_per_node
- /_cluster/state
- /_cluster/stats
- /_count
- /_opendistro/_security
- /_opendistro/_sql
- /_percolate
- /_plugin/kibana
- /_plugins/_replication
- /_rank_eval

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des `/_tasks`-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für `/_search/scroll` mit einem Nachrichtentext müssen `"Content-Length"` im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in `scroll_id` Werten zu vermeiden, verwenden Sie den Hauptteil der Anfrage, nicht die Abfragezeichenfolge, um `scroll_id` Werte an Service zu OpenSearch übergeben.
3. Überlegungen zur Verwendung von Skripts finden Sie unter the section called “Andere unterstützte Ressourcen”.
4. Verweist auf die PUT-Methode. Weitere Information zur GET-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen Elasticsearch-Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.
5. Siehe the section called “Shrink”.
6. Legacy-Indexvorlagen (`_template`) wurden durch zusammensetzbare Vorlagen (`_index_template`), beginnend mit Elasticsearch 7.8, ersetzt. Zusammensetzbare Vorlagen haben Vorrang vor Legacy-Vorlagen. Wenn keine zusammensetzbare Vorlage mit einem bestimmten Index übereinstimmt, kann eine Legacy-Vorlage weiterhin übereinstimmen und angewendet werden. Der `_template` Vorgang funktioniert immer noch auf OpenSearch und

späteren Versionen von Elasticsearch OSS, aber GET-Aufrufe an die beiden Vorlagentypen liefern unterschiedliche Ergebnisse.

Elasticsearch Version 7.9

Für Elasticsearch 7.9 unterstützt OpenSearch Service die folgenden Operationen.

- Alle Operationen im Index-Pfad (bspw. `/index-name /_forcemerge` , `/index-name /update/id` und `/index-name /_close`)
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (außer `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` für mehrere Eigenschaften[4]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_index_template` [6]
- `/_ingest/pipeline`
- `/_ltr`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_opendistro/_alerting`
- `/_opendistro/_anomaly_detection`
- `/_opendistro/_ism`
- `/_opendistro/_ppl`
- `/_opendistro/_security`
- `/_opendistro/_sql`
- `/_percolate`
- `/_plugin/kibana`
- `/_rank_eval`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_resolve/index`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template` [6]
- `/_update_by_query` [1]
- `/_validate`

  - `indices.breaker.total.limit`
  - `cluster.max_shards_per_node`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des `/_tasks`-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für `/_search/scroll` mit einem Nachrichtentext müssen `"Content-Length"` im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in `scroll_id` Werten zu vermeiden, verwenden Sie den Hauptteil der Anfrage, nicht die Abfragezeichenfolge, um `scroll_id` Werte an OpenSearch Service zu übergeben.
3. Überlegungen zur Verwendung von Skripts finden Sie unter the section called “Andere unterstützte Ressourcen”.
4. Verweist auf die `PUT`-Methode. Weitere Information zur `GET`-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen OpenSearch Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.
5. Siehe the section called “Shrink”.
6. Legacy-Indexvorlagen (`_template`) wurden durch zusammensetzbare Vorlagen (`_index_template`), beginnend mit Elasticsearch 7.8, ersetzt. Zusammensetzbare Vorlagen haben Vorrang vor Legacy-Vorlagen. Wenn keine zusammensetzbare Vorlage mit einem bestimmten Index übereinstimmt, kann eine Legacy-Vorlage weiterhin übereinstimmen und angewendet werden. Der `_template` Vorgang funktioniert immer noch auf OpenSearch und späteren Versionen von Elasticsearch OSS, aber GET-Aufrufe an die beiden Vorlagentypen liefern unterschiedliche Ergebnisse.

Elasticsearch Version 7.8

Für Elasticsearch 7.8 unterstützt OpenSearch Service die folgenden Operationen.

- Alle Operationen im Index-Pfad (bspw. */index-name* /_forcemerge , */index-name* /update/*id* und */index-name* /_close)
- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (außer /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings für mehrere Eigenschaften[4]:
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
  - cluster.max_shards_per_node
- /_cluster/state
- /_cluster/stats
- /_count
- /_delete_by_query [1]
- /_explain
- /_field_caps
- /_field_stats
- /_flush
- /_index_template [6]
- /_ingest/pipeline
- /_ltr
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_opendistro/_alerting
- /_opendistro/_anomaly_detection
- /_opendistro/_ism
- /_opendistro/_security
- /_opendistro/_sql
- /_percolate
- /_plugin/kibana
- /_rank_eval
- /_refresh
- /_reindex [1]
- /_render
- /_rollover
- /_scripts [3]
- /_search[2]
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template [6]
- /_update_by_query [1]
- /_validate

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des `/_tasks`-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für `/_search/scroll` mit einem Nachrichtentext müssen `"Content-Length"` im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in `scroll_id` Werten zu vermeiden, verwenden Sie den Hauptteil der Anfrage, nicht die Abfragezeichenfolge, um `scroll_id` Werte an OpenSearch Service zu übergeben.
3. Überlegungen zur Verwendung von Skripts finden Sie unter the section called “Andere unterstützte Ressourcen”.
4. Verweist auf die PUT-Methode. Weitere Information zur GET-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen Elasticsearch-Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.
5. Siehe the section called “Shrink”.
6. Legacy-Indexvorlagen (`_template`) wurden durch zusammensetzbare Vorlagen (`_index_template`), beginnend mit Elasticsearch 7.8, ersetzt. Zusammensetzbare Vorlagen haben Vorrang vor Legacy-Vorlagen. Wenn keine zusammensetzbare Vorlage mit einem bestimmten Index übereinstimmt, kann eine Legacy-Vorlage weiterhin übereinstimmen und angewendet werden. Der `_template` Vorgang funktioniert immer noch auf OpenSearch und späteren Versionen von Elasticsearch OSS, aber GET-Aufrufe an die beiden Vorlagentypen liefern unterschiedliche Ergebnisse.

Elasticsearch Version 7.7

Für Elasticsearch 7.7 unterstützt OpenSearch Service die folgenden Operationen.

- Alle Operationen im Index-Pfad (bspw. `/index-name /_forcemerge` , `/index-name /update/id` und `/index-name /_close`)
- `/_alias`
- `/_aliases`
- `/_all`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_rollover`
- `/_scripts` [3]
- `/_search` [2]
- `/_search profile`

- `/_analyze`
- `/_bulk`
- `/_cat` (außer `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` für mehrere Eigenschaften[4]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
  - `indices.breaker.total.limit`
  - `cluster.max_shards_per_node`
- `/_flush`
- `/_ingest/pipeline`
- `/_ltr`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_opendistro/_alerting`
- `/_opendistro/_anomaly_detection`
- `/_opendistro/_ism`
- `/_opendistro/_security`
- `/_opendistro/_sql`
- `/_percolate`
- `/_plugin/kibana`
- `/_rank_eval`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des `/_tasks`-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für `/_search/scroll` mit einem Nachrichtentext müssen `"Content-Length"` im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in `scroll_id` Werten zu vermeiden, verwenden Sie den Hauptteil der Anfrage, nicht die Abfragezeichenfolge, um `scroll_id` Werte an OpenSearch Service zu übergeben.
3. Überlegungen zur Verwendung von Skripts finden Sie unter the section called “Andere unterstützte Ressourcen”.

4. Verweist auf die PUT-Methode. Weitere Information zur GET-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen Elasticsearch-Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.
5. Siehe the section called “Shrink”.

Elasticsearch Version 7.4

Für Elasticsearch 7.4 unterstützt OpenSearch Service die folgenden Operationen.

- Alle Operationen im Index-Pfad (bspw. `/index-name /_forcemerge` , `/index-name /update/id` und `/index-name /_close`)
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (außer `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` für mehrere Eigenschaften[4]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_opendistro/_alerting`
- `/_opendistro/_anomaly_detection`
- `/_opendistro/_ism`
- `/_opendistro/_security`
- `/_opendistro/_sql`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

- `indices.breaker.fielddata.limit`
- `indices.breaker.request.limit`
- `indices.breaker.total.limit`
- `cluster.max_shards_per_node`

- `/_percolate`
- `/_plugin/kibana`
- `/_rank_eval`

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des `/_tasks`-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für `/_search/scroll` mit einem Nachrichtentext müssen `"Content-Length"` im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in `scroll_id` Werten zu vermeiden, verwenden Sie den Hauptteil der Anfrage, nicht die Abfragezeichenfolge, um `scroll_id` Werte an OpenSearch Service zu übergeben.
3. Überlegungen zur Verwendung von Skripts finden Sie unter the section called “Andere unterstützte Ressourcen”.
4. Verweist auf die `PUT`-Methode. Weitere Information zur `GET`-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen Elasticsearch-Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.
5. Siehe the section called “Shrink”.

Elasticsearch Version 7.1

Für Elasticsearch 7.1 unterstützt OpenSearch Service die folgenden Operationen.

- Alle Operationen im Index-Pfad (bspw. `/index-name /_forcemerge` und `/index-name /update/id`) außer `/index-name /_close`

- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query` [1]

- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_rollover`

- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (außer /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings für mehrere Eigenschaften[4]:
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
  - cluster.max_shards_per_node
- /_explain
- /_field_caps
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_opendistro/_alerting
- /_opendistro/_ism
- /_opendistro/_security
- /_opendistro/_sql
- /_percolate
- /_plugin/kibana
- /_rank_eval
- /_scripts [3]
- /_search[2]
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des /_tasks-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für /_search/scroll mit einem Nachrichtentext müssen "Content-Length" im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in scroll_id Werten zu vermeiden, verwenden Sie den

Hauptteil der Anfrage, nicht die Abfragezeichenfolge, um `scroll_id` Werte an OpenSearch Service zu übergeben.

3. Überlegungen zur Verwendung von Skripts finden Sie unter the section called “Andere unterstützte Ressourcen”.
4. Verweist auf die PUT-Methode. Weitere Information zur GET-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen Elasticsearch-Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.
5. Siehe the section called “Shrink”.

Elasticsearch Version 6.8

Für Elasticsearch 6.8 unterstützt OpenSearch Service die folgenden Operationen.

- Alle Operationen im Index-Pfad (bspw. `/index-name /_forcemerge` und `/index-name /update/id`) außer `/index-name /_close`
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (außer `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` für mehrere Eigenschaften[4]:
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_opendistro/_alerting`
- `/_opendistro/_ism`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

- `action.auto_create_index`
- `action.search.shard_count.limit`
- `indices.breaker.fielddata.limit`
- `indices.breaker.request.limit`
- `indices.breaker.total.limit`
- `cluster.max_shards_per_node`
- `cluster.blocks.read_only`
- `/_opendistro/_security`
- `/_opendistro/_sql`
- `/_percolate`
- `/_plugin/kibana`
- `/_rank_eval`

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des `/_tasks`-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für `/_search/scroll` mit einem Nachrichtentext müssen `"Content-Length"` im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in `scroll_id` Werten zu vermeiden, verwenden Sie den Hauptteil der Anfrage, nicht die Abfragezeichenfolge, um `scroll_id` Werte an OpenSearch Service zu übergeben.
3. Überlegungen zur Verwendung von Skripts finden Sie unter the section called “Andere unterstützte Ressourcen”.
4. Verweist auf die `PUT`-Methode. Weitere Information zur `GET`-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen Elasticsearch-Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.
5. Siehe the section called “Shrink”.

Elasticsearch Version 6.7

Für Elasticsearch 6.7 unterstützt OpenSearch Service die folgenden Operationen.

- Alle Operationen im Index-Pfad (bspw. */index-name* */_forcemerge* und */index-name* */update/id*) außer */index-name* */_close*
- */_alias*
- */_aliases*
- */_all*
- */_analyze*
- */_bulk*
- */_cat* (außer */_cat/nodeattrs*)
- */_cluster/allocation/explain*
- */_cluster/health*
- */_cluster/pending_tasks*
- */_cluster/settings* für mehrere Eigenschaften[4]:
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
- */_cluster/state*
- */_cluster/stats*
- */_count*
- */_delete_by_query* [1]
- */_explain*
- */_field_caps*
- */_field_stats*
- */_flush*
- */_ingest/pipeline*
- */_mapping*
- */_mget*
- */_msearch*
- */_mtermvectors*
- */_nodes*
- */_opendistro/_alerting*
- */_opendistro/_security*
- */_opendistro/_sql*
- */_percolate*
- */_plugin/kibana*
- */_rank_eval*
- */_refresh*
- */_reindex* [1]
- */_render*
- */_rollover*
- */_scripts* [3]
- */_search*[2]
- */_search profile*
- */_shard_stores*
- */_shrink*[5]
- */_snapshot*
- */_split*
- */_stats*
- */_status*
- */_tasks*
- */_template*
- */_update_by_query* [1]
- */_validate*

- `cluster.max_shards_per_node`

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des `/_tasks`-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für `/_search/scroll` mit einem Nachrichtentext müssen `"Content-Length"` im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in `scroll_id` Werten zu vermeiden, verwenden Sie den Hauptteil der Anfrage, nicht die Abfragezeichenfolge, um `scroll_id` Werte an OpenSearch Service zu übergeben.
3. Überlegungen zur Verwendung von Skripts finden Sie unter the section called “Andere unterstützte Ressourcen”.
4. Verweist auf die PUT-Methode. Weitere Information zur GET-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen Elasticsearch-Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.
5. Siehe the section called “Shrink”.

Elasticsearch Version 6.5

Für Elasticsearch 6.5 unterstützt OpenSearch Service die folgenden Operationen.

- Alle Operationen im Index-Pfad (bspw. */index-name* `/_forcemerge` und */index-name* `/update/`*id*) außer */index-name* `/_close`
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_mapping`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`

- `/_cat` (außer `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` für mehrere Eigenschaften[4]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
  - `indices.breaker.total.limit`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_opendistro/_alerting`
- `/_opendistro/_sql`
- `/_percolate`
- `/_plugin/kibana`
- `/_rank_eval`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des `/_tasks`-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für `/_search/scroll` mit einem Nachrichtentext müssen `"Content-Length"` im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in `scroll_id` Werten zu vermeiden, verwenden Sie den Hauptteil der Anfrage, nicht die Abfragezeichenfolge, um `scroll_id` Werte an OpenSearch Service zu übergeben.
3. Überlegungen zur Verwendung von Skripts finden Sie unter the section called “Andere unterstützte Ressourcen”.
4. Verweist auf die `PUT`-Methode. Weitere Information zur `GET`-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen Elasticsearch-Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.

5. Siehe the section called “Shrink”.

Elasticsearch Version 6.4

Für Elasticsearch 6.4 unterstützt OpenSearch Service die folgenden Operationen.

- Alle Operationen im Index-Pfad (bspw. */index-name /_forcemerge* und */index-name /update/id*) außer */index-name /_close*
- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (außer /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings für mehrere Eigenschaften[4]:
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
- /_cluster/state
- /_cluster/stats
- /_count
- /_delete_by_query [1]
- /_explain
- /_field_caps
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_opendistro/_alerting
- /_percolate
- /_plugin/kibana
- /_rank_eval
- /_refresh
- /_reindex [1]
- /_render
- /_rollover
- /_scripts [3]
- /_search[2]
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

- `indices.breaker.total.limit`

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des `/_tasks`-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für `/_search/scroll` mit einem Nachrichtentext müssen `"Content-Length"` im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in `scroll_id` Werten zu vermeiden, verwenden Sie den Hauptteil der Anfrage, nicht die Abfragezeichenfolge, um `scroll_id` Werte an OpenSearch Service zu übergeben.
3. Überlegungen zur Verwendung von Skripts finden Sie unter the section called “Andere unterstützte Ressourcen”.
4. Verweist auf die PUT-Methode. Weitere Information zur GET-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen Elasticsearch-Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.
5. Siehe the section called “Shrink”.

Elasticsearch Version 6.3

Für Elasticsearch 6.3 unterstützt OpenSearch Service die folgenden Operationen.

- Alle Operationen im Index-Pfad (bspw. */index-name /_forcemerge* und */index-name /update/id*) außer */index-name /_close*
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_mapping`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_rollover`
- `/_scripts` [3]
- `/_search` [2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink` [5]
- `/_snapshot`

- `/_cat` (außer `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` für mehrere Eigenschaften[4]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
  - `indices.breaker.total.limit`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_opendistro/_alerting`
- `/_percolate`
- `/_plugin/kibana`
- `/_rank_eval`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des `/_tasks`-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für `/_search/scroll` mit einem Nachrichtentext müssen `"Content-Length"` im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in `scroll_id` Werten zu vermeiden, verwenden Sie den Hauptteil der Anfrage, nicht die Abfragezeichenfolge, um `scroll_id` Werte an OpenSearch Service zu übergeben.
3. Überlegungen zur Verwendung von Skripts finden Sie unter the section called “Andere unterstützte Ressourcen”.
4. Verweist auf die `PUT`-Methode. Weitere Information zur `GET`-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen Elasticsearch-Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.

5. Siehe the section called “Shrink”.

Elasticsearch Version 6.2

Für Elasticsearch 6.2 unterstützt OpenSearch Service die folgenden Operationen.

- Alle Operationen im Index-Pfad (bspw. */index-name /_forcemerge* und */index-name /update/id*) außer */index-name /_close*
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (außer `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` für mehrere Eigenschaften[4]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_opendistro/_alerting`
- `/_percolate`
- `/_plugin/kibana`
- `/_rank_eval`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

- indices.breaker.total.limit

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des `/_tasks`-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für `/_search/scroll` mit einem Nachrichtentext müssen `"Content-Length"` im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in `scroll_id` Werten zu vermeiden, verwenden Sie den Hauptteil der Anfrage, nicht die Abfragezeichenfolge, um `scroll_id` Werte an OpenSearch Service zu übergeben.
3. Überlegungen zur Verwendung von Skripts finden Sie unter the section called “Andere unterstützte Ressourcen”.
4. Verweist auf die PUT-Methode. Weitere Information zur GET-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen Elasticsearch-Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.
5. Siehe the section called “Shrink”.

Elasticsearch Version 6.0

Für Elasticsearch 6.0 unterstützt OpenSearch Service die folgenden Operationen.

- Alle Operationen im Index-Pfad (bspw. */index-name* `/_forcemerge` und */index-name* `/update/`*id*) außer */index-name* `/_close`
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_mapping`
- `/_render`
- `/_rollover`
- `/_scripts` [3]
- `/_search` [2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink` [5]
- `/_snapshot`
- `/_stats`
- `/_status`

- `/_cat` (außer `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` für mehrere Eigenschaften[4]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
  - `indices.breaker.total.limit`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_percolate`
- `/_plugin/kibana`
- `/_refresh`
- `/_reindex` [1]
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des `/_tasks`-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für `/_search/scroll` mit einem Nachrichtentext müssen `"Content-Length"` im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in `scroll_id` Werten zu vermeiden, verwenden Sie den Hauptteil der Anfrage, nicht die Abfragezeichenfolge, um `scroll_id` Werte an OpenSearch Service zu übergeben.
3. Überlegungen zur Verwendung von Skripts finden Sie unter the section called “Andere unterstützte Ressourcen”.
4. Verweist auf die `PUT`-Methode. Weitere Information zur `GET`-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen Elasticsearch-Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.

5. Siehe the section called “Shrink”.

Elasticsearch Version 5.6

Für Elasticsearch 5.6 unterstützt OpenSearch Service die folgenden Operationen.

- Alle Operationen im Index-Pfad (bspw. */index-name /_forcemerge* und */index-name /update/id*) außer */index-name /_close*
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (außer `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` für mehrere Eigenschaften[4]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_percolate`
- `/_plugin/kibana`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

- `indices.breaker.total.limit`

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des `/_tasks`-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für `/_search/scroll` mit einem Nachrichtentext müssen `"Content-Length"` im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in `scroll_id` Werten zu vermeiden, verwenden Sie den Hauptteil der Anfrage, nicht die Abfragezeichenfolge, um `scroll_id` Werte an OpenSearch Service zu übergeben.
3. Überlegungen zur Verwendung von Skripts finden Sie unter the section called “Andere unterstützte Ressourcen”.
4. Verweist auf die PUT-Methode. Weitere Information zur GET-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen Elasticsearch-Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.
5. Siehe the section called “Shrink”.

Elasticsearch Version 5.5

Für Elasticsearch 5.5 unterstützt OpenSearch Service die folgenden Operationen.

- Alle Operationen im Index-Pfad (bspw. */index-name* `/_forcemerge` und */index-name* `/update/`*id*) außer */index-name* `/_close`
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_mapping`
- `/_render`
- `/_rollover`
- `/_scripts` [3]
- `/_search` [2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink` [5]
- `/_snapshot`
- `/_stats`
- `/_status`

- `/_cat` (außer `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` für mehrere Eigenschaften[4]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
  - `indices.breaker.total.limit`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_percolate`
- `/_plugin/kibana`
- `/_refresh`
- `/_reindex` [1]
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des `/_tasks`-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für `/_search/scroll` mit einem Nachrichtentext müssen `"Content-Length"` im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in `scroll_id` Werten zu vermeiden, verwenden Sie den Hauptteil der Anfrage, nicht die Abfragezeichenfolge, um `scroll_id` Werte an OpenSearch Service zu übergeben.
3. Überlegungen zur Verwendung von Skripts finden Sie unter the section called “Andere unterstützte Ressourcen”.
4. Verweist auf die `PUT`-Methode. Weitere Information zur `GET`-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen Elasticsearch-Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.

5. Siehe the section called “Shrink”.

Elasticsearch Version 5.3

Für Elasticsearch 5.3 unterstützt OpenSearch Service die folgenden Operationen.

- Alle Operationen im Index-Pfad (bspw. */index-name /_forcemerge* und */index-name /update/id*) außer */index-name /_close*
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (außer `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` für mehrere Eigenschaften [3]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_percolate`
- `/_plugin/kibana`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_rollover`
- `/_search` [2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink` [4]
- `/_snapshot`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

- `indices.breaker.total.limit`

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des `/_tasks`-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für `/_search/scroll` mit einem Nachrichtentext müssen `"Content-Length"` im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in `scroll_id` Werten zu vermeiden, verwenden Sie den Hauptteil der Anfrage, nicht die Abfragezeichenfolge, um `scroll_id` Werte an OpenSearch Service zu übergeben.
3. Verweist auf die `PUT`-Methode. Weitere Information zur `GET`-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen Elasticsearch-Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.
4. Siehe the section called “Shrink”.

Elasticsearch Version 5.1

Für Elasticsearch 5.1 unterstützt OpenSearch Service die folgenden Operationen.

- Alle Operationen im Index-Pfad (bspw. */index-name* */_forcemerge* und */index-name* */update/id*) außer */index-name* */_close*
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (außer `/_cat/nodeattrs`)
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_mapping`
- `/_mget`
- `/_render`
- `/_rollover`
- `/_search`[2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[3]
- `/_snapshot`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`

- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` für mehrere Eigenschaften (nur PUT):
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
  - `indices.breaker.total.limit`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_percolate`
- `/_plugin/kibana`
- `/_refresh`
- `/_reindex` [1]
- `/_update_by_query` [1]
- `/_validate`

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des `/_tasks`-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für `/_search/scroll` mit einem Nachrichtentext müssen `"Content-Length"` im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in `scroll_id` Werten zu vermeiden, verwenden Sie den Hauptteil der Anfrage, nicht die Abfragezeichenfolge, um `scroll_id` Werte an OpenSearch Service zu übergeben.
3. Siehe the section called “Shrink”.

Elasticsearch Version 2.3

Für Elasticsearch 2.3 unterstützt OpenSearch Service die folgenden Operationen.

- Alle Operationen im Index-Pfad (bspw. */index-name* `/_forcemerge` und */index-name* `/_recovery`) außer */index-name* `/_close`
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cache/clear` (nur Index)
- `/_cat` (außer `/_cat/nodeattrs`)
- `/_cluster/health`
- `/_cluster/settings` für mehrere Eigenschaften (nur PUT):
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
  - `indices.breaker.total.limit`
  - `threadpool.get.queue_size`
  - `threadpool.bulk.queue_size`
  - `threadpool.index.queue_size`
  - `threadpool.percolate.queue_size`
  - `threadpool.search.queue_size`
  - `threadpool.suggest.queue_size`
- `/_cluster/stats`
- `/_count`
- `/_flush`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_nodes`
- `/_percolate`
- `/_plugin/kibana`
- `/_refresh`
- `/_render`
- `/_search`
- `/_snapshot`
- `/_stats`
- `/_status`
- `/_template`

Elasticsearch Version 1.5

Für Elasticsearch 1.5 unterstützt OpenSearch Service die folgenden Operationen.

- Alle Operationen im Index-Pfad, bspw. */index-name* `/_optimize` und
- `/_cluster/stats`

/*index-name* /_warmer, außer /*index-name* /_close
- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat
- /_cluster/health
- /_cluster/settings für mehrere Eigenschaften (nur PUT):
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
  - threadpool.get.queue_size
  - threadpool.bulk.queue_size
  - threadpool.index.queue_size
  - threadpool.percolate.queue_size
  - threadpool.search.queue_size
  - threadpool.suggest.queue_size
- /_count
- /_flush
- /_mapping
- /_mget
- /_msearch
- /_nodes
- /_percolate
- /_plugin/kibana
- /_plugin/kibana3
- /_plugin/migration
- /_refresh
- /_search
- /_snapshot
- /_stats
- /_status
- /_template

Amazon OpenSearch Service-Kontingente

Ihr AWS Konto verfügt über Standardkontingente, die früher als Limits bezeichnet wurden, für jeden AWS Service. Wenn nicht anders angegeben, gilt jedes Kontingent spezifisch für eine Region.

Die Kontingente für OpenSearch Service-Domains und -Instances, Amazon OpenSearch Serverless und Amazon OpenSearch Ingestion finden Sie unter Amazon OpenSearch Service-Kontingente in der. Allgemeine AWS-Referenz

Um die Kontingente für OpenSearch Service in der anzuzeigen AWS Management Console, öffnen Sie die Konsole Service Quotas. Wählen Sie im Navigationsbereich AWS Services und dann Amazon OpenSearch Service aus. Informationen zur Erhöhung eines Kontingents finden Sie unter Anfordern einer Kontingenterhöhung im Service-Quotas-Benutzerhandbuch.

UltraWarm Speicherkontingente

In der folgenden Tabelle sind die UltraWarm Instanztypen und die maximale Speichermenge aufgeführt, die jeder Typ verwenden kann. Weitere Informationen zu finden UltraWarm Sie unterthe section called “UltraWarm Speicher”.

Instance-Typ	Maximaler Speicher
ultrawarm1.medium.search	1,5 TiB
ultrawarm1.large.search	20 TiB

Anzahl der Datenknoten pro AZ

In der folgenden Tabelle ist die Gesamtzahl der Datenknoten für die AZ-Bereitstellung aufgeführt. Die Gesamtgrenze gibt die Anzahl der Datenknoten pro Limit an, einschließlich der Anzahl der heißen und warmen Knoten. Speicher, den jeder Typ verwenden kann.

AZ-Konfiguration	Limit für die Anzahl heißer Knoten	Limit für die Anzahl warmer Knoten	Gesamtlimit (heiß + warm)
1 - AZ	334	250	334
2 - AZ	668	500	668
3 - WIE	1.002	750	1.002

Gesamtzahl der Knoten pro Instanzfamilie

In der folgenden Tabelle ist das Gesamtknotenlimit nach Instanzfamilien aufgeführt.

Instance-Familie	ElasticSearch OpenSearch bis zu 2,15	OpenSearch 2.17 und höher	Standardlimit
T2	10	10	10
T3	10	10	10
M3, C4, M4, R4, C5, M5, R5, I2, I3	10	200	80
Gravitation 2, Schwerkraft 3	200	400	80
C7, R7i, M7i, I4i	200	400	80
OR1.mittel.suche OR1.große.suche OR2.mittelgroße Suche OR2.große.suche OM2.large.search	200	400	80
OR1.xlarge.search und höher OR2.xlarge.search und höher OM2.xlarge.search und höher	200	1.002	80
Ultrawarm 1	150	750	150

EBS-Volume-Größenkontigente

Die folgende Tabelle zeigt die Mindest- und Höchstgrößen für EBS-Volumes für jeden Instance-Typ, OpenSearch den Service unterstützt. Informationen darüber, welche Instance-Typen Instance-Speicher und zusätzliche Hardwaredetails beinhalten, finden Sie unter Amazon OpenSearch Service-Preise.

- Wenn Sie bei der Erstellung Ihrer Domain Magnetspeicher unter dem Volumetyp EBS wählen, beträgt die maximale Volume-Größe 100 GiB für alle Instance-Typen außer t2.small und t2.medium sowie für alle Graviton-Instances (m6g, C6g, R6g und R6gd), die Magnetspeicher nicht unterstützen. Wählen Sie für die maximalen Größen in der folgenden Tabelle eine der SSD-Optionen aus.
- Einige Instance-Typen älterer Generation umfassen Instance-Speicher, unterstützen aber auch EBS-Speicher. Wenn Sie EBS-Speicher für einen dieser Instance-Typen wählen, gelten die Speicher-Volumes nicht additiv. Sie können entweder ein EBS-Volume oder Instance-Speicher verwenden, nicht aber beides.

