aws

Entwicklerhandbuch

Amazon DocumentDB

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon DocumentDB: Entwicklerhandbuch

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Die Handelsmarken und die Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. 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 DocumentDB ... 1
-Übersicht ... 1
Cluster ... 3
Instances ... 4
Regionen und AZs ... 8
Regionen ... 8
Availability Zones ... 8
Preisgestaltung ... 11
Kostenlose Testversion ... 12
Überwachen ... 12
Schnittstellen ... 12
AWS-Managementkonsole ... 12
AWS CLI ... 13
MongoDB-Treiber ... 13
Als nächstes ... 13
Funktionsweise ... 14
Amazon DocumentDB DocumentDB-Versionen ... 14
Amazon DocumentDB DocumentDB-Endpunkte ... 17
TLS-Unterstützung ... 21
Amazon DocumentDB DocumentDB-Speicher ... 21
Amazon DocumentDB DocumentDB-Replikation ... 22
Zuverlässigkeit von Amazon DocumentDB ... 22
Lesen Sie die Einstellungsoptionen ... 24
TTL löscht ... 29
Abrechnungsfähige Ressourcen ... 29
Was ist eine Dokumentendatenbank? ... 32
Anwendungsfälle ... 33
Dokumente verstehen ... 34
Arbeiten mit Dokumenten ... 40
Leitfaden für die ersten Schritte ... 53
Voraussetzungen ... 54
Schritt 1: Erstellen eines Clusters ... 55
Schritt 2: Connect zu Ihrem Cluster her ... 58
Schritt 3: Daten einfügen und abfragen ... 59

Schritt 4: Erkunden ... 61
Funktionen und Konfigurationen ... 62
Status der Engine ... 62
Clustertypen ... 62
Features ... 63
Instance-Typen ... 64
AWS Integrationen ... 65
Schneller Start mit CloudFormation ... 67
Voraussetzungen ... 68
Erforderliche IAM-Berechtigungen ... 68
Amazon-EC2-Schlüsselpaar ... 68
Eine Amazon DocumentDB starten CloudFormation Stack ... 68
Zugreifen auf den Amazon DocumentDB-Cluster ... 74
Kündigungsschutz und Löschschutz ... 75
MongoDB-Kompatibilität ... 76
MongoDB 8.0-Kompatibilität ... 76
Was ist neu in Amazon DocumentDB 8.0 ... 76
Erste Schritte mit Amazon DocumentDB ... 77
Upgrade oder Migration auf Amazon DocumentDB 5.0 oder 8.0 ... 78
Funktionelle Unterschiede ... 78
MongoDB 5.0-Kompatibilität ... 78
Was ist neu in Amazon DocumentDB 5.0 ... 79
Was ist neu in Amazon DocumentDB 5.0.1 ... 79
Erste Schritte mit Amazon DocumentDB 5.0 ... 77
Upgrade oder Migration auf Amazon DocumentDB 5.0 ... 78
Funktionelle Unterschiede ... 78
MongoDB 4.0-Kompatibilität ... 83
Funktionen von Amazon DocumentDB 4.0 ... 83
Erste Schritte mit Amazon DocumentDB 4.0 ... 84
Upgrade oder Migration zu Amazon DocumentDB 4.0 ... 85
Funktionelle Unterschiede ... 85
Transaktionen ... 87
Voraussetzungen ... 87
Best Practices ... 88
Einschränkungen ... 88
Überwachung und Diagnose ... 89

Isolationsstufe für Transaktionen 90
Anwendungsfälle 90
Multi-Statement Transaktionen 91
Multi-collection Transaktionen 92
Beispiele für Transaktions-APIs für die Callback-API 94
Beispiele für Transaktions-APIs für die Kern-API 94
Unterstützte Befehle 128
Nicht unterstützte Funktionen 129
Sitzungen 130
Kausale Konsistenz 130
Wiederholbare Schreibvorgänge 131
Transaktionsfehler 132
Best Practices 133
Grundlegende Anleitungen für den Betrieb 133
Dimensionierung der Instanzen 135
Arbeiten mit Indizes 136
Erstellen von Indizes 136
Index-Selektivität 137
Auswirkung von Indizes auf das Schreiben von Daten 137
Identifizierung fehlender Indizes 138
Identifizieren ungenutzter Indizes 138
Bewährte Methoden für die Gewährleistung der Sicherheit 138
Kostenoptimierung 139
Verwendung von Metriken zur Identifizierung von Problemen mit der Leistung 140
Anzeigen von Leistungsmetriken 140
Einen CloudWatch Alarm einrichten 141
Auswerten von Leistungsmetriken 141
Auswertung der Nutzung von Amazon DocumentDB DocumentDB-Instances anhand von Metriken CloudWatch 143
Optimieren von Abfragen 144
TTL- und Zeitreihen-Workloads 145
Migrationen 145
Arbeiten mit Cluster-Parametergruppen 146
Abfragen in der Aggregationspipeline 146
`BatchInsert und BatchUpdate` 146
Funktionale Unterschiede zu MongoDB 147

Funktionale Vorteile von Amazon DocumentDB ... 147
Implizite Transaktionen ... 147
Funktionelle Unterschiede wurden aktualisiert ... 148
Array-Indizierung ... 149
Multi-key Indizes ... 150
Nullzeichen in Zeichenketten ... 151
Role-based Zugriffskontrolle ... 151
`$regex-Indizierung` ... 151
Projektion für verschachtelte Dokumente ... 152
Funktionale Unterschiede zu MongoDB ... 152
`$ VectorSearch-Operator` ... 153
`OpCountersCommand` ... 153
Admin-Datenbanken und Sammlungen ... 153
`CursorMaxTimeMS` ... 153
explain() ... 154
Der Index wird erstellt ... 154
Suche mit leerem Schlüssel im Pfad ... 154
MongoDB-APIs, Operationen und Datentypen ... 155
`Dienstprogramme mongodump und mongorestore` ... 155
Reihenfolge der Ergebnisse ... 155
Wiederholbare Schreibvorgänge ... 156
Sparse Index ... 156
`Verwenden von $elemMatch innerhalb eines $all-Ausdrucks` ... 157
Dollar ($) und Punkt (.) in Feldnamen ... 157
`$lookup` ... 158
`$natural` und umgekehrte Sortierung ... 161
Unterstützte MongoDB-APIs, Operationen und Datentypen ... 162
Befehle für die Datenbank ... 163
Administrative Befehle ... 163
Aggregation ... 165
Authentifizierung ... 165
Diagnosebefehle ... 166
Abfrage- und Schreiboperationen ... 167
Befehle zur Rollenverwaltung ... 168
Befehle für Sitzungen ... 169
Benutzerverwaltung ... 169

Sharding-Befehle ... 170
Abfrage- und Projektionsoperatoren ... 172
Array-Operatoren ... 172
Bitweise Operatoren ... 173
Operator kommentieren ... 173
Vergleichsoperatoren ... 173
Elementoperatoren ... 174
Operatoren für Bewertungsabfragen ... 174
Logische Operatoren ... 175
Projektionsoperatoren ... 175
Operatoren aktualisieren ... 176
Array-Operatoren ... 176
Bitweise Operatoren ... 176
Feldoperatoren ... 177
Modifikatoren aktualisieren ... 177
Geodaten ... 178
Geometrie-Spezifizierer ... 178
Selektoren abfragen ... 178
Cursor-Methoden ... 179
Operatoren für Aggregationspipelines ... 181
Akkumulatorausdrücke ... 182
Arithmetische Operatoren ... 184
Array-Operatoren ... 185
Boolesche Operatoren ... 186
Vergleichsoperatoren ... 186
Operatoren für bedingte Ausdrücke ... 187
Datentyp-Operator ... 187
Operator zur Datengröße ... 187
Datumsoperatoren ... 187
Wörtlicher Operator ... 189
Operator zusammenführen ... 189
Natürlicher Operator ... 189
Satzoperatoren ... 190
Betreiber der Bühne ... 190
Zeichenfolgenoperatoren ... 193
Systemvariablen ... 194

Operator für die Textsuche ... 194
Geben Sie Konvertierungsoperatoren ein ... 195
Operatoren für Variablen ... 195
Verschiedene Betreiber ... 196
Datentypen ... 196
Indizes und Indexeigenschaften ... 197
Indizes ... 198
Eigenschaften indizieren ... 198
Betreiber von Aggregationspipelines ... 199
$$DESCEND ... 204
$$KEEP ... 207
$$PRUNE ... 210
$ WURZEL ... 212
$abs ... 217
$add ... 219
$ hinzufügen ToSet ... 221
$addFields ... 224
$ alles ElementsTrue ... 227
$and ... 229
$ beliebig ElementTrue ... 232
$array ElemAt ... 234
$array ToObject ... 237
$avg ... 239
$bucket ... 241
$ceil ... 245
$ Stream ändern ... 247
$cmp ... 250
$collStats ... 253
$concat ... 256
$concatArrays ... 258
$cond ... 261
$ konvertieren ... 264
$count ... 267
$currentOp ... 270
$DateAdd ... 272
$DateDiff ... 275

$datum FromString 279
$DateSubtrahieren 282
$datum ToString 285
$DateTrunc 289
$Tag OfMonth 292
$Tag OfWeek 295
$Tag OfYear 297
$divide 300
$eq 302
$exp 305
$filter 307
$first 310
$floor 313
$geoNear 316
$group 318
$gt 321
$gte 324
$hour 326
$ifNull 330
$in 333
$ index OfArray 335
$ index OfBytes 337
$indexOfCP 340
$indexStats 342
$isArray 344
$ iso DayOfWeek 347
$isoWeek 350
$ iso WeekYear 352
$last 355
$let 358
$limit 362
$literal 365
$ln 368
$log 370
$log10 372
$lt 375

$lte 378
$lookup 380
$ ltrim 384
$map 387
$match 389
$max 392
$meta 394
$ zusammenführen 396
$mergeObjects 399
$millisecond 402
$min 405
$minute 407
$mod 410
$month 413
$multiply 416
$ natürlich 419
$ne 421
$not 424
$objekt ToArray 426
$or 431
$out 433
$pow 436
$push 438
$project 441
$ Rand 443
$range 446
$redact 449
$reduce 452
$RegexFind 455
$ regulärer Ausdruck FindAll 458
$RegexMatch 461
$ Alles ersetzen 464
$ ersetzenEins 468
$replaceRoot 472
$ ersetzendurch 474
$reverseArray 477

$rtrim 480
$sample 483
$suche 486
$second 488
$set 490
$setDifference 493
$setEquals 496
$setIntersection 498
$ gesetzt IsSubset 501
$setUnion 503
$skip 506
$slice 508
$size 511
$sort 513
$split 515
$sqrt 518
$str LenBytes 520
$strLenCP 523
$strcasecmp 526
$substr 528
$substrBytes 531
$substrCP 533
$subtract 536
$sum 539
$switch 542
$ zu Bool 546
$ bis Datum 548
$ zu Dezimal 551
$ bis verdoppeln 553
$ zu Int 556
$ zu Long 558
$toLower 561
$ bis ObjectId 563
$ toString 565
$toUpper 567
$trim 569

$type ... 571
$unset ... 574
$unwind ... 576
$VectorSearch ... 578
$week ... 582
$year ... 585
$zip ... 587
Geodaten ... 590
$geometry ... 591
$geoIntersects ... 595
$geoWithin ... 598
$maxDistance ... 602
$minDistance ... 605
$near ... 608
$nearSphere ... 612
Abfrage- und Projektionsoperatoren ... 615
$ ... 616
$all ... 618
$and ... 621
$ Bits AllClear ... 623
$ Bits AllSet ... 625
$ Bits AnyClear ... 628
$ Bits AnySet ... 630
$comment ... 632
$elemMatch ... 634
$eq ... 636
$exists ... 638
$expr ... 640
$gt ... 643
$gte ... 644
$in ... 646
$jsonSchema ... 648
$lt ... 651
$mod ... 653
$lte ... 655
$meta ... 657

$ne ... 660
$nin ... 662
$nor ... 664
$not ... 667
$or ... 669
$regex ... 671
$slice ... 673
$size ... 675
$text ... 677
$type ... 680
Operatoren aktualisieren ... 682
$ ... 683
$[] ... 685
$ [<Kennung>] ... 687
$ hinzufügen ToSet ... 690
$bit ... 692
$currentDate ... 694
$each ... 697
$inc ... 699
$max ... 701
$min ... 703
$mul ... 705
$pop ... 708
$position ... 710
$pull ... 713
$pullAll ... 716
$push ... 718
$rename ... 720
$set ... 723
$ gesetzt OnInsert ... 725
$slice ... 729
$sort ... 731
$unset ... 734
Generative KI ... 737
SageMaker Leinwand ... 737
Wie erstellt man ML-Modelle ohne Code mit AI Canvas SageMaker ... 737

Konfiguration der SageMaker AI-Domäne und des Benutzerprofils ... 738
Konfiguration von IAM-Zugriffsberechtigungen für Amazon DocumentDB und AI Canvas SageMaker ... 738
Datenbankbenutzer und Rollen für SageMaker AI Canvas erstellen ... 739
Verfügbare Regionen ... 739
Vektor-Suche ... 740
Vektoren einfügen ... 741
Einen Vektorindex erstellen ... 741
Eine Indexdefinition abrufen ... 745
Abfragen von Vektoren ... 746
Funktionen und Einschränkungen ... 750
Best Practices ... 752
Zu DocumentDB migrieren ... 753
Schnellstart-Anleitung ... 753
Bereiten Sie die DMS-Quelle vor ... 753
DMS einrichten ... 754
DocumentDB-Komprimierung aktivieren ... 754
Erstellen Sie eine Replikationsaufgabe ... 754
Überwachen des Fortschritts ... 755
Zusätzliche Informationen ... 755
Runbook für die Migration ... 756
Kompatibilität ... 756
Workload-Erkennung ... 760
Indexmigration ... 763
Benutzermigration ... 765
Datenmigrationen ... 767
Überwachen ... 779
Validierung ... 782
Migration von Couchbase Server ... 787
Einführung ... 787
Vergleich mit Amazon DocumentDB ... 788
Erkennung ... 790
Planung ... 796
Migration ... 799
Validierung ... 808
DocumentDB aktualisieren ... 812

Termine für die Unterstützung der Engine-Version ... 812
Veröffentlichungskalender für Amazon DocumentDB DocumentDB-Hauptversionen ... 812
Veröffentlichungskalender für Amazon DocumentDB-Nebenversionen ... 813
Aktualisierung einer Hauptversion der Engine ... 814
Unterstützte Upgrade-Pfade ... 814
Voraussetzungen ... 815
Best Practices ... 816
Was ändert sich nach dem Upgrade von Amazon DocumentDB 5.0 auf 8.0 ... 820
Post-upgrade Überlegungen zu Clustern, die von 3.6 oder 4.0 aktualisiert wurden ... 821
Das Upgrade wird durchgeführt ... 821
Fehlerbehebung ... 824
Aktualisierung einer kleineren Engine-Version ... 824
Vor dem Durchführen eines Nebenversions-Upgrades ... 824
Durchführen eines Nebenversions-Upgrades ... 825
Das Upgrade der Nebenversion wird überprüft ... 826
Ein Upgrade durchführen mit AWS DMS ... 826
Schritt 1: Change Streams aktivieren ... 827
Schritt 2: Ändern Sie die Aufbewahrungsdauer für Change-Streams ... 827
Schritt 3: Migrieren Sie Ihre Indizes ... 828
Schritt 4: Erstellen Sie ein AWS DMS replication instance ... 829
Schritt 5: Erstellen Sie eine AWS DMS Quell-Endpunkt ... 831
Schritt 6: Erstellen Sie eine AWS DMS Zielendpunkt ... 834
Schritt 7: Erstellen Sie eine Migrationsaufgabe und führen Sie sie aus ... 836
Schritt 8: Ändern des Anwendungsendpunkts auf den Amazon DocumentDB DocumentDB-Zielcluster ... 838
Long-Term Support- (LTS, Langzeit-Support) Versionen nutzen ... 838
Aktuelle LTS-Version ... 838
Wer sollte LTS verwenden ... 839
Wie erstelle ich einen neuen LTS-Cluster ... 839
Wie führe ich ein Upgrade von Engine-Version 3.6.0 oder 4.0.0 auf einen 5.0.0 LTS-Cluster durch ... 840
Wie überprüfe ich, ob mein vorhandener Engine-Cluster mit Version 5.0.0 auf LTS läuft ... 840
Erweiterter Support ... 842
Überblick über den erweiterten Support ... 843
Gebühren für erweiterten Support ... 843
Verantwortlichkeiten ... 844

Sicherheit 845
Passwortverwaltung mit AWS Secrets Manager 846
Einschränkungen für die Secrets Manager Manager-Integration mit Amazon DocumentDB . 847
Überblick über die Verwaltung von Primärbenutzerkennwörtern mit AWS Secrets Manager 847
Durchsetzung der Amazon DocumentDB DocumentDB-Verwaltung des primären Benutzerkennworts in AWS Secrets Manager 848
Verwaltung des primären Benutzerpassworts für einen Cluster mit Secrets Manager 849
Datenschutz 849
Client-side Verschlüsselung auf Feldebene 850
Verschlüsseln von Daten im Ruhezustand 857
Verschlüsseln von Daten während der Übertragung 866
Schlüsselverwaltung 878
Identitäts- und Zugriffsverwaltung 878
Zielgruppe 879
Authentifizierung mit Identitäten 879
Verwalten des Zugriffs mit Richtlinien 881
So funktioniert Amazon DocumentDB mit IAM 882
Identity-based Beispiele für Richtlinien 889
Fehlerbehebung 893
Verwaltung der Zugriffsberechtigungen für Ihre Amazon DocumentDB DocumentDB-Ressourcen 895
Verwenden von identitätsbasierten Richtlinien (IAM-Richtlinien) 901
AWS verwaltete Richtlinien für Amazon DocumentDB 905
Referenz zu Amazon DocumentDB DocumentDB-API-Berechtigungen 925
Cross-service verwirrter Stellvertreter, Prävention 934
Authentifizierung mit IAM-Identität 935
Erste Schritte mit IAM-Benutzern und -Rollen 936
Compute-Typen konfigurieren 939
Überwachung von Authentifizierungsanfragen 940
Verwenden der IAM-Authentifizierung 941
Treiber, die IAM unterstützen 941
Häufig gestellte Fragen zur IAM-Identitätsauthentifizierung 941
Amazon DocumentDB DocumentDB-Benutzer verwalten 942
Primär- und `Serviceadmin-Benutzer` 943
Zusätzliche Benutzer erstellen 943

Automatisches Rotieren von Passwörtern ... 946
Role-Based Zugriffskontrolle ... 946
RBAC-Konzepte ... 947
Erste Schritte mit den integrierten RBAC-Rollen ... 949
Erste Schritte mit benutzerdefinierten RBAC-Rollen ... 953
Als Benutzer eine Verbindung zu Amazon DocumentDB herstellen ... 957
Allgemeine Befehle ... 959
Funktionelle Unterschiede ... 964
Einschränkungen ... 964
Datenbankzugriff mit Role-Based Access Control ... 965
Protokollierung und Überwachung ... 973
Aktualisierung von Zertifikaten ... 974
Aktualisierung Ihrer Anwendung und Ihres Amazon DocumentDB-Clusters ... 975
Automatische Rotation von Serverzertifikaten ... 979
Fehlerbehebung ... 980
Häufig gestellte Fragen ... 981
Compliance-Validierung ... 988
Ausfallsicherheit ... 989
Sicherheit der Infrastruktur ... 990
VPC-Endpunkte (AWS PrivateLink) ... 991
Überlegungen zu VPC-Endpunkten ... 992
Verfügbarkeit in Regionen ... 992
Erstellen eines VPC-Schnittstellen-Endpunkts für die Amazon DocumentDB DocumentDB-API ... 993
Erstellen einer VPC-Endpunktrichtlinie für die Amazon DocumentDB DocumentDB-API ... 994
Bewährte Methoden für die Gewährleistung der Sicherheit ... 995
Prüfereignisse ... 996
Unterstützte Ereignisse ... 997
Auditing aktivieren ... 1003
Auditing deaktivieren ... 1010
Greifen Sie auf Ihre Ereignisse zu ... 1013
DML-Ereignisse filtern ... 1013
Amazon VPC und Amazon DocumentDB ... 1019
DocumentDB-Cluster in einer VPC ... 1019
Zugreifen auf einen Cluster in einer VPC ... 1033
Eine IPv4-only VPC für einen Cluster erstellen ... 1035

Erstellen Sie eine Dual-Stack-VPC für einen Cluster ... 1043
Sichern und Wiederherstellen ... 1055
Sichern und Wiederherstellen: Konzepte ... 1056
Grundlegendes zur Sicherungsspeicher-Nutzung in ... 1059
Daten speichern, wiederherstellen, importieren und exportieren ... 1061
`Mongodump` ... 1061
`mongorestore` ... 1062
`mongoexport` ... 1062
`Mongoimport` ... 1063
Tutorial ... 1064
Überlegungen zu Cluster-Snapshots ... 1066
Backup-Speicher ... 1067
Backup window ... 1068
Aufbewahrungszeitraum für Backups ... 1070
Kopieren Sie die Cluster-Snapshot- ... 1070
Vergleich von automatischen und manuellen Snapshots ... 1071
Einen manuellen Cluster-Snapshot erstellen ... 1073
Einen Cluster-Snapshot kopieren ... 1076
Kopieren freigegebener Snapshots ... 1077
Schnappschüsse werden kopiert AWS-Regionen ... 1077
Einschränkungen ... 1077
Umgang mit Verschlüsselungen ... 1078
Überlegungen zu Parametergruppen ... 1078
Einen Cluster-Snapshot kopieren ... 1079
Freigeben eines Cluster-Snapshots ... 1089
Freigeben eines verschlüsselten Snapshots ... 1089
Freigeben eines Snapshots ... 1093
Wiederherstellung aus einem Cluster-Snapshot ... 1097
Zu einem bestimmten Zeitpunkt wiederherstellen ... 1104
Löschen eines Cluster-Snapshots ... 1111
Amazon DocumentDB verwalten ... 1114
Überblick über die operativen Aufgaben ... 1115
Hinzufügen eines Replikats zu einem Amazon DocumentDB-Cluster ... 1115
Beschreibung von Clustern und Instanzen ... 1116
Einen Cluster-Snapshot erstellen ... 1118
Wiederherstellung aus einem Snapshot ... 1119

Eine Instanz aus einem Cluster entfernen ... 1121
Löschen eines Clusters ... 1121
Globale Cluster ... 1122
Was ist ein globaler Cluster? ... 1122
Wie sind globale Cluster nützlich? ... 1122
Was sind die aktuellen Einschränkungen globaler Cluster? ... 1123
Schnellstart-Anleitung ... 1123
Verwaltung globaler Cluster ... 1136
Globale Cluster verbinden ... 1144
Überwachung globaler Cluster ... 1144
Notfallwiederherstellung ... 1145
Verwalten von Clustern ... 1162
Cluster verstehen ... 1163
Cluster-Einstellungen ... 1166
Cluster-Speicherkonfigurationen ... 1168
Den Status eines Clusters ermitteln ... 1172
Cluster-Lebenszyklus ... 1173
Skalierung von Clustern ... 1217
Klonen eines Volumes für einen Cluster ... 1221
Grundlegendes zur Cluster-Fehlertoleranz ... 1235
Verwalten von Instances ... 1236
Den Status einer Instance ermitteln ... 1237
Instance-Lebenszyklus ... 1237
Instanzklassen verwalten ... 1261
NVMe-backed Instanzen ... 1274
Verwaltung von Subnetzgruppen ... 1277
Erstellen einer Subnetzgruppe ... 1278
Beschreibung einer Subnetzgruppe ... 1284
Ändern einer Subnetzgruppe ... 1286
Löschen einer Subnetzgruppe ... 1290
Hohe Verfügbarkeit und Replikation ... 1291
Skalierung von Lesevorgängen ... 1292
Hohe Verfügbarkeit ... 1292
Hinzufügen von -Replicas ... 1294
Failover ... 1294
Replikationsverzögerung ... 1299

Verwalten von Indexen ... 1300
Amazon DocumentDB DocumentDB-Indexerstellung ... 1301
Pflege Amazon DocumentDB DocumentDB-Indizes ... 1307
Verwaltung der Dokumentenkomprimierung ... 1309
Verwaltung der Dokumentenkomprimierung ... 1310
Überwachung der Dokumentenkomprimierung ... 1312
Verwaltung der wörterbuchbasierten Komprimierung ... 1313
Performanceaspekte ... 1314
Aktivierung der wörterbuchbasierten Komprimierung ... 1314
Erste Schritte ... 1315
Überwachen ... 1316
Verwaltung von Ereignissen ... 1317
Veranstaltungskategorien anzeigen ... 1317
Amazon DocumentDB DocumentDB-Ereignisse anzeigen ... 1320
Auswahl von Regionen und Availability Zones ... 1323
Verfügbarkeit in Regionen ... 1324
Verwaltung von Cluster-Parametergruppen ... 1326
Beschreibung von Cluster-Parametergruppen ... 1327
Cluster-Parametergruppen erstellen ... 1335
Cluster-Parametergruppen ändern ... 1338
Modifizieren von Clustern zur Verwendung benutzerdefinierter Cluster-Parametergruppen 1343
Cluster-Parametergruppen werden kopiert ... 1345
Cluster-Parametergruppen werden zurückgesetzt ... 1347
Cluster-Parametergruppen löschen ... 1350
Referenz zu den Cluster-Parametern ... 1353
Endpunkte verstehen ... 1376
Die Endpunkte eines Clusters finden ... 1377
Den Endpunkt einer Instanz finden ... 1379
Verbindung zu Endpunkten herstellen ... 1383
Grundlegendes zu Amazon DocumentDB DocumentDB-ARNs ... 1384
Konstruieren eines ARN ... 1385
Suchen eines ARNs ... 1389
Taggen von Ressourcen ... 1391
Übersicht über -Ressourcen-Tags ... 1391
Tag-Einschränkungen ... 1393
Hinzufügen oder Aktualisieren von Tags ... 1393

Auflisten von Tags ... 1395
Entfernen von Tags ... 1396
Wartung von Amazon DocumentDB ... 1398
Versionsnummerierung ... 1399
Wartungsfenster verwalten ... 1400
Engine-Patch-Benachrichtigungen ... 1403
Ausstehende Wartungsarbeiten anzeigen ... 1405
Engine-Updates ... 1408
Nebenversionen ... 1411
Betriebssystemupdates ... 1412
User-initiated Aktualisierungen ... 1415
Globale Cluster ... 1416
Grundlegendes zu Rollen im Zusammenhang mit Services ... 1417
Service-linked Rollenberechtigungen ... 1418
Erstellen einer serviceverknüpften Rolle ... 1420
Änderung einer serviceverknüpften Rolle ... 1420
Löschen einer serviceverknüpften Rolle ... 1420
Unterstützte Regionen für serviceverknüpfte Amazon DocumentDB DocumentDB-Rollen ... 1421
Change-Streams verwenden ... 1421
Unterstützte Vorgänge ... 1422
Fakturierung ... 1423
Einschränkungen ... 1423
Change-Streams aktivieren ... 1424
Change-Streams mit Python verwenden ... 1426
Vollständige Suche nach Dokumenten ... 1429
Wiederaufnahme eines Change-Streams ... 1430
Wiederaufnahme mit `startAtOperationTime` ... 1431
Wiederaufnahme mit `postBatchResumeToken` ... 1433
Transaktionen ... 1434
Änderung der Aufbewahrungsdauer von Protokollen ... 1435
Streams auf sekundären Instanzen ändern ... 1438
Sortierung verwenden ... 1440
Einschränkungen ... 1440
Ansichten verwenden ... 1441
Bewährte Methoden ... 1441
Kompatibilität mit Aggregator-Operatoren ... 1442

Nutzung von Indizes und Ansichten ... 1442
Verwenden AWS Lambda mit Change-Streams ... 1443
Einschränkungen ... 1444
Verwendung elastischer Cluster ... 1445
Anwendungsfälle für elastische Cluster ... 1446
Benutzerprofile ... 1446
Inhaltsverwaltung und historische Aufzeichnungen ... 1446
Vorteile elastischer Cluster ... 1446
AWS Serviceintegration ... 1447
Verfügbarkeit von Regionen und Versionen ... 1447
Regionale Verfügbarkeit für elastische Cluster ... 1447
Verfügbarkeit der Versionen ... 1448
Einschränkungen ... 1448
Elastisches Cluster-Management ... 1448
Abfrage- und Schreiboperationen ... 1449
Sammlungs- und Indexverwaltung ... 1449
Verwaltung und Diagnose ... 1450
Opt-in features ... 1450
Funktionsweise ... 1450
Elastisches Cluster-Sharding von Amazon DocumentDB ... 1451
Elastische Cluster-Migration ... 1455
Elastische Cluster-Skalierung ... 1455
Zuverlässigkeit elastischer Cluster ... 1455
Elastischer Cluster-Speicher und Verfügbarkeit ... 1455
Funktionale Unterschiede zwischen Amazon DocumentDB 4.0 und Elastic Clusters ... 1456
Erste Schritte ... 1457
Voraussetzungen ... 1458
Schritt 1: Erstellen Sie einen elastischen Cluster ... 1459
Schritt 2: Connect zu Ihrem Elastic Cluster her ... 1466
Schritt 3: Teilen Sie Ihre Sammlung, fügen Sie Daten ein und fragen Sie sie ab ... 1467
Schritt 4: Erkunden ... 1470
Best Practices ... 1471
Shard-Schlüssel auswählen ... 1471
Verbindungsverwaltung ... 1472
Sammlungen, die nicht geteilt wurden ... 1472
Skalierung elastischer Cluster ... 1472

Überwachung elastischer Cluster ... 1473
Verwaltung elastischer Cluster ... 1473
Modifizieren elastischer Cluster-Konfigurationen ... 1474
Überwachen eines elastischen Clusters ... 1477
Löschen eines elastischen Clusters ... 1481
Verwaltung von Elastic Cluster-Snapshots ... 1483
Stoppen und Starten eines elastischen Clusters ... 1499
Aufrechterhaltung elastischer Cluster ... 1503
Datenverschlüsselung im Ruhezustand ... 1512
So verwenden elastische Amazon DocumentDB-Cluster Zuschüsse in AWS KMS ... 1514
Erstellen eines kundenseitig verwalteten Schlüssels ... 1515
Überwachung Ihrer Verschlüsselungsschlüssel für Amazon DocumentDB Elastic Clusters 1516
Weitere Informationen ... 1522
Service-linked Rollen ... 1522
Service-linked Rollenberechtigungen für elastische Cluster ... 1522
Amazon DocumentDB überwachen ... 1527
Den Status eines Clusters überwachen ... 1529
Werte für den Cluster-Status ... 1529
Den Status eines Clusters überwachen ... 1531
Den Status einer Instance überwachen ... 1533
Instance-Statuswerte ... 1533
Überwachen Sie den Instance-Status mit dem AWS-Managementkonsole oder AWS CLI . 1536
Werte für den Integritätsstatus der Instanz ... 1538
Überwachen des Zustands der Instanz mit dem AWS-Managementkonsole ... 1538
Amazon DocumentDB DocumentDB-Empfehlungen anzeigen ... 1540
Ereignisabonnements ... 1543
Abonnieren von Ereignissen ... 1544
-Abonnements verwalten ... 1546
Kategorien und Nachrichten ... 1550
Überwachen von Amazon DocumentDB mit CloudWatch ... 1553
Amazon DocumentDB-Metriken ... 1553
CloudWatch Daten anzeigen ... 1573
Abmessungen von Amazon DocumentDB ... 1580
Überwachung von Opcounter-Metriken ... 1580
Überwachen von Datenbankverbindungen ... 1580
Protokollieren Amazon DocumentDB DocumentDB-API-Aufrufen mit CloudTrail ... 1581

Amazon DocumentDB DocumentDB-Informationen in CloudTrail 1581
Profilierung von Vorgängen 1582
Unterstützte Vorgänge 1583
Einschränkungen 1584
Den Profiler aktivieren 1584
Den Profiler deaktivieren 1589
Export von Profiler-Protokollen deaktivieren 1590
Greifen Sie auf Ihre Profiler-Protokolle zu 1592
Häufig gestellte Fragen 1593
Überwachung mit Performance Insights 1593
Konzepte von Performance Insights 1595
Aktivieren und Deaktivieren von Performance Insights 1599
Konfigurieren von Zugriffsrichtlinien für Performance Insights 1602
Analyse der Metriken mit dem Performance-Insights-Dashboard 1606
Abrufen von Metriken mit der Performance-Insights-API 1627
CloudWatch Amazon-Metriken für Performance Insights 1642
Performance Insights für Zählermetriken 1644
OpenSearch Integration 1647
Amazon OpenSearch Service als Ziel 1647
Schritt 1: Amazon OpenSearch Service-Domain oder OpenSearch serverlose Sammlung erstellen 1648
Schritt 2: Change-Streams auf dem Amazon DocumentDB-Cluster aktivieren 1648
Schritt 3: Richten Sie die Pipeline-Rolle mit Schreibberechtigungen für den Amazon S3 S3-Bucket und die Zieldomäne oder Sammlung ein 1648
Schritt 4: Fügen Sie die Berechtigungen hinzu, die für die zu erstellende Pipeline-Rolle erforderlich sind X-ENI 1649
Schritt 5: Erstellen Sie die Pipeline 1650
Einschränkungen 1651
DocumentDB serverlos verwenden 1652
Anwendungsfälle für Serverless 1652
Serverlose Nutzung von Amazon DocumentDB für bestehende bereitgestellte Workloads . 1654
Vorteile von Amazon DocumentDB serverlos 1655
Wie funktioniert Serverless 1656
-Übersicht 1656
Konfigurationen für Amazon DocumentDB-Cluster 1658
Serverlose Skalierungskapazität von Amazon DocumentDB 1658

Serverlose Skalierung von Amazon DocumentDB ... 1660
Ruhezustand (0,5 DCUs) ... 1662
Anforderungen und Einschränkungen für serverlose Server ... 1663
Anforderungen an die Funktionen ... 1663
Einen Cluster erstellen, der Serverless verwendet ... 1664
Einen serverlosen Amazon DocumentDB-Cluster erstellen ... 1665
Hinzufügen einer serverlosen Amazon DocumentDB DocumentDB-Instance ... 1668
Migration zu serverlosem System ... 1668
Migration vorhandener DocumentDB-Cluster auf Serverless ... 1669
Migration von MongoDB zu DocumentDB serverlos ... 1674
Verwaltung von serverlosen Systemen ... 1674
Die Konfiguration des Skalierungskapazitätsbereichs eines Clusters anzeigen und ändern 1674
Die Promotion-Stufe für serverlose Lesegeräte anzeigen und ändern ... 1678
Grenzwerte für serverlose Instances ... 1680
Konfiguration für serverlose Skalierung ... 1683
Auswahl des Skalierungskapazitätsbereichs für einen serverlosen DocumentDB-Cluster .. 1683
`MinCapacity`Einstellung für einen serverlosen DocumentDB-Cluster auswählen ... 1683
`MaxCapacity`Einstellung für einen serverlosen DocumentDB-Cluster auswählen ... 1686
Vermeiden von Fehlern aufgrund von zu wenig Speicher ... 1688
Warum wird meine serverlose Instance nicht herunterskaliert? ... 1689
Serverlose Überwachung ... 1690
Nicht genügend Arbeitsspeicher: Status inkompatibler Parameter ... 1690
CloudWatch Amazon-Metriken für DocumentDB serverlos ... 1691
Überwachung der serverlosen Leistung von DocumentDB mit Performance Insights ... 1696
Entwickeln mit Amazon DocumentDB ... 1697
Mit DocumentDB Connect ... 1697
Programmgesteuert eine Verbindung herstellen ... 1697
Verbindung von außerhalb einer Amazon VPC herstellen ... 1726
Als Replikatsatz eine Verbindung herstellen ... 1728
Connect mit Studio 3T her ... 1733
Connect mit DataGrip ... 1743
Stellen Sie mithilfe von Amazon EC2 eine Verbindung her ... 1748
Stellen Sie mithilfe des JDBC-Treibers eine Verbindung her ... 1787
Stellen Sie mithilfe des ODBC-Treibers eine Verbindung her ... 1804
Programm mit DocumentDB ... 1818
DocumentDB Java-Programmierhandbuch ... 1818

Verwenden der JSON-Schemavalidierung ... 1852
Kontingente und -Einschränkungen ... 1863
Unterstützte Instance-Typen ... 1863
Unterstützte -Regionen ... 1865
Regionale Kontingente ... 1867
Aggregationsgrenzen ... 1870
Cluster-Grenzwerte ... 1870
Instance-Limits ... 1872
Benennungseinschränkungen: ... 1878
TTL-Einschränkungen ... 1880
Elastische Cluster-Grenzwerte ... 1880
Limits für elastische Cluster-Shards ... 1881
CPU-, Speicher-, Verbindungs- und Cursorlimits für Elastic Cluster pro Shard ... 1882
Abfrage ... 1883
Dokumente abfragen ... 1883
Alle Dokumente werden abgerufen ... 1884
Passende Feldwerte ... 1884
Eingebettete Dokumente ... 1884
Feldwerte in eingebetteten Dokumenten ... 1885
Abgleich mit einem Array ... 1885
Übereinstimmende Werte in einem Array ... 1885
Verwenden von Operatoren ... 1886
Plan abfragen ... 1886
Abfrageplan ... 1886
Plan-Cache abfragen ... 1888
Erläutern Sie die Ergebnisse ... 1889
Phase des Scannens und Filterns ... 1890
Index-Kreuzung ... 1891
Indexunion ... 1891
Mehrfacher Index intersection/union ... 1892
Zusammengesetzter Index ... 1893
Phase sortieren ... 1893
Gruppenphase ... 1894
Abfrageplaner v2 ... 1894
Voraussetzungen ... 1894
Planner Version 2.0 als Standard-Abfrageplaner auswählen ... 1895

Best Practices ... 1895
Einschränkungen ... 1896
Verbesserungen bei den Operatoren „Suchen und Aktualisieren“ ... 1896
Planen Sie die Cache-Filter-API ... 1899
Mögliche Verhaltensunterschiede zwischen Planner Version 1.0, 2.0 und MongoDB ... 1901
Planner Version 2.0 schließt Verhaltenslücke mit MongoDB ... 1908
Abfrageplaner v3 ... 1910
Voraussetzungen ... 1911
Auswahl der Planner-Version 3.0 als Standard-Abfrageplaner ... 1911
Best Practices ... 1911
Einschränkungen ... 1912
Verbesserungen bei aggregierten und unterschiedlichen Operatoren ... 1912
Mögliche Verhaltensunterschiede zwischen Planner Version 1.0, 3.0 und MongoDB ... 1914
Koordinatenbasierte Daten ... 1915
-Übersicht ... 1
Indizierung und Speicherung von Geodaten ... 1916
Abfragen von koordinatenbasierten Daten ... 1917
Einschränkungen ... 1921
Teilweiser Index ... 1921
Erstellen Sie einen Teilindex ... 1922
Unterstützte Operatoren ... 1922
Abfrage mit einem Teilindex ... 1922
Funktionen des partiellen Indexes ... 1923
Einschränkungen des partiellen Indexes ... 1928
Textsuche ... 1929
Unterstützte Funktionen ... 1929
Verwenden des Amazon DocumentDB-Textindex ... 1930
Unterschiede zu MongoDB ... 1935
Bewährte Verfahren und Richtlinien ... 1936
Textindex V2 ... 1936
Einschränkungen ... 1937
Indizes ... 1938
Indexverwaltung ... 1938
Indexerstellung ... 1938
Verwaltung von Indizes ... 1945
Bewährte Methoden für die Arbeit mit Indizes ... 1947

Indextypen ... 1949
Indizes für einzelne Felder ... 1949
Zusammengesetzte Indizes ... 1951
Multi-key Indizes ... 1953
Textindizes ... 1954
Geospatiale Indizes ... 1955
Vektor-Indizes ... 1956
Indexeigenschaften ... 1958
Topics ... 1958
Name ... 1959
eindeutig ... 1962
Sparse ... 1965
teilweise FilterExpression ... 1969
ablaufen AfterSeconds ... 1973
Optimierung der Leistung ... 1976
Allgemeine Leistungsprobleme ... 1976
Hohe CPU-Auslastung ... 1976
Probleme mit der Verbindung ... 1978
Die Abfrage läuft langsam ... 1986
Anti-patterns ... 1990
Zusammengesetzter Index mit Anti-Pattern und mehr als 3 Attributen ... 1991
Abfragen mit langer Laufzeit ... 1993
Wenig genutzte und redundante Indizes ... 1996
Multi-key Indizes mit großen Arrays ... 1999
Tipps zur Leistungsverbesserung ... 2000
1. Verwenden Sie $match als erste Phase in Aggregationspipelines ... 2000
2. Verwenden Sie $project in der Aggregationspipeline, um die Größe der Pipeline-Daten zu minimieren ... 2000
3. Aktivieren Sie die Dokumentenkomprimierung, um die Speicherkosten und Kosten zu I/O senken und die Abfrageleistung zu verbessern ... 2001
4. Nutzen Sie Indizes für eine optimale Abfrageleistung ... 2002
5. Optimieren Sie Datenmodelle auf der Grundlage von Abfragemustern ... 2003
Plananalyse abfragen ... 2005
Allgemeiner Zeitplan ... 2007
Phasen der Ausführung ... 2007
Grundlegendes zu DocsExamined in Explain Plan Execution Stats ... 2009

Fehlerbehebung 2018
Probleme mit der Verbindung 2018
Es kann keine Verbindung zu einem Amazon DocumentDB DocumentDB-Endpunkt hergestellt werden 2018
Testen einer Verbindung zu einer Amazon DocumentDB DocumentDB-Instance 2024
Verbindung zu einem ungültigen Endpunkt herstellen 2024
Die Treiberkonfiguration wirkt sich auf die Anzahl der Verbindungen aus 2025
Indizes 2026
Die Indexerstellung schlägt fehl 2026
Latenzprobleme und Fehler bei der Indexerstellung im Hintergrund 2026
Indexblähung 2027
Leistung und Ressourcennutzung 2028
Statistiken zum Einfügen, Aktualisieren und Löschen anzeigen 2029
Analysieren Sie die Cache-Leistung 2031
Finden und Beenden von langsamen und blockierten Abfragen? 2032
Anzeigen eines Abfrageplans und Optimieren einer Abfrage 2033
Wie kann ich mir einen Abfrageplan in elastischen Clustern ansehen? 2036
Auflisten aller aktuell auf einer Instance ausgeführten Operationen 2038
Ermitteln, wann eine Abfrage Fortschritte macht 2041
Ermitteln, warum ein System plötzlich langsam ausgeführt wird 2044
Ermitteln der Ursache einer hohen CPU-Nutzung 2045
Finde die offenen Cursor auf einer Instanz 2046
Aktuelle Version der Amazon DocumentDB DocumentDB-Engine anzeigen 2047
Analysieren Sie die Indexnutzung und identifizieren Sie ungenutzte Indizes 2047
Identifizieren Sie fehlende Indizes 2049
Wie stelle ich fest, dass die Datenbanksammlung überlastet ist? 2051
Zusammenfassung nützlicher Abfragen 2053
Müllabfuhr 2054
Grundlegendes zur Müllabfuhr in Amazon DocumentDB 2054
Prozess der Müllabfuhr 2055
Speicherarchitektur und erweiterter Speicher 2056
Überwachung der Müllabfuhr 2057
Beispiel für eine CollStats-Ausgabe 2060
Häufig gestellte Fragen 2062
Versionshinweise 2065
Versionshinweise zur Amazon DocumentDB DocumentDB-Engine 2065

Allgemeine Versionshinweise zu Amazon DocumentDB 2125
Versionshinweise zu Amazon DocumentDB Elastic Clusters 2129
Dokumentverlauf 2134
..... mmcxlvii

Was ist Amazon DocumentDB (mit MongoDB-Kompatibilität)

Amazon DocumentDB (mit MongoDB-Kompatibilität) ist ein schneller, zuverlässiger und vollständig verwalteter Datenbankservice. Amazon DocumentDB macht es einfach, MongoDB-compatible Datenbanken in der Cloud einzurichten, zu betreiben und zu skalieren. Mit Amazon DocumentDB können Sie denselben Anwendungscode ausführen und dieselben Treiber und Tools verwenden, die Sie mit MongoDB verwenden.

Bevor Sie Amazon DocumentDB verwenden, sollten Sie sich mit den unter beschriebenen Konzepten und Funktionen vertraut machen. Funktionsweise Anschließend führen Sie die Schritte unter Leitfaden für die ersten Schritte aus.

Themen

- Überblick über Amazon DocumentDB
- Cluster
- Instances
- Regionen und Availability Zones
- Amazon DocumentDB — Preise
- Überwachen
- Schnittstellen
- Als nächstes
- Amazon DocumentDB: So funktioniert es
- Was ist eine Dokumentendatenbank?

Überblick über Amazon DocumentDB

Im Folgenden sind einige wichtige Funktionen von Amazon DocumentDB aufgeführt:

- Amazon DocumentDB unterstützt zwei Arten von Clustern: instanzbasierte Cluster und elastische Cluster. Elastic Cluster unterstützen Workloads mit einer Speicherkapazität von Millionen reads/writes pro Sekunde und Petabyte. Weitere Informationen zu elastischen Clustern finden Sie unter. Verwendung elastischer Amazon DocumentDB-Cluster Der folgende Inhalt bezieht sich auf Amazon DocumentDB DocumentDB-Instance-basierte Cluster.

- Amazon DocumentDB vergrößert automatisch die Größe Ihres Speichervolumens, wenn Ihr Datenbankspeicherbedarf steigt. Ihr Speichervolumen wächst in Schritten von 10 GB bis zu einem Maximum von 128 TiB. Sie müssen in Hinblick auf zukünftiges Wachstum keinen zusätzlichen Speicher für Ihren Cluster bereitstellen.
- Mit Amazon DocumentDB können Sie den Lesedurchsatz erhöhen, um umfangreiche Anwendungsanfragen zu unterstützen, indem Sie bis zu 15 Replikat-Instances erstellen. Amazon DocumentDB DocumentDB-Replikate nutzen denselben zugrunde liegenden Speicher, wodurch die Kosten gesenkt werden und Schreibvorgänge an den Replikatknoten vermieden werden müssen. Diese Funktion setzt mehr Rechenleistung für die Bearbeitung von Leseanforderungen frei und reduziert die Replikatverzögerung — oft bis auf einstellige Millisekunden. Sie können Replikate unabhängig von der Größe des Speichervolumens innerhalb von Minuten hinzufügen. Amazon DocumentDB bietet auch einen Leser-Endpunkt, sodass die Anwendung eine Verbindung herstellen kann, ohne dass Replikate nachverfolgt werden müssen, wenn sie hinzugefügt und entfernt werden.
- Mit Amazon DocumentDB können Sie die Rechen- und Speicherressourcen für jede Ihrer Instances nach oben oder unten skalieren. Skalierungsvorgänge bei der Datenverarbeitung dauern in der Regel nur wenige Minuten.
- Amazon DocumentDB wird in Amazon Virtual Private Cloud (Amazon VPC) ausgeführt, sodass Sie Ihre Datenbank in Ihrem eigenen virtuellen Netzwerk isolieren können. Sie können auch Firewalleinstellungen so konfigurieren, dass der Netzwerkzugriff auf Ihren Cluster gesteuert wird.
- Amazon DocumentDB überwacht kontinuierlich den Zustand Ihres Clusters. Bei einem Instance-Ausfall startet Amazon DocumentDB die Instance und die zugehörigen Prozesse automatisch neu. Amazon DocumentDB benötigt keine Wiederholung von Datenbank-Redo-Logs bei der Wiederherstellung nach einem Absturz, wodurch die Neustartzeiten erheblich reduziert werden. Amazon DocumentDB isoliert außerdem den Datenbank-Cache vom Datenbankprozess, sodass der Cache einen Instance-Neustart übersteht.
- Bei einem Instance-Ausfall automatisiert Amazon DocumentDB den Failover auf eines von bis zu 15 Amazon DocumentDB DocumentDB-Replikaten, die Sie in anderen Availability Zones erstellen. Wenn keine Replikate bereitgestellt wurden und ein Fehler auftritt, versucht Amazon DocumentDB, automatisch eine neue Amazon DocumentDB DocumentDB-Instance zu erstellen.
- Die Backup-Funktion in Amazon DocumentDB ermöglicht eine Point-in-Time-Wiederherstellung für Ihren Cluster. Diese Funktion ermöglicht Ihnen, Ihren Cluster zu jeder Sekunde innerhalb der Aufbewahrungsfrist bis zu den letzten 5 Minuten wiederherzustellen. Sie können den Aufbewahrungszeitraum für automatische Backups auf maximal 35 Tage festlegen. Automatisierte Backups werden im Amazon Simple Storage Service (Amazon S3) gespeichert, der für eine

Haltbarkeit von 99,999999999% ausgelegt ist. Amazon DocumentDB-Backups sind automatisch, inkrementell und kontinuierlich und haben keine Auswirkungen auf die Leistung Ihres Clusters.