Instance-Typ	EBS-Mindestgröße	Maximale EBS-Größe (gp2)	Maximale EBS-Größe (gp3)
t2.micro.search	10 GiB	35 GiB	N/A
t2.small.search	10 GiB	35 GiB	N/A
t2.medium.search	10 GiB	35 GiB	N/A
t3.small.search	10 GiB	100 GiB	100 GiB
t3.medium.search	10 GiB	200 GiB	200 GiB
m3.medium.search	10 GiB	100 GiB	N/A
m3.large.search	10 GiB	512 GiB	N/A
m3.xlarge.search	10 GiB	512 GiB	N/A
m3.2xlarge.search	10 GiB	512 GiB	N/A
m4.large.search	10 GiB	512 GiB	N/A
m4.xlarge.search	10 GiB	1 TiB	N/A
m4.2xlarge.search	10 GiB	1,5 TiB	N/A
m4.4xlarge.search	10 GiB	1,5 TiB	N/A

Instance-Typ	EBS-Mindestgröße	Maximale EBS-Größe (gp2)	Maximale EBS-Größe (gp3)
m4.10xlarge.search	10 GiB	1,5 TiB	N/A
m5.large.search	10 GiB	512 GiB	1 TiB
m5.xlarge.search	10 GiB	1 TiB	2 TiB
m5.2xlarge.search	10 GiB	1,5 TiB	3 TiB
m5.4xlarge.search	10 GiB	3 TiB	6 TiB
m5.12xlarge.search	10 GiB	9 TiB	18 TiB
m6g.large.search	10 GiB	512 GiB	1 TiB
m6g.xlarge.search	10 GiB	1 TiB	2 TiB
m6g.2xlarge.search	10 GiB	1,5 TiB	3 TiB
m6g.4xlarge.search	10 GiB	3 TiB	6 TiB
m6g.8xlarge.search	10 GiB	6 TiB	12 TiB
m6g.12xlarge.search	10 GiB	9 TiB	18 TiB
c4.large.search	10 GiB	100 GiB	N/A
c4.xlarge.search	10 GiB	512 GiB	N/A
c4.2xlarge.search	10 GiB	1 TiB	N/A
c4.4xlarge.search	10 GiB	1,5 TiB	N/A
c4.8xlarge.search	10 GiB	1,5 TiB	N/A
c5.large.search	10 GiB	256 GiB	256 GiB
c5.xlarge.search	10 GiB	512 GiB	512 GiB

Instance-Typ	EBS-Mindestgröße	Maximale EBS-Größe (gp2)	Maximale EBS-Größe (gp3)
c5.2xlarge.search	10 GiB	1 TiB	1 TiB
c5.4xlarge.search	10 GiB	1,5 TiB	1,5 TiB
c5.9xlarge.search	10 GiB	3,5 TiB	3,5 TiB
c5.18xlarge.search	10 GiB	7 TiB	7 TiB
c6g.large.search	10 GiB	256 GiB	256 GiB
c6g.xlarge.search	10 GiB	512 GiB	512 GiB
c6g.2xlarge.search	10 GiB	1 TiB	1 TiB
c6g.4xlarge.search	10 GiB	1,5 TiB	1,5 TiB
c6g.8xlarge.search	10 GiB	3 TiB	3 TiB
c6g.12xlarge.search	10 GiB	4.5 TiB	4.5 TiB
r3.large.search	10 GiB	512 GiB	N/A
r3.xlarge.search	10 GiB	512 GiB	N/A
r3.2xlarge.search	10 GiB	512 GiB	N/A
r3.4xlarge.search	10 GiB	512 GiB	N/A
r3.8xlarge.search	10 GiB	512 GiB	N/A
r4.large.search	10 GiB	1 TiB	N/A
r4.xlarge.search	10 GiB	1,5 TiB	N/A
r4.2xlarge.search	10 GiB	1,5 TiB	N/A
r4.4xlarge.search	10 GiB	1,5 TiB	N/A

Instance-Typ	EBS-Mindestgröße	Maximale EBS-Größe (gp2)	Maximale EBS-Größe (gp3)
r4.8xlarge.search	10 GiB	1,5 TiB	N/A
r4.16xlarge.search	10 GiB	1,5 TiB	N/A
r5.large.search	10 GiB	1 TiB	2 TiB
r5.xlarge.search	10 GiB	1,5 TiB	3 TiB
r5.2xlarge.search	10 GiB	3 TiB	6 TiB
r5.4xlarge.search	10 GiB	6 TiB	12 TiB
r5.12xlarge.search	10 GiB	12 TiB	24 TiB
r6g.large.search	10 GiB	1 TiB	2 TiB
r6g.xlarge.search	10 GiB	1,5 TiB	3 TiB
r6g.2xlarge.search	10 GiB	3 TiB	6 TiB
r6g.4xlarge.search	10 GiB	6 TiB	12 TiB
r6g.8xlarge.search	10 GiB	8 TiB	16 TiB
r6g.12xlarge.search	10 GiB	12 TiB	24 TiB
r6gd.large.search	N/A	–	N/A
r6gd.xlarge.search	N/A	–	N/A
r6gd.2xlarge.search	N/A	–	N/A
r6gd.4xlarge.search	N/A	–	N/A
r6gd.8xlarge.search	N/A	–	N/A
r6gd.12xlarge.search	N/A	–	N/A

Instance-Typ	EBS-Mindestgröße	Maximale EBS-Größe (gp2)	Maximale EBS-Größe (gp3)
r6gd.16xlarge.search	N/A	–	N/A
i2.xlarge.search	10 GiB	512 GiB	N/A
i2.2xlarge.search	10 GiB	512 GiB	N/A
i3.large.search	N/A	–	N/A
i3.xlarge.search	N/A	–	N/A
i3.2xlarge.search	N/A	–	N/A
i3.4xlarge.search	N/A	–	N/A
i3.8xlarge.search	N/A	–	N/A
i3.16xlarge.search	N/A	–	N/A
oder 1.medium.search	20 GiB	N/A	768 GiB
oder 1.large.search	20 GiB	N/A	1532 GiB
oder 1.xlarge.search	20 GiB	N/A	3 TiB
oder 1.2xlarge.search	20 GiB	N/A	6 TiB
oder 1,4xlarge.search	20 GiB	N/A	12 TiB
oder 1,8xlarge.search	20 GiB	N/A	16 TiB
oder 1.12xlarge.search	20 GiB	N/A	24 TiB
oder 1.16xlarge.search	20 GiB	N/A	36 TiB
oder 2.medium.search	20 GiB	N/A	768 GiB
oder 2.large.search	20 GiB	N/A	1532 GiB

Instance-Typ	EBS-Mindestgröße	Maximale EBS-Größe (gp2)	Maximale EBS-Größe (gp3)
oder 2.xlarge.search	20 GiB	N/A	3 TiB
oder 2.2xlarge.search	20 GiB	N/A	6 TiB
oder 2,4xlarge.search	20 GiB	N/A	12 TiB
oder 2,8xlarge.search	20 GiB	N/A	16 TiB
oder 2,12xlarge.search	20 GiB	N/A	24 TiB
oder 2.16xlarge.search	20 GiB	N/A	36 TiB
om2.large.search	20 GiB	N/A	768 GiB
om2.xlarge.search	20 GiB	N/A	2 Wanne
om2.2xlarge.search	20 GiB	N/A	3 Tib
om2.4xlarge.search	20 GiB	N/A	6 Tib
om2.8xlarge.search	20 GiB	N/A	12 Tonnen
om2.12xlarge.search	20 GiB	N/A	18 Tib
om2.16xlarge.search	20 GiB	N/A	24 Tonnen
im4gn.large.search	N/A	–	N/A
im4gn.xlarge.search	N/A	–	N/A
im4gn.2xlarge.search	N/A	–	N/A
im4gn.4xlarge.search	N/A	–	N/A
im4gn.8xlarge.search	N/A	–	N/A
im4gn.16xlarge.search	N/A	–	N/A

Instance-Typ	EBS-Mindestgröße	Maximale EBS-Größe (gp2)	Maximale EBS-Größe (gp3)
C7G.Large.Suche	10 GiB	N/A	256 GiB
C7G.XLarge.Search	10 GiB	N/A	512 GiB
C7G.2xLarge.Suche	10 GiB	N/A	1 TiB
C7G.4xLarge.Suche	10 GiB	N/A	1,5 TiB
C7G.8XLarge.Suche	10 GiB	N/A	3 TiB
C7G.12XLarge.Suche	10 GiB	N/A	4.5 TiB
C7G.16xLarge.Suche	10 GiB	N/A	6 TiB
M7G.Medium.Search	10 GiB	N/A	512 GiB
M7G.Large.Suche	10 GiB	N/A	768 GiB
M7G.XLarge.Search	10 GiB	N/A	2 TiB
M7G.2XLarge.Suche	10 GiB	N/A	3 TiB
M7G.4xLarge.Suche	10 GiB	N/A	6 TiB
M7G.8XLarge.Suche	10 GiB	N/A	12 TiB
M7G.12XLarge.Suche	10 GiB	N/A	18 TiB
M7G.16x Large.Suche	10 GiB	N/A	24 TiB
R7G.Medium.Search	10 GiB	N/A	768 GiB
R7G.Large.Search	10 GiB	N/A	1,5 TiB
R7G.XLarge.Search	10 GiB	N/A	3 TiB
R7G.2xLarge.Suche	10 GiB	N/A	6 TiB

Instance-Typ	EBS-Mindestgröße	Maximale EBS-Größe (gp2)	Maximale EBS-Größe (gp3)
R7G.4x Large.Suche	10 GiB	N/A	12 TiB
R7G.8XLarge.Suche	10 GiB	N/A	16 TiB
R7G.12xLarge.Suche	10 GiB	N/A	24 TiB
R7G.16x Large. Suche	10 GiB	N/A	36 TiB
R7 GD.Large.Suche	N/A	–	N/A
R7GD.XLarge.Search	N/A	–	N/A
R7GD.2xLarge.Suche	N/A	–	N/A
R7GD.4xLarge.Suche	N/A	–	N/A
R7GD.8XLarge.Suche	N/A	–	N/A
R7GD.12xLarge.Suche	N/A	–	N/A
R7GD.16xLarge.Suche	N/A	–	N/A
i4i.large.search	10 GiB	N/A	N/A
i4i.xlarge.search	10 GiB	N/A	N/A
i4i.2xlarge.search	10 GiB	N/A	N/A
i4i.4xlarge.search	10 GiB	N/A	N/A
i4i.8xlarge.search	10 GiB	N/A	N/A
i4i.12xlarge.search	10 GiB	N/A	N/A
i4i.16xlarge.search	10 GiB	N/A	N/A
i4i.24xlarge.search	10 GiB	N/A	N/A

Instance-Typ	EBS-Mindestgröße	Maximale EBS-Größe (gp2)	Maximale EBS-Größe (gp3)
i4i.32xlarge.search	10 GiB	N/A	N/A
i4g.large.search	10 GiB	N/A	N/A
i4g.xlarge.search	10 GiB	N/A	N/A
i4g.2xlarge.search	10 GiB	N/A	N/A
i4g.4xlarge.search	10 GiB	N/A	N/A
i4g.8xlarge.search	10 GiB	N/A	N/A
i4g.16xlarge.search	10 GiB	N/A	N/A
c7i.large.search	10 GiB	N/A	256 GiB
c7i.xlarge.search	10 GiB	N/A	512 GiB
c7i.2xlarge.search	10 GiB	N/A	1 TiB
c7i.4xlarge.search	10 GiB	N/A	1,5 TiB
c7i.8xlarge.search	10 GiB	N/A	3 TiB
c7i.12xlarge.search	10 GiB	N/A	4.5 TiB
c7i.16xlarge.search	10 GiB	N/A	6 TiB
m7i.large.search	10 GiB	N/A	768 GiB
m7i.xlarge.search	10 GiB	N/A	2 TiB
m7i.2xlarge.search	10 GiB	N/A	3 TiB
m7i.4xlarge.search	10 GiB	N/A	6 TiB
m7i.8xlarge.search	10 GiB	N/A	12 TiB

Instance-Typ	EBS-Mindestgröße	Maximale EBS-Größe (gp2)	Maximale EBS-Größe (gp3)
m7i.12xlarge.search	10 GiB	N/A	18 TiB
m7i.16xlarge.search	10 GiB	N/A	24 TiB
r7i.large.search	10 GiB	N/A	1,5 TiB
r7i.xlarge.search	10 GiB	N/A	3 TiB
r7i.2xlarge.search	10 GiB	N/A	6 TiB
r7i.4xlarge.search	10 GiB	N/A	12 TiB
r7i.8xlarge.search	10 GiB	N/A	16 TiB
r7i.12xlarge.search	10 GiB	N/A	24 TiB
r7i.12xlarge.search	10 GiB	N/A	36 TiB

Netzwerk-Kontingente

Die folgende Tabelle zeigt die maximale Größe von HTTP-Anforderungsnutzlasten.

Instance-Typ	Maximale Größe von HTTP-Anforderungsnutzlasten
t2.micro.search	10 MiB
t2.small.search	10 MiB
t2.medium.search	10 MiB
t3.small.search	10 MiB
t3.medium.search	10 MiB
m3.medium.search	10 MiB

Instance-Typ	Maximale Größe von HTTP-Anforderungsnutzlasten
m3.large.search	10 MiB
m3.xlarge.search	100 MiB
m3.2xlarge.search	100 MiB
m4.large.search	10 MiB
m4.xlarge.search	100 MiB
m4.2xlarge.search	100 MiB
m4.4xlarge.search	100 MiB
m4.10xlarge.search	100 MiB
m5.large.search	10 MiB
m5.xlarge.search	100 MiB
m5.2xlarge.search	100 MiB
m5.4xlarge.search	100 MiB
m5.12xlarge.search	100 MiB
m6g.large.search	10 MiB
m6g.xlarge.search	100 MiB
m6g.2xlarge.search	100 MiB
m6g.4xlarge.search	100 MiB
m6g.8xlarge.search	100 MiB
m6g.12xlarge.search	100 MiB
c4.large.search	10 MiB

Instance-Typ	Maximale Größe von HTTP-Anforderungsnutzlasten
c4.xlarge.search	100 MiB
c4.2xlarge.search	100 MiB
c4.4xlarge.search	100 MiB
c4.8xlarge.search	100 MiB
c5.large.search	10 MiB
c5.xlarge.search	100 MiB
c5.2xlarge.search	100 MiB
c5.4xlarge.search	100 MiB
c5.9xlarge.search	100 MiB
c5.18xlarge.search	100 MiB
c6g.large.search	10 MiB
c6g.xlarge.search	100 MiB
c6g.2xlarge.search	100 MiB
c6g.4xlarge.search	100 MiB
c6g.8xlarge.search	100 MiB
c6g.12xlarge.search	100 MiB
r3.large.search	10 MiB
r3.xlarge.search	100 MiB
r3.2xlarge.search	100 MiB
r3.4xlarge.search	100 MiB

Instance-Typ	Maximale Größe von HTTP-Anforderungsnutzlasten
r3.8xlarge.search	100 MiB
r4.large.search	100 MiB
r4.xlarge.search	100 MiB
r4.2xlarge.search	100 MiB
r4.4xlarge.search	100 MiB
r4.8xlarge.search	100 MiB
r4.16xlarge.search	100 MiB
r5.large.search	100 MiB
r5.xlarge.search	100 MiB
r5.2xlarge.search	100 MiB
r5.4xlarge.search	100 MiB
r5.12xlarge.search	100 MiB
r6g.large.search	100 MiB
r6g.xlarge.search	100 MiB
r6g.2xlarge.search	100 MiB
r6g.4xlarge.search	100 MiB
r6g.8xlarge.search	100 MiB
r6g.12xlarge.search	100 MiB
r6gd.large.search	100 MiB
r6gd.xlarge.search	100 MiB

Instance-Typ	Maximale Größe von HTTP-Anforderungsnutzlasten
r6gd.2xlarge.search	100 MiB
r6gd.4xlarge.search	100 MiB
r6gd.8xlarge.search	100 MiB
r6gd.12xlarge.search	100 MiB
r6gd.16xlarge.search	100 MiB
i2.xlarge.search	100 MiB
i2.2xlarge.search	100 MiB
i3.large.search	100 MiB
i3.xlarge.search	100 MiB
i3.2xlarge.search	100 MiB
i3.4xlarge.search	100 MiB
i3.8xlarge.search	100 MiB
i3.16xlarge.search	100 MiB
oder 1.medium.search	10 MiB
oder 1.large.search	100 MiB
oder 1.xlarge.search	100 MiB
oder 1.2xlarge.search	100 MiB
oder 1,4xlarge.search	100 MiB
oder 1,8xlarge.search	100 MiB
oder 1.12xlarge.search	100 MiB

Instance-Typ	Maximale Größe von HTTP-Anforderungsnutzlasten
oder 1.16xlarge.search	100 MiB
oder 2.medium.search	100 MiB
oder 2.large.search	100 MiB
oder 2.xlarge.search	100 MiB
oder 2.2xlarge.search	100 MiB
oder 2,4xlarge.search	100 MiB
oder 2,8xlarge.search	100 MiB
oder 2,12xlarge.search	100 MiB
oder 2.16xlarge.search	100 MiB
om2.large.search	100 MiB
om2.xlarge.search	100 MiB
om2.2xlarge.search	100 MiB
om2.4xlarge.search	100 MiB
om2.8xlarge.search	100 MiB
om2.12xlarge.search	100 MiB
om2.16xlarge.search	100 MiB
im4gn.large.search	100 MiB
im4gn.xlarge.search	100 MiB
im4gn.2xlarge.search	100 MiB
im4gn.4xlarge.search	100 MiB

Instance-Typ	Maximale Größe von HTTP-Anforderungsnutzlasten
im4gn.8xlarge.search	100 MiB
im4gn.16xlarge.search	100 MiB
i4i.large.search	100 MiB
i4i.xlarge.search	100 MiB
i4i.2xlarge.search	100 MiB
i4i.4xlarge.search	100 MiB
i4i.8xlarge.search	100 MiB
i4i.12xlarge.search	100 MiB
i4i.16xlarge.search	100 MiB
i4i.24xlarge.search	100 MiB
i4i.32xlarge.search	100 MiB
i4g.large.search	100 MiB
i4g.xlarge.search	100 MiB
i4g.2xlarge.search	100 MiB
i4g.4xlarge.search	100 MiB
i4g.8xlarge.search	100 MiB
i4g.16xlarge.search	100 MiB
c7i.large.search	100 MiB
c7i.xlarge.search	100 MiB
c7i.2xlarge.search	100 MiB

Instance-Typ	Maximale Größe von HTTP-Anforderungsnutzlasten
c7i.4xlarge.search	100 MiB
c7i.8xlarge.search	100 MiB
c7i.12xlarge.search	100 MiB
c7i.16xlarge.search	100 MiB
m7i.large.search	100 MiB
m7i.xlarge.search	100 MiB
m7i.2xlarge.search	100 MiB
m7i.4xlarge.search	100 MiB
m7i.8xlarge.search	100 MiB
m7i.12xlarge.search	100 MiB
m7i.16xlarge.search	100 MiB
r7i.large.search	100 MiB
r7i.xlarge.search	100 MiB
r7i.2xlarge.search	100 MiB
r7i.4xlarge.search	100 MiB
r7i.8xlarge.search	100 MiB
r7i.12xlarge.search	100 MiB
r7i.16xlarge.search	100 MiB

Kontingente für die Größe von Shards

Im folgenden Abschnitt sind die maximalen Shard-Größen für verschiedene Instance-Familien aufgeführt.

Instance-Typ	Multi-AZ ohne Standby	Multi-AZ mit Standby
R5, C5, M5	N/A	65 GiB
I3	N/A	65 GiB
R6 g, C6 g, M6 g, R6 Gd	N/A	65 GiB
OR1, OR2, OM2	100 GiB	65 GiB
Im4gn	N/A	65 GiB

Um eine Erhöhung des Kontingents zu beantragen, wenden Sie sich an den AWS Support.

Anzahl der Kontingente

Im folgenden Abschnitt ist die maximale Anzahl an Shards für OpenSearch Versionen aufgeführt.

Version der Engine	Limit	Hinweise
Elasticsearch 1.5 bis 6.x	Kein Standardlimit	
Elasticsearch 7.x	1000	Das Standardlimit kann über die Einstellung cluster.max_shards_per_node geändert werden.
OpenSearch 1.x auf 2.15	1000	Das Standardlimit kann über die Einstellung cluster.max_shards_per_node geändert werden.
OpenSearch 2.17 und höher	1000 pro 16 GB Heap bis maximal 4000	Das Standardlimit kann nicht geändert werden.

Java-Prozess-Kontingente

OpenSearch Der Service begrenzt Java-Prozesse auf eine Heap-Größe von 32 GiB. Fortgeschrittene Benutzer können den Prozentanteil des Heap für Felddaten angeben. Weitere Informationen erhalten Sie unter the section called “Erweiterte Clustereinstellungen” und the section called “JVM OutOfMemoryError”.

Domain-Richtlinien-Kontingente

OpenSearch Der Service beschränkt die Zugriffsrichtlinien für Domains auf 100 KiB.

Reserved Instances in Amazon OpenSearch Service

Reserved Instances (RIs) in Amazon OpenSearch Service bieten verglichen mit Standard-On-Demand-Instances beträchtliche Rabatte. Die Instances selbst sind identisch, sie RIs sind nur ein Abrechnungsrabatt, der auf On-Demand-Instances in Ihrem Konto angewendet wird. Bei langlebigen Anwendungen mit vorhersehbarer Nutzung RIs kann dies im Laufe der Zeit zu erheblichen Einsparungen führen.

OpenSearch RIs Für den Service gelten eine Laufzeit von einem Jahr oder drei Jahren und verfügen über drei Zahlungsoptionen, die sich auf den discount auswirken:

- No Upfront - Sie leisten keine Zahlung im Voraus. Sie zahlen einen ermäßigten Stundensatz für jede Stunde während der Laufzeit.
- Partial Upfront - Sie zahlen einen Teil der Kosten im Voraus und zahlen einen ermäßigten Stundensatz für jede Stunde während der Laufzeit.
- All Upfront - Sie zahlen den gesamten Betrag im Voraus. Sie zahlen keinen Stundensatz für die Laufzeit.

Im Allgemeinen bedeutet eine größere Vorauszahlung einen größeren Rabatt. Reserved Instances können nicht storniert werden. Wenn Sie sie reservieren, verpflichten Sie sich, für die gesamte Laufzeit zu zahlen. Außerdem sind Vorauszahlungen nicht rückerstattungsfähig.

RIs sind nicht flexibel, sie gelten nur für den genauen Instance-Typ, den Sie reservieren. Eine Reservierung für acht `c5.2xlarge.search`-Instances gilt beispielsweise nicht für sechzehn `c5.xlarge.search`-Instanzen oder vier `c5.4xlarge.search`-Instanzen. Verknüpfte Konten, die Teil einer Organisation in sind, AWS Organizations können jedoch von allen ungenutzten

Rabattanträgen des Eigentümerkontos der RI profitieren, sofern die Instance-Typen, Region, Familie und Größe übereinstimmen. Weitere Informationen finden Sie unter Preise und häufig gestellte Fragen zu Amazon OpenSearch Service.

Erwerben von Reserved Instances (Konsole)

Mithilfe der Konsole können Sie Ihre vorhandenen Reserved Instances anzeigen und neue erwerben.

So erwerben Sie eine Reservierung

1. Melden Sie sich bei der https://aws.amazon.com an und wählen Sie dann Sign In to the Console (Bei der Konsole anmelden) aus.
2. Wählen Sie unter Analytics Amazon OpenSearch Service aus.
3. Wählen Sie im Navigationsbereich Reserved Instance Leases aus.

   Auf dieser Seite erhalten Sie einen Überblick über Ihre vorhandenen Reservierungen. Sie können zahlreiche vorhandene Reservierungen filtern, um eine bestimmte Reservierung leichter identifizieren und anzuzeigen zu können.

   > **Tip**
   >
   > Wenn der Link Reserved Instance Leases nicht angezeigt wird, erstellen Sie eine Domäne in der AWS-Region.

4. Wählen Sie Reserved Instances bestellen aus.
5. Geben Sie einen eindeutigen und aussagekräftigen Namen ein.
6. Wählen Sie einen Instance-Typ und die Anzahl der Instances aus. Anleitungen finden Sie unter the section called “Größenanpassung von Domains”.
7. Wählen Sie eine Laufzeit und eine Zahlungsoption aus. Überprüfen Sie die Zahlungsinformationen sorgfältig.
8. Wählen Sie Weiter aus.
9. Überprüfen Sie die Kaufübersicht sorgfältig. Erworbene Reserved Instances sind nicht erstattungsfähig.
10. Klicken Sie auf Bestellung.

Erwerben von Reserved Instances (AWS CLI)

Das AWS CLI enthält Befehle zum Ansehen von Angeboten, zum Kauf einer Reservierung und zum Anzeigen Ihrer Reservierungen. Das folgende Beispiel und das Antwortbeispiel zeigen die Angebote für eine bestimmte AWS-Region:

```
aws opensearch describe-reserved-instance-offerings --region us-east-1
{
  "ReservedInstanceOfferings": [
    {
      "FixedPrice": x,
      "ReservedInstanceOfferingId": "1a2a3a4a5-1a2a-3a4a-5a6a-1a2a3a4a5a6a",
      "RecurringCharges": [
        {
          "RecurringChargeAmount": y,
          "RecurringChargeFrequency": "Hourly"
        }
      ],
      "UsagePrice": 0.0,
      "PaymentOption": "PARTIAL_UPFRONT",
      "Duration": 31536000,
      "InstanceType": "m4.2xlarge.search",
      "CurrencyCode": "USD"
    }
  ]
}
```

Eine Beschreibung der einzelnen Rückgabewerte finden Sie in der folgenden Tabelle.

Feld	Beschreibung
`FixedPrice`	Die Vorauszahlungskosten der Reservierung.
`ReservedInstanceOfferingId`	Die Angebots-ID. Notieren Sie diesen Wert, wenn Sie das Angebot reservieren möchten.
`RecurringCharges`	Der Stundensatz für die Reservierung.
`UsagePrice`	Ein Legacy-Feld. Für OpenSearch Service ist dieser Wert immer 0.

Feld	Beschreibung
`PaymentOption`	„No Upfront“ (Keine Vorauszahlung), „Partial Upfront“ (Teilweise Vorauszahlung) oder „All Upfront“ (Komplette Vorauszahlung).
`Duration`	Laufzeitlänge in Sekunden: • 31536000 Sekunden entsprechen einem Jahr. • 94608000 Sekunden entsprechen drei Jahren.
`InstanceType`	Der Instance-Typ für die Reservierung. Informationen über die Hardware-Ressourcen, die jedem Instance-Typ zugeordnet sind, finden Sie unter Amazon OpenSearch Service — Preise.
`CurrencyCode`	Die Währung für `FixedPrice` und `RecurringChargeAmount` .

In diesem nächsten Beispiel wird eine Reservierung erworben:

```
aws opensearch purchase-reserved-instance-offering --reserved-instance-offering-
id 1a2a3a4a5-1a2a-3a4a-5a6a-1a2a3a4a5a6a --reservation-name my-reservation --instance-
count 3 --region us-east-1
{
  "ReservationName": "my-reservation",
  "ReservedInstanceId": "9a8a7a6a-5a4a-3a2a-1a0a-9a8a7a6a5a4a"
}
```

Schließlich können Sie entsprechend dem folgenden Beispiel Ihre Reservierungen für einen bestimmten Zeitraum auflisten:

```
aws opensearch describe-reserved-instances --region us-east-1
{
  "ReservedInstances": [
    {
```

```
      "FixedPrice": x,
      "ReservedInstanceOfferingId": "1a2a3a4a5-1a2a-3a4a-5a6a-1a2a3a4a5a6a",
      "ReservationName": "my-reservation",
      "PaymentOption": "PARTIAL_UPFRONT",
      "UsagePrice": 0.0,
      "ReservedInstanceId": "9a8a7a6a-5a4a-3a2a-1a0a-9a8a7a6a5a4a",
      "RecurringCharges": [
        {
          "RecurringChargeAmount": y,
          "RecurringChargeFrequency": "Hourly"
        }
      ],
      "State": "payment-pending",
      "StartTime": 1522872571.229,
      "InstanceCount": 3,
      "Duration": 31536000,
      "InstanceType": "m4.2xlarge.search",
      "CurrencyCode": "USD"
    }
  ]
}
```

> **Note**
>
> `StartTime` ist die Zeit seit Unix-Epoche. Dies ist die Anzahl der Sekunden, die seit Mitternacht UTC am 1. Januar 1970 verstrichen sind. Beispielsweise entspricht 1522872571 in der Zeit seit Unix-Epoche 20:09:31 UTC am 4. April 2018. Sie können Online-Konverter verwenden.

Weitere Informationen über die in den vorherigen Beispielen verwendeten Befehle finden Sie in der AWS CLI -Befehlsreferenz.

Erwerben von Reserved Instances (AWS SDKs)

Die AWS SDKs (außer Android und iOS SDKs) unterstützen alle Operationen, die in der API-Referenz für Amazon OpenSearch Service definiert sind, einschließlich der folgenden:

- `DescribeReservedInstanceOfferings`
- `PurchaseReservedInstanceOffering`
- `DescribeReservedInstances`

Dieses Beispielskript verwendet den OpenSearchServiceLow-Level-Python-Client von AWS SDK für Python (Boto3) , um reservierte Instances zu kaufen. Sie müssen einen Wert für `instance_type` angeben.

```
import boto3
from botocore.config import Config

# Build the client using the default credential configuration.
# You can use the CLI and run 'aws configure' to set access key, secret
# key, and default region.

my_config = Config(
    # Optionally lets you specify a region other than your default.
    region_name='us-east-1'
)

client = boto3.client('opensearch', config=my_config)

instance_type = '' # e.g. m4.2xlarge.search


def describe_RI_offerings(client):
    """Gets the Reserved Instance offerings for this account"""

    response = client.describe_reserved_instance_offerings()
    offerings = (response['ReservedInstanceOfferings'])
    return offerings


def check_instance(offering):
    """Returns True if instance type is the one you specified above"""

    if offering['InstanceType'] == instance_type:
        return True

    return False


def get_instance_id():
    """Iterates through the available offerings to find the ID of the one you
 specified"""

    instance_type_iterator = filter(
```

```
        check_instance, describe_RI_offerings(client))
    offering = list(instance_type_iterator)
    id = offering[0]['ReservedInstanceOfferingId']
    return id


def purchase_RI_offering(client):
    """Purchase Reserved Instances"""

    response = client.purchase_reserved_instance_offering(
        ReservedInstanceOfferingId = get_instance_id(),
        ReservationName = 'my-reservation',
        InstanceCount = 1
    )
    print('Purchased reserved instance offering of type ' + instance_type)
    print(response)


def main():
    """Purchase Reserved Instances"""
    purchase_RI_offering(client)
```

Weitere Informationen über die Installation und Verwendung von finden Sie unter AWS -Software-Entwicklungs-Kits. AWS SDKs

Untersuchen der Kosten

Cost Explorer ist ein kostenloses Tool, mit dem Sie Daten zu Ihren Ausgaben für die letzten 13 Monate anzeigen können. Durch die Analyse dieser Daten können Sie Trends erkennen und herausfinden, ob sie RIs für Ihren Anwendungsfall geeignet sind. Falls Sie dies bereits getan haben RIs, können Sie nach Kaufoption gruppieren und die amortisierten Kosten anzeigen, um diese Ausgaben mit Ihren Ausgaben für On-Demand-Instances zu vergleichen. Sie können auch Nutzungsbudgets festlegen, um sicherzustellen, dass Sie alle Vorteile Ihrer Reservierungen nutzen. Weitere Informationen finden Sie unter Analysieren von Kosten mit Cost Explorer im AWS Billing - Benutzerhandbuch.

Andere unterstützte Ressourcen in Amazon OpenSearch Service

In diesem Thema werden zusätzliche Ressourcen beschrieben, die Amazon OpenSearch Service unterstützt.

bootstrap.memory_lock

OpenSearch Service aktiviert `bootstrap.memory_lock` in`opensearch.yml`, wodurch der JVM-Speicher gesperrt wird und verhindert wird, dass das Betriebssystem ihn auf die Festplatte auslagert. Dies gilt für alle unterstützten Instance-Typen außer den Folgenden:

- `t2.micro.search`
- `t2.small.search`
- `t2.medium.search`
- `t3.small.search`
- `t3.medium.search`

Scripting-Modul

OpenSearch Der Service unterstützt Scripting für Elasticsearch 5. Domänen x und höher. Er unterstützt kein Scripting für 1.5 oder 2.3.

Unterstützte Scripting-Optionen umfassen die Folgenden:

- Painless
- Lucene Expressions
- Mustache

Für Elasticsearch-Domains ab Version 5.5 und alle OpenSearch Domains unterstützt OpenSearch Service gespeicherte Skripts, die den `_scripts` Endpunkt verwenden. Elasticsearch 5.3- und 5.1-Domains unterstützen nur Inline-Skripts.

TLS-Transport

OpenSearch Der Service unterstützt HTTP auf Port 80 und HTTPS auf Port 443, unterstützt jedoch keinen TLS-Transport.

Amazon OpenSearch Service-Anleitungen

Dieses Kapitel enthält mehrere start-to-finish Tutorials für die Arbeit mit Amazon OpenSearch Service, darunter die Migration zum Service, die Erstellung einer einfachen Suchanwendung und die Erstellung einer Visualisierung in OpenSearch Dashboards.

Themen

- Tutorial: Erstellen und Suchen von Dokumenten in Amazon OpenSearch Service
- Tutorial: Migration zu Amazon Service OpenSearch
- Tutorial: Eine Suchanwendung mit Amazon OpenSearch Service erstellen
- Tutorial: Visualisierung von Kunden-Support-Aufrufen mit OpenSearch Service und Dashboards OpenSearch

Tutorial: Erstellen und Suchen von Dokumenten in Amazon OpenSearch Service

In diesem Tutorial erfahren Sie, wie Sie ein Dokument in Amazon OpenSearch Service erstellen und suchen. Sie fügen Daten zu einem Index im Formular eines JSON-Dokuments hinzu. OpenSearch Service erstellt einen Index anhand des ersten von Ihnen hinzugefügten Dokuments.

In diesem Tutorial wird erläutert, wie Sie HTTP-Anforderungen zum Erstellen von Dokumenten stellen, automatisch eine ID für ein Dokument generieren und grundlegende und erweiterte Suchvorgänge für Ihre Dokumente durchführen.

> **Note**
>
> Dieses Tutorial verwendet eine Domain mit offenem Zugriff. Für ein Höchstmaß an Sicherheit empfehlen wir, Ihre Domain in eine Virtual Private Cloud (VPC) zu legen.

Voraussetzungen

Für dieses Tutorial müssen die folgenden Voraussetzungen erfüllt sein:

- Sie benötigen ein AWS-Konto.

- Sie müssen über eine aktive OpenSearch Service-Domain verfügen.

Hinzufügen eines Dokuments zu einem Index

Um ein Dokument zu einem Index hinzuzufügen, können Sie ein beliebiges HTTP-Tool verwenden, z. B. Postman, cURL oder die OpenSearch Dashboards-Konsole. In diesen Beispielen wird davon ausgegangen, dass Sie die Entwicklerkonsole in OpenSearch Dashboards verwenden. Wenn Sie ein anderes Tool verwenden, passen Sie es entsprechend an, indem Sie bei Bedarf die vollständige URL und Anmeldeinformationen angeben.

Fügen Sie ein Dokument wie folgt einem Index hinzu

1. Navigieren Sie zur OpenSearch Dashboards-URL für Ihre Domäne. Sie finden die URL auf dem Dashboard der Domain in der OpenSearch Service-Konsole. Die URL weist das folgende Format auf:

   ```
   domain-endpoint/_dashboards/
   ```

2. Melden Sie sich mit Ihrem Hauptbenutzernamen und -passwort an.
3. Öffnen Sie den linken Navigationsbereich und wählen Sie Dev Tools (Entwickler-Tools) aus.
4. Das HTTP-Verb zum Erstellen einer neuen Ressource ist PUT, das Sie zum Erstellen eines neuen Dokuments und Indexes verwenden. Geben Sie in der Konsole den folgenden Befehl ein:

   ```
   PUT fruit/_doc/1
   {
     "name":"strawberry",
     "color":"red"
   }
   ```

   Die PUT-Anforderung erstellt einen Index namens fruit und erstellt ein einzelnes Dokument gemäß des Indexes mit der ID 1. Sie erzeugt folgende Antwort:

   ```
   {
     "_index" : "fruit",
     "_type" : "_doc",
     "_id" : "1",
     "_version" : 1,
     "result" : "created",
     "_shards" : {
   ```

```
    "total" : 2,
    "successful" : 2,
    "failed" : 0
  },
  "_seq_no" : 0,
  "_primary_term" : 1
}
```

Erstellen automatisch generierter IDs

OpenSearch Service kann automatisch eine ID für Ihre Dokumente generieren. Der zu generierende Befehl IDs verwendet eine POST-Anforderung anstelle einer PUT-Anforderung und erfordert keine Dokument-ID (im Vergleich zur vorherigen Anforderung).

Geben Sie die folgende Anforderung in der Entwicklerkonsole ein:

```
POST veggies/_doc
{
  "name":"beet",
  "color":"red",
  "classification":"root"
}
```

Diese Anfrage erstellt einen Index mit dem Namen veggies und fügt das Dokument dem Index hinzu. Sie erzeugt folgende Antwort:

```
{
  "_index" : "veggies",
  "_type" : "_doc",
  "_id" : "3WgyS4IB5DLqbRIvLxtF",
  "_version" : 1,
  "result" : "created",
  "_shards" : {
    "total" : 2,
    "successful" : 2,
    "failed" : 0
  },
  "_seq_no" : 0,
  "_primary_term" : 1
}
```

Beachten Sie das zusätzliche `_id` Feld in der Antwort, das anzeigt, dass automatisch eine ID erstellt wurde.

> **Note**
>
> Nach `_doc` geben Sie nichts mehr in der URL an, wo normalerweise die ID steht. Da Sie ein Dokument mit einer generierten ID erstellen, geben Sie noch keine an. Diese ist für Updates reserviert.

Aktualisieren eines Dokuments mit einem POST-Befehl

Um ein Dokument zu aktualisieren, verwenden Sie einen HTTP-`POST`-Befehl mit der ID-Nummer.