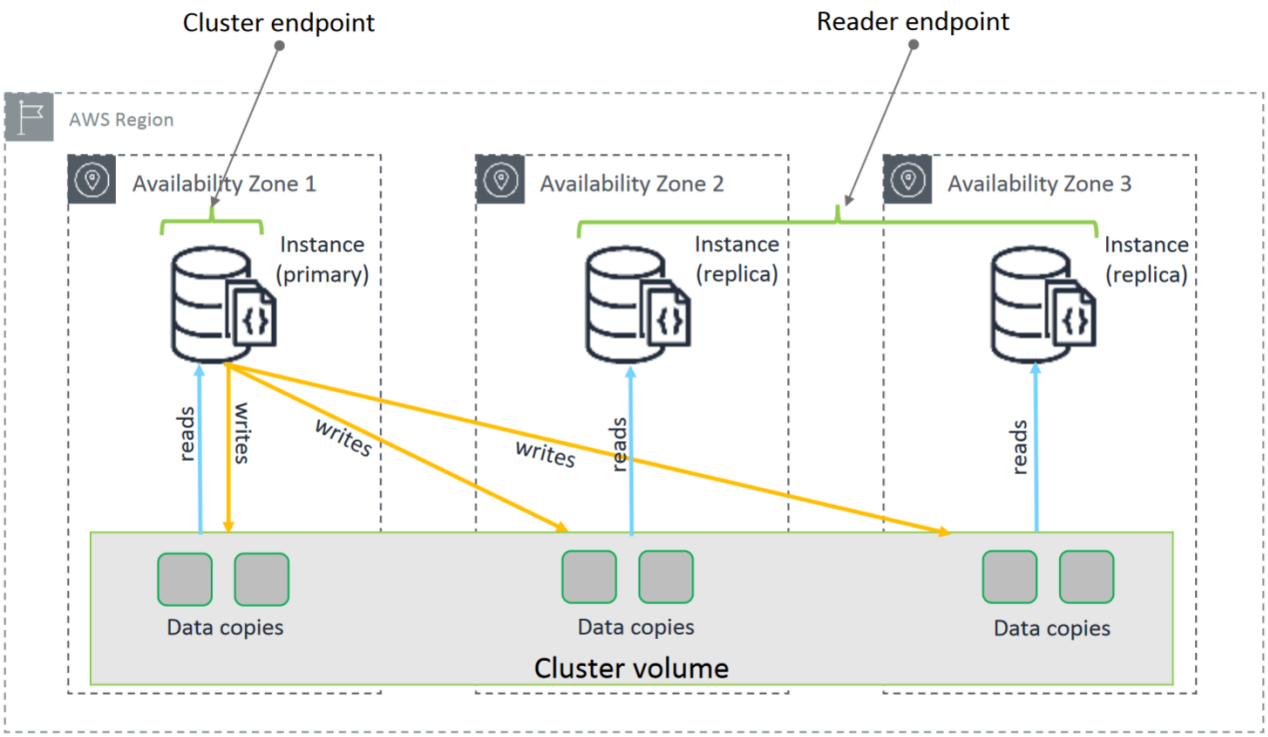
- Mit Amazon DocumentDB können Sie Ihre Datenbanken mit Schlüsseln verschlüsseln, die Sie über AWS Key Management Service ()AWS KMS erstellen und kontrollieren. In einem Datenbank-Cluster, der mit Amazon DocumentDB DocumentDB-Verschlüsselung ausgeführt wird, werden Daten, die im Ruhezustand im zugrunde liegenden Speicher gespeichert sind, verschlüsselt. Die automatischen Sicherungen, Snapshots und Replicas im gleichen Cluster werden ebenfalls verschlüsselt.
- Amazon DocumentDB ist im Rahmen des Federal Risk and Authorization Management Program (FedRAMP) autorisiert. Es verfügt über eine FedRAMP High-Autorisierung für AWS GovCloud (US-) Regionen und eine FedRAMP Moderate-Autorisierung für US-Regionen. AWS East/West Einzelheiten zu den Compliance-Maßnahmen AWS und den Bemühungen zur Einhaltung der Vorschriften finden Sie unter AWS Services im Umfang nach Compliance-Programmen.

Wenn Sie mit AWS Services noch nicht vertraut sind, finden Sie in den folgenden Ressourcen weitere Informationen:

- AWS bietet Dienste für Datenverarbeitung, Datenbanken, Speicherung, Analyse und andere Funktionen. Eine Übersicht über alle AWS Services finden Sie unter Cloud Computing with Amazon Web Services.
- AWS bietet eine Reihe von Datenbankdiensten. Hinweise dazu, welcher Dienst für Ihre Umgebung am besten geeignet ist, finden Sie unter Datenbanken auf AWS.

Cluster

Ein Cluster besteht aus 0 bis 16 Instances und einem Cluster-Speichervolume, das die Daten für diese Instances verwaltet. Alle Schreibvorgänge erfolgen über die primäre Instance. Alle Instances (primäre und Replicas) unterstützen Lesevorgänge. Die Daten des Clusters werden im Cluster-Volume gespeichert, mit Kopien in drei verschiedenen Availability Zones.



Instanzbasierte Amazon DocumentDB 5.0-Cluster unterstützen zwei Speicherkonfigurationen für einen Datenbankcluster: Amazon DocumentDB-Standard und Amazon DocumentDB. I/O-optimized Weitere Informationen finden Sie unter Amazon DocumentDB-Cluster-Speicherkonfigurationen.

Instances

Eine Amazon DocumentDB DocumentDB-Instance ist eine isolierte Datenbankumgebung in der Cloud. Eine Instance kann mehrere von Benutzern erstellte Datenbanken enthalten. Sie können eine Instance mit dem AWS-Managementkonsole oder dem AWS CLI erstellen und ändern.

Die Rechenleistung und die Speicherkapazität einer Instanz werden durch ihre Instanzklasse bestimmt. Sie können die Instance auswählen, die Ihren Anforderungen am besten entspricht. Wenn sich Ihre Anforderungen im Laufe der Zeit ändern, können Sie eine andere Instance-Klasse wählen. Spezifikationen für DB-Instance-Klassen finden Sie unter Spezifikationen der Instanzklasse

Amazon DocumentDB DocumentDB-Instances werden nur in der Amazon VPC-Umgebung ausgeführt. Amazon VPC gibt Ihnen die Kontrolle über Ihre virtuelle Netzwerkumgebung: Sie können Ihren eigenen IP-Adressbereich wählen, Subnetze erstellen und Routing- und Zugriffskontrolllisten (ACLs) konfigurieren.

Bevor Sie Amazon DocumentDB DocumentDB-Instances erstellen können, müssen Sie einen Cluster erstellen, der die Instances enthält.

Nicht alle Instance-Klassen werden in allen Regionen unterstützt. Die folgende Tabelle gibt an, welche Instance-Klassen von in den jeweiligen Regionen unterstützt werden.

> **Note**
>
> Eine vollständige Liste der Instance-Typen, die von Amazon DocumentDB in jeder Instance-Klasse unterstützt werden, finden Sie unterSpezifikationen der Instanzklasse.

Unterstützte Instance-Klassen nach Region

Region	R8G	R6GD	R6G	R5	R4	T4 G	T3	Serverless
USA Ost (Ohio)	Unterstützt	Unterstützt	Unterstützt	Unterstützt	Unterstützt	Unterstützt	Unterstützt	Unterstützt
USA Ost (Nord-Virginia)	Unterstützt	Unterstützt	Unterstützt	Unterstützt	Unterstützt	Unterstützt	Unterstützt	Unterstützt
USA West (Oregon)	Unterstützt	Unterstützt	Unterstützt	Unterstützt	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Afrika (Kapstadt)			Unterstützt	Unterstützt		Unterstützt	Unterstützt	Unterstützt
Südamerika (São Paulo)		Unterstützt	Unterstützt	Unterstützt		Unterstützt	Unterstützt	Unterstützt
Asien-Pazifik (Hongkong)			Unterstützt	Unterstützt		Unterstützt	Unterstützt	Unterstützt
Asien-Pazifik (Hyderabad)			Unterstützt	Unterstützt		Unterstützt	Unterstützt	Unterstützt
Asien-Pazifik (Malaysia)			Unterstützt			Unterstützt	Unterstützt	

Region	R8G	R6GD	R6G	R5	R4	T4 G	T3	Serverless
Asien-Pazifik (Mumbai)	Unterstützt	Unterstützt	Unterstützt	Unterstützt		Unterstützt	Unterstützt	Unterstützt
Asien-Pazifik (Osaka)		Unterstützt	Unterstützt	Unterstützt		Unterstützt	Unterstützt	
Asien-Pazifik (Seoul)	Unterstützt	Unterstützt	Unterstützt	Unterstützt		Unterstützt	Unterstützt	Unterstützt
Asien-Pazifik (Sydney)	Unterstützt	Unterstützt	Unterstützt	Unterstützt		Unterstützt	Unterstützt	Unterstützt
Asien-Pazifik (Jakarta)	Unterstützt	Unterstützt	Unterstützt	Unterstützt		Unterstützt	Unterstützt	
Asien-Pazifik (Melbourne)			Unterstützt	Unterstützt		Unterstützt	Unterstützt	
Asien-Pazifik (Singapur)	Unterstützt	Unterstützt	Unterstützt	Unterstützt		Unterstützt	Unterstützt	Unterstützt
Asien-Pazifik (Thailand)			Unterstützt			Unterstützt	Unterstützt	
Asien-Pazifik (Tokio)	Unterstützt	Unterstützt	Unterstützt	Unterstützt		Unterstützt	Unterstützt	Unterstützt
Kanada (Zentral)	Unterstützt	Unterstützt	Unterstützt	Unterstützt		Unterstützt	Unterstützt	Unterstützt
Kanada West (Calgary)			Unterstützt	Unterstützt		Unterstützt	Unterstützt	
Europa (Frankfurt)	Unterstützt	Unterstützt	Unterstützt	Unterstützt		Unterstützt	Unterstützt	Unterstützt

Region	R8G	R6GD	R6G	R5	R4	T4 G	T3	Serverless
Europa (Zürich)		Unterstützt	Unterstützt	Unterstützt		Unterstützt	Unterstützt	
Europa (Irland)	Unterstützt	Unterstützt	Unterstützt	Unterstützt	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Europa (London)		Unterstützt	Unterstützt	Unterstützt		Unterstützt	Unterstützt	Unterstützt
Europa (Milan)			Unterstützt	Unterstützt		Unterstützt	Unterstützt	Unterstützt
Europa (Paris)		Unterstützt	Unterstützt	Unterstützt		Unterstützt	Unterstützt	Unterstützt
Europa (Spain)	Unterstützt	Unterstützt	Unterstützt	Unterstützt		Unterstützt	Unterstützt	Unterstützt
Europa (Stockholm)	Unterstützt	Unterstützt	Unterstützt	Unterstützt		Unterstützt	Unterstützt	
Mexiko (Zentral)			Unterstützt			Unterstützt	Unterstützt	
Naher Osten (VAE)			Unterstützt	Unterstützt		Unterstützt	Unterstützt	Unterstützt
China (Peking)		Unterstützt	Unterstützt	Unterstützt		Unterstützt	Unterstützt	Unterstützt
China (Ningxia)			Unterstützt	Unterstützt		Unterstützt	Unterstützt	Unterstützt
Israel (Tel Aviv)			Unterstützt	Unterstützt		Unterstützt	Unterstützt	

Region	R8G	R6GD	R6G	R5	R4	T4 G	T3	Serverless
AWS GovCloud (US-West)	Unterstützt	Unterstützt	Unterstützt	Unterstützt			Unterstützt	Unterstützt
AWS GovCloud (US-East)		Unterstützt	Unterstützt	Unterstützt		Unterstützt	Unterstützt	Unterstützt

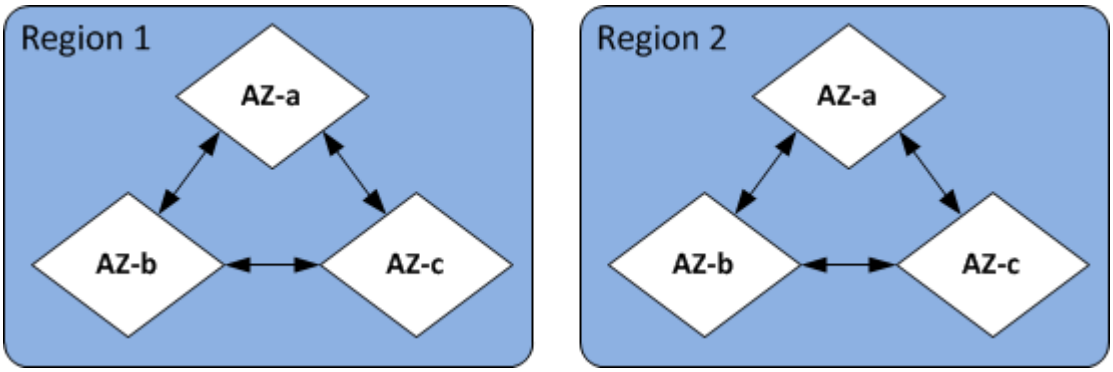
Regionen und Availability Zones

Regionen und Availability Zones definieren die physischen Standorte und Instances Ihres Clusters.

Regionen

AWS Cloud-Computing-Ressourcen sind in hochverfügbaren Rechenzentren in verschiedenen Regionen der Welt (z. B. Nordamerika, Europa oder Asien) untergebracht. Jeder Rechenzentrumsstandort wird als Region bezeichnet.

Jede AWS Region ist so konzipiert, dass sie vollständig von den anderen AWS Regionen isoliert ist. Innerhalb jeder gibt es mehrere Availability Zones (Verfügbarkeitszonen). Durch das Starten Ihrer Knoten in verschiedenen Availability Zones können Sie eine größtmögliche Fehlertoleranz zu erreichen. Das folgende Diagramm zeigt einen allgemeinen Überblick über die Funktionsweise von AWS Regionen und Availability Zones.



Availability Zones

Jede AWS Region enthält mehrere unterschiedliche Standorte, die als Availability Zones bezeichnet werden. Jede Availability Zone wurde so konzipiert, dass sie von Fehlern in anderen Availability Zones isoliert ist und eine kostengünstige Netzwerkverbindung mit geringer Latenz zu anderen

Availability Zones in derselben Region bereitstellt. Indem Instances für einen bestimmten Cluster in mehreren Availability Zones gestartet werden, können Sie Ihre Anwendungen vor dem unwahrscheinlichen Fall des Fehlschlagens einer Availability Zone schützen.

Die Amazon DocumentDB DocumentDB-Architektur trennt Speicher und Datenverarbeitung. Für die Speicherebene repliziert Amazon DocumentDB sechs Kopien Ihrer Daten in drei AWS Availability Zones. Wenn Sie beispielsweise einen Amazon DocumentDB-Cluster in einer Region starten, die nur zwei Availability Zones unterstützt, wird Ihr Datenspeicher auf sechs Arten in drei Availability Zones repliziert, aber Ihre Compute-Instances sind nur in zwei Availability Zones verfügbar.

In der folgenden Tabelle ist die Anzahl der Availability Zones aufgeführt, die Sie in einer bestimmten Umgebung verwenden können AWS-Region , um Recheninstanzen für Ihren Cluster bereitzustellen.

Name der Region	Region	Availability Zones (Compute)
USA Ost (Ohio)	`us-east-2`	3
USA Ost (Nord-Virginia)	`us-east-1`	6
USA West (Oregon)	`us-west-2`	4
Afrika (Kapstadt)	`af-south-1`	3
Südamerika (São Paulo)	`sa-east-1`	3
Asien-Pazifik (Hongkong)	`ap-east-1`	3
Asien-Pazifik (Hyderabad)	`ap-south-2`	3
Asien-Pazifik (Malaysia)	`ap-southeast-5`	3
Asien-Pazifik (Mumbai)	`ap-south-1`	3
Asien-Pazifik (Osaka)	`ap-northeast-3`	3

Name der Region	Region	Availability Zones (Compute)
Asien-Pazifik (Seoul)	ap-northeast-2	4
Asien-Pazifik (Singapur)	ap-southeast-1	3
Asien-Pazifik (Sydney)	ap-southeast-2	3
Asien-Pazifik (Jakarta)	ap-southeast-3	3
Asien-Pazifik (Melbourne)	ap-southeast-4	3
Asien-Pazifik (Thailand)	ap-southeast-7	3
Asien-Pazifik (Tokio)	ap-northeast-1	3
Kanada (Zentral)	ca-central-1	3
Kanada West (Calgary)	ca-west-1	3
Region China (Peking)	cn-north-1	3
China (Ningxia)	cn-northwest-1	3
Europa (Frankfurt)	eu-central-1	3
Europa (Zürich)	eu-central-2	3
Europa (Irland)	eu-west-1	3
Europa (London)	eu-west-2	3
Europa (Milan)	eu-south-1	3

Name der Region	Region	Availability Zones (Compute)
Europa (Paris)	`eu-west-3`	3
Europa (Spain)	`eu-south-2`	3
Europa (Stockholm)	`eu-north-1`	3
Mexiko (Zentral)	`mx-central-1`	3
Naher Osten (VAE)	`me-central-1`	3
Israel (Tel Aviv)	`il-central-1`	3
AWS GovCloud (US-West)	`us-gov-west-1`	3
AWS GovCloud (US-East)	`us-gov-east-1`	3

Amazon DocumentDB — Preise

Amazon DocumentDB-Cluster werden auf der Grundlage der folgenden Komponenten abgerechnet:

- Instance-Stunden (pro Stunde) — Basierend auf der Instance-Klasse der Instance (z. B.). `db.r5.xlarge` Die Preise werden auf Stundenbasis aufgeführt, aber Rechnungen werden jetzt auf die Sekunde genau kalkuliert und zeigen die Zeiten im Dezimalformat an. Die Nutzung von Amazon DocumentDB wird in Sekundenschritten mit einer Mindestdauer von 10 Minuten abgerechnet. Weitere Informationen finden Sie unter Instanzklassen verwalten.
- I/O Anfragen (pro 1 Million Anfragen pro Monat) — Gesamtzahl der I/O Speicheranforderungen, die Sie in einem Abrechnungszeitraum stellen.
- Backup-Speicher (pro GiB pro Monat) — Backup-Speicher ist der Speicher, der automatisierten Datenbank-Backups und allen aktiven Datenbank-Snapshots, die Sie erstellt haben, zugeordnet ist. Wenn Sie die Aufbewahrungszeit Ihrer Backups erhöhen oder zusätzliche Datenbank-Snapshots erstellen, belegt Ihre Datenbank dementsprechend mehr Backup-Speicher. Backup-Speicher wird gemessen GB-months und gilt nicht pro Sekunde. Weitere Informationen finden Sie unter Sichern und Wiederherstellen in Amazon DocumentDB.

- Datenübertragung (pro GB) — Datenübertragung innerhalb und außerhalb Ihrer Instance vom oder ins Internet oder in andere AWS Regionen.

Weitere Informationen finden Sie unter Amazon DocumentDB DocumentDB-Preise.

Kostenlose Testversion

Sie können Amazon DocumentDB mit der einmonatigen kostenlosen Testversion kostenlos testen. Weitere Informationen finden Sie unter Kostenlose Testversion in den Preisen von Amazon DocumentDB oder in den häufig gestellten Fragen zur kostenlosen Amazon DocumentDB-Testversion.

Überwachen

Es gibt verschiedene Möglichkeiten, die Leistung und den Zustand einer Instance zu überwachen. Sie können den kostenlosen CloudWatch Amazon-Service verwenden, um die Leistung und den Zustand einer Instance zu überwachen. Leistungsdiagramme finden Sie in der Amazon DocumentDB DocumentDB-Konsole. Sie können Amazon DocumentDB DocumentDB-Ereignisse abonnieren, um benachrichtigt zu werden, wenn Änderungen an einer Instance, einem Snapshot, einer Parametergruppe oder einer Sicherheitsgruppe auftreten.

Weitere Informationen finden Sie hier:

- Überwachen von Amazon DocumentDB mit CloudWatch
- Protokollieren Amazon DocumentDB DocumentDB-API-Aufrufen mit AWS CloudTrail

Schnittstellen

Es gibt mehrere Möglichkeiten, mit Amazon DocumentDB zu interagieren, einschließlich der AWS-Managementkonsole und der AWS CLI.

AWS-Managementkonsole

Das AWS-Managementkonsole ist eine einfache webbasierte Benutzeroberfläche. Sie können Ihre Cluster und Instances von der Konsole aus verwalten, ohne dass eine Programmierung erforderlich ist. Um auf die Amazon DocumentDB DocumentDB-Konsole zuzugreifen, melden Sie sich bei der an

AWS-Managementkonsole und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter. https://console.aws.amazon.com/docdb

AWS CLI

Sie können die AWS Command Line Interface (AWS CLI) verwenden, um Ihre Amazon DocumentDB-Cluster und -Instances zu verwalten. Mit minimaler Konfiguration können Sie beginnen, alle Funktionen der Amazon DocumentDB DocumentDB-Konsole von Ihrem bevorzugten Terminalprogramm aus zu nutzen.

- Informationen zur AWS CLI Installation von finden Sie unter Installation der AWS Befehlszeilenschnittstelle.
- Informationen zur Verwendung von AWS CLI für Amazon DocumentDB finden Sie unter AWS Command Line Interface Reference for Amazon DocumentDB.

MongoDB-Treiber

Für die Entwicklung und das Schreiben von Anwendungen für einen Amazon DocumentDB-Cluster können Sie die MongoDB-Treiber auch mit Amazon DocumentDB verwenden. Weitere Informationen finden Sie auf der Registerkarte MongoDB-Shell unter Verbindung bei aktiviertem TLS herstellen oderVerbindung bei deaktiviertem TLS herstellen.

Als nächstes

In den vorangegangenen Abschnitten wurden Sie mit den grundlegenden Infrastrukturkomponenten von Amazon DocumentDB vertraut gemacht. Was sollten Sie als nächstes tun? Je nach Ihren Umständen finden Sie einen Einstieg in eines der folgenden Themen:

- Beginnen Sie mit Amazon DocumentDB, indem Sie einen Cluster und eine Instance mithilfe CloudFormation Amazon DocumentDB DocumentDB-Schnellstart mit CloudFormation von erstellen.
- Beginnen Sie mit Amazon DocumentDB, indem Sie einen Cluster und eine Instance anhand der Anweisungen in unserem Leitfaden für die ersten Schritte erstellen.
- Beginnen Sie mit Amazon DocumentDB, indem Sie mithilfe der Anweisungen unter einen elastischen Cluster erstellen. Erste Schritte mit Amazon DocumentDB Elastic Clusters
- Migrieren Sie Ihre MongoDB-Implementierung zu Amazon DocumentDB mithilfe der Anleitung unter Migration zu Amazon DocumentDB

Amazon DocumentDB: So funktioniert es

Amazon DocumentDB (mit MongoDB-Kompatibilität) ist ein vollständig verwalteter MongoDB-compatible Datenbankservice. Mit Amazon DocumentDB können Sie denselben Anwendungscode ausführen und dieselben Treiber und Tools verwenden, die Sie mit MongoDB verwenden. Amazon DocumentDB ist mit MongoDB 3.6, 4.0, 5.0 und 8.0 kompatibel.

Themen

- Amazon DocumentDB DocumentDB-Versionen
- Amazon DocumentDB DocumentDB-Endpunkte
- TLS-Unterstützung
- Amazon DocumentDB DocumentDB-Speicher
- Amazon DocumentDB DocumentDB-Replikation
- Zuverlässigkeit von Amazon DocumentDB
- Lesen Sie die Einstellungsoptionen
- TTL löscht
- Abrechnungsfähige Ressourcen

Amazon DocumentDB DocumentDB-Versionen

> **Note**
>
> Die kleinere Versionsnummerierung gilt für Amazon DocumentDB 5.0 und höher. Amazon DocumentDB 3.6 und 4.0 verwenden nur Hauptversionen mit Engine-Patches.

Ab Amazon DocumentDB 5.0 verwendet die Engine-Version ein vierstufiges Nummerierungsschema: major.major.minor.patch.

- Hauptversion — Identifiziert durch die ersten beiden Nummern der Version (z. B. 5.0). Die Hauptversion stellt den MongoDB-Kompatibilitätsgrad dar. Hauptversionen führen neue Funktionen, Leistungsverbesserungen und MongoDB-Kompatibilitätsupdates ein. Für ein Upgrade zwischen Hauptversionen (z. B. von 4.0 auf 5.0) ist ein Hauptversions-Upgrade (MVU) erforderlich. Weitere Informationen finden Sie unter Direktes Upgrade der Hauptversion von Amazon DocumentDB.

- Nebenversion — Identifiziert durch die dritte Versionsnummer (z. B. die 1 in 5.0.1). Nebenversionen enthalten Verbesserungen wie neue Funktionen, Sicherheitskorrekturen und Bugfixes innerhalb derselben Hauptversion. Sie können manuell auf eine neue Nebenversion aktualisieren. Weitere Informationen finden Sie unter Upgrade der Nebenversion von Amazon DocumentDB.
- Patch-Version — Engine-Patches werden innerhalb einer Nebenversion angewendet und enthalten wichtige Sicherheits- und Bugfixes. Die Patch-Version wird anhand der Engine-Patch-Version (z. B.`3.0.17983`) nachverfolgt, die Sie überprüfen können, indem Sie sie ausführen`db.runCommand({getEngineVersion: 1})`. Patches werden während des Wartungsfensters Ihres Clusters installiert. Weitere Informationen finden Sie unter Wartung von Amazon DocumentDB.