Erstellen Sie zunächst ein Dokument mit der ID `42`:

```
POST fruits/_doc/42
{
  "name":"banana",
  "color":"yellow"
}
```

Verwenden Sie dann diese ID, um das Dokument zu aktualisieren:

```
POST fruits/_doc/42
{
  "name":"banana",
  "color":"yellow",
  "classification":"berries"
}
```

Dieser Befehl aktualisiert das Dokument mit dem neuen Feld `classification`. Sie erzeugt folgende Antwort:

```
{
  "_index" : "fruits",
  "_type" : "_doc",
  "_id" : "42",
  "_version" : 2,
  "result" : "updated",
```

```
  "_shards" : {
    "total" : 2,
    "successful" : 2,
    "failed" : 0
  },
  "_seq_no" : 1,
  "_primary_term" : 1
}
```

> **Note**
>
> Wenn Sie versuchen, ein Dokument zu aktualisieren, das nicht existiert, erstellt OpenSearch Service das Dokument.

Ausführen von Massenaktionen

Sie können die API-Operation `POST _bulk` zum Ausführen mehrerer Aktionen für einen oder mehrere Indizes in einer Anforderung verwenden. Befehle für Massenaktionen haben folgendes Format:

```
POST /_bulk
<action_meta>\n
<action_data>\n
<action_meta>\n
<action_data>\n
```

Jede Aktion erfordert zwei JSON-Zeilen. Zuerst geben Sie die Beschreibung der Aktion oder Metadaten an. In der nächsten Zeile geben Sie die Daten ein. Jeder Teil wird durch einen Zeilenumbruch (\n) getrennt. Eine Aktionsbeschreibung für eine Einfügung kann wie folgt aussehen:

```
{ "create" : { "_index" : "veggies", "_type" : "_doc", "_id" : "7" } }
```

Und die nächste Zeile mit den Daten könnte folgendermaßen aussehen:

```
{ "name":"kale", "color":"green", "classification":"leafy-green" }
```

Zusammengenommen stellen die Metadaten und die Daten eine einzelne Aktion in einem Massenvorgang dar. Sie können wie folgt viele Operationen in einer Anfrage ausführen:

```
POST /_bulk
{ "create" : { "_index" : "veggies", "_id" : "35" } }
{ "name":"kale", "color":"green", "classification":"leafy-green" }
{ "create" : { "_index" : "veggies", "_id" : "36" } }
{ "name":"spinach", "color":"green", "classification":"leafy-green" }
{ "create" : { "_index" : "veggies", "_id" : "37" } }
{ "name":"arugula", "color":"green", "classification":"leafy-green" }
{ "create" : { "_index" : "veggies", "_id" : "38" } }
{ "name":"endive", "color":"green", "classification":"leafy-green" }
{ "create" : { "_index" : "veggies", "_id" : "39" } }
{ "name":"lettuce", "color":"green", "classification":"leafy-green" }
{ "delete" : { "_index" : "vegetables", "_id" : "1" } }
```

Beachten Sie, dass die letzte Aktion vom Typ `delete` ist. Es gibt keine Daten nach der `delete`-Aktion.

Suchen nach Dokumenten

Jetzt, da Daten in Ihrem Cluster vorhanden sind, können Sie danach suchen. Sie können beispielsweise nach allen Wurzelgemüsen suchen oder eine Anzahl aller Blattgemüse ermitteln oder die Anzahl der pro Stunde protokollierten Fehler ermitteln.

Einfache Suchen

Eine einfache Suche sieht etwa folgendermaßen aus:

```
GET veggies/_search?q=name:l*
```

Die Anfrage erzeugt eine JSON-Antwort, die das Dokument zu Salaten enthält.

Erweiterte Suchen

Sie können erweiterte Suchvorgänge durchführen, indem Sie die Abfrageoptionen als JSON im Anfragetext angeben:

```
GET veggies/_search
{
  "query": {
    "term": {
      "name": "lettuce"
```

```
    }
  }
}
```

Dieses Beispiel erzeugt auch eine JSON-Antwort mit dem Dokument zu Salaten.

Sortieren

Sie können mehrere dieser Art von Abfragen mithilfe der Sortierung ausführen. Zuerst müssen Sie den Index neu erstellen, da bei der automatischen Feldzuordnung Typen ausgewählt wurden, die standardmäßig nicht sortiert werden können. Senden Sie die folgenden Anfragen, um den Index zu löschen und neu zu erstellen:

```
DELETE /veggies

PUT /veggies
{
   "mappings":{
      "properties":{
         "name":{
            "type":"keyword"
         },
         "color":{
            "type":"keyword"
         },
         "classification":{
            "type":"keyword"
         }
      }
   }
}
```

Füllen Sie dann den Index erneut mit Daten:

```
POST /_bulk
{ "create" : { "_index" : "veggies", "_id" : "7"  } }
{ "name":"kale", "color":"green", "classification":"leafy-green" }
{ "create" : { "_index" : "veggies", "_id" : "8" } }
{ "name":"spinach", "color":"green", "classification":"leafy-green" }
{ "create" : { "_index" : "veggies", "_id" : "9" } }
{ "name":"arugula", "color":"green", "classification":"leafy-green" }
{ "create" : { "_index" : "veggies", "_id" : "10" } }
```

```
{ "name":"endive", "color":"green", "classification":"leafy-green" }
{ "create" : { "_index" : "veggies", "_id" : "11" } }
{ "name":"lettuce", "color":"green", "classification":"leafy-green" }
```

Jetzt können Sie mit einer Sortierung suchen. Diese Anforderung fügt eine aufsteigende Sortierung nach der Klassifizierung hinzu:

```
GET veggies/_search
{
  "query" : {
    "term": { "color": "green" }
  },
  "sort" : [
      "classification"
  ]
}
```

Zugehörige Ressourcen

Weitere Informationen finden Sie in den folgenden Ressourcen:

- Erste Schritte
- Indizierung von Daten
- Suchen von Daten

Tutorial: Migration zu Amazon Service OpenSearch

Index-Snapshots sind eine beliebte Methode, um von einem selbstverwalteten OpenSearch oder älteren Elasticsearch-Cluster zu Amazon Service zu migrieren. OpenSearch Im Großen und Ganzen besteht der Prozess aus den folgenden Schritten:

1. Erstellen Sie einen Snapshot des vorhandenen Clusters, und laden Sie den Snapshot in einen Amazon S3-Bucket hoch.
2. Erstellen Sie eine Service-Domain OpenSearch .
3. Erteilen Sie dem OpenSearch Service Berechtigungen für den Zugriff auf den Bucket und stellen Sie sicher, dass Sie über die erforderlichen Berechtigungen für die Arbeit mit Snapshots verfügen.
4. Stellen Sie den Snapshot in der OpenSearch Service-Domain wieder her.

Dieser Walkthrough enthält detailliertere Schritte und gegebenenfalls alternative Optionen.

Snapshot erstellen und hochladen

Sie können zwar das Repository-S3-Plugin verwenden, um Snapshots direkt in S3 zu erstellen, aber Sie müssen das Plugin auf jedem Knoten installieren, Anpassungen vornehmen `opensearch.yml` (oder, `elasticsearch.yml` falls Sie einen Elasticsearch-Cluster verwenden), jeden Knoten neu starten, Ihre AWS Anmeldeinformationen hinzufügen und schließlich den Snapshot erstellen. Das Plugin ist eine großartige Option für den laufenden Einsatz oder für die Migration größerer Cluster.

Bei kleineren Clustern besteht ein einmaliger Ansatz darin, einen gemeinsamen Dateisystem-Snapshot zu erstellen und ihn dann zu verwenden, um ihn auf S3 hochzuladen. AWS CLI Wenn Sie bereits einen Snapshot haben, fahren Sie mit Schritt 4 fort.

So erstellen Sie einen Snapshot und laden ihn auf Amazon S3 hoch

1. Fügen Sie die `path.repo`-Einstellung zu `opensearch.yml` (oder `Elasticsearch.yml`) auf allen Knoten hinzu, und starten Sie dann jeden Knoten neu.

   ```
   path.repo: ["/my/shared/directory/snapshots"]
   ```

2. Sie müssen ein Snapshot-Repository registrieren, bevor Sie einen Schnappschuss erstellen können. Ein Repository ist nur ein Speicherort: ein freigegebenes Dateisystem, Amazon S3, Hadoop Distributed File System (HDFS) usw. In diesem Fall verwenden wir ein freigegebenes Dateisystem („fs“):

   ```
   PUT _snapshot/my-snapshot-repo-name
   {
     "type": "fs",
     "settings": {
       "location": "/my/shared/directory/snapshots"
     }
   }
   ```

3. Erstellen Sie den Snapshot:

   ```
   PUT _snapshot/my-snapshot-repo-name/my-snapshot-name
   {
     "indices": "migration-index1,migration-index2,other-indices-*",
     "include_global_state": false
   }
   ```

4. Installieren Sie die AWS CLI, und führen Sie `aws configure` aus, um Ihre Anmeldeinformationen hinzuzufügen.
5. Navigieren Sie zum Snapshot-Verzeichnis. Führen Sie dann die folgenden Befehle aus, um einen neuen S3-Bucket zu erstellen, und laden Sie den Inhalt des Snapshot-Verzeichnisses in diesen Bucket hoch:

   ```
   aws s3 mb s3://amzn-s3-demo-bucket --region us-west-2
   aws s3 sync . s3://amzn-s3-demo-bucket --sse AES256
   ```

   Abhängig von der Größe des Snapshots und der Geschwindigkeit Ihrer Internetverbindung kann dieser Vorgang eine Weile dauern.

Domain erstellen

Die Konsole ist zwar der einfachste Weg, eine Domain zu erstellen, aber in diesem Fall haben Sie das Terminal bereits geöffnet und AWS CLI installiert. Ändern Sie den folgenden Befehl, um eine Domain zu erstellen, die Ihren Anforderungen entspricht:

```
aws opensearch create-domain \
  --domain-name migration-domain \
  --engine-version OpenSearch_1.0 \
  --cluster-config InstanceType=c5.large.search,InstanceCount=2 \
  --ebs-options EBSEnabled=true,VolumeType=gp2,VolumeSize=100 \
  --node-to-node-encryption-options Enabled=true \
  --encryption-at-rest-options Enabled=true \
  --domain-endpoint-options EnforceHTTPS=true,TLSSecurityPolicy=Policy-Min-
TLS-1-2-2019-07 \
  --advanced-security-options
 Enabled=true,InternalUserDatabaseEnabled=true,MasterUserOptions='{MasterUserName=master-
user,MasterUserPassword=master-user-password}' \
  --access-policies '{"Version":"2012-10-17","Statement":
[{"Effect":"Allow","Principal":{"AWS":["*"]},"Action":
["es:ESHttp*"],"Resource":"arn:aws:es:us-west-2:123456789012:domain/migration-domain/
*"}]}' \
  --region us-west-2
```

Mit dem Befehl wird eine für das Internet zugängliche Domain mit zwei Datenknoten erstellt, die jeweils 100 GiB Speicher aufweisen. Er ermöglicht auch eine differenzierte Zugriffskontrolle mit HTTP-Standardauthentifizierung und allen Verschlüsselungseinstellungen. Verwenden Sie die

OpenSearch Servicekonsole, wenn Sie eine erweiterte Sicherheitskonfiguration benötigen, z. B. eine VPC.

Bevor Sie den Befehl ausführen, ändern Sie den Domain-Namen, die Anmeldeinformationen des Master-Benutzers und die Kontonummer. Geben Sie dieselbe Version an AWS-Region , die Sie für den S3-Bucket verwendet haben, und eine OpenSearch/Elasticsearch Version, die mit Ihrem Snapshot kompatibel ist.

> **Important**
>
> Snapshots sind nur vorwärtskompatibel und auch nur mit einer Hauptversion. Sie können beispielsweise keinen Snapshot aus einem Snapshot OpenSearch wiederherstellen. x-Cluster auf einem Elasticsearch 7. x Cluster, nur ein OpenSearch 1. x oder 2. x-Cluster. Kleinere Versionen sind ebenfalls von Bedeutung. Sie können keinen Snapshot aus einem selbstverwalteten 5.3.3-Cluster auf einer OpenSearch 5.3.2-Servicedomäne wiederherstellen. Wir empfehlen, die neueste Version von OpenSearch oder Elasticsearch zu wählen, die Ihr Snapshot unterstützt. Eine Tabelle mit kompatiblen Versionen finden Sie unter the section called “Verwenden eines Snapshots zum Migrieren von Daten”.

Erteilen Sie Berechtigungen für den Zugriff auf den S3-Bucket

Erstellen Sie in der AWS Identity and Access Management (IAM-) Konsole eine Rolle mit den folgenden Berechtigungen und der folgenden Vertrauensbeziehung. Wählen Sie beim Erstellen der Rolle S3 als AWS -Service aus. Nennen Sie die Rolle `OpenSearchSnapshotRole`, damit sie leicht zu finden ist.

Berechtigungen

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
      "Action": [
        "s3:ListBucket"
      ],
      "Effect": "Allow",
      "Resource": [
```

```
        "arn:aws:s3:::amzn-s3-demo-bucket"
      ]
    },
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ]
    }
  ]
}
```

Vertrauensstellung

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
      "Effect": "Allow",
      "Principal": {
        "Service": "es.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Geben Sie dann Ihrer persönlichen IAM-Rolle die Berechtigungen, `OpenSearchSnapshotRole` zu übernehmen. Erstellen Sie die folgende Richtlinie und fügen Sie sie Ihrer Identität hinzu:

Berechtigungen

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::123456789012:role/OpenSearchSnapshotRole"
    }
  ]
}
```

Ordnen Sie die Snapshot-Rolle in OpenSearch Dashboards zu (wenn Sie eine differenzierte Zugriffskontrolle verwenden)

Wenn Sie distanzierte Zugriffskontrolle aktiviert haben, selbst wenn Sie HTTP-Basisauthentifizierung für alle anderen Zwecke verwenden, müssen Sie die`manage_snapshots`-Rolle zu Ihrer IAM-Rolle verwenden, damit Sie mit Snapshots arbeiten können.

Um Ihrer Identität Berechtigungen für die Arbeit mit Snapshots zu erteilen

1. Melden Sie sich mit den Masterbenutzeranmeldedaten, die Sie bei der Erstellung der Service-Domain angegeben haben, bei Dashboards an. OpenSearch Sie finden die Dashboard-URL in der OpenSearch Servicekonsole. Er hat die Form `https://`*domain-endpoint*`/_dashboards/`.
2. Wählen Sie im Hauptmenü Sicherheit, Rollen, und wählen Sie die Rolle manage_snapshots.
3. Wählen Sie Zugeordnete Benutzer, Mapping verwalten.
4. Fügen Sie den Domain-ARN Ihrer persönlichen IAM-Rolle in das entsprechende Feld ein. Der ARN nimmt eines der folgenden Formate an:

   ```
   arn:aws:iam::123456789123:user/user-name
   ```

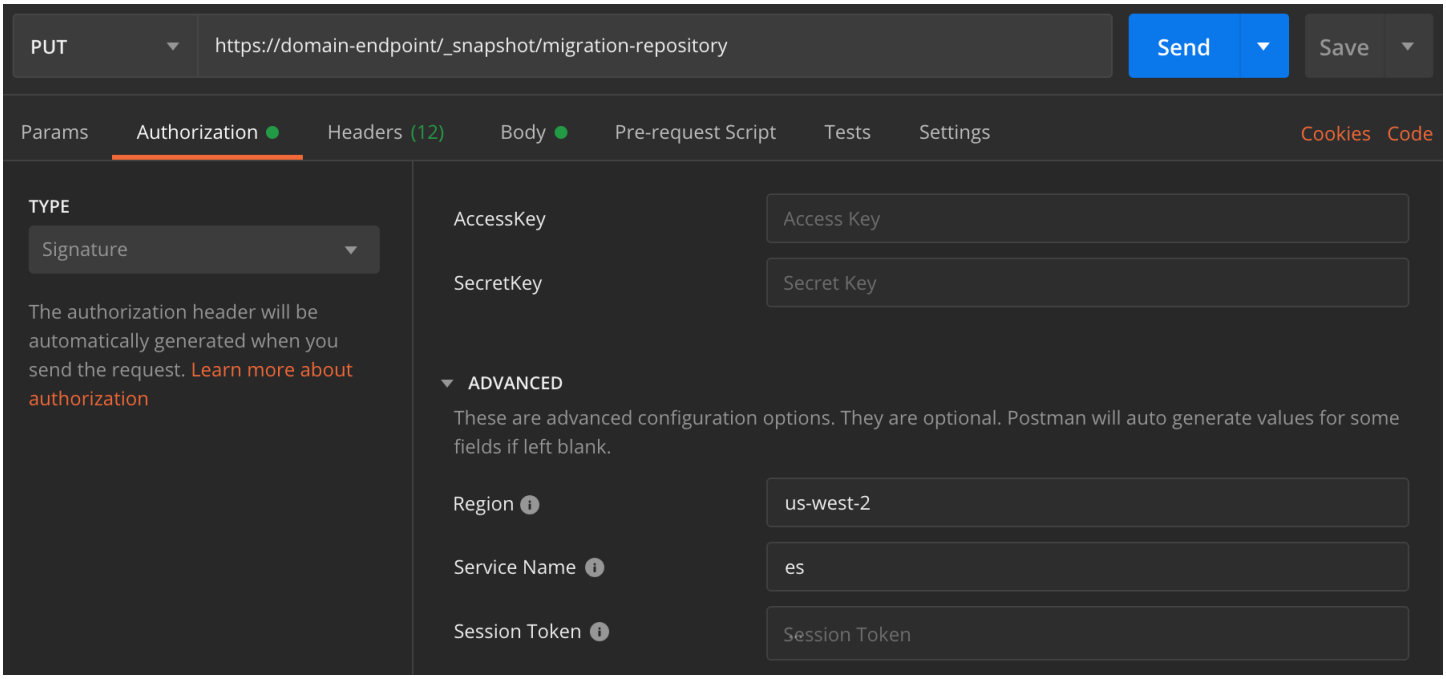
   ```
   arn:aws:iam::123456789123:role/role-name
   ```

5. Wählen Sie Map (Zuordnen) aus und bestätigen Sie, dass die Rolle unter Mapped users (Zugeordnete Benutzer) angezeigt wird.

Stellen Sie den Snapshot wieder her

Derzeit haben Sie zwei Möglichkeiten, auf Ihre OpenSearch Service-Domain zuzugreifen: HTTP-Basisauthentifizierung mit Ihren Master-Benutzeranmeldedaten oder AWS Authentifizierung mit Ihren IAM-Anmeldeinformationen. Da Snapshots Amazon S3 verwenden, das kein Konzept für den Master-Benutzer hat, müssen Sie Ihre IAM-Anmeldeinformationen verwenden, um das Snapshot-Repository in Ihrer OpenSearch Service-Domain zu registrieren.

Die meisten Programmiersprachen verfügen über Bibliotheken, die Sie beim Signieren von Anfragen unterstützen. Der einfachere Ansatz besteht jedoch darin, ein Tool wie Postman zu verwenden und Ihre IAM-Anmeldeinformationen im Abschnitt Autorisierung einzugeben.



So stellen Sie den Snapshot wieder her

1. Unabhängig davon, wie Sie Ihre Anfragen signieren, besteht der erste Schritt darin, das Repository zu registrieren:

```
PUT _snapshot/my-snapshot-repo-name
{
  "type": "s3",
  "settings": {
    "bucket": "amzn-s3-demo-bucket",
    "region": "us-west-2",
    "role_arn": "arn:aws:iam::123456789012:role/OpenSearchSnapshotRole"
  }
```

```
}
```

2. Führen Sie dann die Snapshots im Repository auf, und suchen Sie die Snapshots, die Sie wiederherstellen möchten. An diesem Punkt können Sie Postman weiter verwenden oder zu einem Werkzeug wie curl wechseln.

   Kurzschrift

   ```
   GET _snapshot/my-snapshot-repo-name/_all
   ```

   curl

   ```
   curl -XGET -u 'master-user:master-user-password' https://domain-endpoint/
   _snapshot/my-snapshot-repo-name/_all
   ```

3. Stellen Sie den Snapshot wieder her.

   Kurzschrift

   ```
   POST _snapshot/my-snapshot-repo-name/my-snapshot-name/_restore
   {
     "indices": "migration-index1,migration-index2,other-indices-*",
     "include_global_state": false
   }
   ```

   curl

   ```
   curl -XPOST -u 'master-user:master-user-password' https://domain-endpoint/
   _snapshot/my-snapshot-repo-name/my-snapshot-name/_restore \
     -H 'Content-Type: application/json' \
     -d '{"indices":"migration-index1,migration-index2,other-indices-
   *","include_global_state":false}'
   ```

4. Überprüfen Sie abschließend, ob Ihre Indizes wie erwartet wiederhergestellt wurden.

   Kurzschrift

   ```
   GET _cat/indices?v
   ```

   curl

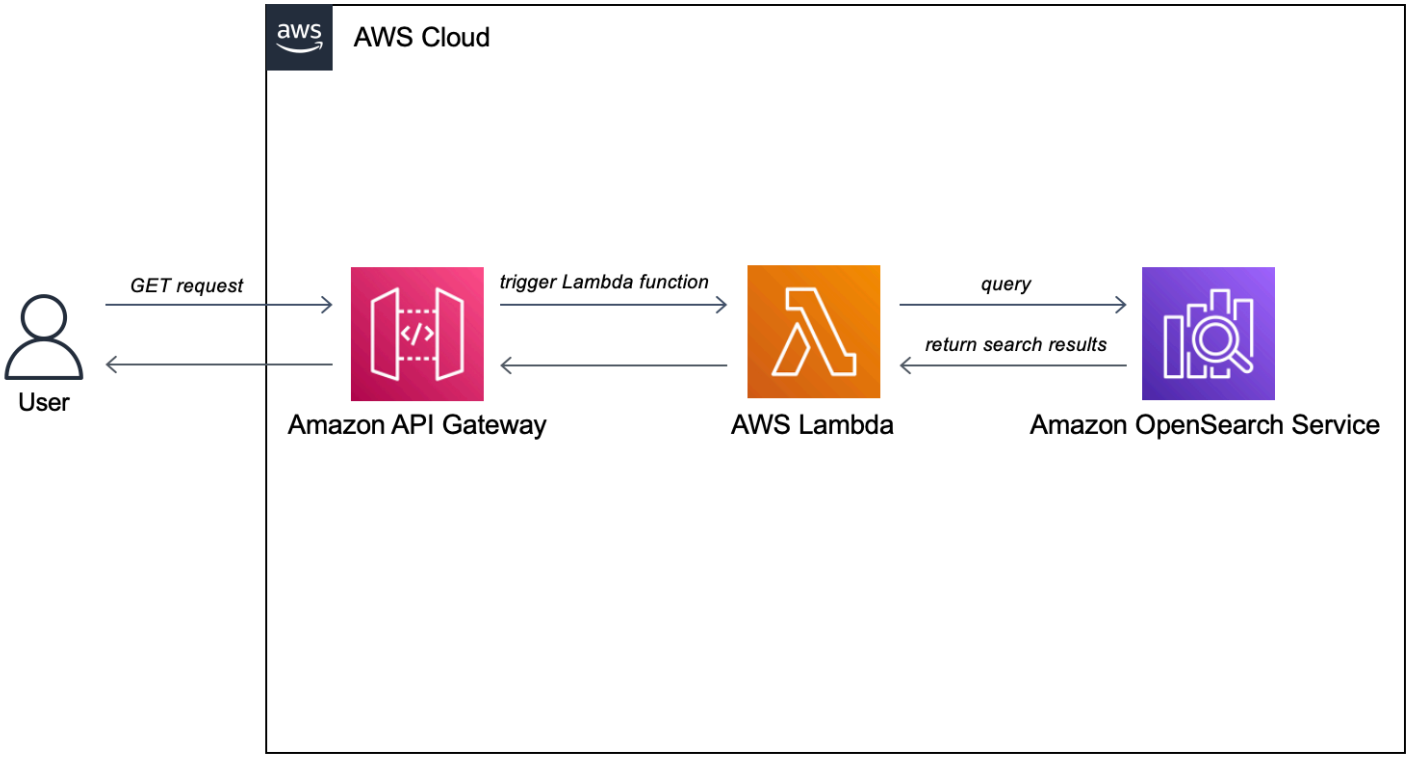
```
curl -XGET -u 'master-user:master-user-password' https://domain-endpoint/_cat/
indices?v
```

Zu diesem Zeitpunkt ist die Migration abgeschlossen. Sie können Ihre Clients so konfigurieren, dass sie den neuen OpenSearch Service-Endpunkt verwenden, die Größe der Domain an Ihre Arbeitslast anpassen, die Anzahl der Shards für Ihre Indizes überprüfen, zu einem IAM-Masterbenutzer wechseln oder mit der Erstellung von Visualisierungen in Dashboards beginnen. OpenSearch

Tutorial: Eine Suchanwendung mit Amazon OpenSearch Service erstellen

Eine gängige Methode, um eine Suchanwendung mit Amazon OpenSearch Service zu erstellen, besteht darin, Webformulare zu verwenden, um Benutzeranfragen an einen Server zu senden. Anschließend können Sie den Server autorisieren, den OpenSearch APIs direkt aufzurufen und den Server Anfragen an den OpenSearch Service senden zu lassen. Wenn Sie clientseitigen Code schreiben möchten, der nicht auf einen Server angewiesen ist, sollten Sie jedoch die Sicherheits- und Leistungsrisiken ausgleichen. OpenSearch APIs Es wird davon abgeraten, unsignierten, öffentlichen Zugriff auf den zuzulassen. Die Benutzer können auf ungesicherte Endpunkte zugreifen oder die Cluster-Leistung durch übermäßig umfangreiche Abfragen (oder zu viele Abfragen) beeinflussen.

In diesem Kapitel wird eine Lösung vorgestellt: Verwenden Sie Amazon API Gateway, um Benutzer auf eine Teilmenge von zu beschränken OpenSearch APIs und Anfragen von API Gateway AWS Lambda to OpenSearch Service zu signieren.



> **Note**
>
> Es gilt die standardmäßige API-Gateway- und Lamda-Preisgestaltung, aber innerhalb der begrenzten Nutzung dieses Tutorials sollten die Kosten vernachlässigbar sein.

Voraussetzungen

Voraussetzung für dieses Tutorial ist eine OpenSearch Service-Domain. Wenn Sie noch keine haben, folgen Sie den Schritten unter Erstellen einer OpenSearch Dienstdomäne, um eine zu erstellen.

Schritt 1: Indizieren von Beispieldaten

Laden Sie sample-movies.zip herunter, dekomprimieren Sie sie und verwenden Sie die _bulk-API-Operation zum Hinzufügen der 5 000 Dokumente in den `movies`-Index:

```
POST https://search-my-domain.us-west-1.es.amazonaws.com/_bulk
{ "index": { "_index": "movies", "_id": "tt1979320" } }
{"directors":["Ron
 Howard"],"release_date":"2013-09-02T00:00:00Z","rating":8.3,"genres":
```

```
["Action","Biography","Drama","Sport"],"image_url":"http://ia.media-imdb.com/images/
M/MV5BMTQyMDE0MTY0OV5BMl5BanBnXkFtZTcwMjI2OTI0OQ@@._V1_SX400_.jpg","plot":"A re-
creation of the merciless 1970s rivalry between Formula One rivals James Hunt and
 Niki Lauda.","title":"Rush","rank":2,"running_time_secs":7380,"actors":["Daniel
 Brühl","Chris Hemsworth","Olivia Wilde"],"year":2013,"id":"tt1979320","type":"add"}
{ "index": { "_index": "movies", "_id": "tt1951264" } }
{"directors":["Francis Lawrence"],"release_date":"2013-11-11T00:00:00Z","genres":
["Action","Adventure","Sci-Fi","Thriller"],"image_url":"http://ia.media-imdb.com/
images/M/
MV5BMTAyMjQ3OTAxMzNeQTJeQWpwZ15BbWU4MDU0NzA1MzAx._V1_SX400_.jpg","plot":"Katniss
 Everdeen and Peeta Mellark become targets of the Capitol after
 their victory in the 74th Hunger Games sparks a rebellion in
 the Districts of Panem.","title":"The Hunger Games: Catching
 Fire","rank":4,"running_time_secs":8760,"actors":["Jennifer Lawrence","Josh
 Hutcherson","Liam Hemsworth"],"year":2013,"id":"tt1951264","type":"add"}
...
```

Beachten Sie, dass es sich bei dem obigen Befehl um einen Beispielbefehl mit einer kleinen Teilmenge der verfügbaren Daten handelt. Um den `_bulk` Vorgang auszuführen, müssen Sie den gesamten Inhalt der `sample-movies` Datei kopieren und einfügen. Weitere Anweisungen finden Sie unterthe section called “Option 2: Hochladen mehrerer Dokumente”.

Sie können auch den folgenden curl-Befehl verwenden, um dasselbe Ergebnis zu erzielen:

```
curl -XPOST -u 'master-user:master-user-password' 'domain-endpoint/_bulk' --data-binary
 @bulk_movies.json -H 'Content-Type: application/json'
```

Schritt 2: Lambda-Funktion erstellen und bereitstellen

Bevor Sie Ihre API in API Gateway erstellen, erstellen Sie die Lambda-Funktion, an die Anfragen weitergeleitet werden.

So erstellen Sie die Lambda-Funktion:

In dieser Lösung leitet API Gateway Anfragen an eine Lambda-Funktion weiter, die OpenSearch Service abfragt und Ergebnisse zurückgibt. Da diese Beispielfunktion externe Bibliotheken verwendet, müssen Sie ein Bereitstellungspaket erstellen und es auf Lambda hochladen.

Erstellen des Bereitstellungspakets

1. Öffnen Sie eine Eingabeaufforderung und erstellen Sie ein `my-opensearch-function`-Projektverzeichnis. Zum Beispiel unter macOS:

```
mkdir my-opensearch-function
```

2. Navigieren Sie zum `my-sourcecode-function`-Projektverzeichnis.

```
cd my-opensearch-function
```

3. Kopieren Sie den Inhalt des folgenden Python-Beispielcodes und speichern Sie ihn in einer neuen Datei mit dem Namen`opensearch-lambda.py`. Fügen Sie der Datei Ihre Region und Ihren Host-Endpunkt hinzu.

```
import boto3
import json
import requests
from requests_aws4auth import AWS4Auth

region = '' # For example, us-west-1
service = 'es'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
 session_token=credentials.token)

host = '' # The OpenSearch domain endpoint with https:// and without a trailing
 slash
index = 'movies'
url = host + '/' + index + '/_search'

# Lambda execution starts here
def lambda_handler(event, context):

    # Put the user query into the query DSL for more accurate search results.
    # Note that certain fields are boosted (^).
    query = {
        "size": 25,
        "query": {
            "multi_match": {
                "query": event['queryStringParameters']['q'],
                "fields": ["title^4", "plot^2", "actors", "directors"]
            }
        }
    }

    # Elasticsearch 6.x requires an explicit Content-Type header
```

```
    headers = { "Content-Type": "application/json" }

    # Make the signed HTTP request
    r = requests.get(url, auth=awsauth, headers=headers, data=json.dumps(query))

    # Create the response and add some extra content to support CORS
    response = {
        "statusCode": 200,
        "headers": {
            "Access-Control-Allow-Origin": '*'
        },
        "isBase64Encoded": False
    }

    # Add the search results to the response
    response['body'] = r.text
    return response
```

4. Installieren Sie die externen Bibliotheken in einem neuen `package` Verzeichnis.

```
pip3 install --target ./package boto3
pip3 install --target ./package requests
pip3 install --target ./package requests_aws4auth
```

5. Erstellen Sie ein Bereitstellungspaket, an dessen Stamm die installierte Bibliothek angefügt ist. Der folgende Befehl generiert eine `my-deployment-package.zip` Datei in Ihrem Projektverzeichnis.

```
cd package
zip -r ../my-deployment-package.zip .
```

6. Fügen Sie die `opensearch-lambda.py`-Datei dem Stamm der ZIP-Datei hinzu.

```
cd ..
zip my-deployment-package.zip opensearch-lambda.py
```

Weitere Informationen zum Erstellen von Lambda-Funktionen und Bereitstellungspaketen finden Sie unter Bereitstellen von Python-Lambda-Funktionen mit ZIP-Dateiarchiven imAWS Lambda - Entwicklerhandbuch und the section called “Erstellen des Lambda-Bereitstellungspakets” in diesem Leitfaden.

So erstellen Sie Ihre Funktion mit der Lambda-Konsole

1. Navigieren Sie zu https://console.aws.amazon.com/lambda/Hause zur Lambda-Konsole. Wählen Sie im linken Navigationsbereich Funktionen aus.
2. Wählen Sie Funktion erstellen aus.
3. Konfigurieren Sie die folgenden Felder:

   - Funktionsname: opensearch-function
   - Laufzeit: Python 3.9
   - Architektur: x86_64

   Behalten Sie alle anderen Standardoptionen bei und wählen Sie Funktion erstellen.
4. Wählen Sie auf der Seite mit der Funktionsübersicht im Abschnitt „Codequelle“ die Dropdownliste „Von hochladen“ und wählen Sie „.zip-Datei“ aus. Suchen Sie die **`my-deployment-package.zip`** Datei, die Sie erstellt haben, und wählen Sie Speichern aus.
5. Der Handler ist die Methode in Ihrem Funktions-Code, die Ereignisse verarbeitet. Wählen Sie unter Runtime-Einstellungen die Option Bearbeiten und ändern Sie den Namen des Handlers entsprechend dem Namen der Datei in Ihrem Bereitstellungspaket, in der sich die Lambda-Funktion befindet. Da Ihre Datei benannt ist`opensearch-lambda.py`, benennen Sie den Handler in um*`opensearch-lambda`*`.lambda_handler`. Weitere Informationen finden Sie unter Lambda-Funktions-Handler in Python.

Schritt 3: Erstellen Sie die API in API Gateway

Mit API Gateway können Sie eine eingeschränktere API erstellen und die Interaktion mit der OpenSearch `_search` API vereinfachen. Mit API Gateway können Sie Sicherheitsfunktionen wie die Amazon-Cognito-Authentifizierung und die Anforderungsdrosselung aktivieren. Führen Sie die folgenden Schritte aus, um eine API zu erstellen und bereitzustellen:

Erstellen und Konfigurieren Sie die API

So erstellen Sie Ihre API über die API-Gateway-Konsole

1. Navigieren Sie zu https://console.aws.amazon.com/apigateway/Hause zur API Gateway Gateway-Konsole. Wählen Sie im linken Navigationsbereich APIs.
2. Suchen Sie die REST-API (nicht privat) und wählen Sie Build aus.