Wenn Sie einen neuen Cluster erstellen, können Sie jede verfügbare Engine-Version angeben. Informationen zu verfügbaren Versionen und Support-Daten finden Sie unterUnterstützungstermine der Amazon DocumentDB DocumentDB-Engine-Version.

Wenn Sie Amazon DocumentDB verwenden, erstellen Sie zunächst einen Cluster. Ein DB-Cluster besteht aus null oder mehreren Datenbank-Instances und einem Cluster-Volume, das die Daten für diese Instances verwaltet. Ein Amazon DocumentDB-Cluster-Volume ist ein virtuelles Datenbankspeicher-Volume, das sich über mehrere Availability Zones erstreckt. Jede Availability Zone verfügt über eine Kopie der Cluster-Daten.

Ein Amazon DocumentDB-Cluster besteht aus zwei Komponenten:

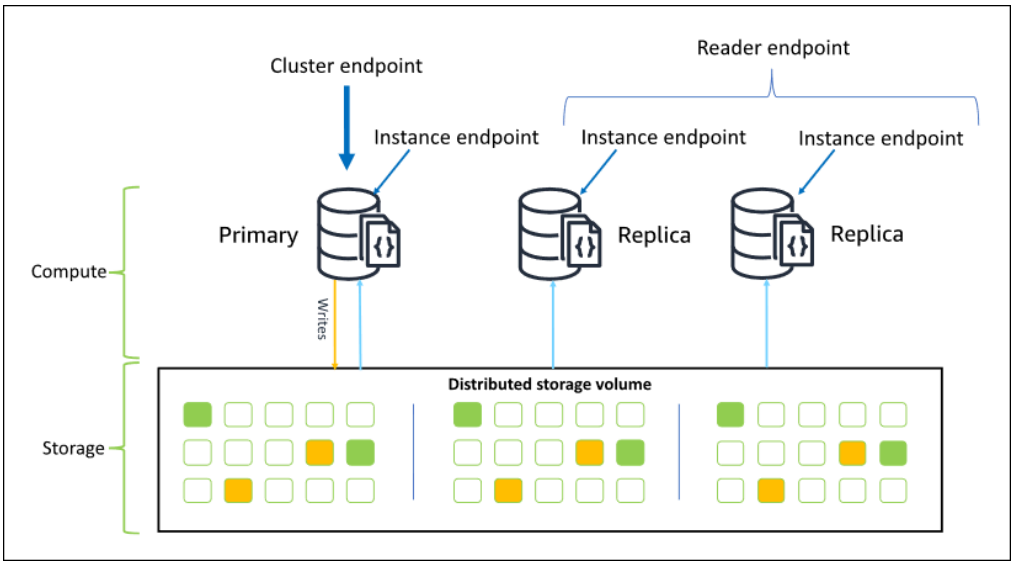
- Cluster-Volume — Verwendet einen Cloud-nativen Speicherservice, um Daten auf sechs Arten über drei Availability Zones hinweg zu replizieren und bietet so äußerst beständigen und verfügbaren Speicher. Ein Amazon DocumentDB-Cluster hat genau ein Cluster-Volume, das bis zu 128 TiB an Daten speichern kann.
- Instances — Stellen die Rechenleistung für die Datenbank bereit, indem sie Daten auf das Cluster-Speichervolume schreiben und Daten aus dem Cluster-Speichervolume lesen. Ein Amazon DocumentDB-Cluster kann 0—16 Instances haben.

Instances erfüllen eine von zwei Rollen:

- Primäre Instance — Unterstützt Lese- und Schreibvorgänge und führt alle Datenänderungen am Cluster-Volume durch. Jeder Amazon DocumentDB-Cluster hat eine primäre Instance.

- Replica-Instance — Unterstützt nur Lesevorgänge. Ein Amazon DocumentDB-Cluster kann zusätzlich zur primären Instance bis zu 15 Replikate haben. Die Verwendung mehrerer Replikate ermöglicht es Ihnen, die Leseauslastungen zu verteilen. Darüber hinaus erhöhen Sie durch die Platzierung von Replikaten in separaten Availability Zones auch die Cluster-Verfügbarkeit.

Das folgende Diagramm veranschaulicht die Beziehung zwischen dem Cluster-Volume, der primären Instance und den Replikaten in einem Amazon DocumentDB-Cluster:



Cluster-Instances müssen nicht von derselben Instance-Klasse sein. Sie können beliebig bereitgestellt und beendet werden. Mit dieser Architektur können Sie die Rechenkapazität Ihres Clusters unabhängig von seiner Storage-Funktionalität skalieren.

Wenn Ihre Anwendung Daten in die Primär-Instance schreibt, schreibt diese die Daten dauerhaft in das Cluster-Volume. Anschließend repliziert es den Status dieses Schreibvorgangs (nicht die Daten) auf jedes aktive Replikat. Amazon DocumentDB DocumentDB-Replikate sind nicht an der Verarbeitung von Schreibvorgängen beteiligt, weshalb Amazon DocumentDB DocumentDB-Replikate für die Leseskalierung von Vorteil sind. Lesevorgänge von Amazon DocumentDB DocumentDB-Repliken sind letztlich konsistent mit minimaler Replikatverzögerung — in der Regel weniger als 100 Millisekunden, nachdem die primäre Instance die Daten geschrieben hat. Lesezugriffe von den Replikaten werden garantiert in der Reihenfolge gelesen, in der sie auf die primäre Instance geschrieben wurden. Die Replikationsverzögerung hängt von der Rate der Datenänderung ab. Perioden mit hoher Schreibaktivität können die Replikationsverzögerung erhöhen. Weitere Informationen finden Sie in den `ReplicationLag`-Metriken unter Amazon DocumentDB-Metriken.

Amazon DocumentDB DocumentDB-Endpunkte

Amazon DocumentDB bietet mehrere Verbindungsoptionen für eine Vielzahl von Anwendungsfällen. Um eine Verbindung zu einer Instance in einem Amazon DocumentDB-Cluster herzustellen, geben Sie den Endpunkt der Instance an. Ein Endpunkt ist eine Host-Adresse und eine Portnummer, getrennt durch einen Doppelpunkt.

Es wird empfohlen, dass Sie mithilfe des Clusterendpunkts und im Replikatsatzmodus eine Verbindung mit dem Cluster herstellen (siehe Als Replikatsatz eine Verbindung zu Amazon DocumentDB herstellen), es sei denn, es liegt ein bestimmter Anwendungsfall für die Verbindung mit dem Reader-Endpunkt oder einem Instanceendpunkt vor. Um Anforderungen an Ihre Replikate weiterzuleiten, wählen Sie eine Treibereinstellung für die Leseeinstellung aus, die die Leseskalierung maximiert und gleichzeitig die Anforderungen für die Lesekonsistenz Ihrer Anwendung erfüllt. Die Leseeinstellung `secondaryPreferred` ermöglicht Replica-Lesevorgänge, sodass die primäre Instance produktiver sein kann.

Die folgenden Endpunkte sind in einem Amazon DocumentDB-Cluster verfügbar.

Cluster-Endpunkt

Der Cluster-Endpunkt verbindet sich mit der aktuellen primären Instance Ihres Clusters. Der Cluster-Endpunkt kann für Lese- und Schreibvorgänge verwendet werden. Ein Amazon DocumentDB-Cluster hat genau einen Cluster-Endpunkt.

Der Cluster-Endpunkt bietet Failover-Support für Lese-/Schreibverbindungen zum Cluster. Wenn die aktuelle primäre Instance Ihres Clusters ausfällt und Ihr Cluster mindestens eine aktive Read Replica hat, leitet der Cluster-Endpunkt Verbindungsanforderungen automatisch an eine neue primäre Instance weiter. Wenn Sie eine Verbindung zu Ihrem Amazon DocumentDB-Cluster herstellen, empfehlen wir, dass Sie die Verbindung zu Ihrem Cluster über den Cluster-Endpunkt und im Replikatsatzmodus herstellen (siheAls Replikatsatz eine Verbindung zu Amazon DocumentDB herstellen).

Im Folgenden finden Sie ein Beispiel für einen Amazon DocumentDB-Cluster-Endpunkt:

```
sample-cluster.cluster-123456789012.us-east-1.docdb.amazonaws.com:27017
```

Im Folgenden finden Sie ein Beispiel für eine Verbindungszeichenfolge für diesen Cluster-Endpunkt:

```
mongodb://username:password@sample-cluster.cluster-123456789012.us-
east-1.docdb.amazonaws.com:27017
```

Informationen zum Suchen der Endpunkte eines Clusters finden Sie unter Die Endpunkte eines Clusters finden.

Leser-Endpunkt

Der Reader-Endpunkt agiert als Load-Balancer für schreibgeschützte Verbindungen für alle verfügbaren Replikate in Ihrem Cluster. Ein Cluster-Reader-Endpunkt fungiert als Cluster-Endpunkt, wenn Sie eine Verbindung über den `replicaSet` Modus herstellen, d. h. in der Verbindungszeichenfolge lautet der Replikatsatzparameter. `&replicaSet=rs0` In diesem Fall können Sie Schreibvorgänge auf der Primärseite ausführen. Wenn Sie jedoch eine Verbindung zu dem angegebenen Cluster herstellen`directConnection=true`, führt der Versuch, einen Schreibvorgang über eine Verbindung zum Leser-Endpunkt auszuführen, zu einem Fehler. Ein Amazon DocumentDB-Cluster hat genau einen Leser-Endpunkt.

Wenn der Cluster nur eine (primäre) Instance enthält, verbindet sich der Reader-Endpunkt mit der primären Instance. Wenn Sie Ihrem Amazon DocumentDB-Cluster eine Replikat-Instance hinzufügen, öffnet der Reader-Endpunkt schreibgeschützte Verbindungen zu dem neuen Replikat, nachdem es aktiv ist.

Im Folgenden finden Sie ein Beispiel für einen Reader-Endpunkt für einen Amazon DocumentDB-Cluster:

```
sample-cluster.cluster-ro-123456789012.us-east-1.docdb.amazonaws.com:27017
```

Im Folgenden finden Sie ein Beispiel für eine Verbindungszeichenfolge unter Verwendung eines Reader-Endpunkts:

```
mongodb://username:password@sample-cluster.cluster-ro-123456789012.us-
east-1.docdb.amazonaws.com:27017
```

Der Reader-Endpunkt verteilt nur die Last der Read-only-Verbindungen – nicht die der Leseanforderungen. Wenn einige Reader-Endpunktverbindungen stärker genutzt werden als andere, sind Ihre Leseanforderungen möglicherweise nicht gleichmäßig zwischen Instances im Cluster verteilt. Es wird empfohlen, dass Sie zum Verteilen von Anforderungen eine Verbindung zum

Clusterendpunkt als Replikatsatz herstellen und die Lesevorstellungsoption secondaryPreferred nutzen.

Informationen zum Suchen der Endpunkte eines Clusters finden Sie unter Die Endpunkte eines Clusters finden.

Instance-Endpunkt

Ein Instance-Endpunkt verbindet sich mit einer bestimmten Instance innerhalb Ihres Clusters. Der Instance-Endpunkt für die aktuelle Primär-Instance kann für Lese- und Schreibvorgänge verwendet werden. Der Versuch, Schreiboperationen auf einen Instance-Endpunkt für ein Lesereplikat durchzuführen, führt jedoch zu einem Fehler. Ein Amazon DocumentDB-Cluster hat einen Instance-Endpunkt pro aktiver Instance.

Ein Instance-Endpunkt bietet für Szenarien, in denen der Cluster-Endpunkt oder der Lese-Endpunkt möglicherweise nicht geeignet ist, direkte Kontrolle über Verbindungen zu einer bestimmten Instance. Ein Beispiel für einen Anwendungsfall ist die Bereitstellung für einen periodischen Read-Only-Analyse-Workload. Sie können eine Replikat-Instance bereitstellen, die größer als üblich ist, sich direkt mit der neuen größeren Instance und ihrem Instance-Endpunkt verbinden, die Analyseabfragen ausführen und die Instance dann beenden. Die Verwendung des Instance-Endpunkts verhindert, dass sich der Analyseverkehr auf andere Cluster-Instances auswirkt.

Im Folgenden finden Sie ein Beispiel für einen Instance-Endpunkt für eine einzelne Instance in einem Amazon DocumentDB-Cluster:

```
sample-instance.123456789012.us-east-1.docdb.amazonaws.com:27017
```

Im Folgenden finden Sie ein Beispiel für eine Verbindungszeichenfolge mit diesem Instance-Endpunkt:

```
mongodb://username:password@sample-instance.123456789012.us-
east-1.docdb.amazonaws.com:27017
```

> **Note**
>
> Die Rolle einer Instance als "Primär" oder "Replikat" kann sich aufgrund eines Failover-Ereignisses ändern. Ihre Anwendungen sollten niemals davon ausgehen, dass ein bestimmter Instance-Endpunkt die primäre Instance ist. Es wird nicht empfohlen, eine Verbindung zu Instance-Endpunkten für Produktionsanwendungen herzustellen. Stattdessen

wird empfohlen, dass Sie mithilfe des Clusterendpunkts und im Replikatsatzmodus eine Verbindung zum Cluster herstellen (siehe Als Replikatsatz eine Verbindung zu Amazon DocumentDB herstellen). Weitere Informationen zur erweiterten Kontrolle der Instance-Failover-Priorität finden Sie unter Grundlegendes zur Amazon DocumentDB-Cluster-Fehlertoleranz.

Informationen zum Suchen der Endpunkte eines Clusters finden Sie unter Den Endpunkt einer Instanz finden.

Replikat-Set-Modus

Sie können im Replikatsatzmodus eine Verbindung zu Ihrem Amazon DocumentDB-Cluster-Endpunkt herstellen, indem Sie den Namen des Replikatsatzes angeben. `rs0` Die Verbindung im Replikatsatzmodus bietet die Möglichkeit, die Optionen Read Concern, Write Concern und Read Preference festzulegen. Weitere Informationen finden Sie unter Lesekonsistenz.

Im Folgenden finden Sie ein Beispiel für eine Verbindungszeichenfolge, die im Replikatsatzmodus verbunden ist:

```
mongodb://username:password@sample-cluster.cluster-123456789012.us-
east-1.docdb.amazonaws.com:27017/?replicaSet=rs0
```

Wenn Sie eine Verbindung im Replikatgruppenmodus herstellen, wird Ihr Amazon DocumentDB-Cluster Ihren Treibern und Clients als Replikatsatz angezeigt. Instances, die Ihrem Amazon DocumentDB-Cluster hinzugefügt und daraus entfernt wurden, werden automatisch in der Konfiguration des Replikatsatzes wiedergegeben.

Jeder Amazon DocumentDB-Cluster besteht aus einem einzelnen Replikatsatz mit dem Standardnamen. `rs0` Der Name des Replikatsatzes kann nicht geändert werden.

Die Verbindung mit dem Cluster-Endpunkt im Replikatsatzmodus ist die empfohlene Methode für den allgemeinen Gebrauch.

> **Note**
>
> Alle Instances in einem Amazon DocumentDB-Cluster überwachen denselben TCP-Port auf Verbindungen.

TLS-Unterstützung

Weitere Informationen zur Verbindung mit Amazon DocumentDB mithilfe von Transport Layer Security (TLS) finden Sie unterVerschlüsseln von Daten während der Übertragung.

Amazon DocumentDB DocumentDB-Speicher

Amazon DocumentDB DocumentDB-Daten werden in einem Cluster-Volume gespeichert, bei dem es sich um ein einzelnes virtuelles Volume handelt, das Solid-State-Laufwerke (SSDs) verwendet. Ein Cluster-Volume besteht aus sechs Kopien Ihrer Daten, die automatisch über mehrere Availability Zones hinweg in einer einzigen repliziert werden. AWS-Region Diese Replikation trägt dazu bei, dass Ihre Daten sehr langlebig sind und weniger Datenverlust möglich ist. Sie trägt außerdem dazu bei, dass Ihr Cluster während eines Failovers besser verfügbar ist, da Kopien Ihrer Daten bereits in anderen Availability Zones vorhanden sind. Diese Kopien können weiterhin Datenanfragen an die Instances in Ihrem Amazon DocumentDB-Cluster bearbeiten.

Informationen zur Abrechnung des -Datenspeichers

Amazon DocumentDB erhöht automatisch die Größe eines Cluster-Volumes, wenn die Datenmenge zunimmt. Ein Amazon DocumentDB-Cluster-Volume kann auf eine maximale Größe von 128 TiB anwachsen. Ihnen wird jedoch nur der Speicherplatz in Rechnung gestellt, den Sie in einem Amazon DocumentDB-Cluster-Volume verwenden. Ab Amazon DocumentDB 4.0 verringert sich der zugewiesene Speicherplatz um einen vergleichbaren Betrag, wenn Daten entfernt werden, z. B. durch Löschen einer Sammlung oder eines Indexes. Somit können Sie die Speichergebühren senken, indem Sie Sammlungen, Indizes und Datenbanken löschen, die Sie nicht mehr benötigen. In Amazon DocumentDB Version 3.6 kann das Cluster-Volume Speicherplatz wiederverwenden, der beim Entfernen von Daten frei wird, aber das Volume selbst nimmt nie an Größe ab. Daher werden Sie in Version 3.6 möglicherweise keine Änderung des Speicherplatzes feststellen, wenn Sie eine Sammlung oder einen Index löschen, obwohl der freigewordene Speicherplatz wiederverwendet wird.

> **Note**
>
> Bei Amazon DocumentDB 3.6 basieren die Speicherkosten auf der Speichergrenze (der Höchstmenge, die dem Amazon DocumentDB-Cluster zu einem beliebigen Zeitpunkt zugewiesen wurde). Sie können die Kosten kontrollieren, indem Sie ETL-Praktiken vermeiden, die große Mengen temporärer Informationen erzeugen oder große Mengen neuer Daten laden, bevor nicht benötigte ältere Daten entfernt werden. Wenn das Entfernen von Daten aus einem Amazon DocumentDB-Cluster dazu führt, dass eine beträchtliche Menge

an zugewiesenem, aber ungenutztem Speicherplatz zur Verfügung steht, müssen Sie zum Zurücksetzen der Höchstgrenze einen logischen Datendump und eine Wiederherstellung auf einem neuen Cluster mit einem Tool wie oder durchführen. `mongodump` `mongorestore` Das Erstellen und Wiederherstellen eines Snapshots führt nicht zur Reduzierung des zugeteilten Speichers, da das physische Layout des zugrunde liegenden Speichers im wiederhergestellten Snapshot unverändert bleibt.

> **Note**
>
> Für die Nutzung von `mongodump` Hilfsprogrammen `mongorestore` fallen I/O Gebühren an, die von der Größe der Daten abhängen, die auf das Speichervolume gelesen und geschrieben werden.

Informationen zur Amazon DocumentDB-Datenspeicherung und zu den I/O Preisen finden Sie in den häufig gestellten Fragen zu Preisen und Preisen von Amazon DocumentDB (mit MongoDB-Kompatibilität).

Amazon DocumentDB DocumentDB-Replikation

In einem Amazon DocumentDB-Cluster macht jede Replikatinstanz einen unabhängigen Endpunkt verfügbar. Diese Replikat-Endpunkte bieten Lesezugriff auf die Daten im Cluster-Volume. Mit ihnen können Sie die Leselast für Ihre Daten über mehrere replizierte Instances hinweg skalieren. Sie tragen auch dazu bei, die Leistung von Datenlesevorgängen zu verbessern und die Verfügbarkeit der Daten in Ihrem Amazon DocumentDB-Cluster zu erhöhen. Amazon DocumentDB-Replikate sind auch Failover-Ziele und werden schnell hochgestuft, wenn die primäre Instance für Ihren Amazon DocumentDB-Cluster ausfällt.

Zuverlässigkeit von Amazon DocumentDB

Amazon DocumentDB ist darauf ausgelegt, zuverlässig, robust und fehlertolerant zu sein. (Um die Verfügbarkeit zu verbessern, sollten Sie Ihren Amazon DocumentDB-Cluster so konfigurieren, dass er über mehrere Replikat-Instances in verschiedenen Availability Zones verfügt.) Amazon DocumentDB umfasst mehrere automatische Funktionen, die es zu einer zuverlässigen Datenbanklösung machen.

Automatische Speicherplatzreparatur

Amazon DocumentDB verwaltet mehrere Kopien Ihrer Daten in drei Availability Zones, wodurch das Risiko eines Datenverlusts aufgrund eines Speicherausfalls erheblich reduziert wird. Amazon DocumentDB erkennt automatisch Fehler im Cluster-Volume. Wenn ein Segment eines Cluster-Volumes ausfällt, repariert Amazon DocumentDB das Segment sofort. Es verwendet die Daten der anderen Volumes, aus denen sich das Cluster-Volumen zusammensetzt, um sicherzustellen, dass die Daten im reparierten Segment aktuell sind. Dadurch vermeidet Amazon DocumentDB Datenverluste und reduziert die Notwendigkeit, eine Point-in-Time-Wiederherstellung durchzuführen, um die Wiederherstellung nach einem Instance-Ausfall durchzuführen.

Überlebensfähiges Cache-Warming

Amazon DocumentDB verwaltet seinen Seiten-Cache in einem von der Datenbank getrennten Prozess, sodass der Seiten-Cache unabhängig von der Datenbank bestehen kann. Im unwahrscheinlichen Fall eines Datenbankausfalls, bleibt der Seiten-Cache im Arbeitsspeicher. Auf diese Weise wird sichergestellt, dass der Pufferpool beim Neustart der Datenbank mit dem aktuellen Zustand vorbereitet wird.

Wiederherstellung nach einem Ausfall

Amazon DocumentDB ist so konzipiert, dass es nach einem Absturz fast sofort wiederhergestellt wird und Ihre Anwendungsdaten weiterhin bereitgestellt werden. Amazon DocumentDB führt die Wiederherstellung nach einem Absturz asynchron auf parallel Threads durch, sodass Ihre Datenbank nach einem Absturz fast unmittelbar geöffnet und verfügbar ist.

Verwaltung von Ressourcen

Amazon DocumentDB schützt Ressourcen, die für die Ausführung kritischer Prozesse im Service benötigt werden, wie z. B. Zustandsprüfungen. Zu diesem Zweck drosselt Amazon DocumentDB Anfragen, wenn eine Instance unter hohem Speicherdruck steht. Daher können einige Operationen in die Warteschlange gestellt werden, um darauf zu warten, dass der Speicherdruck nachlässt. Wenn die Speicherauslastung anhält, kann es bei Vorgängen in der Warteschlange zu einer Zeitüberschreitung kommen. Anhand der folgenden CloudWatch Messwerte können Sie überwachen, ob der Dienst aufgrund von zu wenig Arbeitsspeicher Drosselungen durchführt oder nicht:`LowMemThrottleQueueDepth`,. `LowMemThrottleMaxQueueDepth` `LowMemNumOperationsThrottled` `LowMemNumOperationsTimedOut` Weitere Informationen finden Sie unter Amazon DocumentDB überwachen mit CloudWatch. Wenn Sie aufgrund der

LowMem CloudWatch Metriken einen anhaltenden Speicherdruck auf Ihrer Instance feststellen, empfehlen wir Ihnen, Ihre Instance hochzuskalieren, um zusätzlichen Speicher für Ihre Arbeitslast bereitzustellen.

Lesen Sie die Einstellungsoptionen

Amazon DocumentDB verwendet einen Cloud-nativen Shared Storage-Service, der Daten sechsmal über drei Availability Zones hinweg repliziert, um ein hohes Maß an Haltbarkeit zu gewährleisten. Amazon DocumentDB ist nicht darauf angewiesen, Daten auf mehrere Instanzen zu replizieren, um Haltbarkeit zu erreichen. Die Daten Ihres Clusters sind beständig, unabhängig davon, ob sie eine einzelne Instance oder 15 Instances enthalten.

Themen

- Haltbarkeit beim Schreiben
- Isolierung lesen
- Lesekonsistenz
- Hohe Verfügbarkeit
- Lesevorgänge skalieren

Haltbarkeit beim Schreiben

Amazon DocumentDB verwendet ein einzigartiges, verteiltes, fehlertolerantes, selbstheilendes Speichersystem. Dieses System repliziert sechs Kopien (V=6) Ihrer Daten in drei AWS Availability Zones, um eine hohe Verfügbarkeit und Beständigkeit zu gewährleisten. Beim Schreiben von Daten stellt Amazon DocumentDB sicher, dass alle Schreibvorgänge dauerhaft auf den meisten Knoten aufgezeichnet werden, bevor der Schreibvorgang an den Client bestätigt wird. Wenn Sie einen MongoDB-Replikatsatz mit drei Knoten ausführen, `{w:3, j:true}` würde die Verwendung eines Schreibproblems von die bestmögliche Konfiguration im Vergleich zu Amazon DocumentDB ergeben.