3. Suchen Sie auf der folgenden Seite nach dem Abschnitt Neue API erstellen und stellen Sie sicher, dass Neue API ausgewählt ist.
4. Konfigurieren Sie die folgenden Felder:
   - API-Name: opensearch-api
   - Beschreibung: Öffentliche API für die Suche nach einer Amazon OpenSearch Service-Domain
   - Endpunkttyp: Regional
5. Wählen Sie Create API (API erstellen) aus.
6. Wählen Sie Aktionen und Methode erstellen aus.
7. Wählen Sie im Dropdown-Menü GET aus und klicken Sie zur Bestätigung auf das Häkchen.
8. Konfigurieren Sie die folgenden Einstellungen und wählen Sie dann Speichern:

Einstellung	Wert
Integrationstyp	Lambda-Funktion
Lambda-Proxy-Integration verwenden	Ja
Lambda-Region	*us-west-1*
Lambda-Funktion	`opensearch-lambda`
Standardzeitüberschreitung verwenden	Ja

Konfigurieren Sie die Methodenanforderung

Klicken Sie auf Methodenanforderung und konfigurieren Sie die folgenden Einstellungen:

Einstellung	Wert
Autorisierung	NONE
Anforderungs-Validator	Abfragezeichenfolgeparameter und Header validieren
API-Schlüssel erforderlich	false

Wählen Sie unter URL-Abfragezeichenfolge-Parameter die Option Abfragezeichenfolge hinzufügen aus und konfigurieren Sie den folgenden Parameter:

Einstellung	Wert
Name	q
Erforderlich	Ja

Stellen Sie die API bereit und Konfigurieren Sie eine Stufe

Mit der API Gateway-Konsole können Sie eine API bereitstellen, indem Sie eine Bereitstellung erstellen und sie mit einer neuen oder bestehenden Stufe verknüpfen.

1. Wählen Sie Aktionen und Bereitstellen der API aus.
2. Für Bereitstellungsstufe, wählen Sie Neue Stufe und nennen Sie die Stufe `opensearch-api-test`.
3. Wählen Sie Bereitstellen.
4. Konfigurieren Sie die folgenden Einstellungen im Stufen-Editor und wählen Sie dann Änderungen speichern:

Einstellung	Wert
Drosselung aktivieren	Ja
Rate (Tarif)	1000
Burst	500

Diese Einstellungen konfigurieren eine API, die nur über eine Methode verfügt: eine `GET`-Anforderung an den Endpunkt-Root (`https://`*`some-id`*`.execute-api.`*`us-west-1`*`.amazonaws.com/search-es-api-test`). Die Anforderung erfordert einen einzelnen Parameter (`q`), die Abfragezeichenfolge, nach der gesucht werden soll. Beim Aufruf übergibt die Methode die Anforderung an Lambda, die die `opensearch-lambda`-Funktion ausführt. Weitere Informationen finden Sie unter Erstellen einer API in Amazon API Gateway und Bereitstellen einer REST API in Amazon API Gateway.

Schritt 4: (Optional) Ändern der Domain-Zugriffsrichtlinie

Ihre OpenSearch Service-Domain muss es der Lambda-Funktion ermöglichen, `GET` Anfragen an den `movies` Index zu stellen. Wenn Ihre Domain eine offene Zugriffsrichtlinie hat, bei der eine abgestufte Zugriffssteuerung aktiviert ist, können Sie sie so wie sie ist belassen:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": "es:*",
      "Resource": "arn:aws:es:us-west-1:123456789012:domain/domain-name/*"
    }
  ]
}
```

Alternativ können Sie Ihre Domain-Zugriffsrichtlinie detaillierter gestalten. Beispielsweise gewährt die folgende Richtlinie `opensearch-lambda-role` (erstellt durch Lambda) Schreibzugriff auf den `movies`-Index. Um den genauen Namen der Rolle zu erhalten, die Lambda automatisch erstellt, gehen Sie zur AWS Identity and Access Management (IAM-) Konsole, wählen Sie Rollen und suchen Sie nach „Lambda“.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:role/service-role/opensearch-lambda-
role-1abcdefg"
      },
```

```
      "Action": "es:ESHttpGet",
      "Resource": "arn:aws:es:us-west-1:123456789012:domain/domain-name/movies/
_search"
    }
  ]
}
```

> **Important**
>
> Wenn Sie eine detaillierte Zugriffskontrolle für die Domain aktiviert haben, müssen Sie die Rolle auch einem Benutzer in OpenSearch Dashboards zuordnen, andernfalls werden Berechtigungsfehler angezeigt.

Berechtigungen für Lambda-Ausführungsrollen konfigurieren

Neben der Konfiguration der Domänenzugriffsrichtlinie müssen Sie auch sicherstellen, dass die Lambda-Ausführungsrolle über die erforderlichen IAM-Berechtigungen für den Zugriff auf Ihre OpenSearch Service-Domain verfügt. Für die Lambda-Funktion sind je nachdem, ob Sie eine verwaltete Domain oder eine OpenSearch Service Serverless-Sammlung verwenden, bestimmte Berechtigungen erforderlich.

Für verwaltete OpenSearch Servicedomänen:

Fügen Sie Ihrer Lambda-Ausführungsrolle die folgende IAM-Richtlinie hinzu, damit sie Anfragen an Ihre OpenSearch Service-Domain stellen kann:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "es:ESHttpGet",
        "es:ESHttpPost"
      ],
      "Resource": "arn:aws:es:us-west-1:123456789012:domain/domain-name/*"
```

```
    }
  ]
}
```

Für OpenSearch Service Serverless-Sammlungen:

Wenn Sie OpenSearch Service Serverless verwenden, fügen Sie Ihrer Lambda-Ausführungsrolle die folgende IAM-Richtlinie hinzu:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "aoss:*",
      "Resource": "arn:aws:aoss:us-west-1:123456789012:collection/collection-id"
    }
  ]
}
```

So fügen Sie diese Richtlinien Ihrer Lambda-Ausführungsrolle hinzu:

1. Navigieren Sie zur IAM-Konsole unter. https://console.aws.amazon.com/iam/
2. Wählen Sie Rollen und suchen Sie nach Ihrer Lambda-Ausführungsrolle (normalerweise benanntopensearch-lambda-role-*xxxxxxxx*).
3. Wählen Sie Berechtigungen hinzufügen und dann Inline-Richtlinie erstellen aus.
4. Wählen Sie die Registerkarte JSON und fügen Sie die entsprechende Richtlinie von oben ein. Ersetzen Sie dabei die Platzhalterwerte durch Ihre tatsächliche Ressource ARNs.
5. Wählen Sie Richtlinie überprüfen, geben Sie einen Namen wie `OpenSearchAccess` ein und wählen Sie Richtlinie erstellen aus.

> **Note**
>
> Ohne diese IAM-Berechtigungen erhält Ihre Lambda-Funktion beim Versuch, Ihre OpenSearch Service-Domain abzufragen, die Fehlermeldung „Zugriff verweigert“, auch wenn die Domänenzugriffsrichtlinie die Anfragen zulässt.

Weitere Informationen zu Zugriffsrichtlinien finden Sie unter the section called “Konfigurieren von Zugriffsrichtlinien”.

Zuordnen der Lambda-Rolle (bei Verwendung einer differenzierten Zugriffskontrolle)

Die differenzierte Zugriffskontrolle führt einen zusätzlichen Schritt ein, bevor Sie die Anwendung testen können. Auch wenn Sie die HTTP-Standardauthentifizierung für alle anderen Zwecke verwenden, müssen Sie die Lambda-Rolle einem Benutzer zuordnen, andernfalls werden Berechtigungsfehler angezeigt.

1. Navigieren Sie zur OpenSearch Dashboard-URL für die Domain.
2. Wählen Sie im Hauptmenü Sicherheit, Rollen und dann den Link zu der Rolle aus`all_access`, der Sie die Lambda-Rolle zuordnen müssen.
3. Wählen Sie Zugeordnete Benutzer, Mapping verwalten.
4. Fügen Sie unter Backend roles (Backend-Rollen) den Amazon-Ressourcennamen (ARN) der Lambda-Rolle hinzu. Der ARN sollte die Form von habe`arn:aws:iam::`*`123456789123`*`:role/service-role/`*`opensearch-lambda-role-1abcdefg`*.
5. Wählen Sie Zuordnen und bestätigen Sie, dass der Benutzer oder die Rolle unter Zugeordnete Benutzer angezeigt wird.

Schritt 5: Testen der Webanwendung

So testen Sie die Webanwendung

1. Laden Sie sample-site.zip herunter, dekomprimieren Sie sie und öffnen Sie `scripts/search.js` in Ihrem bevorzugten Texteditor.

2. Aktualisieren Sie die `apigatewayendpoint` Variable so, dass sie auf Ihren API-Gateway-Endpunkt zeigt, und fügen Sie am Ende des angegebenen Pfads einen Backslash hinzu. Sie können den Endpunkt schnell im API Gateway finden, indem Sie Phasen und den Namen der API auswählen. Die `apigatewayendpoint` Variable sollte die Form /haben. `https://`*`some-id`*`.execute-api.`*`us-west-1`*`.amazonaws.com/opensearch-api-test`
3. Öffnen Sie `index.html` und versuchen Sie, nach thor, house und einigen anderen Begriffen zu suchen.

Movie Search

thor

Found 7 results.



Thor

2011 — The powerful but arrogant god Thor is cast out of Asgard to live amongst humans in Midgard (Earth), where he soon becomes one of their finest defenders.



Thor: The Dark World

2013 — Faced with an enemy that even Odin and Asgard cannot withstand, Thor must embark on his most perilous and personal journey yet, one that will reunite him with Jane Foster and force him to sacrifice everything to save us all.



Vikingdom

2013 — A forgotten king, Eirick, is tasked with the impossible odds to defeat Thor, the God of Thunder.

Beheben von CORS-Fehlern

Auch wenn die Lambda-Funktion Inhalte in die Antwort einschließt, um CORS zu unterstützen, kann der folgende Fehler auftreten:

```
Access to XMLHttpRequest at '<api-gateway-endpoint>' from origin 'null' has been
 blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present in the
 requested resource.
```

Versuchen Sie in diesem Fall Folgendes:

1. Aktivieren Sie CORS in der GET-Ressource. Unter Advanced legen Sie Access-Control-Allow-Credentials auf `'true'` fest.
2. Stellen Sie Ihre API erneut in API Gateway (Aktionen,API bereitstellen) bereit.
3. Löschen Sie Ihren Lambda-Funktionsauslöser und fügen Sie ihn erneut hinzu. Fügen Sie sie hinzu, fügen Sie sie erneut hinzu, wählen Sie Auslöser hinzufügen und erstellen Sie den HTTP-Endpunkt, der Ihre Funktion aufruft. Der Auslöser muss die folgende Konfiguration haben:

Auslöser	API	Bereitstellungsstufe	Sicherheit
API Gateway	opensearch-api	opensearch-api-test	Öffnen

Nächste Schritte

Dieses Kapitel ist nur ein Ausgangspunkt zur Demonstration eines Konzepts. Sie sollten die folgenden Änderungen in Erwägung ziehen:

- Fügen Sie der OpenSearch Service-Domain Ihre eigenen Daten hinzu.
- Fügen Sie Methoden Ihrer API hinzu.
- Ändern Sie in der Lambda-Funktion die Suchanfrage oder steigern Sie andere Felder.
- Gestalten Sie die Ergebnisse unterschiedlich oder ändern Sie `search.js`, um dem Benutzer verschiedene Felder anzuzeigen.

Tutorial: Visualisierung von Kunden-Support-Aufrufen mit OpenSearch Service und Dashboards OpenSearch

Dieses Kapitel enthält eine vollständige Schritt-für-Schritt-Anleitung für folgendes Szenario: In einem Unternehmen geht eine bestimmte Anzahl an Anrufen beim Kundensupport ein. Diese sollen analysiert werden. Wie lauteten die Themen der einzelnen Anrufe? Wie viele Gespräche waren positiv? Wie viele Gespräche waren negativ? Wie können Vorgesetzte nach den Transkripten der Anrufe suchen oder diese überprüfen?

Zu einem manuellen Workflow könnte das Anhören von Aufzeichnungen, das Notieren des Themas des Anrufs und die Feststellung, ob die Interaktion mit dem Kunden positiv war, gehören.

Dieser Prozess wäre aber sehr arbeitsaufwendig. Wenn man von einer durchschnittlichen Anrufdauer von 10 Minuten ausgeht, können Mitarbeiter 48 Anrufe pro Tag entgegennehmen. Ohne menschliche Voreingenommenheit wären die Daten, die generiert werden würden, sehr zuverlässig, die Menge der Daten aber minimal: Sie würden nur Aufschluss über das Thema des Anrufs und darüber geben, ob ein Kunde zufrieden war oder nicht. Weitere Daten, beispielsweise ein vollständiges Transkript, würde enorm viel Zeit in Anspruch nehmen.

Mit Amazon S3, Amazon Transcribe, Amazon Comprehend und Amazon OpenSearch Service können Sie einen ähnlichen Prozess mit sehr wenig Code automatisieren und am Ende viel mehr Daten erhalten. Sie könnten beispielsweise ein vollständiges Transkript des Anrufs bekommen sowie Schlüsselwörter und eine Angabe zur allgemeinen "Stimmung" des Anrufs (positiv, negativ, neutral oder gemischt). Anschließend können Sie mit OpenSearch und OpenSearch Dashboards Daten suchen und visualisieren.

Sie können diese Anleitung unverändert nutzen. Die Idee dahinter ist jedoch, eine Idee davon zu bekommen, wie Sie Ihre JSON-Dokumente anreichern können, ehe Sie diese in OpenSearch Service indizieren.

Geschätzte Kosten

Im Allgemeinen sollte die Durchführung der Schritte in dieser Anleitung weniger als 2 USD kosten. Es werden folgende Ressourcen verwendet:

- S3-Bucket mit weniger als 100 MB übertragenen und gespeicherten Daten

  Weitere Informationen finden Sie unter Amazon S3 – Preise.

- OpenSearch Service-Domain mit einer `t2.medium` Instanz und 10 GiB EBS-Speicher für mehrere Stunden

  Weitere Informationen hierzu finden Sie unter OpenSearch Amazon-Open-Preise.
- Mehrere Aufrufe von Amazon Transcribe

  Weitere Informationen finden Sie unter Amazon Transcribe – Preise.
- Mehrere natürliche Sprachverarbeitungsaufrufe an Amazon Comprehend

  Weitere Informationen finden Sie unter Amazon Comprehend – Preise.

Themen

- Schritt 1: Konfigurieren der Voraussetzungen
- Schritt 2: Kopieren des Beispiel-Codes
- (Optional) Schritt 3: Indizieren von Beispieldaten
- Schritt 4: Analysieren und Visualisieren Sie Ihre Daten
- Schritt 5: Bereinigen Sie Ressourcen und nächste Schritte

Schritt 1: Konfigurieren der Voraussetzungen

Zum Fortfahren benötigen Sie die folgenden Ressourcen.

Voraussetzung	Beschreibung
Amazon-S3-Bucket	Weitere Informationen erhalten Sie unter Erstellen eines Buckets im Benutzerhandbuch für Amazon Simple Storage Service.
OpenSearch Service-Domain	Das Ziel für die Daten. Weitere Informationen finden Sie unter OpenSearch Dienstdomänen erstellen.

Wenn Sie noch nicht über diese Ressourcen verfügen, können Sie diese mit den folgenden AWS CLI -Befehlen erstellen:

```
aws s3 mb s3://my-transcribe-test --region us-west-2
```

```
aws opensearch create-domain --domain-name my-transcribe-test --engine-version
 OpenSearch_1.0 --cluster-config  InstanceType=t2.medium.search,InstanceCount=1
 --ebs-options EBSEnabled=true,VolumeType=standard,VolumeSize=10 --access-
policies '{"Version":"2012-10-17","Statement":[{"Effect":"Allow","Principal":
{"AWS":"arn:aws:iam::123456789012:root"},"Action":"es:*","Resource":"arn:aws:es:us-
west-2:123456789012:domain/my-transcribe-test/*"}]}' --region us-west-2
```

> **Note**
>
> Diese Befehle verwenden die `us-west-2`-Region. Sie können jedoch jede Region nutzen, die von Amazon Comprehend unterstützt wird. Weitere Informationen finden Sie in unter Allgemeine AWS-Referenz.

Schritt 2: Kopieren des Beispiel-Codes

1. Kopieren Sie den folgenden Python-3-Beispiel-Code in eine neue Datei namens `call-center.py`:

```
import boto3
import datetime
import json
import requests
from requests_aws4auth import AWS4Auth
import time
import urllib.request

# Variables to update
audio_file_name = '' # For example, 000001.mp3
bucket_name = '' # For example, my-transcribe-test
domain = '' # For example, https://search-my-transcribe-test-12345.us-
west-2.es.amazonaws.com
index = 'support-calls'
type = '_doc'
region = 'us-west-2'

# Upload audio file to S3.
s3_client = boto3.client('s3')

audio_file = open(audio_file_name, 'rb')
```

```
print('Uploading ' + audio_file_name + '...')
response = s3_client.put_object(
    Body=audio_file,
    Bucket=bucket_name,
    Key=audio_file_name
)

# # Build the URL to the audio file on S3.
# # Only for the us-east-1 region.
# mp3_uri = 'https://' + bucket_name + '.s3.amazonaws.com/' + audio_file_name

# Get the necessary details and build the URL to the audio file on S3.
# For all other regions.
response = s3_client.get_bucket_location(
    Bucket=bucket_name
)
bucket_region = response['LocationConstraint']
mp3_uri = 'https://' + bucket_name + '.s3-' + bucket_region + '.amazonaws.com/' +
 audio_file_name

# Start transcription job.
transcribe_client = boto3.client('transcribe')

print('Starting transcription job...')
response = transcribe_client.start_transcription_job(
    TranscriptionJobName=audio_file_name,
    LanguageCode='en-US',
    MediaFormat='mp3',
    Media={
        'MediaFileUri': mp3_uri
    },
    Settings={
        'ShowSpeakerLabels': True,
        'MaxSpeakerLabels': 2 # assumes two people on a phone call
    }
)

# Wait for the transcription job to finish.
print('Waiting for job to complete...')
while True:
    response =
 transcribe_client.get_transcription_job(TranscriptionJobName=audio_file_name)
    if response['TranscriptionJob']['TranscriptionJobStatus'] in ['COMPLETED',
 'FAILED']:
```

```
        break
    else:
        print('Still waiting...')
    time.sleep(10)

transcript_uri = response['TranscriptionJob']['Transcript']['TranscriptFileUri']

# Open the JSON file, read it, and get the transcript.
response = urllib.request.urlopen(transcript_uri)
raw_json = response.read()
loaded_json = json.loads(raw_json)
transcript = loaded_json['results']['transcripts'][0]['transcript']

# Send transcript to Comprehend for key phrases and sentiment.
comprehend_client = boto3.client('comprehend')

# If necessary, trim the transcript.
# If the transcript is more than 5 KB, the Comprehend calls fail.
if len(transcript) > 5000:
    trimmed_transcript = transcript[:5000]
else:
    trimmed_transcript = transcript

print('Detecting key phrases...')
response = comprehend_client.detect_key_phrases(
    Text=trimmed_transcript,
    LanguageCode='en'
)

keywords = []
for keyword in response['KeyPhrases']:
    keywords.append(keyword['Text'])

print('Detecting sentiment...')
response = comprehend_client.detect_sentiment(
    Text=trimmed_transcript,
    LanguageCode='en'
)

sentiment = response['Sentiment']

# Build the Amazon OpenSearch Service URL.
id = audio_file_name.strip('.mp3')
url = domain + '/' + index + '/' + type + '/' + id
```

```
# Create the JSON document.
json_document = {'transcript': transcript, 'keywords': keywords, 'sentiment':
 sentiment, 'timestamp': datetime.datetime.now().isoformat()}

# Provide all details necessary to sign the indexing request.
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region,
 'opensearchservice', session_token=credentials.token)

# Index the document.
print('Indexing document...')
response = requests.put(url, auth=awsauth, json=json_document, headers=headers)

print(response)
print(response.json())
```

2. Aktualisieren Sie die ersten sechs Variablen.
3. Installieren Sie die erforderlichen Pakete mit den folgenden Befehlen:

```
pip install boto3
pip install requests
pip install requests_aws4auth
```

4. Platzieren Sie Ihre Datei MP3 in demselben Verzeichnis wie `call-center.py` und führen Sie das Skript aus. Hier ein Beispiel für eine Ausgabe:

```
$ python call-center.py
Uploading 000001.mp3...
Starting transcription job...
Waiting for job to complete...
Still waiting...
Still waiting...
Still waiting...
Still waiting...
Still waiting...
Still waiting...
Still waiting...
Detecting key phrases...
Detecting sentiment...
Indexing document...
<Response [201]>
```

```
{u'_type': u'call', u'_seq_no': 0, u'_shards': {u'successful': 1, u'failed': 0,
 u'total': 2}, u'_index': u'support-calls4', u'_version': 1, u'_primary_term': 1,
 u'result': u'created', u'_id': u'000001'}
```

`call-center.py` führt eine Reihe von Operationen durch:

1. Das Skript lädt eine Audiodatei (in diesem Fall eine MP3, Amazon Transcribe unterstützt jedoch mehrere Formate) in Ihren S3-Bucket hoch.
2. Es sendet die URL der Audio-Datei an Amazon Transcribe und wartet, bis der Transkriptionsauftrag abgeschlossen ist.

   Die Zeit bis zum Abschließen des Transkriptionsauftrags hängt von der Länge der Audiodatei ab. Gehen Sie aber von Minuten und nicht Sekunden aus.

   > **Tip**
   >
   > Zur Verbesserung der Qualität der Transkription können Sie ein benutzerdefiniertes Vokabular für Amazon Transcribe konfigurieren.

3. Nach Abschluss des Transkriptionsauftrag extrahiert das Skript das Transkript, kürzt es auf 5.000 Zeichen und sendet es zwecks Schlüsselwort- und Stimmungsanalyse an Amazon Comprehend.
4. Abschließend fügt das Skript das vollständige Transkript, die Schlüsselwörter, die Stimmungsdaten und den aktuellen Zeitstempel zum JSON-Dokument hinzu und indiziert es in Service. OpenSearch

> **Tip**
>
> LibriVoxhat gemeinfreie Hörbücher, die Sie zum Testen verwenden können.

(Optional) Schritt 3: Indizieren von Beispieldaten

Wenn Sie keine Aufrufaufzeichnungen zur Hand haben – und wer hat das schon? – können Sie die Beispieldokumente in der Datei sample-calls.zip indizieren, die mit dem vergleichbar sind, was `call-center.py` produziert.

1. Erstellen Sie eine Datei namens `bulk-helper.py`:

```
import boto3
from opensearchpy import OpenSearch, RequestsHttpConnection
import json
from requests_aws4auth import AWS4Auth

host = '' # For example, my-test-domain.us-west-2.es.amazonaws.com
region = '' # For example, us-west-2
service = 'es'

bulk_file = open('sample-calls.bulk', 'r').read()

credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
 session_token=credentials.token)

search = OpenSearch(
    hosts = [{'host': host, 'port': 443}],
    http_auth = awsauth,
    use_ssl = True,
    verify_certs = True,
    connection_class = RequestsHttpConnection
)

response = search.bulk(bulk_file)
print(json.dumps(response, indent=2, sort_keys=True))
```

2. Aktualisieren Sie die ersten zwei Variablen für `host` und `region`.
3. Installieren Sie das erforderlich Paket mit folgendem Befehl:

```
pip install opensearch-py
```

4. Laden Sie die Datei sample-calls.zip herunter und entpacken Sie sie.
5. Speichern Sie `sample-calls.bulk` in demselben Verzeichnis wie `bulk-helper.py` und führen Sie das Helferobjekt aus. Hier ein Beispiel für eine Ausgabe:

```
$ python bulk-helper.py
{
  "errors": false,
  "items": [
    {
      "index": {
```

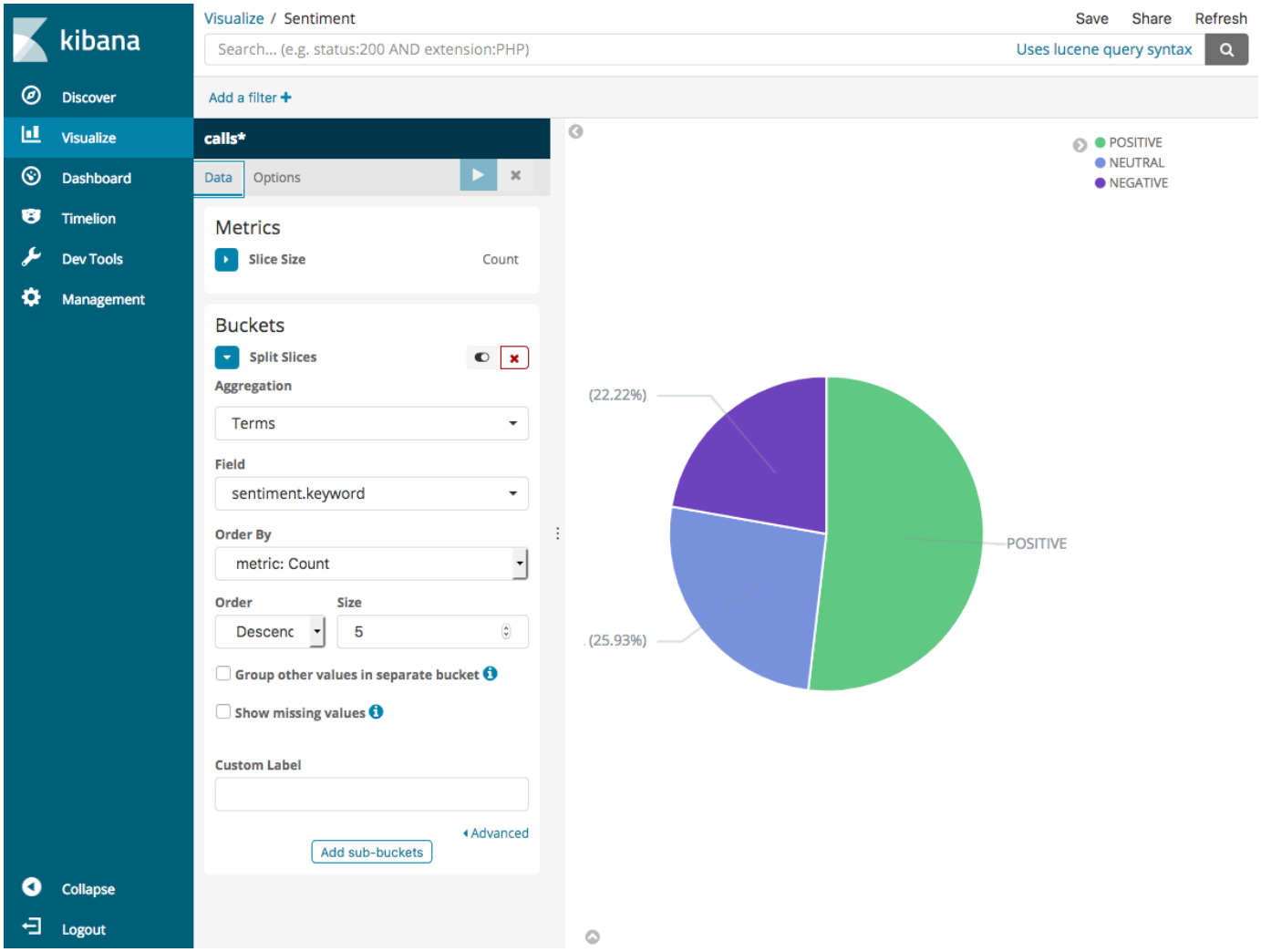
```
        "_id": "1",
        "_index": "support-calls",
        "_primary_term": 1,
        "_seq_no": 42,
        "_shards": {
          "failed": 0,
          "successful": 1,
          "total": 2
        },
        "_type": "_doc",
        "_version": 9,
        "result": "updated",
        "status": 200
      }
    },
    ...
  ],
  "took": 27
}
```

Schritt 4: Analysieren und Visualisieren Sie Ihre Daten

Nachdem Sie nun über einige Daten in OpenSearch Service verfügen, können Sie diese mit OpenSearch Dashboards visuell darstellen.

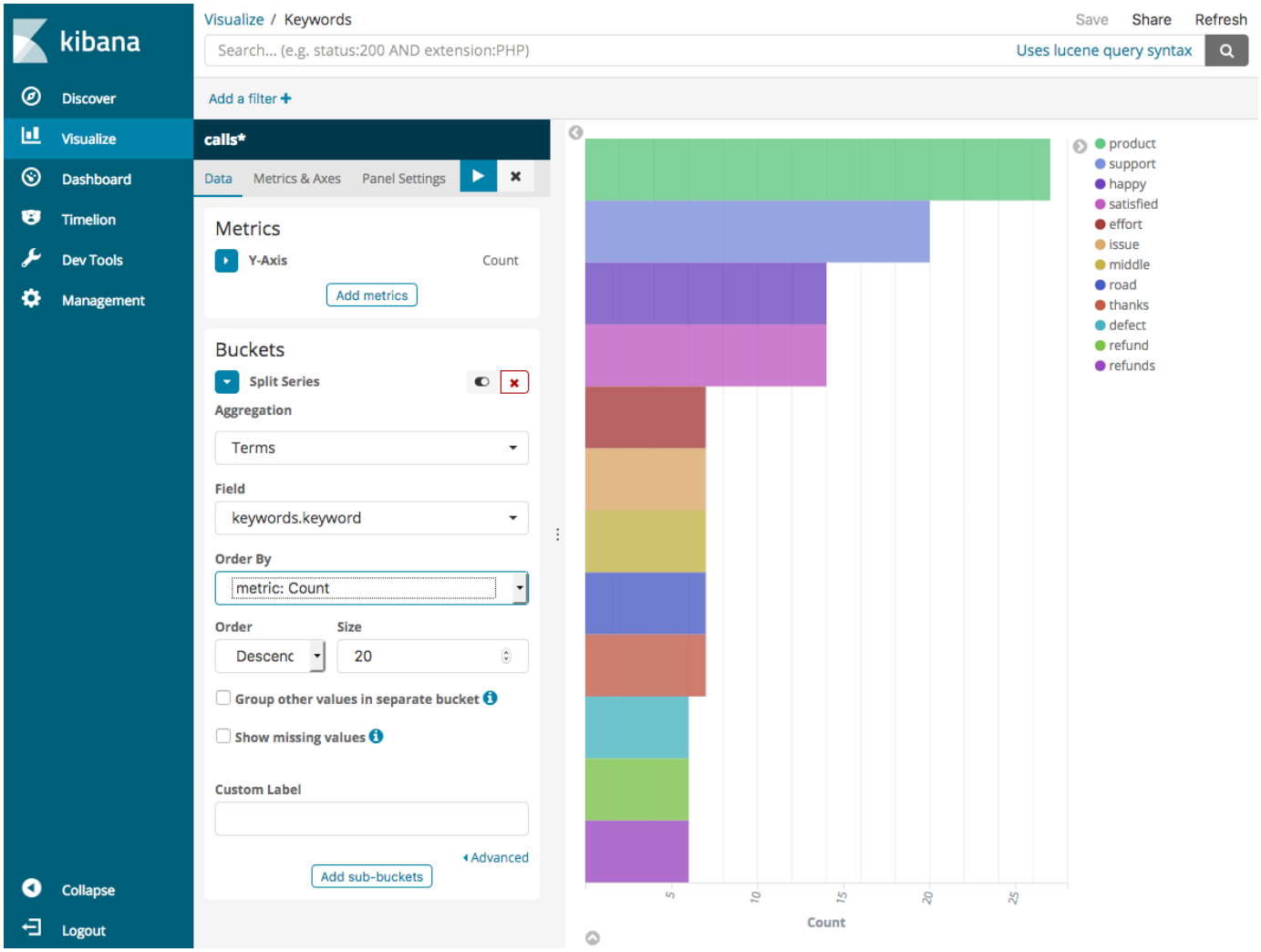
1. Navigieren Sie zu `https://search-`*`domain`*`.`*`region`*`.es.amazonaws.com/_dashboards`.
2. Bevor Sie OpenSearch Dashboards verwenden können, benötigen Sie ein Index-Muster. Dashboards verwendet Index-Muster, um ihre Analyse auf einen oder mehrere Indizes einzugrenzen. Um den `support-calls`-Index abzugleichen, den `call-center.py` erstellt hat, gehen Sie zu Stack Management, Index Patterns, und definieren Sie ein Indexmuster von `support*`, und wählen Sie dann Nächster Schritt.
3. Wählen Sie für Time Filter field name (Feldname für Zeitfilter) die Option timestamp (Zeitstempel) aus.
4. Sie können nun mit dem Generieren von Visualisierungen beginnen. Wählen Sie Visualize (Visualisieren) aus und fügen Sie eine neue Visualisierung hinzu.
5. Wählen Sie das Kreisdiagramm und das `support*`-Index-Muster aus.
6. Die Standardvisualisierung ist eine eher grundlegende. Eine detaillierte Visualisierung erhalten Sie, wenn Sie Split Slices (Slices aufteilen) auswählen.

Wählen Sie unter Aggregation den Eintrag Terms (Bedingungen) aus. Wählen Sie für Field (Feld) sentiment.keyword aus. Klicken Sie dann auf Apply changes (Änderungen übernehmen) und Save (Speichern).