Schreibvorgänge in einen Amazon DocumentDB-Cluster müssen von der Writer-Instance des Clusters verarbeitet werden. Der Versuch, in ein Lesegerät zu schreiben, führt zu einem Fehler. Ein bestätigter Schreibvorgang von einer primären Amazon DocumentDB-Instance ist dauerhaft und kann nicht rückgängig gemacht werden. Amazon DocumentDB ist standardmäßig sehr robust und unterstützt keine nicht dauerhafte Schreiboption. Sie können die Zuverlässigkeitsstufe (d. h. die Option Write Concern) nicht ändern. Amazon DocumentDB ignoriert w=anything und ist effektiv w: 3 und j: true. Sie können es nicht reduzieren.

Da Speicher und Datenverarbeitung in der Amazon DocumentDB DocumentDB-Architektur getrennt sind, ist ein Cluster mit einer einzigen Instanz äußerst robust. Die Zuverlässigkeit wird auf der Speicherschicht geregelt. Dadurch erreichen ein Amazon DocumentDB-Cluster mit einer einzigen Instance und ein Cluster mit drei Instances das gleiche Maß an Haltbarkeit. Sie können Ihren Cluster für Ihren speziellen Anwendungsfall konfigurieren und gleichzeitig für eine hohe Datenbeständigkeit sorgen.

Schreibvorgänge in einen Amazon DocumentDB-Cluster erfolgen innerhalb eines einzigen Dokuments atomar.

Amazon DocumentDB unterstützt `wtimeout` diese Option nicht und gibt keinen Fehler zurück, wenn ein Wert angegeben wird. Schreibvorgänge in die primäre Amazon DocumentDB DocumentDB-Instance werden garantiert nicht auf unbestimmte Zeit blockiert.

Isolierung lesen

Lesevorgänge aus einer Amazon DocumentDB DocumentDB-Instance geben nur Daten zurück, die vor Beginn der Abfrage dauerhaft sind. Lesezugriffe geben niemals Daten zurück, die nach Beginn der Ausführung der Abfrage geändert wurden. Auch "Dirty-Reads" sind unter keinen Umständen möglich.

Lesekonsistenz

Aus einem Amazon DocumentDB-Cluster gelesene Daten sind dauerhaft und werden nicht zurückgesetzt. Sie können die Lesekonsistenz für Amazon DocumentDB-Lesevorgänge ändern, indem Sie die Lesepräferenz für die Anfrage oder Verbindung angeben. Amazon DocumentDB unterstützt keine dauerhafte Leseoption.

Lesevorgänge aus der primären Instance eines Amazon DocumentDB-Clusters sind unter normalen Betriebsbedingungen sehr konsistent und weisen auch beim Lesen nach dem Schreiben eine Konsistenz auf. Tritt zwischen dem Schreiben und dem nachfolgenden Lesen ein Failover-Ereignis auf, kann das System kurzzeitig einen nicht "Strongly Consistent"-Wert zurückgeben. Alle Lesezugriffe auf einer gelesenen Replik sind "Eventually Consistent" und geben die Daten in der gleichen Reihenfolge zurück, oft mit weniger als 100 ms Replikationsverzögerung.

Amazon DocumentDB Leseeinstellungen

Amazon DocumentDB unterstützt das Festlegen einer Lesepräferenzoption nur beim Lesen von Daten vom Cluster-Endpunkt im Replikatsatzmodus. Das Festlegen einer Lesepräferenzoption wirkt

sich darauf aus, wie Ihr MongoDB-Client oder -Treiber Leseanfragen an Instances in Ihrem Amazon DocumentDB-Cluster weiterleitet. Sie können Leseeinstellungen für eine bestimmte Abfrage oder als allgemeine Option in Ihrem MongoDB-Treiber festlegen. (Lesen Sie in der Dokumentation Ihres Clients oder Treibers nach, wie Sie eine Leseeinstellung festlegen können.)

Wenn Ihr Client oder Treiber im Replikatsatzmodus keine Verbindung zu einem Amazon DocumentDB-Cluster-Endpunkt herstellt, ist das Ergebnis der Angabe einer Lesepräferenz undefiniert.

Amazon DocumentDB unterstützt die Einstellung von Tag-Sets als Lesepräferenz nicht.

Unterstützte Leseeinstellungsoptionen

- **`primary`**— Durch die Angabe einer `primary` Lesepräferenz wird sichergestellt, dass alle Lesevorgänge an die primäre Instance des Clusters weitergeleitet werden. Wenn die primäre Instance nicht verfügbar ist, schlägt der Lesevorgang fehl. Die Leseeinstellung `primary` ergibt Lese-After-Write-Konsistenz und eignet sich für Anwendungsfälle, die die Lese-nach-Schreib-Konsistenz über Hochverfügbarkeit und Leseskalierung priorisieren.

  Im folgenden Beispiel wird die Leseeinstellung `primary` angegeben:

  ```
  db.example.find().readPref('primary')
  ```

- **`primaryPreferred`**— Durch die Angabe einer `primaryPreferred` Lesepräferenz werden Lesevorgänge bei normalem Betrieb an die primäre Instance weitergeleitet. Wenn es ein primäres Failover gibt, leitet der Client Anfragen an ein Replikat weiter. Die Leseeinstellung `primaryPreferred` sorgt für Lese-nach-Schreib-Konsistenz im Normalbetrieb und Eventually Consistent-Lesezugriffe während eines Failoverereignisses. Die Leseeinstellung `primaryPreferred` ist für Anwendungsfälle geeignet, die die Lese-nach-Schreib-Konsistenz über Hochverfügbarkeit und Leseskalierung priorisieren, jedoch trotzdem eine Hochverfügbarkeit erfordern.

  Im folgenden Beispiel wird die Leseeinstellung `primaryPreferred` angegeben:

  ```
  db.example.find().readPref('primaryPreferred')
  ```

- **`secondary`**— Durch die Angabe einer `secondary` Lesepräferenz wird sichergestellt, dass Lesevorgänge nur an ein Replikat und niemals an die primäre Instanz weitergeleitet werden. Wenn es in einem Cluster keine Replikat-Instances gibt, schlägt die Leseanforderung fehl. Die Leseeinstellung `secondary` ergibt Eventually Consistent-Lesezugriffe und ist für Anwendungsfälle geeignet, die den Schreibdurchsatz der primären Instance über die Hochverfügbarkeit und die Lesen-nach-Schreiben-Konsistenz priorisiert.

  Im folgenden Beispiel wird die Leseeinstellung `secondary` angegeben:

```
db.example.find().readPref('secondary')
```

- **`secondaryPreferred`**— Durch die Angabe einer `secondaryPreferred` Lesepräferenz wird sichergestellt, dass Lesevorgänge an eine Read Replica weitergeleitet werden, wenn ein oder mehrere Replikate aktiv sind. Wenn es in einem Cluster keine aktiven Replikat-Instances gibt, wird die Leseanforderung an die primäre Instance weitergeleitet. Die Leseeinstellung `secondaryPreferred` ergibt Eventually Consistent-Lesezugriffe, wenn der Lesezugriff durch ein Read Replica bedient wird. Sie liefert eine Lese-nach-Schreib-Konsistenz, wenn das Lesen von der primären Instance bedient wird (mit Ausnahme von Failover-Ereignissen). Die Leseeinstellung `secondaryPreferred` ist für Anwendungsfälle geeignet, die Leseskalierung und Hochverfügbarkeit über Lese-nach-Schreib-Konsistenz priorisieren.

  Im folgenden Beispiel wird die Leseeinstellung `secondaryPreferred` angegeben:

```
db.example.find().readPref('secondaryPreferred')
```

- **`nearest`**— Die Angabe einer `nearest` Lesepräferenz leitet Lesevorgänge ausschließlich auf der Grundlage der gemessenen Latenz zwischen dem Client und allen Instances im Amazon DocumentDB-Cluster weiter. Die Leseeinstellung `nearest` ergibt Eventually Consistent-Lesezugriffe, wenn der Lesezugriff durch ein Read Replica bedient wird. Sie liefert eine Lese-nach-Schreib-Konsistenz, wenn das Lesen von der primären Instance bedient wird (mit Ausnahme von Failover-Ereignissen). Die Leseeinstellung `nearest` ist für Anwendungsfälle geeignet, die das Erreichen einer möglichst geringen Leselatenz und die Hochverfügbarkeit über die Lese-zu-Schreib-Konsistenz und Leseskalierung priorisieren.

  Im folgenden Beispiel wird die Leseeinstellung `nearest` angegeben:

```
db.example.find().readPref('nearest')
```

Hohe Verfügbarkeit

Amazon DocumentDB unterstützt hochverfügbare Cluster-Konfigurationen, indem Repliken als Failover-Ziele für die primäre Instance verwendet werden. Wenn die primäre Instance ausfällt, wird ein Amazon DocumentDB DocumentDB-Replikat zur neuen primären Instance hochgestuft, mit einer kurzen Unterbrechung, während der Lese- und Schreibanforderungen an die primäre Instance mit einer Ausnahme fehlschlagen.

Wenn Ihr Amazon DocumentDB-Cluster keine Replikate enthält, wird die primäre Instance bei einem Ausfall neu erstellt. Das Heraufstufen eines Amazon DocumentDB DocumentDB-Replikats ist jedoch viel schneller als das Neuerstellen der primären Instance. Wir empfehlen daher, ein oder mehrere Amazon DocumentDB DocumentDB-Replikate als Failover-Ziele zu erstellen.

Replikate, die als Failover-Ziele verwendet werden sollen, sollten dieselbe DB-Instance-Klasse haben wie die primäre Instance. Sie sollten von der primären Instance in verschiedenen Availability Zones bereitgestellt werden. Sie können steuern, welche Replikate als Failover-Ziele bevorzugt werden. Bewährte Methoden zur Konfiguration von Amazon DocumentDB für hohe Verfügbarkeit finden Sie unterGrundlegendes zur Amazon DocumentDB-Cluster-Fehlertoleranz.

Lesevorgänge skalieren

Amazon DocumentDB DocumentDB-Repliken eignen sich ideal für die Skalierung von Lesevorgängen. Sie sind in Ihrem Cluster-Volume vollständig auf Lesevorgänge ausgerichtet, d. h. Replikate verarbeiten keine Schreibvorgänge. Die Datenreplikation geschieht innerhalb des Cluster-Volumes und nicht zwischen Instances. Deshalb sind die Replikat-Ressourcen auf die Verarbeitung von Abfragen ausgelegt und nicht auf das Schreiben und Replizieren von Daten.

Wenn Ihre Anwendung mehr Lesekapazität benötigt, können Sie Ihrem Cluster schnell (in der Regel in weniger als zehn Minuten) eine Replik hinzufügen. Wenn Ihr Lesekapazitätsbedarf sinkt, können Sie nicht benötigte Replikate entfernen. Mit Amazon DocumentDB DocumentDB-Repliken zahlen Sie nur für die Lesekapazität, die Sie benötigen.

Amazon DocumentDB unterstützt die clientseitige Leseskalierung mithilfe von Read Preference-Optionen. Weitere Informationen finden Sie unter Amazon DocumentDB Leseeinstellungen.

TTL löscht

Löschungen aus einem TTL-Indexbereich über einen Hintergrundprozess erfolgen nach dem Best-Effort-Prinzip und können nicht für einen bestimmten Zeitrahmen garantiert werden. Faktoren wie Instance-Größe, Instance-Ressourcenauslastung, Dokumentgröße und Gesamtdurchsatz können sich auf den Zeitpunkt einer TTL-Löschung auswirken.

Wenn der TTL-Monitor Ihre Dokumente löscht, entstehen bei jeder Löschung E/A-Kosten, was den Rechnungsbetrag erhöht. Wenn die Durchsatz- und TTL-Löschraten steigen, sollten Sie aufgrund der erhöhten I/O-Auslastung mit einer Erhöhung Ihrer Rechnung rechnen.

Wenn Sie einen TTL-Index für eine bestehende Sammlung erstellen, müssen Sie alle abgelaufenen Dokumente löschen, bevor Sie den Index erstellen. Die aktuelle TTL-Implementierung ist für das Löschen eines kleinen Teils der Dokumente in der Sammlung optimiert. Dies ist typisch, wenn TTL für die Sammlung von Anfang an aktiviert war. Dies kann zu höheren IOPS als nötig führen, wenn eine große Anzahl von Dokumenten gleichzeitig gelöscht werden muss.

Wenn Sie keinen TTL-Index zum Löschen von Dokumenten erstellen möchten, können Sie Dokumente stattdessen nach Zeit in Sammlungen unterteilen und diese Sammlungen einfach löschen, wenn die Dokumente nicht mehr benötigt werden. Beispiel: Sie können eine Sammlung pro Woche erstellen und diese löschen, ohne dass IO-Kosten anfallen. Dies kann deutlich kostengünstiger sein als die Verwendung eines TTL-Index.

Abrechnungsfähige Ressourcen

Identifizieren von kostenpflichtigen Amazon DocumentDB DocumentDB-Ressourcen

Als vollständig verwalteter Datenbankservice berechnet Amazon DocumentDB Gebühren für Instances, Speicher I/Os, Backups und Datenübertragung. Weitere Informationen finden Sie unter Preise für Amazon DocumentDB (mit MongoDB-Kompatibilität).

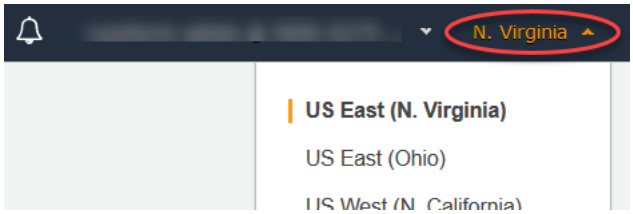
Um abrechnungsfähige Ressourcen in Ihrem Konto zu finden und die Ressourcen möglicherweise zu löschen, können Sie das oder verwenden. AWS-Managementkonsole AWS CLI

Verwendung der AWS-Managementkonsole

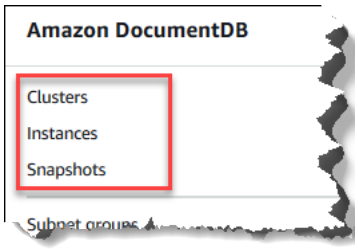
Mithilfe von können Sie die AWS-Managementkonsole Amazon DocumentDB-Cluster, -Instances und -Snapshots ermitteln, die Sie für eine bestimmte Person bereitgestellt haben. AWS-Region

So ermitteln Sie Cluster, Instances und Snapshots:

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Um nach abrechnungsfähigen Ressourcen in einer anderen Region als Ihrer Standardregion zu suchen, wählen Sie in der oberen rechten Ecke des Bildschirms die Region aus, nach der AWS-Region Sie suchen möchten.



3. Wählen Sie im Navigationsbereich die Art der kostenpflichtigen Ressource aus: Clusters (Cluster), Instances oder Snapshots.



4. Im rechten Bereich werden alle bereitgestellten Cluster, Instances oder Snapshots für die Region aufgelistet. Für Cluster, Instances und Snapshots werden Gebühren berechnet.

Verwendung der AWS CLI

Mithilfe von können Sie die AWS CLI Amazon DocumentDB-Cluster, -Instances und -Snapshots ermitteln, die Sie für eine bestimmte Person bereitgestellt haben. AWS-Region

So ermitteln Sie Cluster und Instances:

Der folgende Code listet Ihre gesamten Cluster und Instances für die angegebene Region auf. Wenn Sie nach Clustern und Instances in Ihrer Standardregion suchen möchten, können Sie den Parameter `--region` weglassen.

Example

Für Linux, macOS oder Unix:

```
aws docdb describe-db-clusters \
```

```
    --region us-east-1 \
    --query 'DBClusters[?Engine==`docdb`]' | \
       grep -e "DBClusterIdentifier" -e "DBInstanceIdentifier"
```

Für Windows:

```
aws docdb describe-db-clusters ^
    --region us-east-1 ^
    --query 'DBClusters[?Engine==`docdb`]' | ^
       grep -e "DBClusterIdentifier" -e "DBInstanceIdentifier"
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus.

```
"DBClusterIdentifier": "docdb-2019-01-09-23-55-38",
        "DBInstanceIdentifier": "docdb-2019-01-09-23-55-38",
        "DBInstanceIdentifier": "docdb-2019-01-09-23-55-382",
"DBClusterIdentifier": "sample-cluster",
"DBClusterIdentifier": "sample-cluster2",
```

So ermitteln Sie Snapshots:

Der folgende Code listet Ihre gesamten Snapshots für die angegebene Region auf. Wenn Sie in Ihrer Standardregion nach Snapshots suchen möchten, können Sie den Parameter `--region` weglassen.

Für Linux, macOS oder Unix:

```
aws docdb describe-db-cluster-snapshots \
  --region us-east-1 \
  --query 'DBClusterSnapshots[?Engine==`docdb`].
[DBClusterSnapshotIdentifier,SnapshotType]'
```

Für Windows:

```
aws docdb describe-db-cluster-snapshots ^
  --region us-east-1 ^
  --query 'DBClusterSnapshots[?Engine==`docdb`].
[DBClusterSnapshotIdentifier,SnapshotType]'
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus.

```
[
```

```
    [
        "rds:docdb-2019-01-09-23-55-38-2019-02-13-00-06",
        "automated"
    ],
    [
        "test-snap",
        "manual"
    ]
]
```

Sie müssen nur `manual`-Snapshots löschen. `Automated`-Snapshots werden gelöscht, wenn Sie den Cluster löschen.

Löschen unerwünschter kostenpflichtiger Ressourcen

Um einen Cluster zu löschen, müssen Sie zunächst alle Instances im Cluster löschen.

- Weitere Informationen zum Löschen von Instances finden Sie unter Löschen einer Amazon DocumentDB DocumentDB-Instance.

  > **Important**
  >
  > Auch wenn Sie die Instances in einem Cluster löschen, wird Ihnen die mit diesem Cluster verbundene Speicher- und Sicherungsnutzung in Rechnung gestellt. Um alle Kosten zu stoppen, müssen Sie auch Ihren Cluster und manuelle Snapshots löschen.

- Weitere Informationen zum Löschen von Clustern finden Sie unter Löschen eines Amazon DocumentDB-Clusters.
- Weitere Informationen zum Löschen manueller Snapshots finden Sie unter Löschen eines Cluster-Snapshots.

Was ist eine Dokumentendatenbank?

Einige Entwickler betrachten ihr Datenmodell nicht als normalisierte Zeilen und Spalten. In der Regel werden Daten auf Anwendungsebene als JSON-Dokument dargestellt, da es für Entwickler intuitiver ist, ihr Datenmodell als Dokument zu betrachten.

Die Popularität von Dokumentdatenbanken ist gestiegen, weil Sie mit ihnen Daten in einer Datenbank erhalten können, indem Sie das gleiche Dokumentmodellformat verwenden, das Sie in Ihrem

Anwendungscode verwenden. Dokumentdatenbanken bieten leistungsfähige und intuitive APIs für eine flexible und agile Entwicklung.

Themen

- Anwendungsfälle für Dokumentendatenbanken
- Dokumente verstehen
- Arbeiten mit Dokumenten

Anwendungsfälle für Dokumentendatenbanken

Ihr Anwendungsfall bestimmt, ob Sie eine Dokumentendatenbank oder eine andere Art von Datenbank für die Verwaltung Ihrer Daten benötigen. Dokumentdatenbanken sind nützlich für Workloads, die ein flexibles Schema für eine schnelle, iterative Entwicklung benötigen. Im Folgenden finden Sie einige Beispiele für Anwendungsfälle, bei denen Dokumentendatenbanken erhebliche Vorteile bieten können:

Themen

- Benutzerprofile
- Real-time große Datenmengen
- Verwaltung von Inhalten

Benutzerprofile

Da Dokumentdatenbanken über ein flexibles Schema verfügen, können sie Dokumente speichern, die unterschiedliche Attribute und Datenwerte aufweisen. Dokumentdatenbanken sind eine praktische Lösung für Online-Profile, in denen verschiedene Benutzer unterschiedliche Arten von Informationen bereitstellen. Mit Hilfe einer Dokumentdatenbank können Sie das Profil jedes Benutzers effizient speichern, indem Sie nur die Attribute speichern, die für jeden Benutzer spezifisch sind.

Angenommen, ein Benutzer entscheidet sich dafür, Informationen in seinem Profil hinzuzufügen oder zu entfernen. In diesem Fall könnte ihr Dokument leicht durch eine aktualisierte Version ersetzt werden, die alle kürzlich hinzugefügten Attribute und Daten enthält oder alle neu weggelassenen Attribute und Daten auslässt. Dokumentdatenbanken bewältigen diese Individualität und Fluidität auf einfache Weise.

Real-time große Datenmengen

In der Vergangenheit wurde die Fähigkeit, Informationen aus Betriebsdaten zu extrahieren, dadurch beeinträchtigt, dass operative Datenbanken und analytische Datenbanken in unterschiedlichen Umgebungen verwaltet wurden — den betrieblichen bzw. den jeweiligen. business/reporting Die Fähigkeit, operative Informationen in Echtzeit zu extrahieren, ist in einem hart umkämpften Geschäftsumfeld von entscheidender Bedeutung. Durch die Verwendung von Dokumentendatenbanken kann ein Unternehmen Betriebsdaten aus jeder beliebigen Quelle speichern und verwalten und gleichzeitig die Daten zur Analyse an die BI-Engine seiner Wahl weiterleiten. Es ist nicht erforderlich, dass zwei Umgebungen vorhanden sein müssen.

Verwaltung von Inhalten

Um Inhalte effektiv zu verwalten, müssen Sie in der Lage sein, Inhalte aus einer Vielzahl von Quellen zu sammeln, zu aggregieren und dann an den Client zu liefern. Aufgrund ihres flexiblen Schemas sind Dokumentdatenbanken ideal für die Erfassung und Speicherung jeglicher Art von Daten. Mit ihnen können Sie neue Arten von Inhalten erstellen und integrieren, einschließlich benutzergenerierter Inhalte wie Bilder, Kommentare und Videos.

Dokumente verstehen

Dokumentendatenbanken werden verwendet, um semistrukturierte Daten als Dokument zu speichern, anstatt Daten in mehreren Tabellen zu normalisieren, von denen jede eine eindeutige und feste Struktur hat, wie in einer relationalen Datenbank. Dokumente, die in einer Dokumentdatenbank gespeichert sind, verwenden verschachtelte Schlüssel-Werte-Paare, um die Struktur oder das Schema des Dokuments bereitzustellen. Es können jedoch verschiedene Arten von Dokumenten in derselben Dokumentdatenbank gespeichert werden, wodurch die Anforderung erfüllt wird, ähnliche Daten in unterschiedlichen Formaten zu verarbeiten. Da beispielsweise jedes Dokument selbsterklärend ist, Beispieldokumente in einer Dokumentendatenbank können die im Thema beschriebenen JSON-encoded Dokumente für einen Onlineshop in derselben Dokumentendatenbank gespeichert werden.

Themen

- SQL im Vergleich zu nichtrelationaler Terminologie
- Einfache Dokumente
- Eingebettete Dokumente
- Beispieldokumente in einer Dokumentendatenbank

- Grundlegendes zur Normalisierung in einer Dokumentendatenbank

SQL im Vergleich zu nichtrelationaler Terminologie

Die folgende Tabelle vergleicht die von Dokumentendatenbanken (MongoDB) verwendete Terminologie mit der von SQL-Datenbanken verwendeten Terminologie.

SQL	MongoDB
Tabelle	Sammlung
Zeile	Dokument
Spalte	Feld
Primärschlüssel	ObjectId
Index	Index
Anzeigen	Anzeigen
Verschachtelte(s) Tabelle oder Objekt	Eingebettetes Dokument
Array	Array

Einfache Dokumente

Alle Dokumente in einer Dokumentendatenbank sind selbstbeschreibend. In dieser Dokumentation JSON-like werden formatierte Dokumente verwendet, Sie können jedoch auch andere Kodierungsmethoden verwenden.

Ein einfaches Dokument hat ein oder mehrere Felder, die alle auf der gleichen Ebene innerhalb des Dokuments liegen. Im folgenden Beispiel sind die Felder `SSN`, `LName`, `FName`, `DOB`, `Street`, `City`, `State-Province`, `PostalCode` und `Country` alle Elemente auf derselben Ebene im Dokument.

```
{
   "SSN": "123-45-6789",
   "LName": "Rivera",
   "FName": "Martha",
```

```
   "DOB": "1992-11-16",
   "Street": "125 Main St.",
   "City": "Anytown",
   "State-Province": "WA",
   "PostalCode": "98117",
   "Country": "USA"
}
```

Wenn Informationen in einem einfachen Dokument organisiert sind, wird jedes Feld einzeln verwaltet. Um die Adresse einer Person abzurufen, müssen Sie `Street`, `City`, `State-Province`, `PostalCode` und `Country` als einzelne Datenelemente abrufen.