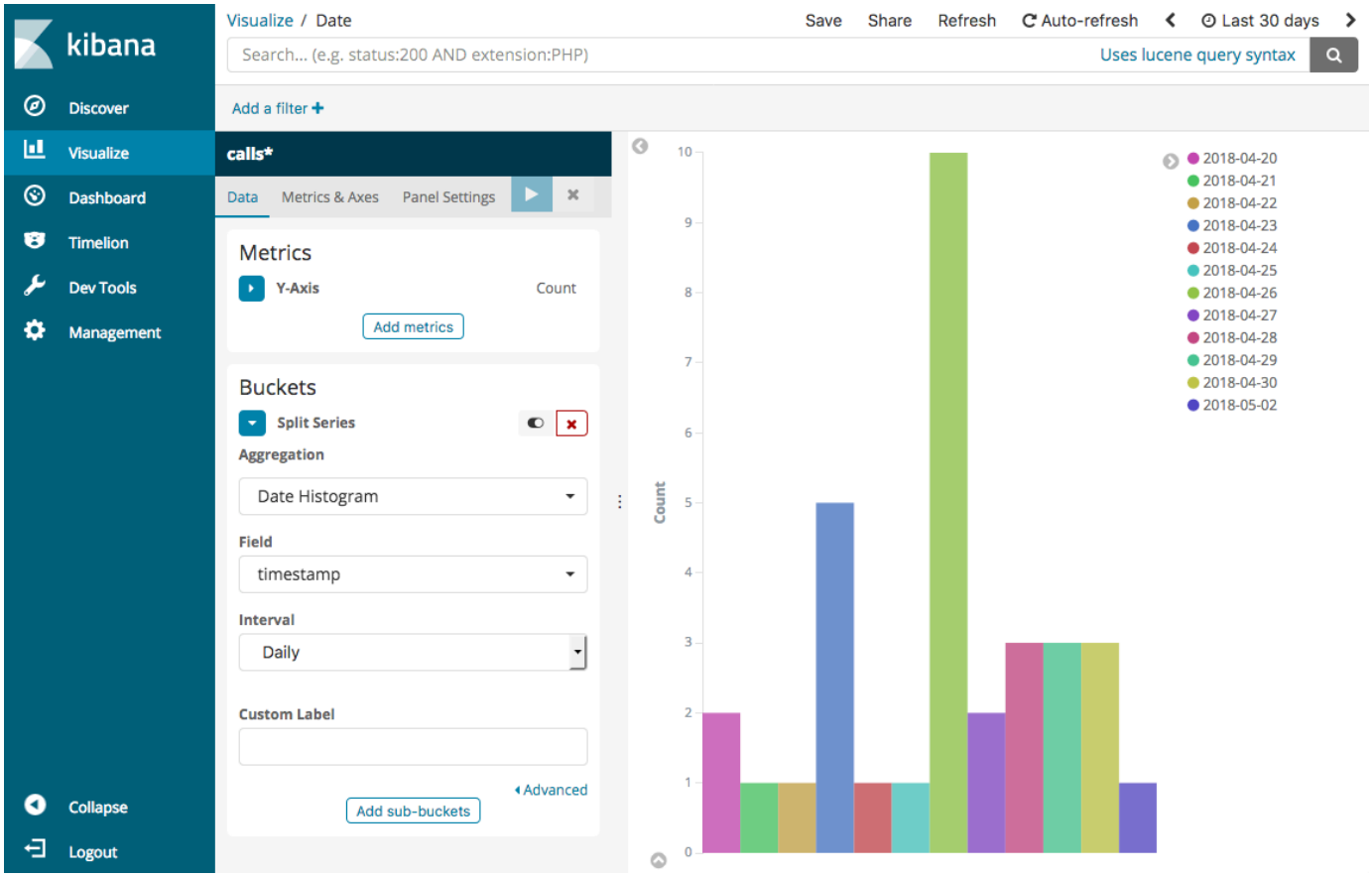


7. Kehren Sie zur Seite Visualize (Visualisieren) zurück und fügen Sie eine weitere Visualisierung hinzu. Wählen Sie dieses Mal das horizontale Balkendiagramm aus.
8. Wählen Sie Split Series (Serie aufteilen) aus.

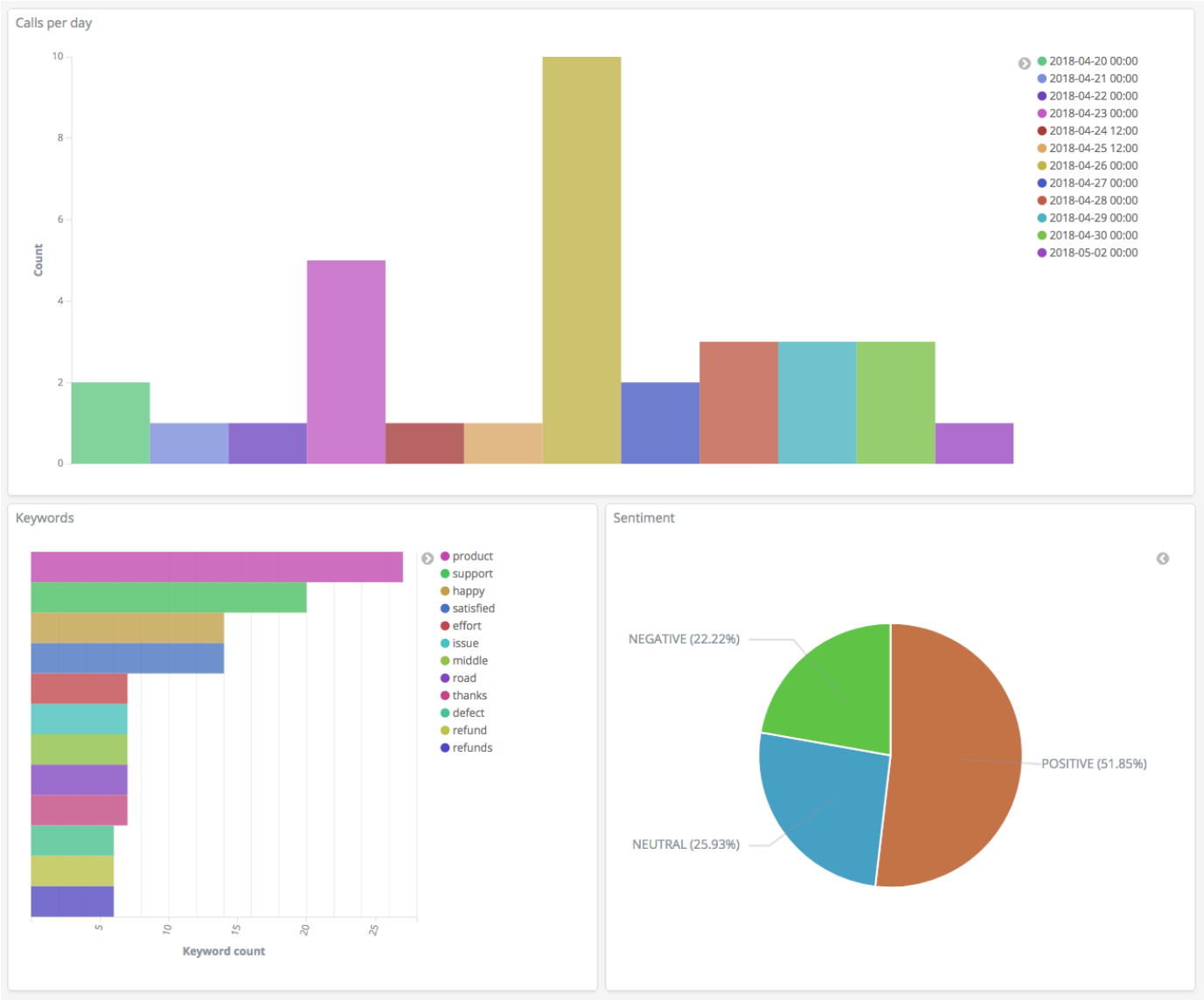
   Wählen Sie unter Aggregation den Eintrag Terms (Bedingungen) aus. Wählen Sie für Field (Feld) keywords.keyword aus und ändern Sie Size (Größe) in 20. Klicken Sie dann auf Apply changes (Änderungen übernehmen) und Save (Speichern).



9. Kehren Sie zur Seite Visualize (Visualisieren) zurück und fügen Sie eine letzte Visualisierung, ein vertikales Balkendiagramm, hinzu.
10. Wählen Sie Split Series (Serie aufteilen) aus. Wählen Sie für Aggregation (Aggregation) Date Histogram (Datumshistogramm) aus. Wählen Sie für Field (Feld) timestamp aus und ändern Sie das Interval (Intervall) in Daily (Täglich).
11. Wählen Sie Metrics & Axes (Metriken & Achsen) aus und ändern Sie den Mode (Modus) in normal.
12. Klicken Sie auf Apply changes (Änderungen übernehmen) und Save (Speichern).



13. Nachdem Sie nun drei Visualisierungen haben, können Sie diese zu einer Dashboard-Visualisierung hinzufügen. Klicken Sie auf Dashboard, erstellen Sie ein Dashboard und fügen Sie Ihre Visualisierungen hinzu.



Schritt 5: Bereinigen Sie Ressourcen und nächste Schritte

Um unnötige Kosten zu vermeiden, löschen Sie den S3-Bucket und die OpenSearch Service-Domain. Weitere Informationen finden Sie unter Löschen eines Buckets im Amazon Simple Storage Service-Benutzerhandbuch und Löschen einer OpenSearch Service-Domain in diesem Handbuch.

Transkripte benötigen viel weniger Speicherplatz als MP3 Dateien. Sie können die Einstellungen für Ihr MP3 Aufbewahrungsfenster ändern — beispielsweise können Sie die dreimonatige Aufbewahrungsdauer für Anrufaufzeichnungen auf einen Monat verkürzen — Transkripte jahrelang aufbewahren und immer noch Speicherkosten sparen.

Sie können auch den Transkriptionsprozess mit AWS Step Functions und Lambda automatisieren, weitere Metadaten vor der Indizierung hinzufügen oder komplexere Visualisierungen generieren, um Ihrem Anwendungsfall gerecht zu werden.

Umbenennung von Amazon OpenSearch Service — Zusammenfassung der Änderungen

Am 8. September 2021 wurde unsere Such- und Analyse-Suite in Amazon OpenSearch Service umbenannt. OpenSearch Service unterstützt OpenSearch genauso wie Legacy-System-Elasticsearch-OSS. In den folgenden Abschnitten werden die verschiedenen Teile des Services beschrieben, die sich mit der Umbenennung geändert haben und welche Maßnahmen Sie ergreifen müssen, um sicherzustellen, dass Ihre Domains weiterhin ordnungsgemäß funktionieren.

Einige dieser Änderungen gelten nur, wenn Sie Ihre Domänen von Elasticsearch auf OpenSearch aktualisieren. In anderen Fällen, z. B. in der Fakturierung- und Kostenmanagement-Konsole, ändert sich die Benutzererfahrung sofort.

Beachten Sie, dass diese Liste nicht vollumfänglich ist. Auch andere Teile des Produkts haben sich geändert, aber diese Updates sind am relevantesten.

Neue API-Version

Die neue Version der OpenSearch Service-Konfigurations-API (2021-01-01) funktioniert sowohl mit Legacy-System-Elasticsearch-OSS OpenSearch als auch mit Legacy-System-Elasticsearch-OSS. 21 API-Operationen wurden durch prägnantere und Engine-agnostische Namen ersetzt (z. B. `CreateElasticsearchDomain` geändert in`CreateDomain`), aber OpenSearch Service unterstützt weiterhin beide API-Versionen.

Wir empfehlen, dass Sie zukünftig die neuen API-Operationen verwenden, um Domains zu erstellen und zu verwalten. Beachten Sie, dass Sie bei Verwendung der neuen API-Operationen zum Erstellen einer Domain den `EngineVersion`-Parameter im Format `Elasticsearch_X.Y` oder `0penSearch_X.Y` und nicht nur die Versionsnummer angeben müssen. Wenn Sie keine Version angeben, wird standardmäßig die neueste Version von OpenSearch verwendet.

Aktualisieren Sie AWS CLI auf Version 1.20.40 oder höher, um Ihre Domains `aws opensearch ...` zu erstellen und zu verwalten. Informationen zum neuen CLI-Format finden Sie in der OpenSearch CLI-Referenz.

Umbenannte Instance-Typen

Instance-Typen in Amazon OpenSearch Service haben jetzt das Format `<type>.<size>.search` —zum Beispiel `m6g.large.search` statt`m6g.large.elasticsearch`. Sie müssen selbst keine Aktion durchführen. Vorhandene Domains werden automatisch auf die neuen Instance-Typen innerhalb der API und in der Fakturierungs- und Kostenmanagementkonsole verweisen.

Falls Sie über Reserved Instances (RIs) verfügen, wird Ihr Vertrag von der Änderung nicht beeinflusst. Die alte Konfigurations-API-Version ist weiterhin kompatibel mit dem alten Benennungsformat, aber wenn Sie die neue API-Version verwenden möchten, müssen Sie das neue Format verwenden.

Änderungen der Zugriffsrichtlinie

In den folgenden Abschnitten wird beschrieben, welche Aktionen Sie ergreifen müssen, um Ihre Zugriffsrichtlinien zu aktualisieren.

IAM-Richtlinien

Wir empfehlen, dass Sie Ihre IAM-Richtlinien, um die umbenannten API-Vorgänge zu verwenden. OpenSearch Service wird jedoch weiterhin bestehende Richtlinien respektieren, indem es intern die alten API-Berechtigungen repliziert. Wenn Sie beispielsweise derzeit über die Berechtigung zum Ausführen des `CreateElasticsearchDomain`-Vorgangs verfügen, können Sie jetzt sowohl `CreateElasticsearchDomain` (alte API-Operation) als auch `CreateDomain` (neue API-Operation) aufrufen. Dasselbe gilt für explizite Zugriffsverweigerungen. Eine Liste der aktualisierten API-Operationen finden Sie in der Richtlinienelementverweis.

SCP-Richtlinien

Service-Kontroll-Richtlinien (SCPs) führen im Vergleich zu Standard-IAM eine zusätzliche Komplexitätsebene ein. Um zu verhindern, dass Ihre SCP-Richtlinien verletzt werden, müssen Sie jeder Ihrer SCP-Richtlinien sowohl die alten als auch die neuen API-Operationen hinzufügen. Wenn ein Benutzer beispielsweise derzeit über Berechtigungen zum Zulassen von `CreateElasticsearchDomain` verfügt, müssen Sie ihm auch Berechtigungen zum Zulassen von `CreateDomain` erteilen, damit er weiterhin Domains beibehalten kann. Dasselbe gilt für explizite Zugriffsverweigerungen.

Zum Beispiel:

```
"Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "es:CreateElasticsearchDomain",
        "es:CreateDomain"
         ...
      ],
    },
      "Effect": "Deny",
      "Action:" [
        "es:DeleteElasticsearchDomain",
        "es:DeleteDomain"
         ...
```

Neue Ressourcentypen

OpenSearch Service führt die folgenden neuen Ressourcentypen ein:

Ressource	Beschreibung
`AWS::OpenSearchService::Domain`	Repräsentiert eine Amazon OpenSearch Service-Domain. Diese Ressource existiert auf Service-Ebene und ist nicht spezifisch für die Software, die in der Domain ausgeführt wird. Sie gilt für Dienste wie AWS CloudFormation- und AWS-Ressourcengruppen, in denen Sie Ressourcen für den Dienst als Ganzes erstellen und verwalten. Anweisungen zum Upgrade CloudFormation von Domains, die in Elasticsearch auf definiert sind OpenSearch, finden Sie unter Anmerkungen im CloudFormation Benutzerhandbuch.
`AWS::OpenSearch::Domain`	Repräsentiert OpenSearch /Elasticsearch-Software, die auf einer Domäne ausgeführt wird. Diese Ressource bezieht sich auf Dienste wie AWS CloudTrailund AWS Config, die auf

Ressource	Beschreibung
	die Software verweisen, die auf der Domain läuft, und nicht auf OpenSearch Service als Ganzes. Diese Dienste enthalten jetzt separate Ressourcentypen für Domänen, auf denen Elasticsearch (`AWS::Elasticsearch ::Domain`) ausgeführt wird, und Domänen, auf denen Elasticsearch OpenSearch (`AWS::OpenSearch::Domain`) ausgeführt wird.

> **Note**
>
> In AWS Configsehen Sie Ihre Daten weiterhin unter der vorhandenen `AWS::Elasticsearch::Domain` Ressourcentyp für mehrere Wochen, auch wenn Sie eine oder mehrere Domänen auf upgraden OpenSearch.

Kibana wurde in Dashboards OpenSearch umbenannt

OpenSearch Dashboards, die AWS -Alternative zu Kibana, ist ein Open-Source-Visualisierungs-Tool, das für die Verwendung entwickelt wurde. OpenSearch Nachdem Sie eine Domain von Elasticsearch auf aktualisiert haben OpenSearch, ändert sich der `/_plugin/kibana` Endpunkt auf. `/_dashboards` OpenSearch Service leitet alle Anfragen an den neuen Endpunkt um. Wenn Sie jedoch den Kibana-Endpunkt in einer Ihrer IAM-Richtlinien verwenden, aktualisieren Sie diese Richtlinien, um auch den neuen `/_dashboards` Endpunkt einzuschließen.

Wenn Sie verwendenthe section called “SAML-Authentifizierung für Dashboards OpenSearch ”, müssen Sie vor dem Upgrade Ihrer Domain auf OpenSearch alle in Ihrem Identitätsanbieter (IdP) URLs konfigurierten Kibana von `/_plugin/kibana` auf ändern. `/_dashboards` Die häufigsten URLs sind Assertion Consumer Service (ACS) URLs und Empfänger URLs.

Die `kibana_read_only` Standardrolle für OpenSearch Dashboards wurde umbenannt in`opensearch_dashboards_read_only`, und die `kibana_user` Rolle wurde umbenannt in. `opensearch_dashboards_user` Die Änderung gilt für alle neu erstellten 1. OpenSearch x Domänen, auf denen Service-Software R20211203 oder höher ausgeführt wird. Wenn Sie

eine bereits vorhandene Domain auf die Service-Software R20211203 aktualisieren, bleiben die Rollennamen gleich.

Umbenannte CloudWatch Kennzahlen

Für laufende Domains ändern sich mehrere CloudWatch Metriken OpenSearch. Wenn Sie eine Domäne auf aktualisieren OpenSearch, ändern sich die Metriken automatisch und Ihre aktuellen CloudWatch Alarme werden unterbrochen. Bevor Sie Ihren Cluster von einer Elasticsearch-Version auf eine OpenSearch Version aktualisieren, müssen Sie Ihre CloudWatch Alarme aktualisieren, um die neuen Metriken zu verwenden.

Die folgenden Metriken haben sich verändert:

Ursprünglicher Metrikname	Neuer Name
`KibanaHealthyNodes`	`OpenSearchDashboardsHealthyNodes`
`KibanaConcurrentConnections`	`OpenSearchDashboardsConcurrentConnections`
`KibanaHeapTotal`	`OpenSearchDashboardsHeapTotal`
`KibanaHeapUsed`	`OpenSearchDashboardsHeapUsed`
`KibanaHeapUtilization`	`OpenSearchDashboardsHeapUtilization`
`KibanaOS1MinuteLoad`	`OpenSearchDashboardsOS1MinuteLoad`
`KibanaRequestTotal`	`OpenSearchDashboardsRequestTotal`
`KibanaResponseTimesMaxInMillis`	`OpenSearchDashboardsResponseTimesMaxInMillis`
`ESReportingFailedRequestSysErrCount`	`KibanaReportingFailedRequestSysErrCount`
`ESReportingRequestCount`	`KibanaReportingRequestCount`

Ursprünglicher Metrikname	Neuer Name
`ESReportingFailedRequestUserErrCount`	`KibanaReportingFailedRequestUserErrCount`
`ESReportingSuccessCount`	`KibanaReportingSuccessCount`
`ElasticsearchRequests`	`OpenSearchRequests`

Eine vollständige Liste der Messwerte, die OpenSearch Service an Amazon sendet CloudWatch, finden Sie unterthe section called “Überwachen von Cluster-Metriken”.

Änderungen Fakturierung und Kostenmanagement

Historische Daten in der Billing and Cost Management -Konsole und in Kosten- und Nutzungsberichten werden weiterhin den alten Service-Namen verwenden. Daher benötigen Sie bei der Suche nach Daten Filter sowohl für Amazon OpenSearch Service als auch für den alten Elasticsearch-Namen. Wenn Sie über gespeicherte Berichte verfügen, aktualisieren Sie die Filter, um sicherzustellen, dass sie auch den OpenSearch Service enthalten. Möglicherweise erhalten Sie zunächst eine Warnung, wenn Ihre Nutzung für Elasticsearch abnimmt und für zunimmt OpenSearch, diese verschwindet jedoch innerhalb weniger Tage.

Zusätzlich zum Service-Namen ändern sich die folgenden Felder für alle Berichte, Rechnungen und Preislisten-API-Vorgänge:

Feld	Altes Format	Neues Format
Instance-Typ	`m5.large.elasticsearch`	`m5.large.search`
Produktfamilie	Elasticsearch-Instance Elasticsearch-Volume	Amazon OpenSearch Service-Instanz OpenSearch Amazon-Service-Volume

Feld	Altes Format	Neues Format
Preisbeschreibung	5,098$ pro c5.18xlarge.elasticsearch-Instance-Stunde (oder Teilstunde) - EU	5,098$ pro c5.18xlarge.search-Instance-Stunde (oder Teilstunde) - EU
Instance-Familie	`ultrawarm.elasticsearch`	`ultrawarm.search`

Neues Ereignisformat

Das Format der Ereignisse, die OpenSearch Service an Amazon EventBridge und Amazon sendet, CloudWatch hat sich geändert, insbesondere das `detail-type` Feld. Das Quellfeld (`aws.es`) bleibt gleich. Das vollständige Format für jeden Ereignistyp finden Sie unter the section called “Überwachung von Ereignissen”. Wenn Sie über vorhandene Ereignisregeln verfügen, die vom alten Format abhängen, stellen Sie sicher, dass sie dem neuen Format entsprechen.

Was bleibt gleich?

Die folgenden Funktionen und Funktionalitäten, unter anderem nicht aufgeführt, bleiben gleich:

- Dienstauftraggeber (`es.amazonaws.com`)
- Anbieter-Code
- Domäne ARNs
- Domains-Endpunkte

Erste Schritte: Aktualisieren Sie Ihre Domains auf OpenSearch 1.x

OpenSearch 1. x unterstützt Upgrades von Elasticsearch Version 6.8 und 7. x. Anweisungen zum Upgrade Ihrer Domain finden Sie unter the section called “Aktualisierung einer Domain (Konsole)”. Wenn Sie die AWS CLI oder Konfigurations-API zum Aktualisieren Ihrer Domäne verwenden, müssen Sie die `TargetVersion` As angeben`OpenSearch_1.x`.

OpenSearch 1. x führt eine zusätzliche Domäneneinstellung namens Kompatibilitätsmodus aktivieren ein. Da bestimmte Elasticsearch OSS-Clients und Plugins die Clusterversion vor der Verbindung

überprüfen, setzt OpenSearch der Kompatibilitätsmodus so ein, dass er dessen Version als 7.10 meldet, damit diese Clients weiterhin funktionieren.

Sie können den Kompatibilitätsmodus aktivieren, wenn Sie OpenSearch Domains zum ersten Mal erstellen oder wenn Sie OpenSearch von einer Elasticsearch-Version aktualisieren. Wenn er nicht gesetzt ist, wird der Parameter standardmäßig auf `false` gesetzt, wenn Sie eine Domain erstellen, und auf `true` wenn Sie eine Domain aktualisieren.

Um den Kompatibilitätsmodus mit der Konfigurations-API zu aktivieren, setzen Sie `override_main_response_version` auf `true`:

```
POST https://es.us-east-1.amazonaws.com/2021-01-01/opensearch/upgradeDomain
{
  "DomainName": "domain-name",
  "TargetVersion": "OpenSearch_1.0",
  "AdvancedOptions": {
    "override_main_response_version": "true"
   }
}
```

Um den Kompatibilitätsmodus für vorhandene OpenSearch Domänen zu aktivieren oder zu deaktivieren, müssen Sie die OpenSearch _cluster/settings API-Operation verwenden:

```
PUT /_cluster/settings
{
  "persistent" : {
    "compatibility.override_main_response_version" : true
  }
}
```

Problembehebung bei Amazon OpenSearch Service

In diesem Thema wird beschrieben, wie Sie häufig auftretende Probleme mit Amazon OpenSearch Service identifizieren und lösen können. Lesen Sie die Informationen in diesem Abschnitt, bevor Sie sich an den AWS -Support wenden.

Ich kann nicht auf OpenSearch Dashboards zugreifen

Der OpenSearch Dashboards-Endpunkt unterstützt keine signierten Anfragen. Wenn durch die Zugriffskontrollrichtlinie Ihrer Domain nur Zugriff auf bestimmte IAM-Rollen gewährt wird und Sie Amazon-Cognito-Authentifizierung nicht konfiguriert haben, erhalten Sie möglicherweise folgende Fehlermeldung, wenn Sie versuchen, auf Dashboards zuzugreifen:

```
"User: anonymous is not authorized to perform: es:ESHttpGet"
```

Wenn Ihre OpenSearch Service-Domain VPC-Zugriff verwendet, erhalten Sie diesen Fehler möglicherweise nicht, aber es kann zu einem Timeout bei der Anfrage kommen. Informationen zur Behebung dieses Problems und zu den verschiedenen verfügbaren Konfigurationsoptionen finden Sie unter the section called “Steuern des Zugriffs auf Dashboards ” the section called “Zugriffsrichtlinien für VPC-Domänen” und the section called “Identitäts- und Zugriffsverwaltung”.

Zugriff auf VPC-Domain nicht möglich

Siehe the section called “Zugriffsrichtlinien für VPC-Domänen” und the section called “Testen von VPC-Domänen”.

Cluster im schreibgeschützten Zustand

Im Vergleich zu früheren Elasticsearch-Versionen OpenSearch und Elasticsearch 7. x verwendet ein anderes System für die Cluster-Koordination. Wenn der Cluster in diesem neuen System das Quorum verliert, ist der Cluster erst verfügbar, wenn Sie Maßnahmen ergreifen. Der Verlust des Quorums kann zwei Formen annehmen:

- Wenn Ihr Cluster dedizierte Hauptknoten verwendet, tritt ein Quorum-Verlust auf, wenn die Hälfte oder mehr nicht verfügbar sind.

- Wenn Ihr Cluster keine dedizierten Hauptknoten verwendet, tritt ein Quorum-Verlust auf, wenn die Hälfte oder mehr Ihrer Datenknoten nicht verfügbar sind.

Wenn ein Quorumverlust auftritt und Ihr Cluster mehr als einen Knoten hat, stellt der OpenSearch Dienst das Quorum wieder her und versetzt den Cluster in einen schreibgeschützten Zustand. Sie haben hierfür zwei Möglichkeiten:

- Entfernen Sie den schreibgeschützten Status und verwenden Sie den Cluster wie er ist.
- Stellen Sie den Cluster oder einzelne Indizes aus einem Snapshot wieder her.

Wenn Sie den Cluster vorziehen, wie er ist, überprüfen Sie mit der folgenden Anforderung, ob der Cluster-Zustand grün ist:

```
GET _cat/health?v
```

Wenn der Cluster-Zustand rot ist, empfehlen wir, den Cluster aus einem Snapshot wiederherzustellen. Informationen zur Fehlerbehebung finden Sie auch unter the section called “Roter Cluster-Status”. Wenn der Cluster-Zustand grün ist, überprüfen Sie mit der folgenden Anforderung, ob alle erwarteten Indizes vorhanden sind:

```
GET _cat/indices?v
```

Führen Sie dann einige Suchanfragen aus, um zu überprüfen, ob die erwarteten Daten vorhanden sind. Wenn dies der Fall ist, können Sie den schreibgeschützten Status mithilfe der folgenden Anforderung entfernen:

```
PUT _cluster/settings
{
  "persistent": {
    "cluster.blocks.read_only": false
  }
}
```

Wenn ein Quorumverlust auftritt und Ihr Cluster nur aus einem Knoten besteht, ersetzt OpenSearch Service den Knoten und versetzt den Cluster nicht in einen schreibgeschützten Zustand. Andernfalls sind Ihre Optionen gleich: Verwenden Sie den Cluster unverändert oder stellen Sie ihn aus einem Snapshot wieder her.

In beiden Situationen sendet OpenSearch Service zwei Ereignisse an Ihren. AWS Health Dashboard Das erste informiert Sie über den Verlust des Quorums. Das zweite Ereignis tritt ein, nachdem OpenSearch Service das Quorum erfolgreich wiederhergestellt hat. Weitere Informationen zur Verwendung von finden Sie im AWS Health Benutzerhandbuch. AWS Health Dashboard

Roter Cluster-Status

Ein roter Clusterstatus bedeutet, dass mindestens ein primärer Shard und seine Replikate keinem Knoten zugewiesen sind. OpenSearch Der Dienst versucht weiterhin, automatische Snapshots aller Indizes unabhängig von ihrem Status zu erstellen, aber die Snapshots schlagen fehl, solange der rote Clusterstatus bestehen bleibt.

Die häufigsten Ursachen für einen roten Cluster-Status sind ausgefallene Cluster-Knoten sowie der Absturz des OpenSearch -Prozesses aufgrund einer kontinuierlichen starken Arbeitslast.

> **Note**
>
> OpenSearch Der Service speichert automatische Snapshots unabhängig vom Clusterstatus 14 Tage lang. Wenn der rote Cluster-Status länger als zwei Wochen anhält, wird daher der letzte fehlerfreie automatisierte Snapshot gelöscht und Sie könnten die Daten Ihres Clusters dauerhaft verlieren. Wenn Ihre OpenSearch Service-Domain den Cluster-Status Rot annimmt, kontaktieren Sie Sie Support möglicherweise, um zu fragen, ob Sie das Problem selbst lösen möchten oder ob Sie möchten, dass Ihnen das Support-Team weiterhilft. Sie können einen CloudWatch Alarm einrichten, der Sie benachrichtigt, wenn ein roter Clusterstatus eintritt.

Letztlich führen rote Shards zu roten Clustern; und rote Indizes verursachen rote Shards. OpenSearch Es ist hilfreich APIs, die Indizes zu identifizieren, die den roten Clusterstatus verursachen.

- `GET /_cluster/allocation/explain` wählt den ersten nicht zugewiesenen Shard aus und erklärt, warum er keinem Knoten zugeordnet werden kann:

```
{
    "index": "test4",
    "shard": 0,
    "primary": true,
```

```
    "current_state": "unassigned",
    "can_allocate": "no",
    "allocate_explanation": "cannot allocate because allocation is not permitted to
 any of the nodes"
}
```

- `GET /_cat/indices?v` zeigt den Zustand, die Anzahl der Dokumente und die Festplattennutzung für jeden Index an:

```
health status index            uuid                   pri rep docs.count docs.deleted
 store.size pri.store.size
green  open   test1            30h1EiMvS5uAFr2t5CEVoQ   5   0        820            0
       14mb           14mb
green  open   test2            sdIxs_WDT56afFGu5KPbFQ   1   0          0            0
       233b           233b
green  open   test3            GGRZp_TBRZuSaZpAGk2pmw   1   1          2            0
     14.7kb          7.3kb
red    open   test4            BJxfAErbTtu5HBjIXJV_7A   1   0
green  open   test5            _8C6MIXOSxCqVYicH3jsEA   1   0          7            0
     24.3kb         24.3kb
```

Das Löschen von roten Indizes ist die schnellste Möglichkeit, einen roten Cluster-Status zu beheben. Abhängig vom Grund für den roten Cluster-Status können Sie dann Ihre OpenSearch Service-Domain skalieren, um größere Instance-Typen, mehr Instances oder mehr EBS-basierten Speicher zu verwenden, und versuchen, die problematischen Indizes neu zu erstellen.

Sollte ein fehlerhafter Index nicht löschbar sein, können Sie einen Snapshot wiederherstellen, Dokumente aus dem Index löschen, die Indexeinstellungen ändern, die Anzahl der Replikate verringern oder andere Indizes löschen, um Speicherplatz freizusetzen. Der wichtige Schritt besteht darin, den roten Clusterstatus zu beheben, bevor Sie Ihre Service-Domain neu konfigurieren. OpenSearch Falls eine Domain mit rotem Cluster-Status neu konfiguriert wird, kann sich das Problem verschlimmern und dazu führen, dass die Domain im Konfigurationsstatus Processing (Verarbeitung) verharrt, bis der rote Status behoben ist.

Automatische Behebung von roten Clustern

Wenn der Status Ihres Clusters länger als eine Stunde ununterbrochen rot ist, versucht OpenSearch Service, das Problem automatisch zu beheben, indem nicht zugewiesene Shards umgeleitet oder Daten aus früheren Snapshots wiederhergestellt werden.

Wenn ein oder mehrere rote Indizes nicht repariert werden können und der Clusterstatus insgesamt 14 Tage lang rot bleibt, ergreift OpenSearch Service nur dann weitere Maßnahmen, wenn der Cluster mindestens eines der folgenden Kriterien erfüllt:

- Hat nur eine Availability Zone
- Hat keine dedizierten Hauptknoten
- Enthält Burstable-Instance-Typen (T2 oder T3)

Wenn Ihr Cluster eines dieser Kriterien erfüllt, sendet Ihnen OpenSearch Service in den nächsten 7 Tagen täglich Benachrichtigungen, in denen erklärt wird, dass alle nicht zugewiesenen Shards gelöscht werden, wenn Sie diese Indizes nicht korrigieren. Wenn Ihr Clusterstatus nach 21 Tagen immer noch rot ist, löscht OpenSearch Service die nicht zugewiesenen Shards (Speicher und Rechenleistung) in allen roten Indizes. Für jedes dieser Ereignisse erhalten Sie im Benachrichtigungsbereich der OpenSearch Servicekonsole Benachrichtigungen. Weitere Informationen finden Sie unter the section called “Ereignisse zum Cluster-Zustand”.