Eingebettete Dokumente

Ein komplexes Dokument organisiert seine Daten, indem es eingebettete Dokumente innerhalb des Dokuments erstellt. Eingebettete Dokumente helfen bei der Verwaltung von Daten in Gruppierungen und als einzelne Datenelemente, je nachdem, was im jeweiligen Fall effizienter ist. Mit dem vorhergehenden Beispiel könnten Sie ein `Address`-Dokument in das Hauptdokument einbetten. Dadurch ergibt sich die folgende Dokumentstruktur:

```
{
   "SSN": "123-45-6789",
   "LName": "Rivera",
   "FName": "Martha",
   "DOB": "1992-11-16",
   "Address":
   {
       "Street": "125 Main St.",
       "City": "Anytown",
       "State-Province": "WA",
       "PostalCode": "98117",
       "Country": "USA"
   }
}
```

Sie können jetzt auf die Daten im Dokument als einzelne Felder (`"SSN":`), als eingebettetes Dokument (`"Address":`) oder als Mitglied eines eingebetteten Dokuments (`"Address": {"Street":}`) zugreifen.

Beispieldokumente in einer Dokumentendatenbank

Da jedes Dokument in einer Dokumentdatenbank selbstbeschreibend ist, kann die Struktur von Dokumenten innerhalb einer Dokumentdatenbank unterschiedlich sein. Die folgenden beiden Dokumente, eines für ein Buch und eines für eine Zeitschrift, sind strukturell unterschiedlich. Beide können sich jedoch in der gleichen Dokumentdatenbank befinden.

Im Folgenden finden Sie ein Beispiel-Buch-Dokument:

```
{
    "_id" : "9876543210123",
    "Type": "book",
    "ISBN": "987-6-543-21012-3",
    "Author":
    {
        "LName":"Roe",
        "MI": "T",
        "FName": "Richard"
    },
    "Title": "Understanding Document Databases"
}
```

Im Folgenden finden Sie ein Beispiel für ein Zeitschriften-Dokument mit zwei Artikeln:

```
{
    "_id" : "0123456789012",
    "Publication": "Programming Today",
    "Issue":
    {
        "Volume": "14",
        "Number": "09"
    },
    "Articles" : [
        {
            "Title": "Is a Document Database Your Best Solution?",
            "Author":
            {
                "LName": "Major",
                "FName": "Mary"
            }
        },
        {
```

```
            "Title": "Databases for Online Solutions",
            "Author":
            {
                "LName": "Stiles",
                "FName": "John"
            }
        }
    ],
    "Type": "periodical"
}
```

Vergleichen Sie die Struktur dieser beiden Dokumente. Bei einer relationalen Datenbank benötigen Sie entweder getrennte Tabellen "Zeitschriften" und "Bücher" oder eine einzelne Tabelle mit unbenutzten Feldern wie "Publikation", "Ausgabe", "Artikel" und "MI" als `null` Werte. Da Dokumentendatenbanken halbstrukturiert sind und jedes Dokument seine eigene Struktur definiert, können diese beiden Dokumente ohne `null`-Felder gleichzeitig in derselben Dokumentendatenbank vorhanden sein. Dokumentdatenbanken sind gut geeignet, um mit lückenhaften Daten umzugehen.

Die Entwicklung auf Basis einer Dokumentdatenbank ermöglicht eine schnelle, iterative Entwicklung. Denn Sie können die Datenstruktur eines Dokuments dynamisch ändern, ohne das Schema für die gesamte Sammlung ändern zu müssen. Dokumentdatenbanken eignen sich hervorragend für agile Entwicklungen und sich dynamisch verändernde Umgebungen.

Grundlegendes zur Normalisierung in einer Dokumentendatenbank

Dokumentdatenbanken werden nicht normalisiert; in einem Dokument gefundene Daten können in einem anderen Dokument wiederholt werden. Darüber hinaus können einige Datenunterschiede zwischen den Dokumenten bestehen. Betrachten Sie beispielsweise das Szenario, in dem Sie einen Einkauf in einem Online-Shop tätigen und alle Details Ihrer Einkäufe in einem einzigen Dokument gespeichert sind. Das Dokument könnte etwa so aussehen wie das folgende JSON-Dokument:

```
{
    "DateTime": "2018-08-15T12:13:10Z",
    "LName" : "Santos",
    "FName" : "Paul",
    "Cart" : [
        {
            "ItemId" : "9876543210123",
            "Description" : "Understanding Document Databases",
            "Price" : "29.95"
        },
```

```
        {
            "ItemId" : "0123456789012",
            "Description" : "Programming Today",
            "Issue": {
                "Volume": "14",
                "Number": "09"
            },
            "Price" : "8.95"
        },
        {
            "ItemId": "234567890-K",
            "Description": "Gel Pen (black)",
            "Price": "2.49"
        }
    ],
    "PaymentMethod" :
    {
        "Issuer" : "MasterCard",
        "Number" : "1234-5678-9012-3456"
    },
    "ShopperId" : "1234567890"
}
```

Alle diese Informationen werden als Dokument in einer Transaktionssammlung gespeichert. Später merken Sie, dass Sie vergessen haben, einen Artikel zu kaufen. Daher melden Sie sich erneut im gleichen Shop an und tätigen einen weiteren Kauf, der auch als ein weiteres Dokument in der Transaktionssammlung gespeichert wird.

```
{
    "DateTime": "2018-08-15T14:49:00Z",
    "LName" : "Santos",
    "FName" : "Paul",
    "Cart" : [
        {
            "ItemId" : "2109876543210",
            "Description" : "Document Databases for Fun and Profit",
            "Price" : "45.95"
        }
    ],
    "PaymentMethod" :
    {
        "Issuer" : "Visa",
        "Number" : "0987-6543-2109-8765"
```

```
    },
    "ShopperId" : "1234567890"
}
```

Beachten Sie die Redundanz zwischen diesen beiden Dokumenten — Ihrem Namen und Ihrer Kunden-ID (und, falls Sie dieselbe Kreditkarte verwendet haben, Ihren Kreditkarteninformationen). Aber das ist in Ordnung, denn die Speicherung ist kostengünstig, und jedes Dokument zeichnet eine einzelne Transaktion vollständig auf, die mit einer einfachen Schlüssel-/Wertabfrage, die keine Verknüpfungen erfordert, schnell abgerufen werden kann.

Es besteht auch eine offensichtliche Diskrepanz zwischen den beiden Dokumenten — Ihren Kreditkarteninformationen. Dies ist nur eine scheinbare Diskrepanz, da es wahrscheinlich ist, dass Sie für jeden Kauf eine andere Kreditkarte verwendet haben. Jedes Dokument entspricht genau der Transaktion, die es dokumentiert.

Arbeiten mit Dokumenten

Als Dokumentendatenbank macht es Amazon DocumentDB einfach, JSON-Daten zu speichern, abzufragen und zu indizieren. In Amazon DocumentDB entspricht eine Sammlung einer Tabelle in einer relationalen Datenbank, außer dass kein einziges Schema für alle Dokumente durchgesetzt wird. Mit Sammlungen können Sie ähnliche Dokumente gruppieren und gleichzeitig alle in derselben Datenbank halten, ohne dass sie in ihrer Struktur identisch sein müssen.

Unter Verwendung der Beispieldokumente aus früheren Abschnitten ist es wahrscheinlich, dass Sie Sammlungen für `reading_material` und `office_supplies` haben werden. Es liegt in der Verantwortung Ihrer Software, die Zugehörigkeit eines Dokuments zu einer bestimmten Sammlung durchzusetzen.

Die folgenden Beispiele zeigen anhand der MongoDB-API, wie Sie Dokumente hinzufügen, abfragen, aktualisieren und löschen können.

Themen

- Dokumente hinzufügen
- Dokumente werden abgefragt
- Dokumente werden aktualisiert
- Dokumente löschen

Dokumente hinzufügen

In Amazon DocumentDB wird eine Datenbank erstellt, wenn Sie ein Dokument zum ersten Mal zu einer Sammlung hinzufügen. In diesem Beispiel erstellen Sie eine Sammlung mit dem Namen `example` in der Datenbank `test`, die die Standarddatenbank ist, wenn Sie eine Verbindung mit einem Cluster herstellen. Da die Sammlung implizit erstellt wird, wenn das erste Dokument eingefügt wird, gibt es bei der Überprüfung des Sammlungsnamens keine Fehler. Das heißt, ein Tippfehler im Sammlungsnamen, wie z. B. `eexample` statt `example` führt dazu, dass das Dokument erstellt und der Sammlung `eexample` und nicht der beabsichtigten Sammlung hinzugefügt wird. Die Fehlerüberprüfung muss von Ihrer Anwendung durchgeführt werden.

Die folgenden Beispiele verwenden die MongoDB-API zum Hinzufügen der Dokumente.

Themen

- Ein einzelnes Dokument hinzufügen
- Hinzufügen mehrerer Dokumente

Ein einzelnes Dokument hinzufügen

Um ein einzelnes Dokument zu einer Sammlung hinzuzufügen, verwenden Sie die Operation `insertOne( {} )` mit dem Dokument, das Sie der Sammlung hinzufügen möchten.

```
db.example.insertOne(
    {
        "Item": "Ruler",
        "Colors": ["Red","Green","Blue","Clear","Yellow"],
        "Inventory": {
            "OnHand": 47,
            "MinOnHand": 40
        },
        "UnitPrice": 0.89
    }
)
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus (JSON-Format).

```
{
    "acknowledged" : true,
    "insertedId" : ObjectId("5bedafbcf65ff161707de24f")
```

```
}
```

Hinzufügen mehrerer Dokumente

Um mehrere Dokumente zu einer Sammlung hinzuzufügen, verwenden Sie die Operation `insertMany( [{},...,{}] )` mit einer Liste der Dokumente, die Sie der Sammlung hinzufügen möchten. Obwohl die Dokumente in dieser Liste unterschiedliche Schemata haben, können sie alle zur gleichen Sammlung hinzugefügt werden.

```
db.example.insertMany(
    [
        {
            "Item": "Pen",
            "Colors": ["Red","Green","Blue","Black"],
            "Inventory": {
                "OnHand": 244,
                "MinOnHand": 72
            }
        },
        {
            "Item": "Poster Paint",
            "Colors": ["Red","Green","Blue","Black","White"],
            "Inventory": {
                "OnHand": 47,
                "MinOnHand": 50
            }
        },
        {
            "Item": "Spray Paint",
            "Colors": ["Black","Red","Green","Blue"],
            "Inventory": {
                "OnHand": 47,
                "MinOnHand": 50,
                "OrderQnty": 36
            }
        }
    ]
)
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus (JSON-Format).

```
{
```

```
    "acknowledged" : true,
    "insertedIds" : [
            ObjectId("5bedb07941ca8d9198f5934c"),
            ObjectId("5bedb07941ca8d9198f5934d"),
            ObjectId("5bedb07941ca8d9198f5934e")
    ]
}
```

Dokumente werden abgefragt

Manchmal müssen Sie möglicherweise den Bestand Ihres Online-Shops nachschlagen, damit Kunden das Angebot sehen und kaufen können. Die Abfrage einer Sammlung ist relativ einfach, unabhängig davon, ob Sie alle Dokumente in der Sammlung haben möchten oder nur die Dokumente, die ein bestimmtes Kriterium erfüllen.

Verwenden Sie die Operation `find()`, um Dokumente abzufragen. Der Befehl `find()` hat einen einzigen Dokumentenparameter, der die Kriterien für die Auswahl der zurückzugebenden Dokumente definiert. Die Ausgabe von `find()` ist ein Dokument, das als einzelne Textzeile ohne Zeilenumbrüche formatiert ist. Um das Ausgabedokument für eine bessere Lesbarkeit zu formatieren, verwenden Sie `find().pretty()`. Alle Beispiele in diesem Thema verwenden `.pretty()` zum Formatieren der Ausgabe.

Verwenden Sie die vier Dokumente, die Sie in den beiden vorherigen Übungen in die `example` Sammlung eingefügt haben — `insertOne()` und`insertMany()`.

Themen

- Alle Dokumente in einer Sammlung abrufen
- Dokumente werden abgerufen, die einem Feldwert entsprechen
- Dokumente werden abgerufen, die einem eingebetteten Dokument entsprechen
- Dokumente werden abgerufen, die einem Feldwert in einem eingebetteten Dokument entsprechen
- Dokumente werden abgerufen, die einem Array entsprechen
- Dokumente werden abgerufen, die einem Wert in einem Array entsprechen
- Dokumente mithilfe von Operatoren abrufen

Alle Dokumente in einer Sammlung abrufen

Um alle Dokumente in Ihrer Sammlung abzurufen, verwenden Sie die Operation `find()` mit einem leeren Abfragedokument.

Die folgende Abfrage gibt alle Dokumente der Sammlung `example` zurück.

```
db.example.find( {} ).pretty()
```

Dokumente werden abgerufen, die einem Feldwert entsprechen

Um alle Dokumente abzurufen, die mit einem Feld und einem Wert übereinstimmen, verwenden Sie die Operation `find()` mit einem Abfragedokument, das die entsprechenden Felder und Werte identifiziert.

Bei Verwendung der vorangegangenen Dokumente gibt diese Abfrage alle Dokumente zurück, bei denen das Feld "Item" (Element) "Pen" (Stift) entspricht.

```
db.example.find( { "Item": "Pen" } ).pretty()
```

Dokumente werden abgerufen, die einem eingebetteten Dokument entsprechen

Um alle Dokumente zu suchen, die mit einem eingebetteten Dokument übereinstimmen, verwenden Sie die Operation `find()` mit einem Abfragedokument, in dem der Name des eingebetteten Dokuments sowie alle Felder und Werte für dieses eingebettete Dokument angegeben werden.

Beim Vergleichen mit einem eingebetteten Dokument muss das eingebettete Dokument denselben Namen haben wie in der Abfrage. Zudem müssen die Felder und Werte im eingebetteten Dokument mit der Abfrage übereinstimmen.

Die folgende Abfrage gibt nur das Dokument "Poster Paint" zurück. Dies liegt daran, dass "Pen" über verschiedene Werte für "`OnHand`" und "`MinOnHand`" verfügt und "Spray Paint" ein weiteres Feld (`OrderQnty`) als das Abfragedokument besitzt.

```
db.example.find({"Inventory": {
    "OnHand": 47,
    "MinOnHand": 50 } } ).pretty()
```

Dokumente werden abgerufen, die einem Feldwert in einem eingebetteten Dokument entsprechen

Um alle Dokumente zu suchen, die mit einem eingebetteten Dokument übereinstimmen, verwenden Sie die Operation `find()` mit einem Abfragedokument, in dem der Name des eingebetteten Dokuments sowie alle Felder und Werte für dieses eingebettete Dokument angegeben werden.

Aufgrund der vorangegangenen Dokumente verwendet die folgende Abfrage "Punktnotation", um das eingebettete Dokument und die Felder von Interesse anzugeben. Jedes Dokument, das damit

übereinstimmt, wird zurückgegeben, unabhängig davon, welche anderen Felder im eingebetteten Dokument vorhanden sind. Die Abfrage gibt "Poster Paint" und "Spray Paint" zurück, weil sie beide den angegebenen Feldern und Werten entsprechen.

```
db.example.find({"Inventory.OnHand": 47, "Inventory.MinOnHand": 50 }).pretty()
```

Dokumente werden abgerufen, die einem Array entsprechen

Um alle Dokumente zu finden, die einem Array entsprechen, verwenden Sie die Operation `find()` mit dem Namen des Arrays, an dem Sie interessiert sind, und allen Werten in diesem Array. Die Abfrage gibt alle Dokumente zurück, in denen sich ein Array mit diesem Namen befindet und in denen die Array-Werte identisch sind und die gleiche Reihenfolge wie in der Abfrage aufweisen.

Die folgende Abfrage gibt nur "Pen" zurück, da "Poster Paint" über eine zusätzlichen Farbe (White) verfügt und die Farben in "Spray Paint" in einer anderen Reihenfolge vorliegen.

```
db.example.find( { "Colors": ["Red","Green","Blue","Black"] } ).pretty()
```

Dokumente werden abgerufen, die einem Wert in einem Array entsprechen

Um alle Dokumente mit einem bestimmten Array-Wert zu finden, verwenden Sie die Operation `find()` mit dem Namen und Wert des Arrays, an dem Sie interessiert sind.

```
db.example.find( { "Colors": "Red" } ).pretty()
```

Bei der vorherigen Operation werden alle drei Dokumente zurückgegeben, da jedes davon ein Array mit dem Namen `Colors` und den Wert "`Red`" irgendwo im Array besitzt. Wenn Sie den Wert "`White`" angeben, gibt die Abfrage nur "Poster Paint" zurück.

Dokumente mithilfe von Operatoren abrufen

Die folgende Abfrage gibt alle Dokumente zurück, in denen der Wert "`Inventory.OnHand`" kleiner als 50 ist.

```
db.example.find(
        { "Inventory.OnHand": { $lt: 50 } } )
```

Eine Liste der unterstützten Abfrageoperatoren finden Sie unter Abfrage- und Projektionsoperatoren.

Dokumente werden aktualisiert

In der Regel sind Ihre Dokumente nicht statisch und werden als Teil Ihrer Anwendungs-Workflows aktualisiert. Die folgenden Beispiele zeigen einige der Möglichkeiten, wie Sie Dokumente aktualisieren können.

Um ein bestehendes Dokument zu aktualisieren, verwenden Sie die Operation`update()`. Die Operation `update()` besitzt zwei Dokumentenparameter. Das erste Dokument gibt an, welche Dokumente aktualisiert werden sollen. Das zweite Dokument gibt an, welche Aktualisierungen durchzuführen sind.

Wenn Sie ein vorhandenes Feld aktualisieren — unabhängig davon, ob es sich bei dem Feld um ein einfaches Feld, ein Array oder ein eingebettetes Dokument handelt — geben Sie den Feldnamen und seine Werte an. Am Ende der Operation wirkt es so, als ob das Feld im alten Dokument durch das neue Feld und die Werte ersetzt wurde.

Themen

- Aktualisierung der Werte eines vorhandenen Felds
- Ein neues Feld hinzufügen
- Ein eingebettetes Dokument ersetzen
- Neue Felder in ein eingebettetes Dokument einfügen
- Ein Feld aus einem Dokument entfernen
- Ein Feld aus mehreren Dokumenten entfernen

Aktualisierung der Werte eines vorhandenen Felds

Verwenden Sie die folgenden vier Dokumente, die Sie zuvor hinzugefügt haben, für die folgenden Aktualisierungsoperationen.

```
{
    "Item": "Ruler",
    "Colors": ["Red","Green","Blue","Clear","Yellow"],
    "Inventory": {
        "OnHand": 47,
        "MinOnHand": 40
    },
    "UnitPrice": 0.89
},
```

```
{
    "Item": "Pen",
    "Colors": ["Red","Green","Blue","Black"],
    "Inventory": {
        "OnHand": 244,
        "MinOnHand": 72
    }
},
{
    "Item": "Poster Paint",
    "Colors": ["Red","Green","Blue","Black","White"],
    "Inventory": {
        "OnHand": 47,
        "MinOnHand": 50
    }
},
{
    "Item": "Spray Paint",
    "Colors": ["Black","Red","Green","Blue"],
    "Inventory": {
        "OnHand": 47,
        "MinOnHand": 50,
        "OrderQnty": 36
    }
}
```

So aktualisieren Sie ein einfaches Feld

Um ein einfaches Feld zu aktualisieren, verwenden Sie `update()` mit `$set`, um den Feldnamen und den neuen Wert anzugeben. Im folgenden Beispiel wird das `Item` von "Pen" in "Gel Pen" geändert.

```
db.example.update(
    { "Item" : "Pen" },
    { $set: { "Item": "Gel Pen" } }
)
```

Ergebnisse dieser Operation sehen in etwa folgendermaßen aus.

```
{
    "Item": "Gel Pen",
    "Colors": ["Red","Green","Blue","Black"],
    "Inventory": {
        "OnHand": 244,
```

```
        "MinOnHand": 72
    }
}
```

So aktualisieren Sie ein Array

Das folgende Beispiel ersetzt das vorhandene Array von Farben mit einem neuen Array, das in der Liste der Farben `Orange` enthält und `White` weglässt. Die neue Liste von Farben liegt in der Reihenfolge vor, die in der Operation `update()` festgelegt wurde.

```
db.example.update(
    { "Item" : "Poster Paint" },
    { $set: { "Colors": ["Red","Green","Blue","Orange","Black"] } }
)
```

Ergebnisse dieser Operation sehen in etwa folgendermaßen aus.

```
{
    "Item": "Poster Paint",
    "Colors": ["Red","Green","Blue","Orange","Black"],
    "Inventory": {
        "OnHand": 47,
        "MinOnHand": 50
    }
}
```

Ein neues Feld hinzufügen

Um ein Dokument durch Hinzufügen eines oder mehrerer neuer Felder zu ändern, verwenden Sie die Operation `update()` mit einem Abfragedokument, das das einzufügende Dokument und die neuen Felder und Werte, die mit dem Operator `$set` eingefügt werden sollen, identifiziert.

Im folgenden Beispiel wird das Feld `UnitPrice` mit dem Wert `3.99` dem Dokument "Spray Paints" hinzugefügt. Beachten Sie, dass der Wert `3.99` numerisch ist und keine Zeichenfolge.

```
db.example.update(
    { "Item": "Spray Paint" },
    { $set: { "UnitPrice": 3.99 } }
)
```

Die Ergebnisse dieser Operation sehen ungefähr wie folgt aus (JSON-Format).

```
{
    "Item": "Spray Paint",
    "Colors": ["Black","Red","Green","Blue"],
    "Inventory": {
        "OnHand": 47,
        "MinOnHand": 50,
        "OrderQnty": 36
    },
    "UnitPrice": 3.99
}
```

Ein eingebettetes Dokument ersetzen

Um ein Dokument durch Ersetzen eines eingebetteten Dokuments zu ändern, verwenden Sie die Operation `update()` mit Dokumenten, die das eingebettete Dokument und seine neuen Felder und Werte mit dem Operator `$set` identifizieren.

Anhand des folgenden Dokuments

```
db.example.insert({
    "DocName": "Document 1",
    "Date": {
        "Year": 1987,
        "Month": 4,
        "Day": 18
    }
})
```

So ersetzen Sie ein eingebettetes Dokument

Im folgenden Beispiel wird das aktuellen Datumsdokument durch ein neues ersetzt, das nur die Felder `Month` und `Day` besitzt; `Year` wurde entfernt.

```
db.example.update(
    { "DocName" : "Document 1" },
    { $set: { "Date": { "Month": 4, "Day": 18 } } }
)
```

Ergebnisse dieser Operation sehen in etwa folgendermaßen aus.

```
{
```

```
    "DocName": "Document 1",
    "Date": {
        "Month": 4,
        "Day": 18
    }
}
```

Neue Felder in ein eingebettetes Dokument einfügen

So fügen Sie einem eingebetteten Dokument neue Felder hinzu

Um ein Dokument durch Hinzufügen eines oder mehrerer neuer Felder zu einem eingebetteten Dokument zu ändern, verwenden Sie die Operation `update()` mit Dokumenten, die das eingebettete Dokument identifizieren, und "Punktnotation" zum Angeben des eingebetteten Dokuments und der neuen Felder und Werte verwenden, die mit dem Operator `$set` eingefügt werden sollen.

Beim folgenden Dokument verwendet der folgende Code "Punktnotierung", um die Felder `DoW` und `Year` im eingebetteten `Date`-Dokument und `Words` im übergeordneten Dokument einzufügen.

```
{
    "DocName": "Document 1",
    "Date": {
        "Month": 4,
        "Day": 18
    }
}
```

```
db.example.update(
    { "DocName" : "Document 1" },
    { $set: { "Date.Year": 1987,
              "Date.DoW": "Saturday",
              "Words": 2482 } }
)
```

Ergebnisse dieser Operation sehen in etwa folgendermaßen aus.

```
{
    "DocName": "Document 1",
    "Date": {
        "Month": 4,
        "Day": 18,
        "Year": 1987,
```

```
        "DoW": "Saturday"
    },
    "Words": 2482
}
```

Ein Feld aus einem Dokument entfernen

Um ein Dokument zu ändern, indem Sie ein Feld aus dem Dokument entfernen, verwenden Sie die Operation `update()` mit einem Abfragedokument, das das Dokument identifiziert, aus dem das Feld entfernt werden soll, und den Operator `$unset`, um das zu entfernende Feld anzugeben.

Das folgende Beispiel entfernt das Feld `Words` aus dem vorangegangen Dokument.

```
db.example.update(
    { "DocName" : "Document 1" },
    { $unset: { Words:1 } }
)
```

Ergebnisse dieser Operation sehen in etwa folgendermaßen aus.

```
{
    "DocName": "Document 1",
    "Date": {
        "Month": 4,
        "Day": 18,
        "Year": 1987,
        "DoW": "Saturday"
    }
}
```

Ein Feld aus mehreren Dokumenten entfernen

Um ein Dokument zu ändern, indem ein Feld aus mehreren Dokumenten entfernt wird, verwenden Sie die Operation `update()` mit dem Operator `$unset` und der Option `multi`, die auf `true` festgelegt ist.