Wiederherstellung nach einem kontinuierlich starken Workload

Um zu ermitteln, ob ein roter Cluster-Status durch einen kontinuierlich starken Workload auf einem Datenknoten verursacht wird, überwachen Sie die folgenden Cluster-Metriken.

Relevante Metrik	Beschreibung	Wiederherstellung
JVMMemoryDruck	Gibt den Prozentsatz des Java-Heap an, der für alle Datenknoten in einem Cluster verwendet wird. Zeigen Sie die Statistik Maximum für diese Metrik an und achten Sie auf eine immer kleiner werdende Verringerung der Speicherbelastung, während der Java Garbage Collector keine ausreichende Arbeitsspeichermenge mehr zurückgewinnt. Dieses Muster wird wahrscheinlich durch komplexe Abfragen oder große Datenfelder verursacht.	Legen Sie Arbeitsspeicher-Leistungsschutzschalter für die JVM fest. Weitere Informationen finden Sie unter the section called “JVM OutOfMemoryError”. Wenn das Problem weiterhin besteht, löschen Sie unnötige Indizes, reduzieren Sie die Anzahl oder Komplexität der Anforderungen an die Domain, fügen Sie Instances hinzu oder

Relevante Metrik	Beschreibung	Wiederherstellung
	x86-Instance-Typen verwenden den Garbage Collector „Concurrent Mark Sweep (CMS)“, der zusammen mit Anwendungs-Threads ausgeführt wird, um Pausen kurz zu halten. Wenn CMS während seiner normalen Sammelvorgänge nicht ausreichend Arbeitsspeicher zurückgewinnen kann, löst es eine vollständige Garbage Collection aus, was zu langen Anwendungspausen und Auswirkungen auf die Clusterstabilität führen kann. ARM-basierte Graviton-Instance-Typen verwenden den Garbage-First (G1) Garbage Collector, der CMS ähnlich ist, jedoch zusätzliche kurze Pausen und Heap-Defragmentierung verwendet, um die Notwendigkeit vollständiger Garbage Collections weiter zu reduzieren. In beiden Fällen OpenSearch stürzt der Computer mit einem Fehler wegen unzureichenden Speichers ab, wenn der Speicherverbrauch über das hinausgeht, was der Garbage-Collector während vollständiger Garbage-Collection-Vorgänge zurückgewinnen kann. Bei allen Instance-Typen gilt als Faustregel, die Nutzung unter 80 % zu halten. Die `_nodes/stats/jvm` -API bietet eine hilfreiche Übersicht über	verwenden Sie größere Instance-Typen.

Relevante Metrik	Beschreibung	Wiederherstellung
	die JVM-Statistiken, Speicherpoolnutzung und Garbage Collection-Informationen: `GET domain-endpoint /_nodes/stats/jvm?pretty`	
CPUUtilization	Gibt den Prozentsatz der CPU-Ressourcen an, die für Datenknoten in einem Cluster verwendet werden. Sehen Sie sich die Statistik Maximum für diese Metrik an und suchen Sie nach einem kontinuierlichen Muster für starke Nutzung.	Fügen Sie Datenknoten hinzu oder erhöhen Sie die Größe der Instance-Typen vorhandener Datenknoten.
Knoten	Gibt die Anzahl der Knoten in einem Cluster an. Sehen Sie sich die Statistik Maximum für diese Metrik an. Dieser Wert schwankt, wenn der Service eine neue Flotte an Instances für einen Cluster bereitstellt.	Fügen Sie Datenknoten hinzu.

Gelber Cluster-Status

Ein gelber Cluster-Status bedeutet, dass die primären Shards für alle Indizes zu Knoten in einem Cluster zugewiesen sind, die Replikat-Shards für mindestens einen Index jedoch nicht. Cluster mit einem Knoten werden immer mit einem gelben Clusterstatus initialisiert, da es keinen anderen Knoten gibt, dem der OpenSearch Dienst ein Replikat zuweisen kann. Erhöhen Sie die Knotenanzahl, um einen grünen Cluster-Status zu erreichen. Weitere Informationen finden Sie unter the section called “Größenanpassung von Domains”.

Cluster mit mehreren Knoten können nach dem Erstellen eines neuen Index oder nach einem Knotenausfall kurzzeitig einen gelben Clusterstatus aufweisen. Dieser Status löst sich von selbst auf, wenn Daten im gesamten Cluster OpenSearch repliziert werden. Ein Mangel an Festplattenspeicher

kann auch zu einem gelben Cluster-Status führen; Der Cluster kann Replikat-Shards nur verteilen, wenn die Knoten über ausreichend Speicherplatz verfügen, um sie aufzunehmen.

ClusterBlockException

Unter Umständen erhalten Sie aus folgenden Gründen den Fehler `ClusterBlockException`.

Zu wenig verfügbarer Speicherplatz

Wenn ein oder mehrere Knoten in Ihrem Cluster über Speicherplatz verfügen, der unter dem Mindestwert von 1) 20% des verfügbaren Speicherplatzes oder 2) 20 GiB Speicherplatz liegt, können grundlegende Schreibvorgänge wie das Hinzufügen von Dokumenten und das Erstellen von Indizes fehlschlagen. the section called “Berechnung der Speicheranforderungen”bietet eine Zusammenfassung darüber, wie OpenSearch Service Festplattenspeicher verwendet.

Um Probleme zu vermeiden, sollten Sie die `FreeStorageSpace` Metrik in der OpenSearch Servicekonsole überwachen und CloudWatch Alarme einrichten, die ausgelöst werden, wenn `FreeStorageSpace` ein bestimmter Schwellenwert unterschritten wird. `GET /_cat/allocation?v`bietet außerdem eine nützliche Zusammenfassung der Shard-Zuweisung und der Festplattennutzung. Um Probleme im Zusammenhang mit fehlendem Speicherplatz zu beheben, skalieren Sie Ihre OpenSearch Service-Domain so, dass sie größere Instance-Typen, mehr Instanzen oder mehr EBS-basierten Speicher verwendet.

Hoher JVM-Speicherdruck

Wenn der Messwert JVMMemoryPressure 30 Minuten lang 92% überschreitet, löst OpenSearch Service einen Schutzmechanismus aus und blockiert alle Schreibvorgänge, um zu verhindern, dass der Cluster den roten Status erreicht. Wenn der Schutz aktiviert ist, schlagen Schreibvorgänge mit einem `ClusterBlockException`-Fehler fehl, es können keine neuen Indizes erstellt werden und der Fehler `IndexCreateBlockException` wird ausgegeben.

Wenn der Messwert JVMMemoryPressure fünf Minuten lang wieder 88% oder weniger erreicht, ist der Schutz deaktiviert und Schreibvorgänge in den Cluster werden aufgehoben.

Ein hoher JVM-Speicherdruck kann durch Spitzen in der Anzahl der Anfragen an den Cluster, unausgewogene Shard-Zuweisungen über Knoten hinweg, zu viele Shards in einem Cluster, Felddaten- oder Indexzuordnungsexplosionen oder Instance-Typen, die eingehende Lasten nicht bewältigen können, verursacht werden. Er kann außerdem auch durch die Verwendung von Aggregationen, Platzhaltern oder großen Zeitbereichen in Abfragen verursacht werden.

Um den Datenverkehr zum Cluster zu reduzieren und Probleme mit hohem JVM-Speicherdruck zu beheben, versuchen Sie eine oder mehrere der folgenden Möglichkeiten:

- Skalieren Sie die Domain so, dass die maximale Heap-Größe pro Knoten 32 GB beträgt.
- Reduzieren Sie die Anzahl der Shards, indem Sie alte oder nicht verwendete Indizes löschen.
- Leeren Sie den Datencache mit dem API-Vorgang `POST index-name/_cache/clear?fielddata=true`. Beachten Sie, dass das Löschen des Caches laufende Abfragen beeinträchtigen kann.

Um künftig einen hohen JVM-Speicherbedarf zu vermeiden, sollten Sie sich allgemein an die folgenden bewährten Methoden halten:

- Vermeiden Sie das Aggregieren in Textfeldern oder ändern Sie den Zuordnungstyp für Ihre Indizes in `keyword`.
- Optimieren Sie Such- und Indizierungsanforderungen durch die Auswahl der richtigen Anzahl von Shards.
- Richten Sie Index State Management (ISM)-Richtlinien ein, um nicht verwendete Indizes regelmäßig zu entfernen.

Fehler bei der Migration zu Multi-AZ mit Standby

Die folgenden Probleme können auftreten, wenn Sie eine bestehende Domain zu Multi-AZ mit Standby migrieren.

Erstellen eines Indexes, einer Indexvorlage oder einer ISM-Richtlinie während der Migration von Domänen ohne Standby zu Domänen mit Standby

Wenn Sie bei der Migration einer Domain von Multi-AZ ohne Standby zu mit Standby einen Index erstellen und die Indexvorlage oder ISM-Richtlinie nicht den empfohlenen Richtlinien für das Kopieren von Daten entspricht, kann dies zu Dateninkonsistenzen führen und die Migration kann fehlschlagen. Um diese Situation zu vermeiden, erstellen Sie den neuen Index mit einer Anzahl von Datenkopien (einschließlich primärer Knoten und Replikate), die ein Vielfaches von drei ist. Sie können den Migrationsfortschritt mithilfe der `DescribeDomainChangeProgress` API überprüfen. Wenn Sie auf einen Fehler bei der Anzahl der Replikate stoßen, beheben Sie den Fehler und wenden Sie sich dann an den AWS Support, um die Migration erneut zu versuchen.

Falsche Anzahl von Datenkopien

Wenn Sie nicht über die richtige Anzahl von Datenkopien in Ihrer Domain verfügen, schlägt die Migration zu Multi-AZ mit Standby fehl.

JVM OutOfMemoryError

Ein JVM-`OutOfMemoryError` bedeutet in der Regel, dass einer der folgenden JVM-Leistungsschutzschalter erreicht wurde.

Leistungsschutzschalter	Beschreibung	Eigenschaft der Cluster-Einstellung
Übergeordneter Schalter	Gesamter JVM-Heap-Arbeitsspeicher in Prozent, der für alle Leitungss chutzschalter zulässig ist. Der Standardwert ist 95 %.	`indices.breaker.total.limit`
Felddaten-Schutzschalter	Prozentsatz des JVM-Heap-Arbeitsspeichers, der für das Laden eines einzelnen Datenfelds in den Arbeitsspeicher zulässig ist. Der Standardwert lautet 40%. Wenn Sie Daten mit großen Feldern hochladen, müssen Sie dieses Limit möglicher weise erhöhen.	`indices.breaker.fielddata.limit`
Anforderungs-Schutzschalter	Prozentsatz des JVM-Heap-Arbeitsspeichers, der zulässig ist für Datenstrukturen, die zur Antwort auf eine Serviceanforderung verwendet werden. Der	`indices.breaker.request.limit`

Leistungsschutzschalter	Beschreibung	Eigenschaft der Cluster-Einstellung
	Standardwert lautet 60%. Wenn Ihre Servicean fragen die Berechnung von Aggregationen beinhalte n, müssen Sie dieses Limit möglicherweise erhöhen.	

Fehlgeschlagene Cluster-Knoten

Amazon EC2 Amazon-Instances kann es zu unerwarteten Abbrüchen und Neustarts kommen. In der Regel startet OpenSearch Service die Knoten für Sie neu. Es ist jedoch möglich, dass einer oder mehrere Knoten in einem OpenSearch-Cluster in einem fehlerhaften Zustand bleiben.

Um zu überprüfen, ob dieser Zustand vorliegt, öffnen Sie Ihr Domain-Dashboard in der OpenSearch Servicekonsole. Wählen Sie die Registerkarte Clusterzustand und anschließend die Gesamte Knoten-Metrik aus. Überprüfen Sie, ob die gemeldete Anzahl an Knoten geringer ist als die Anzahl, die Sie für Ihren Cluster konfiguriert haben. Wenn die Metrik zeigt, dass ein oder mehrere Knoten länger als einen Tag ausgefallen sind, wenden Sie sich bitte an den AWS -Support.

Sie können auch einen CloudWatch Alarm einrichten, der Sie benachrichtigt, wenn dieses Problem auftritt.

> **Note**
>
> Die Knoten-Metrik ist während Änderungen an Ihrer Cluster-Konfiguration und routinemäßigen Wartungen des Services nicht genau. Dieses Verhalten wird erwartet. Die Metrik wird die richtige Anzahl an Cluster-Knoten in Kürze angeben. Weitere Informationen hierzu finden Sie unter the section called “Konfigurationsänderungen”.

Um Ihre Cluster vor unerwarteten Knotenabbrüchen und Neustarts zu schützen, erstellen Sie mindestens ein Replikat für jeden Index in Ihrer OpenSearch Service-Domain.

Maximales Shard-Limit überschritten

OpenSearch sowie 7. x-Versionen von Elasticsearch haben eine Standardeinstellung von nicht mehr als 1.000 Shards pro Knoten. OpenSearch/Elasticsearch gibt einen Fehler aus, wenn eine Anfrage, z. B. die Erstellung eines neuen Indexes, dazu führen würde, dass Sie dieses Limit überschreiten. Wenn dieser Fehler auftritt, haben Sie mehrere Möglichkeiten:

- Fügen Sie dem Cluster weitere Datenknoten hinzu.
- Erhöhen Sie die `_cluster/settings/cluster.max_shards_per_node`-Einstellung.
- Verwenden Sie die _shrink-API, um die Anzahl der Shards auf dem Knoten zu reduzieren.

Domain bleibt im Bearbeitungsstatus hängen

Ihre OpenSearch Service-Domain wechselt in den Status „In Bearbeitung“, wenn sie sich mitten in einer Konfigurationsänderung befindet. Wenn Sie eine Konfigurationsänderung einleiten, ändert sich der Domänenstatus in „In Bearbeitung“, während OpenSearch Service eine neue Umgebung erstellt. In der neuen Umgebung startet der OpenSearch Service einen neuen Satz geeigneter Knoten (z. B. Data, Master oder UltraWarm). Nachdem die Migration abgeschlossen ist, werden die älteren Knoten beendet.

Der Cluster kann im Status „Verarbeitung“ hängen bleiben, wenn eine der folgenden Situationen eintritt:

- Ein neuer Satz von Datenknoten kann nicht gestartet werden.

- Die Shard-Migration auf den neuen Satz von Datenknoten ist nicht erfolgreich.
- Die Validierungsprüfung ist mit Fehlern fehlgeschlagen.

Detaillierte Lösungsschritte für jede dieser Situationen finden Sie unter Warum befindet sich meine Amazon OpenSearch Service-Domain im Status „In Bearbeitung“? .

Niedrige EBS-Burst-Balance

OpenSearch Der Service sendet Ihnen eine Konsolenbenachrichtigung, wenn der EBS-Burst-Saldo auf einem Ihrer General Purpose (SSD) -Volumes unter 70% liegt, und eine Folgebenachrichtigung,

wenn der Saldo unter 20% fällt. Um dieses Problem zu beheben, können Sie entweder Ihren Cluster hochskalieren oder die Lese- und Schreib-IOPS reduzieren, sodass die Burst-Balance gutgeschrieben werden kann. Das Burst-Balance bleibt für Domains mit GP3-Volume-Typen und Domains mit GP2-Volumes mit einer Volume-Größe von über 1.000 GiB bei 0. Weitere Informationen finden Sie unter universelle SSD-Volumes (gp2). Sie können den EBS-Burst-Saldo anhand der `BurstBalance` CloudWatch Metrik überwachen.

Die EBS-Metrik nimmt bei der Größenänderung des Volumens zu

Wenn Sie die Volumengrößen von Amazon Elastic Block Store ändern, stellen Sie möglicherweise einen vorübergehenden Anstieg verschiedener EBS-Metriken wie`Write Throughput`, `Write Throughput Micro burstingDisk Queue Depth`, und `IOPS` fest. Dieses Verhalten ist während der Größenänderung zu erwarten und dauert in der Regel einige Sekunden. Die Dauer kann jedoch je nach der zu ändernden Volumengröße variieren.

Um Latenzprobleme und Ablehnungen von Anfragen zu vermeiden, sollten Sie die Größe des EBS-Volumes nur ändern, wenn der Cluster fehlerfrei ist und der Netzwerkverkehr gering ist.

Prüfungsprotokolle können nicht aktiviert werden

Möglicherweise tritt der folgende Fehler auf, wenn Sie versuchen, die Veröffentlichung von Auditprotokollen über die OpenSearch Servicekonsole zu aktivieren:

Die für die Protokollgruppe CloudWatch Logs angegebene Ressourcenzugriffsrichtlinie gewährt Amazon OpenSearch Service nicht genügend Berechtigungen, um einen Protokollstream zu erstellen. Überprüfen Sie die Ressourcenzugriffsrichtlinie.

Wenn dieser Fehler auftritt, überprüfen Sie, ob das `resource`-Element Ihrer Richtlinie den richtigen Protokollgruppen-ARN enthält. Führen Sie in diesem Fall die folgenden Schritte aus:

1. Warten Sie einige Minuten.
2. Aktualisieren Sie die Seite in Ihrem Webbrowser.
3. Wählen Sie Vorhandene Gruppe auswählen.
4. Wählen Sie für Vorhandene Protokollgruppe die Protokollgruppe aus, die Sie erstellt haben, bevor Sie die Fehlermeldung erhalten.
5. Wählen Sie im Abschnitt Zugriffsrichtlinie die Option Vorhandene Richtlinie auswählen aus.

6. Wählen Sie für Vorhandene Richtlinie die Richtlinie aus, die Sie erstellt haben, bevor Sie die Fehlermeldung erhalten.
7. Wählen Sie Enable (Aktivieren) aus.

Wenn der Fehler nach mehrmaligem Wiederholen des Vorgangs weiterhin besteht, wenden Sie sich an den AWS -Support.

Schließen des Indexes nicht möglich

OpenSearch Der Service unterstützt die `_close`API nur für OpenSearch Elasticsearch-Versionen 7.4 und höher. Wenn Sie eine ältere Version verwenden und einen Index aus einem Snapshot wiederherstellen, können Sie den vorhandenen Index löschen (vor oder nach der erneuten Indizierung).

Prüfungen für Client-Lizenz

Die Standarddistributionen von Logstash und Beats beinhalten eine Prüfung der eigenen Lizenz und können keine Verbindung zur Open-Source-Version von herstellen. OpenSearch Stellen Sie sicher, dass Sie die Apache 2.0 (OSS) -Distributionen dieser Clients mit Service verwenden. OpenSearch

Drosselung anfordern

Wenn Sie dauerhafte `403 Request throttled due to too many requests`- oder `429 Too Many Requests`-Fehler erhalten, sollten Sie eine vertikale Skalierung in Betracht ziehen. Amazon OpenSearch Service drosselt Anfragen, wenn die Nutzlast dazu führen würde, dass die Speichernutzung die maximale Größe des Java-Heaps überschreitet.

SSH im Knoten nicht möglich

Sie können SSH nicht verwenden, um auf einen der Knoten in Ihrem OpenSearch Cluster zuzugreifen, und Sie können Änderungen nicht direkt vornehmen. `opensearch.yml` Verwenden Sie stattdessen die Konsole oder AWS CLI, um Ihre Domain SDKs zu konfigurieren. Sie können mithilfe von OpenSearch REST APIs auch einige Einstellungen auf Clusterebene angeben. Weitere Informationen finden Sie in der Amazon OpenSearch Service API-Referenz undthe section called “Unterstützte Vorgänge”.

Wenn Sie mehr Einblick in die Leistung des Clusters benötigen, können Sie Fehlerprotokolle und langsame Protokolle in CloudWatchveröffentlichen.

Snapshot-Fehler „Nicht gültig für die Speicherklasse des Objekts“

OpenSearch Service-Snapshots unterstützen die Speicherklasse S3 Glacier nicht. Dieser Fehler kann auftreten, wenn Sie versuchen, Snapshots aufzulisten, wenn Ihr S3-Bucket eine Lebenszyklusregel enthält, die einen Übergang der Objekte in die Speicherklasse S3 Glacier bewirkt.

Wenn Sie einen Snapshot aus einem Bucket wiederherstellen müssen, stellen Sie die Objekte aus S3 Glacier wieder her, kopieren Sie die Objekte in einen neuen Bucket und registrieren Sie den neuen Bucket als Snapshot-Repository.

Ungültiger Host-Header

OpenSearch Der Service erfordert, dass die Clients dies `Host` in den Anforderungsheadern angeben. Ein gültiger `Host`-Wert ist der Domain-Endpunkt ohne `https://`, z. B.:

```
Host: search-my-sample-domain-ih2lhn2ew2scurji.us-west-2.es.amazonaws.com
```

Wenn Sie bei einer Anfrage eine `Invalid Host Header` Fehlermeldung erhalten, überprüfen Sie, ob Ihr Client oder Proxy den OpenSearch Service-Domänenendpunkt (und nicht beispielsweise seine IP-Adresse) im `Host` Header enthält.

Ungültiger M3-Instance-Typ

OpenSearch Der Service unterstützt das Hinzufügen oder Ändern von M3-Instances zu bestehenden Domains, auf denen die Elasticsearch-Versionen 6.7 und höher ausgeführt OpenSearch werden, nicht. Sie können weiterhin M3-Instances mit Elasticsearch 6.5 und früher verwenden.

Es wird empfohlen, einen neueren Instance-Typ auszuwählen. Für Domains, die auf Elasticsearch 6.7 oder höher laufen OpenSearch , gelten die folgenden Einschränkungen:

- Wenn Ihre vorhandene Domain keine M3-Instances verwendet, können Sie nicht mehr zu diesen wechseln.
- Wenn Sie eine vorhandene Domain von einem M3-Instance-Typ in einen anderen Instance-Typ ändern, können Sie nicht zurückwechseln.

Hot Queries funktionieren nach der Aktivierung nicht mehr UltraWarm

Wenn Sie die Option für eine Domäne aktivieren und die `search.max_buckets` Einstellung nicht bereits außer Kraft gesetzt wurde, legt OpenSearch Service den Wert automatisch UltraWarm auf fest, um `10000` zu verhindern, dass speicherintensive Abfragen warme Knoten überlasten. Wenn Ihre Hot-Abfragen mehr als 10.000 Buckets verwenden, funktionieren sie möglicherweise nicht mehr, wenn Sie sie aktivieren. UltraWarm

Da Sie diese Einstellung aufgrund des verwalteten Charakters von Amazon OpenSearch Service nicht ändern können, müssen Sie einen Support-Fall eröffnen, um das Limit zu erhöhen. Limiterhöhungen erfordern kein Premium-Support-Abonnement.

Nach einem Upgrade ist kein Downgrade möglich

Direkte Upgrades können nicht mehr rückgängig gemacht werden. Wenn Sie sich jedoch an den AWS Support wenden, können die Mitarbeiter Ihnen helfen, den automatischen Pre-Upgrade-Snapshot auf einer neuen Domain wiederherzustellen. Wenn Sie beispielsweise eine Domain von Elasticsearch 5.6 auf 6.4 aktualisieren, kann der AWS Support Ihnen helfen, den Snapshot vor dem Upgrade auf einer neuen Elasticsearch 5.6-Domain wiederherzustellen. Wenn Sie einen manuellen Snapshot der ursprünglichen Domain erstellen würden, könnten Sie diesen Schritt selbst ausführen.

Erforderliche Zusammenfassung der Domains für alle AWS-Regionen

Das folgende Skript verwendet den AWS CLI Amazon-Befehl EC2 describe-regions, um eine Liste aller Regionen zu erstellen, in denen der OpenSearch Service verfügbar sein könnte. Dann ruft es list-domain-namesfür jede Region auf:

```
for region in `aws ec2 describe-regions --output text | cut -f4`
do
    echo "\nListing domains in region '$region':"
    aws opensearch list-domain-names --region $region --query 'DomainNames'
done
```

Sie erhalten die folgende Ausgabe für jede Region:

```
Listing domains in region:'us-west-2'...
[
  {
    "DomainName": "sample-domain"
  }
]
```

Regionen, in denen der OpenSearch Dienst nicht verfügbar ist, geben „Es konnte keine Verbindung zur Endpunkt-URL hergestellt werden“ zurück.

Browserfehler bei der Verwendung von OpenSearch Dashboards

Ihr Browser verpackt Dienstfehlermeldungen in HTTP-Antwortobjekten, wenn Sie Dashboards verwenden, um Daten in Ihrer OpenSearch Service-Domain anzuzeigen. Sie können die gängigen Entwickler-Tools in Web-Browsern, wie den Entwicklermodus in Chrome, verwenden, um die zugrundeliegenden Servicefehler anzuzeigen und Ihre Debugging-Bemühungen zu unterstützen.

So zeigen Sie Servicefehler in Chrome an

1. Wählen Sie im Menü Anzeigen, Entwickler, Entwickler-Tools aus.
2. Wählen Sie die Registerkarte Network (Netzwerk) aus.
3. Wählen Sie in der Spalte Status eine beliebige HTTP-Sitzung mit dem Status 500 aus.

So zeigen Sie Servicefehler in Firefox an

1. Wählen Sie im Menü Tools, Web Developer (Web-Entwickler), Network (Netzwerk) aus.
2. Wählen Sie eine HTTP-Sitzung mit dem Status 500.
3. Wählen Sie die Registerkarte Response (Antwort) aus, um die Serviceantwort anzuzeigen.

Knoten-Shard und Speicherversatz

Knoten-Shard-Versatz liegt vor, wenn ein oder mehrere Knoten innerhalb eines Clusters deutlich mehr Shards als die anderen Knoten haben. Knoten-Speicherversatz liegt vor, wenn ein oder mehrere Knoten innerhalb eines Clusters deutlich mehr Speicher (`disk.indices`) haben als die anderen Knoten. Während diese beiden Bedingungen vorübergehend auftreten können, z. B. wenn eine Domain einen Knoten ersetzt hat und ihm immer noch Shards zuweist, sollten Sie sie beheben, wenn sie bestehen bleiben.

Um beide Arten von Versatz zu erkennen, führen Sie den API-Vorgang _cat/allocation aus und vergleichen Sie die Einträge `shards` und `disk.indices` in der Antwort:

```
shards    | disk.indices  | disk.used  | disk.avail   | disk.total   | disk.percent |
host     | ip       | node
   264    |      465.3mb  |   229.9mb  |      1.4tb   |      1.5tb   |            0 |
 x.x.x.x  | x.x.x.x  | node1
   115    |        7.9mb  |    83.7mb  |     49.1gb   |     49.2gb   |            0 |
x.x.x.x  | x.x.x.x  | node2
   264    |      465.3mb  |   235.3mb  |      1.4tb   |      1.5tb   |            0 |
 x.x.x.x  | x.x.x.x  | node3
   116    |        7.9mb  |    82.8mb  |     49.1gb   |     49.2gb   |            0 |
x.x.x.x  | x.x.x.x  | node4
   115    |        8.4mb  |      85mb  |     49.1gb   |     49.2gb   |            0 |
x.x.x.x  | x.x.x.x  | node5
```

Während ein gewisser Speicherversatz normal ist, ist alles über 10 % des Durchschnitts signifikant. Wenn die Shard-Verteilung verzerrt ist, kann die Nutzung der CPU-, Netzwerk- und Festplattenbandbreite ebenfalls verzerrt werden. Da mehr Daten im Allgemeinen mehr Indizierungs- und Suchvorgänge bedeuten, sind die schwersten Knoten in der Regel auch die Knoten mit der höchsten Ressourcenbelastung, während die leichteren Knoten eine nicht ausgelastete Kapazität darstellen.

Abhilfe: Verwenden Sie Shard-Zählungen, die ein Vielfaches der Datenknotenanzahl sind, um sicherzustellen, dass jeder Index gleichmäßig über die Datenknoten verteilt wird.

Index-Shard und Speicherversatz

Index-Shard-Versatz liegt vor, wenn ein oder mehrere Knoten mehr Shards eines Index enthalten als die anderen Knoten. Index-Speicher-Versatz liegt vor, wenn ein oder mehrere Knoten eine unverhältnismäßig große Menge des Gesamtspeichers eines Index halten.

Indexversatz ist schwieriger zu erkennen als Knoten-Versatz, da er eine gewisse Manipulation der _cat/shards-API-Ausgabe erfordert. Untersuchen Sie den Indexversatz, wenn es Anzeichen für einen Versatz in den Cluster- oder Knotenmetriken gibt. Im Folgenden finden Sie häufige Anzeichen für Indexversatz:

- HTTP-429-Fehler, die auf einer Teilmenge von Datenknoten auftreten
- Ungleiche Index- oder Suchoperationen-Warteschlangen auf den Datenknoten

- Ungleichmäßige and/or CPU-Auslastung des JVM-Heaps über Datenknoten hinweg

Abhilfe: Verwenden Sie Shard-Zählungen, die ein Vielfaches der Datenknotenanzahl sind, um sicherzustellen, dass jeder Index gleichmäßig über die Datenknoten verteilt wird. Wenn Sie immer noch eine Verschiebung des Indexspeichers oder der Shards feststellen, müssen Sie möglicherweise eine Shard-Neuzuweisung erzwingen, die bei jeder Blau/Grün-Bereitstellung Ihrer Service-Domain erfolgt. OpenSearch

Unautorisierte Operation nach dem Auswählen des VPC-Zugriffs

Wenn Sie mit der OpenSearch Service-Konsole eine neue Domain erstellen, haben Sie die Möglichkeit, VPC oder Public Access auszuwählen. Wenn Sie VPC-Zugriff wählen, fragt der OpenSearch Service nach VPC-Informationen ab und schlägt fehl, wenn Sie nicht über die entsprechenden Berechtigungen verfügen:

```
You are not authorized to perform this operation. (Service: AmazonEC2; Status Code:
 403; Error Code: UnauthorizedOperation
```

Damit diese Abfrage durchgeführt werden kann, benötigen Sie Zugriff auf die Operationen `ec2:DescribeVpcs`, `ec2:DescribeSubnets` und `ec2:DescribeSecurityGroups`. Diese Voraussetzung gilt nur für die Konsole. Wenn Sie die AWS CLI verwenden, um eine Domain mit einem VPC-Endpunkt zu erstellen und zu konfigurieren, benötigen Sie keinen Zugriff auf diese Operationen.

Hängenbleiben im Status "Loading" nach dem Erstellen von VPC-Domains

Es kann vorkommen, dass der Configuration state (Konfigurationsstatus) einer neu erstellten Domain mit VPC-Zugriff dauerhaft Loading bleibt. Wenn dieses Problem auftritt, haben Sie wahrscheinlich AWS Security Token Service (AWS STS) für Ihre Region deaktiviert.

Um VPC-Endpoints zu Ihrer VPC hinzuzufügen, muss OpenSearch Service die Rolle übernehmen. `AWSServiceRoleForAmazonOpenSearchService` Daher AWS STS muss aktiviert sein, um neue Domänen zu erstellen, die VPC-Zugriff in einer bestimmten Region verwenden. Weitere Informationen zur Aktivierung und Deaktivierung AWS STS finden Sie im IAM-Benutzerhandbuch.

Abgelehnte Anfragen an die API OpenSearch

Mit der Einführung der Tag-basierten Zugriffskontrolle für die OpenSearch API werden Ihnen möglicherweise Fehler angezeigt, bei denen der Zugriff verweigert wurde, wo Sie zuvor nicht waren. Dies kann daran liegen, dass eine oder mehrere Ihrer Zugriffsrichtlinien `Deny`enthalten, der den Zustand `ResourceTag` verwendet, und diese Bedingungen jetzt eingehalten werden.

Beispielsweise die folgende Richtlinie zum Verweigern des Zugriffs auf die Aktion `CreateDomain` der Konfigurations-API, wenn die Domain das Tag `environment=production` hatte. Obwohl die Aktionsliste auch `ESHttpPut` enthält, traf die Verweigerungserklärung nicht für diese oder andere `ESHttp*`-Aktionen zu.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": [
      "es:CreateDomain",
      "es:ESHttpPut"
    ],
    "Effect": "Deny",
    "Resource": "*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:ResourceTag/environment": [
          "production"
        ]
      }
    }
  }]
}
```

Mit der zusätzlichen Unterstützung von Tags für OpenSearch HTTP-Methoden führt eine identitätsbasierte IAM-Richtlinie wie die oben beschriebene dazu, dass dem verbundenen Benutzer der Zugriff auf die Aktion verweigert wird. `ESHttpPut` Zuvor hätte der angehängte Benutzer in Ermangelung einer Tag-Validierung weiterhin PUT-Anfragen senden können.

Wenn Sie nach dem Aktualisieren Ihrer Domains auf die Service-Software R20220323 oder höher Fehler beim Zugriff feststellen, überprüfen Sie Ihre identitätsbasierten Zugriffsrichtlinien, um festzustellen, ob dies der Fall ist, und aktualisieren Sie sie gegebenenfalls, um den Zugriff zu ermöglichen.

Verbindung von Alpine Linux kann nicht hergestellt werden

Alpine Linux begrenzt die DNS-Antwortgröße auf 512 Byte. Wenn Sie versuchen, von Alpine Linux Version 3.18.0 oder niedriger aus eine Verbindung zu Ihrer OpenSearch Service-Domain herzustellen, kann die DNS-Auflösung fehlschlagen, wenn sich die Domain in einer VPC befindet und mehr als 20 Knoten hat. Wenn Sie eine Alpine Linux-Version verwenden, die höher als 3.18.0 ist, sollten Sie in der Lage sein, mehr als 20 Hosts aufzulösen. Weitere Informationen finden Sie in den Versionshinweisen zu Alpine Linux 3.18.0.

Wenn sich Ihre Domain in einer VPC befindet, empfehlen wir, andere Linux-Distributionen wie Debian, Ubuntu, CentOS, Red Hat Enterprise Linux oder Amazon Linux 2 zu verwenden, um eine Verbindung herzustellen.

Zu viele Anfragen für Search Backpressure

Bei der CPU-basierten Zugangskontrolle handelt es sich um einen Gatekeeping-Mechanismus, der die Anzahl der Anfragen an einen Knoten auf der Grundlage seiner aktuellen Kapazität proaktiv begrenzt, sowohl bei organischem Anstieg als auch bei Verkehrsspitzen. Übermäßige Anfragen geben bei Ablehnung den HTTP-Statuscode 429 „Zu viele Anfragen“ zurück. Dieser Fehler weist entweder auf unzureichende Clusterressourcen, ressourcenintensive Suchanfragen oder einen unbeabsichtigten Anstieg der Arbeitslast hin.

Der Such-Backpressure liefert den Grund für die Ablehnung, was bei der Feinabstimmung ressourcenintensiver Suchanfragen helfen kann. Bei Datenverkehrsspitzen empfehlen wir clientseitige Wiederholungen mit exponentiellem Backoff und Jitter.

Zertifikatsfehler bei der Verwendung von SDKs

Da AWS SDKs Sie die CA-Zertifikate von Ihrem Computer verwenden, können Änderungen an den Zertifikaten auf den AWS Servern zu Verbindungsfehlern führen, wenn Sie versuchen, ein SDK zu verwenden. Fehlermeldungen variieren, enthalten aber in der Regel den folgenden Text:

```
Failed to query OpenSearch
...
SSL3_GET_SERVER_CERTIFICATE:certificate verify failed
```

Sie können diese Fehler verhindern, indem Sie die CA-Zertifikate und das Betriebssystem Ihres Computers beibehalten up-to-date. Wenn dieses Problem in einer Unternehmensumgebung auftritt und Sie Ihren eigenen Computer nicht selbst verwalten, müssen Sie möglicherweise einen Administrator bitten, bei der Aktualisierung zu helfen.

Die folgende Liste zeigt die Mindestanforderungen an Betriebssystem- und Java-Versionen:

- Microsoft Windows-Versionen, auf denen Updates vom Januar 2005 oder später installiert sind, enthalten mindestens eines der erforderlichen Updates CAs in ihrer Vertrauensliste.
- Mac OS X 10.4 mit Java für Mac OS X 10.4 Release 5 (Februar 2007), Mac OS X 10.5 (Oktober 2007) und spätere Versionen enthalten mindestens eines der erforderlichen Versionen CAs in ihrer Vertrauensliste.
- Red Hat Enterprise Linux 5 (März 2007), 6 und 7 sowie CentOS 5, 6 und 7 enthalten alle mindestens eine der erforderlichen Komponenten CAs in ihrer standardmäßigen Liste vertrauenswürdiger Zertifizierungsstellen.
- Java 1.4.2_12 (Mai 2006), 5 Update 2 (März 2005) und alle späteren Versionen, einschließlich Java 6 (Dezember 2006), 7 und 8, enthalten mindestens eine der erforderlichen Versionen CAs in ihrer standardmäßigen Liste vertrauenswürdiger Zertifizierungsstellen.

Die drei Zertifizierungsstellen sind:

- Amazon Root CA 1
- Starfield Services Root Certificate Authority – G2
- Starfield Class 2 Certification Authority

Stammzertifikate der ersten beiden Behörden sind bei Amazon Trust Services erhältlich, aber up-to-date es ist einfacher, Ihren Computer zu behalten. Weitere Informationen über von ACM bereitgestellte Zertifikate finden Sie unter. AWS Certificate Manager FAQs

> **Note**
>
> Derzeit verwenden OpenSearch Dienstdomänen in der Region US-East-1 Zertifikate von einer anderen Behörde. Wir planen die Aktualisierung der Region zur Verwendung dieser neuen Zertifikatsstellen in naher Zukunft.

Die Installation eines benutzerdefinierten Plugins schlägt aufgrund der Versionskompatibilität fehl

Problem: Die Plugin-Installation ist aufgrund eines Versionskonflikts zwischen dem Plugin und der laufenden OpenSearch Instanz fehlgeschlagen. Das System gibt den folgenden Fehler zurück:

```
PluginValidationFailureReason : The provided plugin could not be loaded.
```

Ursache: Das Plugin wurde für OpenSearch $ kompiliert*{MAJOR}*. $*{MINOR}.{PATCH}*, aber in Ihrer Umgebung läuft OpenSearch $*{MAJOR}*. $ *{MINOR}* .0. OpenSearch erfordert aus Stabilitäts- und Sicherheitsgründen eine exakte Versionsübereinstimmung zwischen den Plugins und der OpenSearch Kerninstallation.

Mögliche Lösung: Erstellen Sie das Plugin mit OpenSearch Version $*{MAJOR}*. $ *{MINOR}* .0, um Ihrer Cluster-Version zu entsprechen.

Um die Version von zu überprüfen und zu aktualisieren OpenSearch

1. Verwenden Sie die API oder das Dashboard Ihres Clusters, um den folgenden Befehl auszuführen. Ersetzen Sie *default placeholder values* durch Ihre Informationen.

   API-Anfrage:

   ```
   curl -X GET your-opensearch-endpoint/
   ```

   Dev Tools-Konsole im Dashboard:

   ```
   GET /
   ```

   Der Befehl gibt Informationen im folgenden Format zurück.