Im folgenden Beispiel wird das Feld `Inventory` aus allen Dokumenten in der Beispielsammlung entfernt. Wenn ein Dokument das Feld `Inventory` nicht hat, wird keine Aktion für dieses Dokument durchgeführt. Wenn `multi: true` weggelassen wird, wird die Aktion nur für das erste Dokument ausgeführt, das das Kriterium erfüllt.

```
db.example.update(
    {},
    { $unset: { Inventory:1 } },
    { multi: true }
)
```

Dokumente löschen

Um ein Dokument aus Ihrer Datenbank zu entfernen, verwenden Sie die Operation `remove()` und geben Sie an, welches Dokument Sie entfernen möchten. Der folgende Code entfernt "Gel Pen" aus Ihrer `example`-Sammlung.

```
db.example.remove( { "Item": "Gel Pen" } )
```

Um alle Dokumente aus Ihrer Datenbank zu entfernen, verwenden Sie den `remove()` Vorgang mit einer leeren Abfrage.

```
db.example.remove( { } )
```

Erste Schritte mit Amazon DocumentDB

Es gibt viele Möglichkeiten, eine Verbindung herzustellen und mit Amazon DocumentDB zu beginnen. Dieses Handbuch ist der schnellste, einfachste und einfachste Weg für Benutzer, mit unserer leistungsstarken Dokumentendatenbank zu beginnen. In diesem Handbuch wird verwendet AWS CloudShell, um eine Verbindung herzustellen und Ihren Amazon DocumentDB-Cluster direkt vom AWS-Managementkonsole abzufragen. Neukunden, die Anspruch auf das AWS kostenlose Kontingent haben, können Amazon DocumentDB CloudShell kostenlos nutzen. Wenn Ihre AWS CloudShell Umgebung oder Ihr Amazon DocumentDB-Cluster Ressourcen nutzt, die über das kostenlose Kontingent hinausgehen, werden Ihnen die normalen AWS Tarife für diese Ressourcen berechnet. Mit diesem Handbuch können Sie in weniger als fünf Minuten mit Amazon DocumentDB beginnen.

> **Note**
>
> Die Anweisungen in diesem Handbuch beziehen sich speziell auf die Erstellung und Verbindung zu instanzbasierten Amazon DocumentDB-Clustern, in denen Amazon DocumentDB und verfügbar sind. AWS CloudShell
>
> - Informationen dazu, wie Sie elastische Amazon DocumentDB-Cluster erstellen und eine Verbindung zu diesen herstellen möchten, finden Sie unterErste Schritte mit Amazon DocumentDB Elastic Clusters.
> - Wenn Sie in Regionen AWS China ansässig sind, finden Sie weitere Informationen unterAmazon EC2 automatisch Connect.

Themen

- Voraussetzungen
- Schritt 1: Erstellen eines Clusters
- Schritt 2: Connect zu Ihrem Cluster her
- Schritt 3: Daten einfügen und abfragen
- Schritt 4: Erkunden

Voraussetzungen

Bevor Sie Ihren ersten Amazon DocumentDB-Cluster erstellen, müssen Sie Folgendes tun:

Erstellen Sie ein Amazon Web Services (AWS) -Konto

Bevor Sie Amazon DocumentDB verwenden können, benötigen Sie ein Amazon Web Services (AWS) -Konto. Das AWS Konto ist kostenlos. Sie zahlen nur für die Services und Ressourcen, die Sie wirklich nutzen.

Wenn Sie noch keinen haben AWS-Konto, führen Sie die folgenden Schritte aus, um einen zu erstellen.

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie https://portal.aws.amazon.com/billing/signup.
2. Folgen Sie den Online-Anweisungen.

   Während der Anmeldung erhalten Sie einen Telefonanruf oder eine Textnachricht und müssen einen Verifizierungscode über die Telefontasten eingeben.

   Wenn Sie sich für eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontoswird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Als bewährte Sicherheitsmethode weisen Sie einem Benutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um Aufgaben auszuführen, die Root-Benutzerzugriff erfordern.

Richten Sie die erforderlichen AWS Identity and Access Management (IAM-) Berechtigungen ein.

Für den Zugriff auf die Verwaltung von Amazon DocumentDB DocumentDB-Ressourcen wie Clustern, Instances und Cluster-Parametergruppen sind Anmeldeinformationen erforderlich, mit denen Sie Ihre Anfragen authentifizieren AWS können. Weitere Informationen finden Sie unter Identity and Access Management für Amazon DocumentDB.

1. Geben Sie in der Suchleiste von IAM ein und wählen Sie im angezeigten Drop-down-Menü IAM aus. AWS-Managementkonsole
2. Sobald Sie sich in der IAM-Konsole befinden, wählen Sie im Navigationsbereich Benutzer aus.
3. Wählen Sie Ihren Nutzernamen aus.

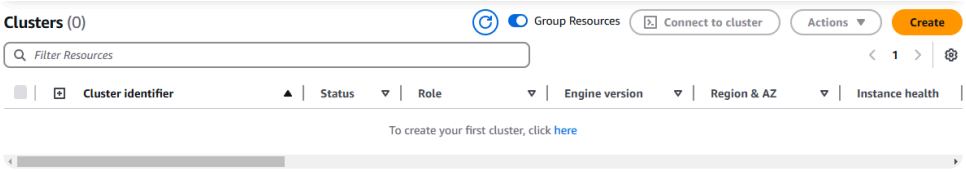
4. Wählen Sie Add permissions (Berechtigungen hinzufügen) aus.
5. Wählen Sie Richtlinien direkt anhängen aus.
6. Geben Sie `AmazonDocDBFullAccess` in die Suchleiste ein und wählen Sie sie aus, sobald sie in den Suchergebnissen erscheint.
7. Wählen Sie Weiter aus.
8. Wählen Sie Add permissions (Berechtigungen hinzufügen) aus.

> **Note**
>
> Ihr AWS Konto enthält in jeder Region eine Standard-VPC. Wenn Sie sich für die Verwendung einer Amazon VPC entscheiden, führen Sie die Schritte im Thema Amazon VPC erstellen im Amazon VPC-Benutzerhandbuch aus.

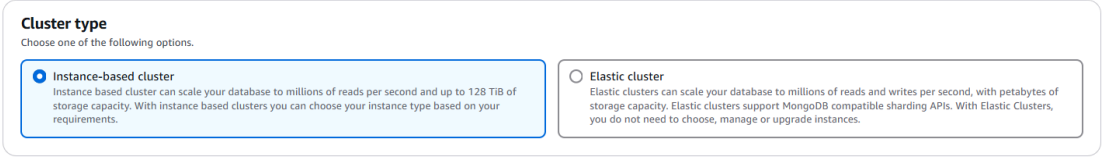
Schritt 1: Erstellen eines Clusters

In diesem Schritt erstellen Sie einen Amazon DocumentDB-Cluster.

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Wählen Sie in der Amazon DocumentDB-Managementkonsole unter Clusters die Option Create aus.



3. Wählen Sie auf der Seite Amazon DocumentDB-Cluster erstellen im Abschnitt Clustertyp die Option Instance-based Cluster aus (dies ist die Standardoption).

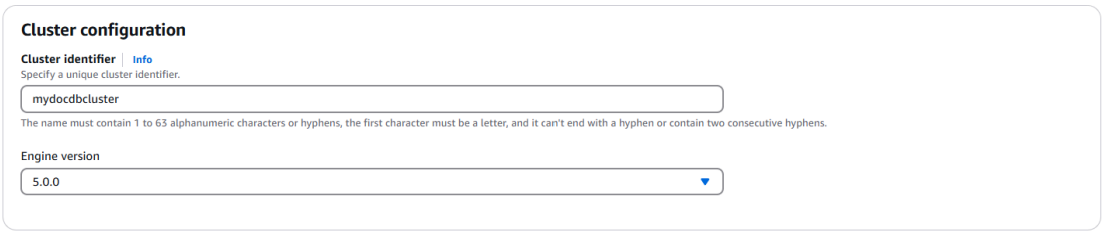


> **Note**
>
> Die andere Option in dieser Kategorie ist Elastic Cluster. Weitere Informationen zu Amazon DocumentDB Elastic Clusters finden Sie unter Verwendung elastischer Amazon DocumentDB-Cluster

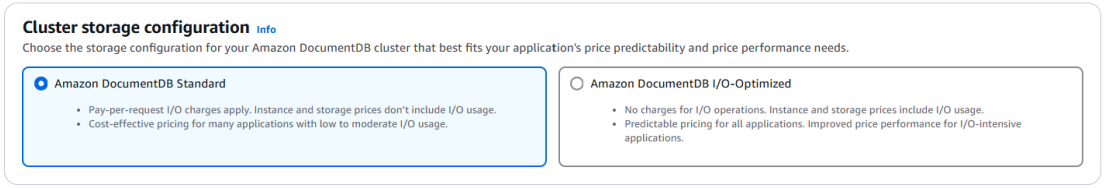
4. Im Abschnitt Cluster-Konfiguration:

   a. Geben Sie als Cluster-ID einen eindeutigen Namen ein, z. **`mydocdbcluster`** B. Beachten Sie, dass die Konsole alle Clusternamen unabhängig von der Art der Eingabe in Kleinbuchstaben ändert.

   b. Wählen Sie für Engine-Version 5.0.0 aus.



5. Wählen Sie im Abschnitt Cluster-Speicherkonfiguration Amazon DocumentDB Standard aus (dies ist die Standardoption).



> **Note**
>
> Die andere Option in dieser Kategorie ist Amazon DocumentDB I/O-Optimized. Weitere Informationen zu den beiden Optionen finden Sie unter Amazon DocumentDB-Cluster-Speicherkonfigurationen

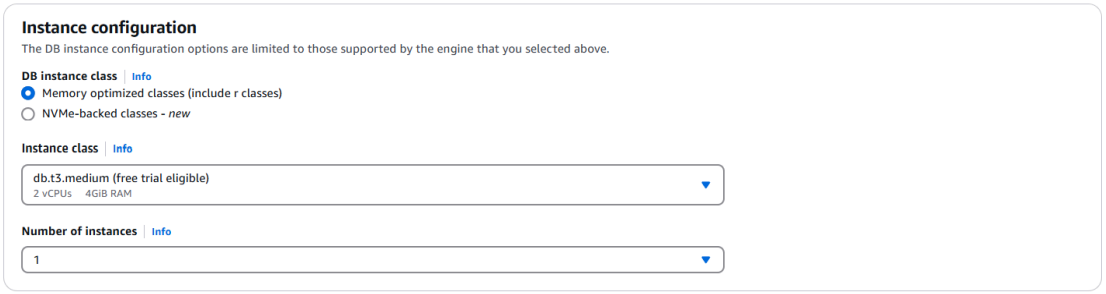
6. Im Abschnitt Instanzkonfiguration:

   a. Wählen Sie für DB-Instance-Klasse die Option Speicheroptimierte Klassen (einschließlich R-Klassen) aus (dies ist die Standardeinstellung).

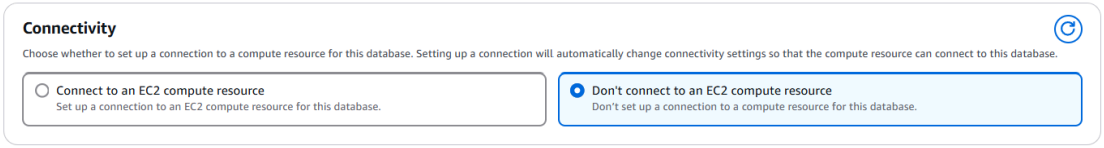
Die andere Instance-Option ist NVMe-backed Klassen. Weitere Informationen hierzu finden Sie unter NVMe-backed Instanzen.

b. Wählen Sie für Instance-Klasse db.t3.medium aus. Dies ist für die kostenlose Testversion berechtigt. AWS

c. Wählen Sie für Anzahl der Instanzen die Option 1 Instanz aus. Die Auswahl einer Instanz trägt zur Kostenminimierung bei. Wenn es sich um ein Produktionssystem handeln würde, würden wir empfehlen, dass Sie drei Instanzen bereitstellen, um eine hohe Verfügbarkeit zu gewährleisten.

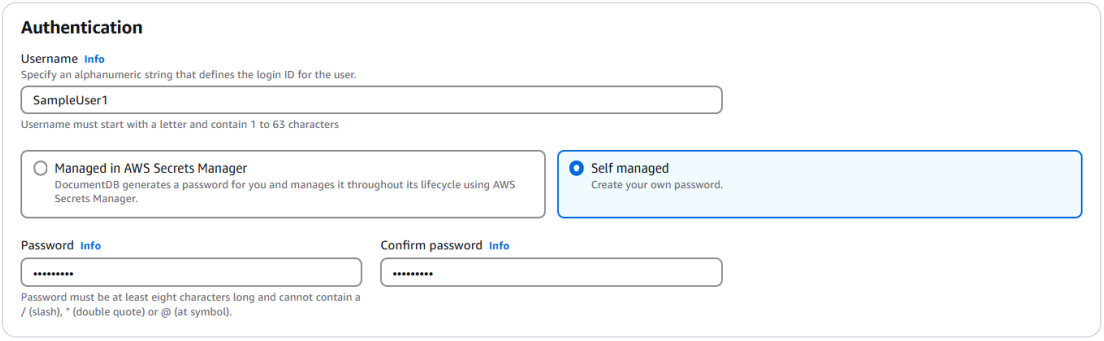


7. Behalten Sie im Abschnitt Konnektivität die Standardeinstellung „Keine Verbindung zu einer EC2-Rechenressource herstellen“ bei.



8. Geben Sie im Abschnitt Authentifizierung einen Benutzernamen für den Hauptbenutzer ein und wählen Sie dann Selbstverwaltet aus. Geben Sie ein Passwort ein und bestätigen Sie es.

   Wenn Sie stattdessen Verwaltet in wählen AWS Secrets Manager, finden Sie Passwortverwaltung mit Amazon DocumentDB und AWS Secrets Manager weitere Informationen unter.



9. Behalten Sie alle anderen Optionen als Standard bei und wählen Sie Cluster erstellen.

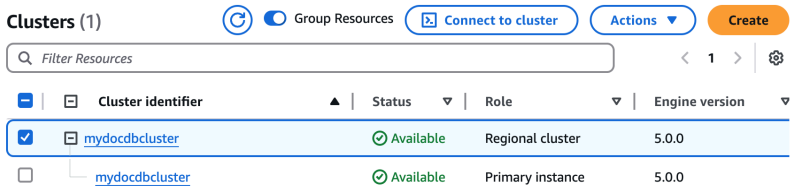
Amazon DocumentDB stellt jetzt Ihren Cluster bereit. Es kann einige Minuten dauern, bis der Vorgang abgeschlossen ist.

> **Note**
>
> Informationen zu Cluster-Statuswerten finden Sie Werte für den Cluster-Status im Kapitel Monitoring Amazon DocumentDB.

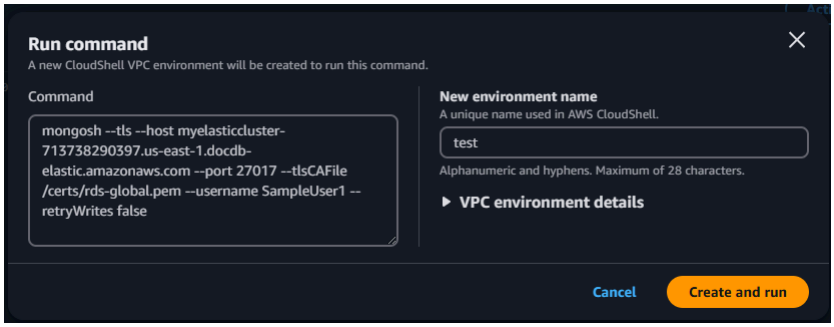
Schritt 2: Connect zu Ihrem Cluster her

Stellen Sie mithilfe AWS CloudShell von Connect zu Ihrem Amazon DocumentDB-Cluster her.

1. Suchen Sie in der Amazon-DocumentDB-Verwaltungskonsole unter Cluster den von Ihnen erstellten Cluster. Wählen Sie Ihren Cluster aus, indem Sie das Kontrollkästchen daneben aktivieren.



2. Wählen Sie Mit Cluster verbinden (neben dem Dropdownmenü Aktionen). Diese Schaltfläche ist erst aktiviert, wenn Sie auf das Kontrollkästchen neben Ihrem Cluster geklickt haben und der Status sowohl des regionalen Clusters als auch der primären Instance (s) als Verfügbar angezeigt wird. Der Befehlsbildschirm CloudShell Ausführen wird angezeigt.
3. Geben Sie im Feld Neuer Umgebungsname einen eindeutigen Namen ein, z. B. „Test“, und wählen Sie Erstellen und ausführen aus. VPC-Umgebungsdetails werden automatisch für Ihre Amazon DocumentDB DocumentDB-Datenbank konfiguriert.



4. Wenn Sie dazu aufgefordert werden, geben Sie das Passwort ein, das Sie in Schritt 1: Amazon DocumentDB-Cluster erstellen (Unterschritt 7) erstellt haben.

   Nachdem Sie Ihr Passwort eingegeben haben und Ihre Aufforderung lautet`rs0 [direct: primary] <env-name>>`, sind Sie erfolgreich mit Ihrem Amazon DocumentDB-Cluster verbunden.

> **Note**
>
> Informationen zur Fehlerbehebung finden Sie unter Problembehandlung bei Amazon DocumentDB.

Schritt 3: Daten einfügen und abfragen

Nachdem Sie nun mit Ihrem Cluster verbunden sind, können Sie einige Abfragen ausführen, um sich mit der Verwendung einer Dokumentendatenbank vertraut zu machen.

1. Um ein einzelnes Dokument einzufügen, geben Sie Folgendes ein:

```
db.collection.insertOne({"hello":"DocumentDB"})
```

   Sie erhalten die folgende Ausgabe:

```
{
  acknowledged: true,
  insertedId: ObjectId('673657216bdf6258466b128c')
}
```

2. Sie können das Dokument lesen, das Sie mit dem `findOne()` Befehl geschrieben haben (weil er nur ein einziges Dokument zurückgibt). Geben Sie Folgendes ein:

```
db.collection.findOne()
```

Sie erhalten die folgende Ausgabe:

```
{ "_id" : ObjectId("5e401fe56056fda7321fbd67"), "hello" : "DocumentDB" }
```

3. Um ein paar weitere Abfragen durchzuführen, sollten Sie einen Anwendungsfall für Spieleprofile in Betracht ziehen. Fügen Sie zunächst einige Einträge in eine Sammlung mit dem Titel ein`profiles`. Geben Sie Folgendes ein:

```
db.profiles.insertMany([{ _id: 1, name: 'Matt', status: 'active', level: 12, score:
 202 },
      { _id: 2, name: 'Frank', status: 'inactive', level: 2, score: 9 },
      { _id: 3, name: 'Karen', status: 'active', level: 7, score: 87 },
      { _id: 4, name: 'Katie', status: 'active', level: 3, score: 27 }
])
```

Sie erhalten die folgende Ausgabe:

```
{ acknowledged: true, insertedIds: { '0': 1, '1': 2, '2': 3, '3': 4 } }
```

4. Verwenden Sie den `find()` Befehl, um alle Dokumente in der Profilsammlung zurückzugeben. Geben Sie Folgendes ein:

```
db.profiles.find()
```

Sie erhalten eine Ausgabe, die den Daten entspricht, die Sie in Schritt 3 eingegeben haben.

5. Verwenden Sie mithilfe eines Filters eine Abfrage für ein einzelnes Dokument. Geben Sie Folgendes ein:

```
db.profiles.find({name: "Katie"})
```

Sie erhalten die folgende Ausgabe:

```
{ "_id" : 4, "name" : "Katie", "status": "active", "level": 3, "score":27}
```

6. Versuchen wir nun, ein Profil zu finden und es mit dem `findAndModify` Befehl zu ändern. Wir geben dem Benutzer Matt zusätzliche 10 Punkte mit dem folgenden Code:

```
db.profiles.findAndModify({
        query: { name: "Matt", status: "active"},
        update: { $inc: { score: 10 } }
    })
```

Sie erhalten die folgende Ausgabe (beachten Sie, dass seine Punktzahl noch nicht gestiegen ist):

```
{
    [{_id : 1, name : 'Matt', status: 'active', level: 12, score: 202}]
```

7. Sie können mit der folgenden Abfrage überprüfen, ob sich sein Punktestand geändert hat:

   ```
   db.profiles.find({name: "Matt"})
   ```

   Sie erhalten die folgende Ausgabe:

   ```
   { "_id" : 1, "name" : "Matt", "status" : "active", "level" : 12, "score" : 212 }
   ```

Schritt 4: Erkunden

Herzlichen Glückwunsch! Sie haben den Leitfaden Erste Schritte für instanzbasierte Amazon DocumentDB-Cluster erfolgreich abgeschlossen.

Was kommt als Nächstes? Erfahren Sie, wie Sie diese Datenbank mit einigen ihrer beliebten Funktionen voll ausschöpfen können:

- Amazon DocumentDB verwalten
- Skalierung
- Sichern und Wiederherstellen

> **Note**
>
> Für den Cluster, den Sie im Rahmen dieser Übung „Erste Schritte“ erstellt haben, fallen weiterhin Kosten an, sofern Sie ihn nicht löschen. Anweisungen finden Sie unter Löschen eines Amazon DocumentDB-Clusters.

Funktionen und Konfigurationen von Amazon DocumentDB

In den folgenden Tabellen werden Funktionen, Fähigkeiten und unterstützte Instance-Typen der Amazon DocumentDB DocumentDB-Engine-Versionen und Elastic Clusters verglichen. Verwenden Sie diese Tabellen, um zu ermitteln, welche Engine-Version Ihren Workload-Anforderungen am besten entspricht.

Status der Engine

Motorstatus nach Version

Merkmal/Fähigkeit	v3.6	v4.0	v5.0	v8.0	
Status der Support	EOL: März 2026	Aktiv	Aktiv (LTS verfügbar)	Aktiv (GA November 2025)	
Erweiterter Support verfügbar	Ja (bezahlt, bis März 2029)	N/A	N/A	N/A	
LTS-Version verfügbar	Nein	Nein	Ja (v5.0 LTS)	Nein	
Elastische Cluster	Nein	Nein	Ja	Nein	

Clustertypen

Clustertypen nach Version

Cluster Type (Clustertyp	v3.6	v4.0	v5.0	v8.0	Elastische Cluster
Instance-based Cluster	Ja	Ja	Ja	Ja	Ja
Serverlose Instanzen	Nein	Nein	Ja	Ja	Nein

Features

Funktionen und Konfigurationen nach Engine-Version

Feature	v3.6	v4.0	v5.0	v8.0	Elastische Cluster
Globale Cluster	Nein	Ja	Ja	Ja	Nein
Multi-AZ (3 AZs)	Ja	Ja	Ja	Ja	Ja (pro Shard)
Read Replicas werden unterstützt	15	15	15	15	15 pro Shard
ACID-Transaktionen	Nein	Ja	Ja	Ja	Nein
Change streams	Ja	Ja	Ja	Ja	Nein
Vektor-Suche	Nein	Nein	Ja	Ja	Nein
Performance Insights	Ja	Ja	Ja	Ja	Nein
In-place Hauptversions-Upgrade (MVU)	Ja (auf 5.0)	Ja (bis 5,0)	Ja (bis 8,0)	Nein (nur Ziel)	Nein
Client-side Verschlüsselung auf Feldebene (FLE)	Nein	Nein	Ja	Ja	Nein
I/O-Optimized Speicher	Nein	Nein	Ja	Ja	Nein
Rotation des TLS-Zertifikats (kein Neustart)	Ja (Patch 1.0.208662+)	Ja (Patch 2.0.10179+)	Ja (Patch 3.0.4780+)	Ja	Ja
Cross-Region Snapshot-Kopie	Ja	Ja	Ja	Ja	Ja

Feature	v3.6	v4.0	v5.0	v8.0	Elastische Cluster
Cross-account Schnappschüsse teilen	Ja	Ja	Ja	Ja	Nein
Protokolle für Prüfungen und langsame Abfragen	Ja	Ja	Ja	Ja	Ja
Dual-stack IPv4/IPv6	Nein	Ja (Patch 2.0.11747 +)	Ja (Patch 3.0.15902 +)	Ja	N/A
Kollation	Nein	Nein	Nein	Ja	Nein
Ansichten	Nein	Nein	Nein	Ja	Nein
Komprimierungsunterstützung	Nein	Nein	LZ4	LZ4/Ztsd	Nein
Textindex	Nein	Nein	V1	V2	Nein
FedRAMP () GovCloud	Nein	Nein	Ja	Ja	Nein

Instance-Typen

Unterstützung des Instanztyps nach Version

Instance-Typ	v3.6	v4.0	v5.0	v8.0	
db.r4 (vorherige Generation)	Ja	Nein	Nein	Nein	
db.r5	Ja	Ja	Ja	Ja	
db.r6g (Graviton2)	Nein	Ja	Ja	Ja	
db.r6gd (NVMe-backed Graviton2)	Nein	Nein	Ja	Ja	

Instance-Typ	v3.6	v4.0	v5.0	v8.0	
db.r8g (Graviton 4)	Nein	Nein	Ja	Ja	
db.t3.medium	Ja	Ja	Ja	Ja	
db.t4g.mittel (Graviton2)	Nein	Ja	Ja	Ja	
Serverless	Nein	Nein	Ja	Ja	

AWS Integrationen

AWS Integrationsunterstützung nach Version

AWS Integration/Funktion	v3.6	v4.0	v5.0	v8.0	Elastische Cluster
AWS Backup	Ja	Ja	Ja	Ja	Nein
AWS Secrets Manager	Ja	Ja	Ja	Ja	Nein
AWS Lambda (natives ESM)	Nein	Ja	Ja	Nein	Nein
Amazon OpenSearch Service-Aufnahme () Zero-ETL	Nein	Ja	Ja	Ja	Nein
AWS DMS Unterstützung bei der Migration	Ja	Ja	Ja	Ja (ab Version 5.0 AWS DMS)	Ja
AWS Identity and Access Management authentication	Nein	Nein	Ja (5.0 instanzbasiert)	Ja	Nein
AWS CloudShell	Nein	Nein	Ja	Ja	Nein

AWS Integration/Funktion	v3.6	v4.0	v5.0	v8.0	Elastische Cluster
AWS Key Management Service	Ja	Ja	Ja	Ja	Ja
AWS CloudTrail	Ja	Ja	Ja	Ja	Ja

Amazon DocumentDB DocumentDB-Schnellstart mit CloudFormation

Dieser Abschnitt enthält Schritte und weitere Informationen, die Ihnen den schnellen Einstieg in die Nutzung von Amazon DocumentDB (mit MongoDB-Kompatibilität) erleichtern sollen. CloudFormation Allgemeine Informationen zu Amazon DocumentDB finden Sie unterWas ist Amazon DocumentDB (mit MongoDB-Kompatibilität).