```
{
  "name": "node-id",
  "cluster_name": "account-id:domain-name",
  "cluster_uuid": "cluster-uuid",
  "version": {
    "distribution": "opensearch",
    "number": "2.17.0",
    "build_type": "tar",
    "build_hash": "unknown",
    "build_date": "2024-12-17T11:00:09.799828091Z",
    "build_snapshot": false,
    "lucene_version": "9.11.1",
    "minimum_wire_compatibility_version": "7.10.0",
    "minimum_index_compatibility_version": "7.0.0"
  },
  "tagline": "The OpenSearch Project: https://opensearch.org/"
}
```

2. Wenn die Versionsnummer nicht $ ist*{MAJOR}*. $ *{MINOR}* .0, erstellen Sie das Plugin neu, indem Sie wie folgt vorgehen:

   a. Aktualisieren Sie die Plugins, `descriptor.properties` um Version $ *{MAJOR}* anzugeben. $ *{MINOR}* .0.

   b. Erstellen Sie das Plugin mit dem Befehl für Ihren Projekttyp neu.

   c. Führen Sie den Befehl update-package mit der neu erstellten Datei aus `.zip`.

   d. Führen Sie den Befehl associate-package aus, um die neueste Plugin-Version zuzuordnen, die erstellt wurde, als Sie den `update-package` Befehl im vorherigen Schritt ausgeführt haben.

Dokumentenverlauf für Amazon OpenSearch Service

In diesem Thema werden wichtige Änderungen an Amazon OpenSearch Service beschrieben. Service-Software-Updates bieten zusätzlich Unterstützung für neue Funktionen, Sicherheits-Patches, Fehlerbehebungen und andere Verbesserungen. Um neue Funktionen zu verwenden, müssen Sie möglicherweise die Service-Software in Ihrer Domain aktualisieren. Weitere Informationen finden Sie unter the section called “Service-Software-Updates”.

Servicefunktionen werden schrittweise dort eingeführt, AWS-Regionen wo ein Service verfügbar ist. Wir aktualisieren diese Dokumentation nur für die erste Version. Wir stellen keine Informationen über die Verfügbarkeit von Regionen zur Verfügung und kündigen auch keine späteren Rollouts von Regionen an. Informationen zur regionalen Verfügbarkeit von Servicefunktionen und zum Abonnieren von Benachrichtigungen über Updates finden Sie unter Was gibt's Neues bei AWS?

Um Benachrichtigungen über Updates zu erhalten, können Sie den RSS-Feed abonnieren.

> **Note**
>
> Patch-Versionen: Bei Service-Softwareversionen, die mit „-P“ und einer Zahl wie R20211203-P4 enden, handelt es sich um Patch-Versionen. Patches werden vermutlich Leistungsverbesserungen, kleinere Bugfixes und Behebungen von Sicherheitslücken oder Verbesserungen der Sicherheitslage beinhalten. Da Patches keine neuen Funktionen oder bahnbrechenden Änderungen enthalten, haben sie in der Regel keine direkten Auswirkungen auf die Benutzer oder die Dokumentation, weshalb die Einzelheiten der einzelnen Patches nicht in diesem Dokumentverlauf enthalten sind.

Änderung	Beschreibung	Datum
Neues Thema: Atlassian -Integration mit Ingestion OpenSearch	Du kannst jetzt Amazon OpenSearch Ingestion-Pipelines verwenden, um Daten aus Atlassian Jira- und Confluence-Diensten zu verarbeiten. Diese Integrati on ermöglicht es Ihnen, eine einheitliche, durchsuch	5. Juni 2025

	bare Wissensdatenbank zu erstellen, indem Sie komplette Jira-Projekte und Confluenc e-Bereiche synchronisieren. OpenSearch Die Integration gewährleistet die Relevanz in Echtzeit durch kontinuierliche Überwachung und automatis che Synchronisation von Updates und bietet gleichzei tig flexible Filteroptionen für bestimmte Projekte, Problemty pen und Inhalte. Weitere Informationen findest du unter Eine OpenSearch Ingestion-Pipeline mit Atlassian Services verwenden.

Benutzerdefiniertes Plugin-Management mit dem AWS CLI	Sie können jetzt benutzerdefinierte Plugins für Amazon OpenSearch Service mit dem verwalten AWS CLI. Mit dieser Funktion können Sie benutzerdefinierte Plugins über einen optimierten Befehlszeilen-Workflow installieren, aktualisieren, sichern und deinstallieren. Sie können Ihre Plugins auch mit AWS KMS Schlüsseln sichern und Plugin-Upgrades verwalten, wenn Sie auf neuere Versionen von aktualisieren. OpenSearch Weitere Informationen finden Sie unter Verwaltung benutzerdefinierter Plug-ins mithilfe der AWS CLI und Amazon OpenSearch Service Custom Package AWS KMS Integration	27. Mai 2025
Support für OpenSearch 2.18 und 2.19	Amazon OpenSearch Service unterstützt die OpenSearch Versionen 2.18 und 2.19. Weitere Informationen finden Sie in den Versionshinweisen zu OpenSearch 2.19 und 2.18. Informationen zu den Vorgängen OpenSearch 2.18 und 2.19 finden Sie in der OpenSearch REST-API-Referenz oder in der API-Referenz für das jeweilige Plugin.	30. April 2025

Neue Unterstützung für die Angabe von Pipeline-Rollen in OpenSearch Ingestion	Wenn Sie eine Pipeline in Amazon OpenSearch Ingestion erstellen oder aktualisieren, müssen Sie in einer Pipeline-Konfiguration im YAML-Format keine Pipeline-Rolle mehr angeben. Stattdessen geben Sie in der Konsole die Rolle in einem neuen Pipeline-Rollenfeld an. Wenn Sie den verwenden AWS CLI, verwenden Sie einen neuen `--pipeline-role-arn` Parameter. Weitere Informationen finden Sie unter den folgenden Themen: • Rollen und Benutzer in Amazon OpenSearch Ingestion einrichten • Amazon OpenSearch Ingestion-Pipelines erstellen • Tutorial: Daten mithilfe von Amazon OpenSearch Ingestion in eine Domain aufnehmen • Tutorial: Daten mit Amazon OpenSearch Ingestion in eine Sammlung aufnehmen • CreatePipeline • UpdatePipeline	22. April 2025

Neues Thema	Das Thema zur Fehlerbehebung schlägt bei der Installation benutzerdefinierter Plug-ins aufgrund der Versionskompatibilität fehl. Hier finden Sie die Schritte, die Sie ergreifen müssen, wenn der Fehler auftritt`PluginValidationFailureReason : The provided plugin could not be loaded` . Dieser Fehler ist in der Regel das Ergebnis eines Versionskonflikts zwischen dem Plugin und der laufenden OpenSearch Instanz.	21. April 2025
Neue Funktion: OpenSearch UI-Kompatibilität mit clusterübergreifender Suche	OpenSearch Die Benutzeroberfläche ist jetzt mit der clusterübergreifenden Suche kompatibel. Auf diese Weise können Sie die OpenSearch Benutzeroberfläche in einer Region verwenden AWS-Region , um auf Cluster in einer anderen Region zuzugreifen. Dazu wird es als Remote-Cluster konfiguriert, der mit einem Cluster in derselben Region verbunden ist. Weitere Informationen finden Sie unter Regions- und kontoübergreifender Datenzugriff mit clusterübergreifender Suche.	16. April 2025

Überarbeiteter Inhalt: „Verwenden der OpenSearch Benutzeroberfläche in Amazon OpenSearch Service“	Wir haben das Kapitel OpenSearch Using UI in Amazon OpenSearch Service überarbeitet und erweitert , einschließlich erweiterter Verfahren, zusätzlicher Einrichtungsdetails und einer neuen Versionshistorie des Amazon OpenSearch Service-Supports für OpenSearch UI.	15. April 2025
Amazon Q Developer für Amazon OpenSearch Service	Die Amazon Q-Integration mit Amazon OpenSearch Service bietet die folgenden generativen Funktionen: • Generieren Sie Visualisierungen in natürlicher Sprache • Sehen Sie sich Zusammenfassungen und Einblicke in Warnmeldungen an • Sehen Sie sich die von Amazon Q generierten Zusammenfassungen der Abfrageergebnisse auf der Discover-Seite an • Sehen Sie sich die empfohlenen Anomaliedetektoren an • Greifen Sie für OpenSearch verwandte Fragen auf den Amazon Q-Chat zu	31. März 2025

Die AmazonOpenSearchServiceRolePolicy verwaltete Richtlinie wurde aktualisiert	Die Richtlinie ermöglicht OpenSearch die Aktualisierung des Zugriffsbereichs jeder AWS IAM Identity Center Anwendung, die nur von verwaltet wird OpenSearch.	28. März 2025
OR2 und OM2 Instances für Amazon OpenSearch Service	Amazon OpenSearch Service unterstützt jetzt OR2 OM2 AD-Instances. In internen Benchmarks OR2 wurde ein um bis zu 26% besserer Indexierungsdurchsatz als bei R7 OR1 und um 70% gegenüber R7 festgestellt. OM2 zeigte bis zu 15% mehr als OR1 und 66% mehr als M7g.	25. März 2025
Direkte Abfrage für CloudWatch Logs und Security Lake	Amazon OpenSearch Service unterstützt jetzt direkte Abfragen zur Abfrage von Daten in CloudWatch Logs und Security Lake.	01. Dezember 2024
k-NN-Indizes	Ab OpenSearch Version 2.17 können Sie k-NN-Indizes auf die Stufen und Cold Storage verschieben. UltraWarm	13. November 2024

OpenSearch 2.17-Unterstützung	Amazon OpenSearch Service unterstützt jetzt OpenSearch Version 2.17. Diese Version enthält alle Funktionen, die Teil der Versionen 2.16 und 2.17 waren. Weitere Informationen finden Sie in den Versionshinweisen zu 2.16 und 2.17.	13. November 2024
OpenSearch 2.15-Unterstützung	Amazon OpenSearch Service unterstützt jetzt OpenSearch Version 2.15. Diese Version enthält alle Funktionen, die Teil der Versionen 2.14 und 2.15 waren. Weitere Informationen finden Sie in den Versionshinweisen zu 2.14 und 2.15.	11. Oktober 2024
Neue serviceverknüpfte Rolle	Amazon OpenSearch Service fügt eine servicebezogene Rolle namens hinzu`AWSServiceRoleForOpensearchIngestionSelfManagedVpce` , die es Amazon OpenSearch Ingestion ermöglicht, Metrikdaten an Amazon CloudWatch für Pipelines mit selbstverwalteten VPC-Endpunkten zu senden.	12. Juni 2024

Direkte Anfragen	Amazon OpenSearch Service unterstützt jetzt das direkte Ausführen von Abfragen auf Daten, die in Amazon S3 gespeichert sind, ohne dass die Daten in einen OpenSearch Index aufgenommen werden müssen.	22. Mai 2024
OpenSearch 2.13-Unterstützung	Amazon OpenSearch Service unterstützt jetzt OpenSearch Version 2.13. Diese Version enthält alle Funktionen, die Teil der Versionen 2.12 und 2.13 waren. Weitere Informationen finden Sie in den Versionshinweisen zu 2.12 und 2.13.	21. Mai 2024
Amazon OpenSearch Ingestion-Unterstützung für Data Prepper Version 2.7	Amazon OpenSearch Ingestion fügt Unterstützung für Data Prepper Version 2.7 hinzu. Weitere Informationen finden Sie in den Versionshinweisen zu 2.7.	4. April 2024
AWS-Service privater Zugriff für OpenSearch serverlose Sammlungen	Sie können jetzt im Rahmen einer Netzwerkzugriffsrichtlinie bestimmten AWS-Services Zugriff auf Ihre OpenSearch serverlosen Sammlungen gewähren, z. B. Amazon Bedrock.	28. März 2024

Direkte EBS-Updates	Sie können jetzt einige EBS-Änderungen an Ihren Domains vornehmen, ohne dass eine blaue/grüne Bereitstellung in Amazon OpenSearch Service erfolgt.	14. Februar 2024
Sichtbarkeit von Konfigurationsänderungen	Sie können jetzt Änderungen an der Domain-Konfiguration in der Amazon OpenSearch Service-Konsole und mithilfe der Konfigurations-API verfolgen.	6. Februar 2024
Allgemeine Verfügbarkeit von Sammlungen mit Vektorsuche	Sammlungen von Amazon OpenSearch Serverless Vector Search sind jetzt allgemein verfügbar. In der Vorschauphase wurden die folgenden bemerkenswerten Verbesserungen vorgenommen: • Vektorsuchsammlungen unterstützen jetzt Workloads mit Milliarden von Vektoren mit jeweils bis zu 128 Dimensionen. • OpenSearch Dashboards unterstützen jetzt Vektorsuchsammlungen.	29. November 2023
OR1 -Instances	Amazon OpenSearch Service unterstützt jetzt OR1 Instance-Typen.	29. November 2023

Direkte Abfragen mit Amazon S3 (Vorschau)	Direkte Abfragen bieten eine vollständig verwaltete Lösung, um Transaktionsdaten innerhalb von Sekunden nach dem Schreiben in einen Amazon S3-Bucket in Amazon OpenSearch Service verfügbar zu machen.	29. November 2023
Kapazität von 10 TiB für Zeitreihenerfassungen	Amazon OpenSearch Serverless bietet Unterstützung für bis zu 10 TiB Indexdaten für Zeitreihenerfassungen. Diese Version unterstützt außerdem eine maximal zulässige Kapazität von 200 OCUs für alle Arten von Sammlungen und die Möglichkeit, Standby-Replikate zu deaktivieren, wenn Sie eine Sammlung erstellen.	29. November 2023
OpenSearch 2.11-Unterstützung	Amazon OpenSearch Service unterstützt jetzt OpenSearch Version 2.11. Diese Version enthält alle Funktionen, die Teil der Versionen 2.10 und 2.11 waren. Weitere Informationen finden Sie in den Versionshinweisen zu 2.10 und 2.11.	17. November 2023

Amazon OpenSearch Ingestion-Unterstützung für Data Prepper Version 2.6	Amazon OpenSearch Ingestion fügt Unterstützung für Data Prepper Version 2.6 hinzu. Weitere Informationen finden Sie in den Versionshinweisen zu 2.6. Darüber hinaus können Sie Amazon DynamoDB als Pipeline-Quelle angeben. Weitere Informationen finden Sie unter Verwenden einer OpenSearch Ingestion-Pipeline mit Amazon DynamoDB.	17. November 2023
Amazon OpenSearch Ingestion-Unterstützung für Data Prepper Version 2.5	Amazon OpenSearch Ingestion fügt Unterstützung für Data Prepper Version 2.5 hinzu. Weitere Informationen finden Sie in den Versionshinweisen zu 2.5. Darüber hinaus können Sie jetzt eine OpenSearch Dienstdomäne oder eine OpenSearch Serverless-Sammlung als Pipeline-Quelle angeben. Weitere Informationen finden Sie im OpenSearch Quell-Plug-In in der Data Prepper-Dokumentation.	17. November 2023

CloudFormation Vorlage für Ferninferenz	Um die Einrichtung von Remote-Inferenzen für die semantische Suche zu vereinfachen, stellt Amazon OpenSearch Service in der Konsole eine AWS CloudFormation Vorlage bereit, die den Prozess der Modellbereitstellung für Sie automatisiert.	7. November 2023
Aktualisierung der Richtlinie für dienstbezogene Rollen	Fügt die Berechtigungen hinzu, die für die Richtlinie für dienstbezogene Rollen zum Zuweisen und Aufheben IPv6 der `AmazonOpenSearchServiceRolePolicy` Zuweisung von Adressen erforderlich sind. Die veraltete Elasticsearch-Richtlinie `AmazonElasticsearchServiceRolePolicy` wurde ebenfalls aktualisiert, um die Abwärtskompatibilität zu gewährleisten.	26. Oktober 2023

Lebenszyklusrichtlinien für Amazon OpenSearch Serverless	Amazon OpenSearch Serverless führt Richtlinien für den Indexlebenszyklus ein, um die Verwaltung der Aufbewahrung und Löschung von Daten zu optimieren. Sie können jetzt eine Konfigura tionsoberfläche in der Konsole verwenden APIs , um Datenaufbewahrungsrichtlini en für Zeitreihenerfassungen festzulegen, sodass Sie keine täglichen Indizes oder Skripts zum Löschen alter Daten erstellen müssen.	25. Oktober 2023
Unterstützung für iM4GN-Ins tanzen	Amazon OpenSearch Service unterstützt jetzt IM4GN-Ins tance-Typen. IM4GN-Ins tances sind für Workloads optimiert, die große Datensätz e verwalten und eine hohe Speicherdichte pro vCPU benötigen.	20. Oktober 2023

Administrative Optionen	Amazon OpenSearch Service bietet jetzt mehrere Verwaltungsoptionen, mit denen Sie detailliert steuern können, ob Sie Probleme mit Ihrer Domain beheben müssen. Zu diesen Optionen gehören die Möglichkeit, den OpenSearch Prozess auf einem Datenknoten neu zu starten, und die Möglichkeit, einen Datenknoten neu zu starten.	17. Oktober 2023
Optionale Plug-ins	Amazon OpenSearch Service bietet Unterstützung für vier neue Sprachanalyse-Plugins: Nori (Koreanisch), Sudachi (Japanisch), Pinyin (Chinesisch) und STConvert Analysis (Chinesisch) sowie das Amazon Personalize Search Ranking-Plugin.	16. Oktober 2023
OpenSearch 2.9-Unterstützung	Amazon OpenSearch Service unterstützt jetzt OpenSearch Version 2.9. Diese Version enthält alle Funktionen, die Teil der Versionen 2.8 und 2.9 waren. Weitere Informationen finden Sie in den Versionshinweisen zu 2.8 und 2.9.	2. Oktober 2023

ML-Steckverbinder	Amazon OpenSearch Service bietet Unterstützung für Machine-Learning-Konnektoren (ML). Konnektoren erleichtern den Zugriff auf ML-Modelle AWS-Services, die auf anderen Plattformen oder auf Plattformen für maschinelles Lernen (ML) von Drittanbietern gehostet werden.	6. September 2023
Amazon OpenSearch Ingestion bietet Unterstützung für Data Prepper Version 2.4	Amazon OpenSearch Ingestion fügt Unterstützung für Data Prepper Version 2.4 hinzu. Weitere Informationen finden Sie in den Versionshinweisen zu 2.4. Darüber hinaus können Sie jetzt Amazon Managed Streaming for Apache Kafka (Amazon MSK) als Pipeline-Quelle angeben.	31. August 2023
Kapazität von 6 TiB für Zeitreihenerfassungen	Amazon OpenSearch Serverless bietet Unterstützung für bis zu 6 TiB Indexdaten für Zeitreihenerfassungen. Diese Version unterstützt außerdem eine maximal zulässige Kapazität von 100 OCUs für Such - und Zeitreihensammlungen.	15. August 2023

Sammlungen für die Vektorsuche	Amazon OpenSearch Serverless bietet die Option, eine Vektorsuchsammlung zu erstellen, in der Sie Vektoreinbettungen speichern können, um Ähnlichkeits- und semantische Suchen zu ermöglichen.	26. Juli 2023
OpenSearch 2.7 Unterstützung	Amazon OpenSearch Service unterstützt jetzt OpenSearch Version 2.7. Diese Version enthält alle Funktionen, die Teil der Versionen 2.6 und 2.7 waren. Weitere Informationen finden Sie in den Versionshinweisen zu 2.6 und 2.7.	10. Juli 2023
Unterstützung für Data Prepper 2.3	Amazon OpenSearch Ingestion fügt Unterstützung für Data Prepper Version 2.3 hinzu. Weitere Informationen finden Sie in den Versionshinweisen zu 2.3. Darüber hinaus können Sie jetzt Amazon Security Lake als Pipeline-Quelle angeben.	26. Juni 2023

Multi-AZ mit Standby	Amazon OpenSearch Service bietet die Option, eine Domain in drei Availability Zones (AZs) bereitzustellen, wobei jede AZ eine vollständige Kopie der Daten enthält und Knoten in einer dieser Zonen als Standby AZs fungieren. Die Bereitstellungsoption Multi-AZ mit Standby bietet eine Verfügbarkeit von 99,99% und eine gleichbleibende Leistung im Falle eines Infrastru kturausfalls.	3. Mai 2023
Neue serviceverknüpfte Rolle	Amazon OpenSearc h Service fügt eine servicebezogene Rolle namens hinzu`AWSServic eRoleForAmazonOpen SearchIngestionSer vice` , an die Amazon OpenSearch Ingestion Metrikdaten senden kann. Amazon CloudWatch	26. April 2023

OpenSearch Einnahme durch Amazon	Amazon OpenSearch Ingestion ist ein vollständig verwalteter Datensammler, der Protokoll- und Ablaufverfolgungsdaten in Echtzeit für OpenSearch Service-Domains und OpenSearch serverlose Sammlungen bereitstellt. OpenSearch Durch die Aufnahme müssen Sie keine Drittanbieterlösungen wie Logstash oder Jaeger verwenden, um Daten in Ihre Domains und Sammlungen aufzunehmen.	26. April 2023
OpenSearch 2.5 Unterstützung	Amazon OpenSearch Service unterstützt jetzt OpenSearch Version 2.5. Diese Version enthält alle Funktionen, die Teil der Versionen 2.4 und 2.5 waren. Weitere Informationen finden Sie in den Versionshinweisen zu 2.4 und 2.5.	13. März 2023

Wartungsfenster außerhalb der Spitzenzeiten	Amazon OpenSearch Service fügt Zeitfenster außerhalb der Spitzenzeiten hinzu, d. h. tägliche 10-Stunden-Zeitblöcke mit geringem Datenverkehr, in denen Service-Software-Updates und Auto-Tune-Optimierungen geplant werden können, für die eine Bereitstellung erforderlich ist. blue/green Updates außerhalb der Spitzenzeiten tragen dazu bei, die Belastung der dedizierten Master-Knoten eines Clusters in Zeiten mit höherem Datenverkehr zu minimieren. Für neue Domains, die nach dem 16. Februar erstellt wurden, wird das Zeitfenster außerhalb der Spitzenzeiten automatisch für die Zeit zwischen 22:00 Uhr und 8:00 Uhr Ortszeit konfiguriert. Für bestehende Domains müssen Sie das Fenster explizit aktivieren.	16. Februar 2023

Konfiguration der SAML-Authentifizierung bei der Domainerstellung	Amazon OpenSearch Service unterstützt jetzt die Konfiguration der SAML-Authentifizierung bei der Domainerstellung. Bisher mussten Sie SAML-Optionen konfigurieren, nachdem die Domain bereits erstellt wurde.	1. Februar 2023
Remote-Neuindizierung für VPC-Domains	Amazon OpenSearch Service fügt die Option für eine VPC-Endpunktverbindung zwischen zwei Domains hinzu. Sie können jetzt Remote-Neuindizierung verwenden, um Indizes ohne Reverse-Proxy von einer VPC-Domain in eine andere zu kopieren. Ihre VPC-Domain muss die Service-Software R20221114 oder höher ausführen, um diese Funktion nutzen zu können.	31. Januar 2023

Allgemeine Verfügbarkeit von Amazon OpenSearch Serverless	Amazon OpenSearch Serverless ist jetzt allgemein verfügbar. In der Vorschaup hase wurden die folgenden bemerkenswerten Verbesser ungen vorgenommen: • Die Kapazität kann jetzt auf das konfigurierte Minimum herunterskaliert werden, OCUs wenn der Verkehr auf dem Sammelendpunkt abnimmt. • Das zulässige Maximum OCUs für Indizierung und Suche wurde von 20 auf 50 erhöht. Jede OCU enthält ausreichend flüchtigen Hot-Speicher für 120 GiB Indexdaten. • Sie können jetzt Datenzugr iffseinstellungen beim Erstellen von Sammlungen konfigurieren, anstatt sie in einem separaten Workflow konfigurieren zu müssen.	25. Januar 2023

Asynchroner Testlauf	Amazon OpenSearch Service unterstützt jetzt den asynchron en Testlauf, mit dem Sie vor einer Konfigurationsände rung eine Validierungsprüfun g durchführen können. Außerdem werden Sie benachrichtigt, wenn Ihre Änderungen zu einer blue/gree n Bereitstellung führen.	19. Januar 2023
Neue serviceverknüpfte Rolle	Amazon OpenSearc h Service fügt eine serviceverknüpfte Rolle namens hinzu`AWSServic eRoleForAmazonOpen SearchServerless` , die es OpenSearch Serverless ermöglicht, Metrikdaten an zu senden. Amazon CloudWatch	29. November 2022
Vorversion von Amazon OpenSearch Serverless	Amazon OpenSearch Serverless ist eine serverlos e On-Demand-Konfigur ation mit auto Skalierung für Amazon OpenSearch Service. Serverless beseitigt die betriebliche Komplexität der Bereitstellung, Konfigura tion und Optimierung Ihrer Cluster. OpenSearch	29. November 2022

OpenSearch 2.3 Unterstützung	Amazon OpenSearch Service unterstützt jetzt OpenSearch Version 2.3. Diese Version enthält alle Funktionen, die Teil der Versionen 2.0, 2.1 und 2.2 waren. Weitere Informationen finden Sie in den Versionshinweisen zu 2.0, 2.1, 2.2 und 2.3. Version 2.3 enthält eine grundlegende Änderung. Weitere Informationen finden Sie unter Unterstützte Upgrade-Pfade.	15. November 2022
Unterstützung für Benachrichtigungs-Plugins	Amazon OpenSearch Service unterstützt jetzt das Notifications-Plugin, das einen zentralen Ort für all Ihre Benachrichtigungen von OpenSearch Plugins bietet. Ab Version 2.0 wurden Warnziele als veraltet eingestuft und durch Benachrichtigungs-Kanäle ersetzt.	15. November 2022

Unterstützung für Kibana 7.1.1	Amazon OpenSearch Service-Domains, auf denen Elasticsearch 7.1 ausgeführt wird, unterstützen jetzt die neueste Patch-Version für Kibana 7.1.1, die Bugfixes hinzufügt und die Sicherheit verbessert. Wenn Sie Ihre 7.1-Domains auf die Service-Software R20221114 aktualisieren, aktualisiert OpenSearch Service sie automatisch auf diese Patch-Version.	15. November 2022
Unterstützung für Kibana 6.8.13	Amazon OpenSearch Service-Domains, auf denen Elasticsearch 6.8 ausgeführt wird, unterstützen jetzt die neueste Patch-Version für Kibana 6.8.13, die Bugfixes hinzufügt und die Sicherheit verbessert. Wenn Sie Ihre 6.8-Domains auf die Service-Software R20221114 aktualisieren, aktualisiert OpenSearch Service sie automatisch auf diese Patch-Version.	15. November 2022

Unterstützung für Kibana 6.3.2	Amazon OpenSearch Service-Domains, auf denen Elasticsearch 6.3 ausgeführt wird, unterstützen jetzt die neueste Patch-Version für Kibana 6.3.2, die Bugfixes hinzufügt und die Sicherheit verbessert. Wenn Sie Ihre 6.3-Domains auf die Service-Software R20221114 aktualisieren, aktualisiert OpenSearch Service sie automatisch auf diese Patch-Version.	15. November 2022

AWS PrivateLink	Mit von Amazon OpenSearch Service verwalteten VPC-Endpunkten können Sie eine direkte Verbindung zu OpenSearch Service-VPC-Domains herstellen, indem Sie einen VPC-Schnittstellen-Endpunkt verwenden, anstatt eine Verbindung über das Internet herzustellen. Auf einen OpenSearch vom Service verwalteten VPC-Endpunkt kann nur innerhalb der VPC zugegriffen werden, in der der Endpunkt bereitgestellt wird, oder von jedem VPCs Peer aus, der mit der VPC verbunden ist, in der der Endpunkt bereitgestellt wird, sofern es die Routing-Tabellen und Sicherheitsgruppen zulassen. Ihre VPC-Domain muss die Service-Software R20220928 oder höher ausführen, um eine Verbindung zu einem Schnittstellen-VPC-Endpunkt herzustellen.	7. November 2022

Fehlerbehebungen und Leistungsverbesserungen	Die Servicesoftware R20220928 enthält Fehlerbehebungen und Leistungsverbesserungen, einschließlich verbesserter SAML-Protokollierung. Das Update ändert auch den Standardmandanten auf `Global` statt auf `Private`.	3. Oktober 2022
Verbesserte API-Referenz	Amazon OpenSearch Service bietet eine verbesserte, umfassende Konfigurations-API-Referenz. Die neuen Referenzen enthalten alle verfügbaren Aktionen und Datentypen, Beispiele für Anforderungs- und Antwortsyntax sowie Links zu den entsprechenden SDK-Verweisen für alle unterstützten Sprachen.	13. September 2022
Blau/Grün-Validierung	Amazon OpenSearch Service führt jetzt vor der blue/green Bereitstellung eine Validierungsprüfung durch und zeigt Validierungsfehler an, wenn Ihre Domain nicht für ein Update in Frage kommt.	16. August 2022
OpenSearch 1.3 Unterstützung	Amazon OpenSearch Service unterstützt jetzt OpenSearch Version 1.3. Weitere Informationen finden Sie unter 1.3 Versionshinweise.	27. Juli 2022

Unterstützung für ML-Commons-Plug-Ins	Amazon OpenSearch Service bietet Unterstützung für das ML Commons-Plugin, das über Transport- und REST-API-Aufrufe eine Reihe gängiger Algorithmen für maschinelles Lernen bereitstellt. Sie können auch über PPL-Befehle mit dem ML-Commons-Plug-In interagieren.	27. Juli 2022
Unterstützung für gp3-Volumes	Amazon OpenSearch Service bietet Unterstützung für den Volumetyp gp3 EBS General Purpose SSD. Sie können zusätzliche bereitgestellte IOPS und Durchsatz angeben, wenn Sie die Domain erstellen oder ändern.	26. Juli 2022
Verbesserte Dokumentation bewährter Methoden	Die Amazon OpenSearch Service-Dokumentation enthält verbesserte betriebliche Best Practices und allgemeine Empfehlungen für die Erstellung und den Betrieb von OpenSearch Service-Domains.	6. Juli 2022
Integration mit Service Quotas	In der Service Quotas-Konsole können Sie jetzt Kontingente für Amazon OpenSearch Service Quotas einsehen und Kontingenterhöhungen beantragen.	29. Juni 2022

Tag-basierte Zugriffskontrolle für die API OpenSearch	Sie können jetzt Tags verwenden, um den Zugriff auf die OpenSearch APIs zu steuern. Bisher konnten Sie nur Tags verwenden, um den Zugriff auf die Konfigurations-API zu steuern.	16. Juni 2022
Cluster-übergreifende Suche in mehreren Regionen	Die clusterübergreifende Suche wird jetzt unterstützt, AWS-Regionen solange auf beiden Domains Elasticsearch Version 7.10 oder höher oder eine beliebige Version von ausgeführt wird. OpenSearch	14. Juni 2022
Support für Single Kibana 5.6	Amazon OpenSearch Service fügt Unterstützung für einzelne Kibana 5.6.16 hinzu. Mit SingleKibana 5.6.16 können Sie Kibana 5.6 als Front-End verwenden, während Sie eine Verbindung mit Elasticse arch in den Versionen 5.1, 5.3, 5.5 und 5.6 herstellen. Sie müssen über Serviceso ftware R20220323 oder neuer verfügen, um Single Kibana 5.6 verwenden zu können.	4. April 2022

R20220323-P1	Amazon OpenSearch Service hat kürzlich das Service-Software-Update R20220323 veröffentlicht, aber das Update wurde anschließend aufgrund eines Problems rückgängig gemacht. Wir empfehlen Ihnen, Ihre Domains auf Patch-Release R20220323-P1 oder höher zu aktualisieren, wodurch das Problem behoben wird.	4. April 2022
OpenSearch 1.2 Unterstützung	Amazon OpenSearch Service unterstützt jetzt OpenSearch Version 1.2. Weitere Informationen finden Sie unter 1.2 Versionshinweise.	4. April 2022
Beobachtbarkeit	Die Standardinstallation von OpenSearch Dashboards for Amazon OpenSearch Service umfasst das Observability-Plugin, mit dem Sie datengesteuerte Ereignisse mithilfe der Piped Processing Language (PPL) visualisieren können, um Ihre Daten zu untersuchen und abzufragen. Das Plugin erfordert OpenSearch 1.2 oder höher und die Servicesoftware R20220323 oder höher.	4. April 2022

Support für Kibana 7.7.1	Amazon OpenSearch Service-Domains, auf denen Elasticsearch 7.7 ausgeführt wird, unterstützen jetzt die neueste Patch-Version für Kibana 7.7, die Bugfixes hinzufügt und die Sicherheit verbessert. Wenn Sie Ihre 7.7-Domains auf die Service-Software R20220323 oder höher aktualisieren, aktualisiert OpenSearch Service sie automatisch auf diese Patch-Version.	4. April 2022
Änderungen der JVM-Speicherdruckmetrik	Amazon OpenSearch Service hat die Logik für die `JVMMemoryPressure` CloudWatch Metriken geändert, um die Speichernutzung genauer wiederzugeben. Zuvor betrachteten die Metriken nur den Speicherpool der alten Generation von JVM-Heap. Nach dieser Änderung berücksichtigt die Metrik auch den Speicherpool der jungen Generation. Nachdem Sie Ihre Domain auf Servicesoftware R20220323 aktualisiert haben, sehen Sie möglicherweise einen Anstieg der `JVMMemoryPressure` -, `MasterJVMMemoryPressure` - und/oder `WarmJVMMemoryPressure` -Metriken.	4. April 2022

Benutzerdefinierte Wörterbücher mit dem IK-Analyse-Plug-in (Chinesisch)	Amazon OpenSearch Service unterstützt jetzt die Verwendung benutzerdefinierter Wörterbücher mit dem Analyse-Plugin IK (Chinese).	4. April 2022
Cluster-übergreifende Replikation auf bestehenden Domain	Amazon OpenSearch Service hat die Einschränkung aufgehoben, dass Sie die clusterübergreifende Suche und clusterübergreifende Replikation nur für Domains implementieren können, die am oder nach dem 3. Juni 2020 erstellt wurden. Sie können diese Funktionen jetzt für alle Domains aktivieren, unabhängig davon, wann sie erstellt wurden. Beide Domain müssen über Serviceso ftware R20220323 oder höher ausgeführt werden.	4. April 2022
Einblick in Blau/Grün-Bereitstellungen	Amazon OpenSearch Service bietet jetzt mehr Einblick in den Fortschritt der Blau/Grün-Implementierungen. Sie können diese Details in der Konsole oder mithilfe der Konfigurations-API überwachen.	27. Januar 2022

Differenzierte Zugriffskontrolle für vorhandene Domains	Sie können nun die differenzierte Zugriffskontrolle für vorhandene Domains aktivieren. Sie können einen temporären Migrationszeitraum für offene/IP-basierte Zugriffsrichtlinien aktivieren, damit Benutzer weiterhin auf Ihre Domain zugreifen können, während Sie Rollen erstellen und zuordnen. Für die Aktivierung einer differenzierten Zugriffskontrolle für vorhandene Domains ist Service-Software R20211203 oder höher erforderlich.	6. Januar 2022
Die Rollen der Dashboards wurden umbenannt OpenSearch	Mit der Service-Software R20211203 wurde die Rolle `kibana_user` in `opensearch_dashboards_user` , und `kibana_read_only` in `opensearch_dashboards_read_only` umbenannt. Diese Änderung gilt für alle neu erstellten 1. OpenSearch X-Domänen. Für bestehende OpenSearch Domänen, die Sie auf die Servicesoftware R20211203 aktualisieren, bleiben die Rollen unverändert.	4. Januar 2022

OpenSearch 1.1 Unterstützung	Amazon OpenSearch Service unterstützt jetzt OpenSearch Version 1.1. Weitere Informationen finden Sie unter 1.1 Versionshinweise.	4. Januar 2022
Visueller Editor ISM	Die Standardinstallation von OpenSearch Dashboards for Amazon OpenSearch Service unterstützt jetzt den visuellen Editor für ISM-Richtlinien. Für diese Funktion ist OpenSearch 1.1 oder höher erforderlich.	4. Januar 2022
Update zur Vermeidung des Problems des verwirrten Stellvertreters (dienstübergreifend)	Amazon OpenSearch Service unterstützt die Verwendung der Kontextschlüssel `aws:SourceArn` und der `aws:SourceAccount` globalen Bedingungsschlüssel in IAM-Ressourcenrichtlinien, um das Problem des verwirrten Stellvertreters zu vermeiden. Sie müssen über Service-Software R20211203 oder höher verfügen, um diese Bedingungsschlüssel verwenden zu können.	4. Januar 2022

Log4j-Patch	Die Service-Software R20211203-P2 aktualisiert die im Service verwendete Version von Log4j, wie in den Hinweisen in CVE-2021-44228 und OpenSearch CVE-2021-45046 empfohlen. Der Patch gilt für Domains, auf denen OpenSearch alle Versionen von Elasticsearch ausgeführt werden. OpenSearch Der Service wird weiterhin verschiedene Log4j-Versionen intern aktualisieren, und diese werden nicht unbedingt auf die neueste Version von Log4j beschränkt sein. Die Log4j-Version auf Ihrer Domain hängt von der Softwareversion ab, die auf der Domain ausgeführt wird. Unabhängig von der Log4j-Version enthalten Ihre Domains jedoch das Log4j-Update, das zur Behebung von CVE-2021-44228 und CVE-2021-45046 erforderlich ist, sofern Sie R20211203-P2 oder höher ausführen.	15. Dezember 2021

Cluster-übergreifende Replikation	Mit der clusterübergreifenden Replikation können Sie Indizes, Mappings und Metadaten von einer Service-Domain in eine andere replizieren. OpenSearch Für die clusterübergreifende Replikation ist eine Domain erforderlich, auf der Elasticsearch 7.10 oder 1.1 oder höher ausgeführt wird. OpenSearch	5. Oktober 2021
Neue verwaltete Richtlinien AWS	Die Einführung von Amazon OpenSearch Service beinhaltet neue AWS verwaltete Richtlinien und die Abschaffung alter Richtlinien.	8. September 2021
Support für Kibana 6.4.3	Amazon OpenSearch Service-Domains, auf denen die Legacy-Elasticsearch-Version 6.4 ausgeführt wird, unterstützen jetzt die neueste Patch-Version für Kibana 6.4, die Bugfixes hinzufügt und die Sicherheit verbessert. OpenSearch Der Service aktualisiert Domains automatisch auf diese Patch-Version.	8. September 2021

Datenströme	Amazon OpenSearch Service bietet Unterstützung für Datenstreams, wodurch die Verwaltung von Zeitreihe ndaten vereinfacht wird. Ihre Domain muss OpenSearc h 1.0 oder höher laufen, um Datenstreams verwenden zu können.	8. September 2021
OpenSearch Amazon-Dienst	AWS benennt Amazon OpenSearch Service um, um das alte Branding „Elastics earch“ zu entfernen. Amazon OpenSearch Service unterstüt zt OpenSearch und veraltete s Elasticsearch OSS. Wenn Sie einen Cluster erstellen, haben Sie die Wahl, welche Suchmaschine Sie verwenden möchten. OpenSearch Der Service bietet umfassende Kompatibilität mit Elasticse arch OSS 7.10, der endgültig en Open-Source-Version der Software.	8. September 2021

Cold Storage	Der Cold Storage ist eine neue Speicherebene für selten aufgerufene oder historische Daten. Cold-Indizes belegen nur S3-Speicher und haben keine angefügte Rechenlei stung. Für den Cold Storage ist eine Domain erforderlich, auf der Elasticsearch 7.9 oder neuer ausgeführt wird, und die Servicesoftware R20210426 oder neuer ausgeführt wird.	13. Mai 2021
ARM-basierte Graviton-Instances	Amazon OpenSearch Service unterstützt jetzt ARM-basie rte Graviton-Instance-Typen (M6G, C6G, R6G und R6GD). Graviton-Instance-Typen sind auf neuen und vorhanden en Domains verfügbar, auf denen Elasticsearch 7.9 oder neuer ausgeführt wird und die Servicesoftware R20210331 oder neuer ausgeführt wird.	4. Mai 2021

ISM-Vorlagen	Amazon OpenSearch Service bietet Unterstützung für ISM-Vorlagen, mit denen Sie automatisch eine ISM-Richtlinie an einen Index anhängen können, wenn der Index einem in der Richtlinie definierten Muster entsprich t. ISM-Vorlagen erfordern Servicesoftware R20210426 oder neuer. Dieses Update veraltert auch die `policy_id` -Einstellung, d. h. Sie können keine Indexvorlagen mehr verwenden, um ISM-Richt linien auf neu erstellte Indizes anzuwenden. Das Update führt eine grundlegende Änderung für bestehende CloudFormation Vorlagen ein, die diese Einstellung verwenden.	27. April 2021
Support für Elasticsearch 7.10	Amazon OpenSearch Service unterstützt jetzt Elasticse arch Version 7.10. Weitere Informationen finden Sie unter 7.10 Versionshinweise.	21. April 2021

Asynchrone Suche	Amazon OpenSearch Service unterstützt jetzt die asynchrone Suche, sodass Sie Suchanfragen im Hintergrund ausführen können. Für die asynchrone Suche ist eine Domain erforderlich, auf der Elasticsearch 7.10 oder neuer ausgeführt wird, und die Servicesoftware R20210331 oder neuer ausgeführt wird.	21. April 2021
Tag-basierte Zugriffskontrolle für die Konfigurations-API	Sie können jetzt AWS Tags verwenden, um den Zugriff auf die Amazon ES-Konfigurations-API zu steuern.	2. März 2021
Automatische Optimierung	Amazon OpenSearch Service fügt Auto-Tune hinzu, das Leistungs- und Nutzungsmetriken aus Ihrem Cluster verwendet, um Änderungen an den JVM-Einstellungen auf Ihren Knoten vorzuschlagen. Für die automatische Optimierung ist eine Domain erforderlich, auf der Elasticsearch 6.7 oder neuer ausgeführt wird, und die Servicesoftware R20201117 oder neuer ausgeführt wird.	24. Februar 2021

Trace Analytics	Die Standardinstallation von Kibana for Amazon OpenSearch Service enthält jetzt das Trace-Analytics-Plugin, mit dem Sie Trace-Daten aus Ihren verteilten Anwendungen überwachen können. Für das Plug-in ist eine Domain erforderlich, auf der Elasticsearch 7.9 oder neuer ausgeführt wird, und die Servicesoftware R20210201 oder neuer ausgeführt wird.	17. Februar 2021
Shard-Metriken	Amazon OpenSearch Service fügt die folgenden CloudWatch Metriken für die Verfolgung des Shard-Status hinzu:`Shards.active` ,`Shards.unassigned` , `Shards.delayedUnassigned` `Shards.activePrimary` ,`Shards.initializing` ,`Shards.relocating` . Die Metriken sind auf Domains mit Service-Software R20210201 oder höher verfügbar.	17. Februar 2021

Kibana-Berichte	Die Standardinstallation von Kibana for Amazon OpenSearch Service unterstützt jetzt On-Demand-Berichte für die Seiten Discover, Visualize und Dashboard. Für diese Funktion ist eine Domain erforderlich, auf der Elasticsearch 7.9 oder neuer und die Servicesoftware R20210201 oder neuer ausgeführt wird.	17. Februar 2021
Support für Kibana 5.6.16	Amazon OpenSearch Service-Domains, auf denen Elasticsearch 5.6 ausgeführt wird, unterstützen jetzt die neueste Patch-Version für Kibana 5.6, die Bugfixes hinzufügt und die Sicherheit verbessert. Amazon ES aktualisiert Domains automatisch auf diese Patch-Version.	17. Februar 2021
Verschlüsselung für vorhandene Domains	Amazon OpenSearch Service unterstützt jetzt die Aktivierung der Verschlüsselung ruhender Daten und der node-to-node Verschlüsselung für bestehende Domains, auf denen Elasticsearch 6.7 oder höher ausgeführt wird. Nachdem Sie diese Einstellungen aktiviert haben, können Sie sie nicht mehr deaktivieren.	27. Januar 2021

Remote-Neuindexierung	Amazon OpenSearch Service unterstützt jetzt die Remote-Neuindizierung, sodass Sie Indizes von Remote-Domains migrieren können. Diese Funktion erfordert Service-Software R20201117 oder neuer.	24. November 2020
Piped Processing Language	Amazon OpenSearch Service unterstützt jetzt Piped Processing Language (PPL), eine Abfragesprache, mit der Sie die Pipe-Syntax (|) verwenden können, um in Elasticsearch gespeicherte Daten abzufragen. Diese Funktion erfordert Service-Software R20201117 oder neuer. Weitere Informationen hierzu finden Sie unter .	24. November 2020
Kibana-Notebooks	Amazon OpenSearch Service bietet Unterstützung für Kibana-Notizbücher, sodass Sie Live-Visualisierungen und erläuternden Text in einer einzigen Oberfläche kombinieren können. Diese Funktion erfordert Service-Software R20201117 oder neuer.	24. November 2020

Gantt-Diagramme	Die Standardinstallation von Kibana for Amazon OpenSearch Service unterstützt jetzt einen neuen Visualisierungstyp, Gantt-Diagramme. Diese Funktion erfordert Service-Software R20201117 oder neuer.	24. November 2020
Support für Elasticsearch 7.9	Amazon OpenSearch Service unterstützt jetzt Elasticsearch Version 7.9. Weitere Informationen finden Sie unter 7.9 Versionshinweise.	24. November 2020
Aktualisierungen für Anomalieerkennung	Die Anomalieerkennung für Amazon OpenSearch Service bietet Unterstützung für hohe Kardinalität, sodass Sie Anomalien anhand von Dimensionen wie IP-Adresse, Produkt-ID, Ländercode usw. kategorisieren können. Diese Funktion erfordert Service-Software R20201117 oder neuer.	24. November 2020

Aktualisierungen für dynamisches Wörterbuch	Mit Amazon OpenSearch Service können Sie jetzt Ihre Suchanalyseprogramme aktualisieren, ohne sie erneut indizieren zu müssen. Sie können die Wörterbuchdateien für einige oder alle Ihrer Domains aktualisieren, und Amazon ES verfolgt Paketversionen im Laufe der Zeit, sodass Sie einen Überblick darüber haben, was sich wann geändert hat. Diese Funktion erfordert Service-Software R20201019 oder neuer.	17. November 2020
Benutzerdefinierte Endpunkte	Amazon OpenSearch Service unterstützt jetzt benutzerdefinierte Endpunkte, mit denen Sie Ihrer Amazon ES-Domain eine neue URL zuweisen können. Wenn Sie je Domain austauschen, können Sie die gleiche URL pflegen. Diese Funktion erfordert Service-Software R20201019 oder neuer.	5. November 2020

Neue Sprach-Plug-ins	Amazon OpenSearch Service unterstützt jetzt die Plug-ins IK (Chinese) Analysis, Vietnamese Analysis und Thai Analysis auf Domains, auf denen Elasticsearch 7.7 oder höher mit der Service-Software R20201019 oder höher ausgeführt wird.	28. Oktober 2020
Support für Elasticsearch 7.8	Amazon OpenSearch Service unterstützt jetzt Elasticsearch Version 7.8. Weitere Informationen finden Sie unter 7.8 Versionshinweise.	28. Oktober 2020
SAML-Authentifizierung für Kibana	Amazon OpenSearch Service unterstützt jetzt die SAML-Authentifizierung für Kibana, sodass Sie externe Identitätsanbieter verwenden können, um sich bei Kibana anzumelden, eine detaillierte Zugriffskontrolle zu verwalten, Ihre Daten zu durchsuchen und Visualisierungen zu erstellen. Diese Funktion erfordert Service-Software R20201019 oder neuer.	27. Oktober 2020
T3-Instances	Amazon OpenSearch Service unterstützt jetzt die `t3.medium` Instance-Typen `t3.small` und.	23. September 2020

Prüfungsprotokolle	Amazon OpenSearch Service unterstützt jetzt Prüfprotokolle für Ihre Daten, mit denen Sie fehlgeschlagene Anmeldeversuche, Benutzerzugriffe auf Indizes, Dokumente und Felder und vieles mehr verfolgen können. Diese Funktion erfordert Service-Software R20200910 oder neuer.	16. September 2020
UltraWarm Aktualisierungen	UltraWarm for Amazon OpenSearch Service fügt neue Metriken, neue Einstellungen, eine größere Migrationswarteschlange und eine Stornierungs-API hinzu. Für diese Updates ist Serviceoftware R20200910 oder neuer erforderlich. Weitere Informationen finden Sie unter .	14. September 2020
Learning to Rank	Amazon OpenSearch Service unterstützt jetzt das Open-Source-Plugin Learning to Rank, mit dem Sie Technologien für maschinelles Lernen verwenden können, um die Suchrelevanz zu verbessern. Diese Funktion erfordert Service-Software R20200721 oder neuer.	27. Juli 2020

k-NN-Kosinus-Ähnlichkeit	Mit k-Nearest Neighbor (k-NN) können Sie nun zusätzlich zur euklidischen Entfernung nach „nächsten Nachbarn“ nach Kosinusähnlichkeit suchen. Diese Funktion erfordert Service-Software R20200721 oder neuer.	23. Juli 2020
gzip-Komprimierung	Amazon OpenSearch Service unterstützt jetzt die GZIP-Komprimierung für die meisten HTTP-Anfragen und -Antworten, wodurch die Latenz reduziert und Bandbreite gespart werden kann. Diese Funktion erfordert Service-Software R20200721 oder neuer.	23. Juli 2020
Support für Elasticsearch 7.7	Amazon OpenSearch Service unterstützt jetzt Elasticsearch Version 7.7. Weitere Informationen finden Sie unter 7.7 Versionshinweise.	23. Juli 2020
Kibana-Karten-Service	Die Standardinstallation von Kibana für Amazon OpenSearch Service umfasst jetzt einen WMS-Kartenserver, mit Ausnahme von Domains in den Regionen Indien und China.	18. Juni 2020

SQL-Verbesserungen	Die SQL-Unterstützung für Amazon OpenSearch Service unterstützt jetzt viele neue Operationen, eine spezielle Kibana-Benutzeroberfläche für die Datenexploration und eine interaktive CLI.	3. Juni 2020
Cluster-übergreifende Suche	Mit Amazon OpenSearch Service können Sie clusterübergreifende Abfragen und Aggregationen für mehrere verbundene Domains durchführen.	3. Juni 2020
Anomalieerkennung	Mit Amazon OpenSearch Service können Sie Anomalien fast in Echtzeit automatisch erkennen.	3. Juni 2020
UltraWarm	UltraWarm Der Speicherplatz für Amazon OpenSearch Service hat die öffentliche Vorschauversion verlassen und ist jetzt allgemein verfügbar. Die Funktion unterstützt jetzt eine größere Auswahl an Versionen und AWS-Regionen. Weitere Informationen finden Sie unter .	5. Mai 2020

Benutzerdefinierte Wörterbücher	Mit Amazon OpenSearch Service können Sie benutzerdefinierte Wörterbuchdateien zur Verwendung mit Ihrem Cluster hochladen. Diese Dateien verbessern Ihre Suchergebnisse, indem sie Elasticsearch anweisen, bestimmte hochfrequente Wörter zu ignorieren oder Begriffe als gleichwertig zu behandeln.	21. April 2020
Support für Elasticsearch 7.4	Amazon OpenSearch Service unterstützt jetzt Elasticsearch Version 7.4. Weitere Informationen finden Sie unter unterstützte Versionen.	12. März 2020
k-NN	Amazon OpenSearch Service bietet Unterstützung für die Suche nach k-Nearest Neighbor (k-NN). k-NN benötigt die Servicesoftware R20200302 oder höher.	3. März 2020
Indexstatusmanagement	Amazon OpenSearch Service fügt Index State Management (ISM) hinzu, mit dem Sie Routineaufgaben automatisieren können, z. B. das Löschen von Indizes, wenn sie ein bestimmtes Alter erreicht haben. Diese Funktion erfordert Service-Software R20200302 oder neuer.	3. März 2020

Support für Elasticsearch 5.6.16	Amazon OpenSearch Service unterstützt jetzt die neueste Patch-Version für Version 5.6, die Bugfixes hinzufügt und die Sicherheit verbessert. Amazon ES aktualisiert vorhandene 5.6-Domains automatisch auf diese Version. Beachten Sie, dass die Versionsnummer dieser Elasticsearch-Version fälschlicherweise als 5.6.17 angegeben wird..	2. März 2020
Differenzierte Zugriffskontrolle	Amazon OpenSearch Service unterstützt jetzt eine differenz ierte Zugriffskontrolle, die Sicherheit auf Index-, Dokument- und Feldebene , Kibana-Mehrmandant enfähigkeit und optionale HTTP-Basisauthentifizierung für Ihren Cluster bietet.	11. Februar 2020
UltraWarm Speicher (Vorschau)	Amazon OpenSearch Service fügt UltraWarm eine neue Warm-Speicherstufe hinzu, die Amazon S3 und eine ausgeklügelte Caching-L ösung zur Leistungssteigerun g verwendet. Für Indizes, in die Sie nicht aktiv schreiben und die Sie seltener abfragen, bietet UltraWarm Speicher deutlich niedrigere Kosten pro GiB.	3. Dezember 2019

Verschlüsselungsfunktionen für Regionen in China	Verschlüsselung ruhender Daten und node-to-node Verschlüsselung sind jetzt in den Regionen `cn-north-1` China (Peking) und `cn-northwest-1` China (Ningxia) verfügbar.	20. November 2019
Erzwingung von HTTPS	Sie können jetzt erzwingen, dass der gesamte Datenverkehr zu Ihren Amazon ES-Domains über HTTPS eingeht. Aktivieren Sie beim Konfigurieren Ihrer Domain das Kontrollkästchen Require HTTPS (Erzwingung von HTTPS). Diese Funktion erfordert Service-Software R20190808 oder neuer.	3. Oktober 2019
Support für Elasticsearch 7.1 und 6.8	Amazon OpenSearch Service unterstützt jetzt Elasticsearch in den Versionen 7.1 und 6.8. Weitere Informationen finden Sie unter unterstützte Versionen.	13. August 2019
Stündliche Snapshots	Statt täglicher Snapshots erstellt Amazon OpenSearch Service jetzt stündlich Schnappschüsse von Domains, auf denen Elasticsearch 5.3 und höher ausgeführt wird, sodass Sie häufiger Backups haben, aus denen Sie Ihre Daten wiederherstellen können.	8. Juli 2019

Support für Elasticsearch 6.7	Amazon OpenSearch Service unterstützt jetzt Elasticsearch Version 6.7. Weitere Informationen finden Sie unter unterstützte Versionen.	29. Mai 2019
SQL-Unterstützung	Mit Amazon OpenSearch Service können Sie Ihre Daten jetzt mit SQL abfragen. SQL-Unterstützung erfordert Service-Software R20190418 oder neuer.	15. Mai 2019
5-Serie-Instance-Typen	Amazon OpenSearch Service unterstützt jetzt die Instance-Typen M5, C5 und R5. Im Vergleich zu Instance-Typen der vorigen Generation bieten diese neuen Typen eine bessere Leistung zu niedrigeren Kosten. Weitere Informationen finden Sie unter Limits.	24. April 2019
Support für Elasticsearch 6.5	Amazon OpenSearch Service unterstützt jetzt Elasticsearch Version 6.5.	8. April 2019
Warnfunktion	Alerting for Amazon OpenSearch Service benachrichtigt Sie, wenn Daten aus einem oder mehreren Amazon ES-Indizes bestimmte Bedingungen erfüllen. Die Warnfunktion erfordert Service-Software R20190221 oder neuer.	25. März 2019

Support für drei Availability Zones	Amazon OpenSearch Service unterstützt jetzt drei Availability Zones in vielen Regionen. Diese Version enthält auch eine optimierte Konsolenumgebung. Dieses Multi-AZ erfordert Service-Software R20181023 oder neuer.	7. Februar 2019
Support für Elasticsearch 6.4	Amazon OpenSearch Service unterstützt jetzt Elasticsearch Version 6.4.	23. Januar 2019
200-Knoten-Cluster	Mit Amazon ES können Sie nun Cluster mit bis zu 200 Datenknoten für insgesamt 3 PB Speicher erstellen.	22. Januar 2019
Service-Software-Updates	Mit Amazon ES können Sie die Service-Software für Ihre Domain jetzt manuell aktualisieren, um neue Funktionen schneller zu nutzen oder um ein Update zu einem Zeitpunkt mit geringem Datenverkehr durchzuführen. Weitere Informationen hierzu finden Sie unter .	20. November 2018
Neue Metriken CloudWatch	Amazon ES bietet jetzt Metriken auf Knotenebene und neue Registerkarten für Cluster-Zustand und Instance-Zustand in der Amazon ES-Konsole.	20. November 2018

Support für China (Peking)	Amazon OpenSearch Service ist jetzt in der Region cn-north-1 verfügbar, wo es die Instance-Typen M4, C4 und R4 unterstützt.	17. Oktober 2018
Node-to-node Verschlüsselung	Amazon OpenSearch Service unterstützt jetzt node-to-node Verschlüsselung, wodurch Ihre Daten verschlüsselt bleiben, während Amazon ES sie in Ihrem Cluster verteilt.	18. September 2018
In-Situ-Versions-Upgrades	Amazon OpenSearch Service unterstützt jetzt direkte Versionsupgrades.	14. August 2018
Support für Elasticsearch 6.3 und 5.6	Amazon OpenSearch Service unterstützt jetzt Elasticsearch in den Versionen 6.3 und 5.6.	14. August 2018
Fehlerprotokolle	Mit Amazon ES können Sie jetzt Elasticsearch-Fehlerprotokolle auf Amazon CloudWatch veröffentlichen.	31. Juli 2018
Reserved Instances in China (Ningxia)	Amazon ES unterstützt jetzt Reserved Instances in der Region China (Ningxia).	29. Mai 2018
Reserved Instances	Amazon ES bietet jetzt Unterstützung für Reserved Instances.	7. Mai 2018

Frühere Aktualisierungen

In der folgenden Tabelle werden die wichtigen Änderungen an Amazon ES vor Mai 2018 beschrieben.

Änderung	Beschreibung	Datum
Amazon Cognito-Authentifizierung für Kibana	Amazon ES bietet nun Schutz für die Anmeldeseite für Kibana. Weitere Informationen hierzu finden Sie unter the section called “Amazon Cognito Cognito-Authentifizierung für Dashboards OpenSearch ”.	2. April 2018
Support für Elasticsearch 6.2	Amazon OpenSearch Service unterstützt jetzt Elasticsearch Version 6.2.	14. März 2018
Koreanisches Analyse-Plug-in	Amazon ES unterstützt nun eine speicheroptimierte Version von Seunjeon, dem koreanischen Analyse-Plug-in.	13. März 2018
Sofortige Updates der Zugriffskontrolle	Änderungen an den Zugriffskontrollrichtlinien auf Amazon ES-Domains werden nun unverzüglich übernommen.	7. März 2018
Petabyte-Größe	Amazon ES unterstützt jetzt I3-Instance-Typen und einen Gesamt-Domain-Speicher von bis zu 1,5 PB. Weitere Informationen hierzu finden Sie unter the section called “Petabyte-Größe”.	19. Dezember 2017
Verschlüsselung gespeicherter Daten	Amazon ES unterstützt nun die Verschlüsselung von Data-at-Rest. Weitere Informationen hierzu finden Sie unter the section called “Verschlüsselung im Ruhezustand”.	7. Dezember 2017
Support für Elasticsearch 6.0	Amazon ES unterstützt jetzt Elasticsearch Version 6.0. Überlegungen und Anweisungen für Migrationen finden Sie unter the section called “Aktualisieren von Domains”.	6. Dezember 2017
VPC-Unterstützung	Amazon ES ermöglicht jetzt das Launchen von Domains in einer Amazon Virtual Private Cloud. Die VPC-Unterstützung bietet zusätzliche Sicherheit und vereinfacht die Kommunikation zwischen Amazon ES und anderen	17. Oktober 2017

Änderung	Beschreibung	Datum
	Services in einer VPC. Weitere Informationen hierzu finden Sie unter the section called “VPC-Unterstützung”.	
Veröffentlichen von Slow-Protokollen	Amazon ES unterstützt jetzt die Veröffentlichung von langsamen Protokollen in CloudWatch Logs. Weitere Informationen hierzu finden Sie unter the section called “Überwachen von Protokollen”.	16. Oktober 2017
Support für Elasticsearch 5.5	Amazon ES unterstützt jetzt Elasticsearch Version 5.5. Sie können jetzt automatische Snapshots wiederherstellen, ohne mit Support Kontakt aufzunehmen und Skripts mithilfe der `_scripts`-API speichern.	7. September 2017
Support für Elasticsearch 5.3	Amazon ES unterstützt jetzt Elasticsearch Version 5.3.	1. Juni 2017
Mehr Instances und EBS-Kapazität pro Cluster	Amazon ES bietet jetzt Unterstützung für bis zu 100 Knoten und 150 TB EBS-Kapazität pro Cluster.	5. April 2017
Unterstützung für Kanada (Zentral) und EU (London)	Amazon ES bietet Unterstützung für die folgenden Regionen: Kanada (Zentral), ca-central-1, und EU (London), eu-west-2.	20. März 2017
Mehr Instances und größere EBS-Volumes	Amazon ES bietet Unterstützung für mehr Instances und größere EBS-Volumes.	21. Februar 2017
Support für Elasticsearch 5.1	Amazon ES unterstützt jetzt Elasticsearch Version 5.1.	30. Januar 2017
Unterstützung für das Phonetic Analysis Plug-in	Amazon ES bietet nun Integration in das Phonetic Analysis-Plug-in, das das Ausführen von "tonähnlichen" Abfragen für Ihre Daten ermöglicht.	22. Dezember 2016

Änderung	Beschreibung	Datum
Unterstützung für USA Ost (Ohio)	Amazon ES bietet Unterstützung für die folgende Region: USA Ost (Ohio), us-east-2.	17. Oktober 2016
Neue Leistungs metrik	Amazon ES verfügt über eine neue Leistungsmetrik, `ClusterUsedSpace` .	29. Juli 2016
Support für Elasticsearch 2.3	Amazon ES unterstützt jetzt Elasticsearch Version 2.3.	27. Juli 2016
Unterstützung für Asien-Pazifik (Mumbai)	Amazon ES bietet Unterstützung für die folgenden Regionen: Asien-Pazifik (Mumbai), ap-south-1.	27. Juni 2016
Mehr Instances pro Cluster	In Amazon ES wurde die maximale Anzahl von Instances (Anzahl der Instances) pro Cluster von 10 auf 20 erhöht.	18. Mai 2016
Unterstützung für Asien-Pazifik (Seoul)	Amazon ES bietet Unterstützung für die folgenden Regionen: Asien-Pazifik (Seoul), ap-northeast-2.	28. Januar 2016
Amazon ES	Erstversion.	1. Oktober 2015

AWS Glossar

Die neueste AWS Terminologie finden Sie im AWS Glossar in der AWS-Glossar Referenz.

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.