Diese Anweisungen verwenden eine AWS CloudFormation Vorlage, um einen Cluster und Instances in Ihrer Standard-Amazon-VPC zu erstellen. Anweisungen zum Erstellen dieser Ressourcen finden Sie unter Erste Schritte mit Amazon DocumentDB.

> **Important**
>
> Der CloudFormation Stack, der durch diese Vorlage erstellt wird, erstellt mehrere Ressourcen, darunter Ressourcen in Amazon DocumentDB (z. B. ein Cluster und Instances) und Amazon Elastic Compute Cloud (z. B. eine Subnetzgruppe).
> Einige dieser Ressourcen sind nicht im kostenlosen Kontingent enthalten. Preisinformationen finden Sie unter Amazon DocumentDB DocumentDB-Preise und Amazon EC2 EC2-Preise.
> Sie können den Stack löschen, wenn Sie ihn nicht mehr benötigen, um Gebühren zu sparen.

Dieser CloudFormation Stapel ist nur für Tutorialzwecke vorgesehen. Wenn Sie diese Vorlage für eine Produktionsumgebung verwenden, empfehlen wir Ihnen, strengere IAM-Richtlinien und Sicherheitsvorkehrungen zu verwenden. Informationen zur Sicherung von Ressourcen finden Sie unter Amazon VPC Security und Amazon EC2 Network and Security.

Themen

- Voraussetzungen
- Eine Amazon DocumentDB starten CloudFormation Stack
- Zugreifen auf den Amazon DocumentDB-Cluster
- Kündigungsschutz und Löschschutz

Voraussetzungen

Bevor Sie einen Amazon DocumentDB-Cluster erstellen, müssen Sie über Folgendes verfügen:

- Eine standardmäßige Amazon-VPC
- Die erforderlichen IAM-Berechtigungen

Erforderliche IAM-Berechtigungen

Die folgenden Berechtigungen erlauben Ihnen das Erstellen von Ressourcen für den CloudFormation -Stack:

AWS Verwaltete Richtlinien

- `AWSCloudFormationReadOnlyAccess`
- `AmazonDocDBFullAccess`

Zusätzliche IAM-Berechtigungen

Die folgende Richtlinie beschreibt die zusätzlichen Berechtigungen, die zum Erstellen und Löschen dieses CloudFormation Stacks erforderlich sind.

Ersetzen Sie in den folgenden Beispielen jedes Beispiel *`user input placeholder`* durch die Informationen Ihrer Ressource.

Amazon-EC2-Schlüsselpaar

In der Region, in der Sie den CloudFormation Stack erstellen möchten, muss ein key pair (und die PEM-Datei) verfügbar sein. Wenn Sie ein key pair erstellen müssen, finden Sie weitere Informationen unter Creating a Key Pair Using Amazon EC2 im Amazon EC2-Benutzerhandbuch.

Eine Amazon DocumentDB starten CloudFormation Stack

In diesem Abschnitt wird beschrieben, wie Sie einen Amazon DocumentDB CloudFormation DocumentDB-Stack starten und konfigurieren.

1. Melden Sie sich AWS-Managementkonsole unter an. https://console.aws.amazon.com/

2. In der folgenden Tabelle sind die Amazon DocumentDB DocumentDB-Stack-Vorlagen für jede AWS-Region Vorlage aufgeführt. Wählen Sie Launch Stack für die AWS-Region Datei, in der Sie Ihren Stack starten möchten.

Region	Vorlage anzeigen	In Designer anzeigen	Starten
USA Ost (Ohio)	Vorlage anzeigen	In Designer anzeigen	
USA Ost (Nord-Virginia)	Vorlage anzeigen	In Designer anzeigen	
USA West (Oregon)	Vorlage anzeigen	In Designer anzeigen	
Asien-Pazifik (Mumbai)	Vorlage anzeigen	In Designer anzeigen	
Asien-Pazifik (Seoul)	Vorlage anzeigen	In Designer anzeigen	
Asien-Pazifik (Singapur)	Vorlage anzeigen	In Designer anzeigen	
Asien-Pazifik (Sydney)	Vorlage anzeigen	In Designer anzeigen	
Asien-Pazifik (Tokio)	Vorlage anzeigen	In Designer anzeigen	
Kanada (Zentral)	Vorlage anzeigen	In Designer anzeigen	
Europa (Frankfurt)	Vorlage anzeigen	In Designer anzeigen	
Europa (Irland)	Vorlage anzeigen	In Designer anzeigen	
Europa (London)	Vorlage anzeigen	In Designer anzeigen	

Region	Vorlage anzeigen	In Designer anzeigen	Starten
Europa (Paris)	Vorlage anzeigen	In Designer anzeigen	Launch Stack

3. Stapel erstellen — Beschreibt die Amazon DocumentDB DocumentDB-Vorlage, die Sie ausgewählt haben. Jeder Stapel basiert auf einer Vorlage — einer JSON- oder YAML-Datei —, die die Konfiguration der AWS Ressourcen enthält, die Sie in den Stapel aufnehmen möchten. Da Sie sich dafür entschieden haben, einen Stapel aus den oben bereitgestellten Vorlagen zu starten, wurde Ihre Vorlage bereits so konfiguriert, dass sie einen Amazon DocumentDB DocumentDB-Stack für die von AWS-Region Ihnen gewählte Vorlage erstellt.

   Wenn Sie einen CloudFormation Stack starten, ist der Löschschutz für Ihren Amazon DocumentDB-Cluster standardmäßig deaktiviert. Wenn Sie den Löschschutz für Ihren Cluster aktivieren möchten, führen Sie die folgenden Schritte aus. Andernfalls wählen Sie Next (Weiter), um mit dem nächsten Schritt fortzufahren.

   So aktivieren Sie den Löschschutz für Ihren Amazon DocumentDB-Cluster:

   1. Wählen Sie in der unteren rechten Ecke der Seite „Stack erstellen“ die Option In Designer anzeigen aus.
   2. Ändern Sie die Vorlage mithilfe des integrierten JSON- und YAML-Editors auf der resultierenden CloudFormation Designer-Seite der Konsole. Blättern Sie zum Abschnitt `Resources` und ändern Sie diesen wie folgt, um den `DeletionProtection` einzubinden. Weitere Informationen zur Verwendung von CloudFormation Designer finden Sie unter Was ist CloudFormation Designer? .

      JSON:

```
"Resources": {
    "DBCluster": {
        "Type": "AWS::DocDB::DBCluster",
        "DeletionPolicy": "Delete",
        "Properties": {
            "DBClusterIdentifier": {
                "Ref": "DBClusterName"
            },
            "MasterUsername": {
                "Ref": "MasterUser"
            },
```

```
            "MasterUserPassword": {
                "Ref": "MasterPassword"
            },
            "DeletionProtection": "true"
        }
    },
```

YAML:

```
Resources:
  DBCluster:
    Type: 'AWS::DocDB::DBCluster'
    DeletionPolicy: Delete
    Properties:
      DBClusterIdentifier: !Ref DBClusterName
      MasterUsername: !Ref MasterUser
      MasterUserPassword: !Ref MasterPassword
      DeletionProtection: 'true'
```

3. Wählen Sie Create Stack (Stack erstellen)
   ( )
   in der oberen linken Ecke der Seite, um Ihre Änderungen zu speichern und einen Stack zu erstellen, bei dem diese Änderungen aktiviert sind.
4. Nachdem Sie Ihre Änderungen gespeichert haben, werden Sie zur Seite Create stack (Stack erstellen) weitergeleitet.
5. Wählen Sie Next (Weiter), um fortzufahren.

4. Stack-Details angeben — Geben Sie den Stack-Namen und die Parameter für Ihre Vorlage ein. Parameter werden in Ihrer Vorlage definiert und ermöglichen Ihnen, benutzerdefinierte Werte einzugeben, wenn Sie einen Stack erstellen oder aktualisieren.
   - Geben Sie unter Stack name (Stack-Name) einen Namen für Ihren Stack ein oder übernehmen Sie den angegebenen Namen. Der Stackname kann Buchstaben (A—Z und a—Z), Zahlen (0—9) und Bindestriche (—) enthalten.
   - Geben Sie unter Parameter, die folgenden Details ein:
     - DBClusterName— Geben Sie einen Namen für Ihren Amazon DocumentDB-Cluster ein oder akzeptieren Sie den angegebenen Namen.

       Einschränkungen bei der Benennung von Clustern:

- Die Länge beträgt [1—63] Buchstaben, Zahlen oder Bindestriche.
- Muss mit einem Buchstaben beginnen.
- Darf nicht mit einem Bindestrich enden oder zwei aufeinanderfolgende Bindestriche enthalten.
- Muss für alle Cluster in Amazon RDS, Neptune und Amazon DocumentDB pro AWS-Konto Region eindeutig sein.

- DBInstanceClass— Wählen Sie aus der Drop-down-Liste die Instance-Klasse für Ihren Amazon DocumentDB-Cluster aus.
- DBInstanceName— Geben Sie einen Namen für Ihre Amazon DocumentDB DocumentDB-Instance ein oder akzeptieren Sie den angegebenen Namen.

  Einschränkungen für Instance-Benennungen:

  - Die Länge beträgt [1—63] Buchstaben, Zahlen oder Bindestriche.
  - Muss mit einem Buchstaben beginnen.
  - Darf nicht mit einem Bindestrich enden oder zwei aufeinanderfolgende Bindestriche enthalten.
  - Muss für alle Instances in Amazon RDS, Neptune und Amazon DocumentDB pro AWS-Konto Region eindeutig sein.
- MasterPassword— Das Passwort für das Datenbank-Administratorkonto.
- MasterUser— Der Benutzername des Datenbank-Administratorkontos. Der MasterUser muss mit einem Buchstaben beginnen und darf nur alphanumerische Zeichen enthalten.

Klicken Sie auf Next (Weiter), um Ihre Änderungen zu speichern und fortzufahren.

5. Stack-Optionen konfigurieren — Konfigurieren Sie die Tags, Berechtigungen und zusätzlichen Optionen Ihres Stacks.
   - Tags — Geben Sie Tag-Paare (Schlüssel-Wert) an, die auf Ihre Ressourcen in Ihrem Stack angewendet werden sollen. Sie können bis zu 50 eindeutige Tags für jeden Stack hinzufügen.
   - Berechtigungen — optional. Wählen Sie eine IAM-Rolle, um explizit zu definieren, wie Ressourcen im Stack erstellt, geändert oder gelöscht werden CloudFormation können. Wenn Sie keine Rolle auswählen, CloudFormation verwendet Berechtigungen, die auf Ihren Benutzeranmeldedaten basieren. Bevor Sie eine Service-Rolle festlegen, stellen Sie sicher, dass Sie über die Berechtigung zum Weiterleiten (`iam:PassRole`) verfügen. Die `iam:PassRole`-Berechtigung gibt an, welche Rollen Sie verwenden können.

> **Note**
>
> Wenn Sie eine Servicerolle angeben, verwendet diese Rolle CloudFormation immer für alle Operationen, die auf diesem Stack ausgeführt werden. Andere Benutzer, die Berechtigungen zum Ausführen von Vorgängen in diesem Stapel haben, können diese Rolle verwenden, selbst wenn Sie keine Berechtigung zum Weiterleiten haben. Wenn die Rolle Berechtigungen umfasst, die der Benutzer nicht haben sollte, können Sie die Berechtigungen eines Benutzers versehentlich weiterleiten. Stellen Sie sicher, dass die Rolle die geringsten Rechte gewährt.

- Erweiterte Optionen — Sie können die folgenden erweiterten Optionen festlegen:
  - Stack-Richtlinie — Optional. Legt die Ressourcen, fest die Sie vor unbeabsichtigten Aktualisierungen während einer Stack-Aktualisierung schützen möchten. Standardmäßig können alle Ressourcen bei einer Stack-Aktualisierung aktualisiert werden.

    Sie können die Stack-Richtlinie direkt im JSON-Format eingeben oder eine JSON-Datei, die die Stack-Richtlinie enthält, hochladen. Weitere Informationen finden Sie unter Prevent Updates to Stack Resources (Verhindern von Aktualisierungen der Stack-Ressourcen).
  - Rollback-Konfiguration — Optional. Geben Sie CloudWatch Log-Alarme CloudFormation an, die bei der Erstellung und Aktualisierung des Stacks überwacht werden sollen. Wenn der Vorgang einen Alarmschwellenwert überschreitet, wird er CloudFormation rückgängig gemacht.
  - Benachrichtigungsoptionen — optional. Geben Sie Themen für das Simple Notification System (SNS) an.
  - Optionen zur Stapelerstellung — Optional. Sie können die folgenden Optionen angeben:
    - Rollback bei einem Fehler — Gibt an, ob der Stack zurückgesetzt werden soll, falls die Stack-Erstellung fehlschlägt.
    - Timeout — Die Anzahl der Minuten, bevor bei der Stack-Erstellung ein Timeout eintritt.
    - Kündigungsschutz — verhindert, dass der Stack versehentlich gelöscht wird.

> **Note**
>
> CloudFormation Der Kündigungsschutz unterscheidet sich vom Löschschutzkonzept von Amazon DocumentDB. Weitere Informationen finden Sie unter Kündigungsschutz und Löschschutz.

Wählen Sie Next (Weiter), um fortzufahren.

6. Überprüfung <stack-name>— Überprüfen Sie Ihre Stack-Vorlage, Details und Konfigurationsoptionen. Sie können auch einen Schnellerstellungs-Link unten auf der Seite öffnen, um Stacks mit denselben Grundkonfigurationen wie diesen zu erstellen.

   - Wählen Sie Create (Erstellen), um den Stack zu erstellen.
   - Alternativ können Sie auch Create change set (Änderungssatz erstellen) wählen. Ein Änderungssatz ist eine Vorschau darauf, wie dieser Stack vor seiner Erstellung konfiguriert wird. Auf diese Weise können Sie verschiedene Konfigurationen prüfen, bevor Sie den Änderungssatz ausführen.

Zugreifen auf den Amazon DocumentDB-Cluster

Sobald der CloudFormation Stack abgeschlossen ist, können Sie eine Amazon EC2 EC2-Instance verwenden, um eine Verbindung zu Ihrem Amazon DocumentDB-Cluster herzustellen. Informationen zum Herstellen einer Verbindung mit einer Amazon EC2 EC2-Instance mithilfe von SSH finden Sie unter Connect to Your Linux Instance im Amazon EC2 EC2-Benutzerhandbuch.

Nachdem Sie die Verbindung hergestellt haben, lesen Sie die folgenden Abschnitte, die Informationen zur Verwendung von Amazon DocumentDB enthalten.

- Schritt 3: Daten einfügen und abfragen
- Verwaltung von Amazon DocumentDB DocumentDB-Ressourcen
- Amazon DocumentDB überwachen

Kündigungsschutz und Löschschutz

Es ist eine bewährte Methode von Amazon DocumentDB, den Löschschutz und den Kündigungsschutz zu aktivieren. CloudFormation Der Kündigungsschutz unterscheidet sich deutlich von der Amazon DocumentDB DocumentDB-Löschschutzfunktion.

- Kündigungsschutz — Sie können verhindern, dass ein Stapel versehentlich gelöscht wird, indem Sie den Kündigungsschutz für Ihren CloudFormation Stack aktivieren. Wenn ein Benutzer versucht, einen Stack mit aktiviertem Beendigungsschutz zu löschen, schlägt das Löschen fehl und der Stack bleibt unverändert. Der Terminierungsschutz ist standardmäßig deaktiviert, wenn Sie einen Stack mit erstellen CloudFormation. Sie können den Beendigungsschutz aktivieren, wenn Sie den Stack erstellen. Weitere Informationen finden Sie unter CloudFormation Stack-Optionen festlegen.
- Löschschutz — Amazon DocumentDB bietet auch die Möglichkeit, den Löschschutz für einen Cluster zu aktivieren. Wenn ein Benutzer versucht, einen Amazon DocumentDB-Cluster mit aktiviertem Löschschutz zu löschen, schlägt der Löschvorgang fehl und der Cluster bleibt unverändert. Wenn der Löschschutz aktiviert ist, schützt er vor versehentlichen Löschungen aus der Amazon DocumentDB AWS-Managementkonsole, und AWS CLI. CloudFormation Weitere Informationen zum Aktivieren und Deaktivieren des Löschschutzes für einen Amazon DocumentDB-Cluster finden Sie unter. Löschschutz

Amazon DocumentDB DocumentDB-Kompatibilität mit MongoDB

Amazon DocumentDB unterstützt MongoDB-Kompatibilität, einschließlich MongoDB 4.0, MongoDB 5.0 und MongoDB 8.0. MongoDB-Kompatibilität bedeutet, dass die überwiegende Mehrheit der Anwendungen, Treiber und Tools, die Sie heute bereits mit Ihren MongoDB-Datenbanken verwenden, mit Amazon DocumentDB verwendet werden können, ohne oder mit wenigen Änderungen. In diesem Abschnitt wird alles beschrieben, was Sie über die Kompatibilität von Amazon DocumentDB mit MongoDB wissen müssen, darunter neue Funktionen und Funktionen, erste Schritte, Migrationspfade und funktionale Unterschiede.

Themen

- MongoDB 8.0-Kompatibilität
- MongoDB 5.0-Kompatibilität
- MongoDB 4.0-Kompatibilität

MongoDB 8.0-Kompatibilität

Themen

- Was ist neu in Amazon DocumentDB 8.0
- Erste Schritte mit Amazon DocumentDB 8.0
- Upgrade oder Migration auf Amazon DocumentDB 5.0 oder 8.0
- Funktionelle Unterschiede

Was ist neu in Amazon DocumentDB 8.0

Amazon DocumentDB 8.0 verbessert die Abfrageleistung um das bis zu 7-fache und die Komprimierungsrate um das bis zu 5-fache, sodass Sie Hochleistungsanwendungen zu geringeren Kosten erstellen können. Amazon DocumentDB 8.0 ist vollständig mit MongoDB 8.0 kompatibel. In der folgenden Zusammenfassung werden einige der wichtigsten Funktionen vorgestellt, die in Amazon DocumentDB 8.0 eingeführt wurden. Eine vollständige Liste der neuen Funktionen finden Sie unterVersionshinweise.

- Bietet Kompatibilität mit MongoDB 8.0, indem Unterstützung für MongoDB 8.0-API-Treiber hinzugefügt wird. Unterstützt auch Anwendungen, die mit den MongoDB-API-Versionen 6.0 und 7.0 erstellt wurden.
- Der neue Abfrageplaner in Amazon DocumentDB 8.0 erweitert Leistungsverbesserungen auf Operatoren in der Aggregationsphase und unterstützt außerdem Aggregationspipeline-Optimierungen und spezielle Befehle.
- Amazon DocumentDB 8.0 unterstützt Sortierung und Ansichten.
- Bietet 6 neue Aggregationsstufen: $replaceWith, $vectorSearch, $merge, $set, $unset, $bucket und 3 neue Aggregationsoperatoren $pow, $rand, $DateTrunc.
- Eine neue Version des Textindexes: Der Textindex v2 in Amazon DocumentDB 8.0 führt zusätzliche Token ein und verbessert so die Textsuchfunktionen.
- Durch die Erstellung parallel Vektorindizes reduziert Amazon DocumentDB 8.0 die Indexerstellungszeit um das bis zu 30-fache.

Erste Schritte mit Amazon DocumentDB 8.0

Informationen zu den ersten Schritten mit Amazon DocumentDB 8.0 finden Sie im Handbuch Erste Schritte. Sie können einen neuen Amazon DocumentDB 8.0-Cluster mit dem AWS-Managementkonsole oder dem AWS SDK, AWS CLI, oder CloudFormation erstellen. Wenn Sie eine Verbindung zu Amazon DocumentDB herstellen, müssen Sie einen MongoDB-Treiber oder ein MongoDB-Tool verwenden, das mit MongoDB 5.0 oder höher kompatibel ist.

> **Note**
>
> Wenn Sie das AWS SDK oder CloudFormation verwenden AWS CLI, wird die Engine-Version standardmäßig auf 5.0.0 gesetzt. Sie müssen den Parameter explizit angeben, `engineVersion = 8.0.0` um einen neuen Amazon DocumentDB 8.0-Cluster oder `engineVersion = 4.0.0` einen neuen Amazon DocumentDB 4.0-Cluster oder einen neuen Amazon DocumentDB 3.6-Cluster `engineVersion = 3.6.0` zu erstellen. Für einen bestimmten Amazon DocumentDB-Cluster können Sie die Cluster-Version ermitteln, indem Sie AWS CLI den aufrufen `describe-db-clusters` oder die Amazon DocumentDB-Managementkonsole verwenden, um die Engine-Versionsnummer für einen bestimmten Cluster anzuzeigen.

Amazon DocumentDB 5.0 und 8.0 unterstützt den Amazon EC2 `r8g` Graviton4-Prozessor und Graviton2-Prozessoren sowie `t4.medium` Instance-Typen für Ihre Cluster `r6g` und ist in allen unterstützten Regionen verfügbar (siehe). Instances Weitere Informationen zur Preisgestaltung finden Sie unter Amazon DocumentDB (mit MongoDB-Kompatibilität) — Preise.

Upgrade oder Migration auf Amazon DocumentDB 5.0 oder 8.0

Sie können von MongoDB 3.6 oder MongoDB 4.0 zu Amazon DocumentDB 5.0 oder Amazon DocumentDB 8.0 migrieren, indem Sie Dienstprogramme wie `mongodump`,, `mongorestore` und verwenden. AWS DMS`mongoimport``mongoexport` Anweisungen zur Migration finden Sie unter. Aktualisieren Ihres Amazon DocumentDB-Clusters mit AWS Database Migration Service

Funktionelle Unterschiede

Funktionale Unterschiede zwischen Amazon DocumentDB 5.0 und 8.0

Mit der Veröffentlichung von Amazon DocumentDB 8.0 gibt es funktionale Unterschiede zwischen Amazon DocumentDB 5.0 und Amazon DocumentDB 8.0:

- Planner v1 ist der Standard-Abfrageplaner in Amazon DocumentDB 5.0, wohingegen der leistungsstärkere Planner v3 der Standard in Amazon DocumentDB 8.0 ist.
- Neue Funktionen in Amazon DocumentDB 8.0, darunter Views, Collation und Operatoren wie $merge, sind nur mit Planner v3 kompatibel.
- Die Komprimierung ist in Amazon DocumentDB 8.0 standardmäßig aktiviert und auf die Verwendung des Zstandard-Algorithmus eingestellt. Darüber hinaus ist „aktiviert“ in Amazon DocumentDB 8.0 keine gültige Wahl mehr. Sie können zwischen Zstd, LZ4 und None wählen.
- Amazon DocumentDB 8.0 unterstützt nur TLS 1.2 und höher für Datenbankverbindungen.

> **Important**
>
> Amazon DocumentDB 8.0 erfordert TLS 1.2 oder höher. TLS 1.0 und TLS 1.1 werden nicht mehr unterstützt.

MongoDB 5.0-Kompatibilität

Themen

- Was ist neu in Amazon DocumentDB 5.0
- Was ist neu in Amazon DocumentDB 5.0.1
- Erste Schritte mit Amazon DocumentDB 5.0
- Upgrade oder Migration auf Amazon DocumentDB 5.0
- Funktionelle Unterschiede

Was ist neu in Amazon DocumentDB 5.0

Amazon DocumentDB 5.0 bietet neue Funktionen und Fähigkeiten, darunter Speicherlimits und clientseitige Verschlüsselung auf Feldebene. In der folgenden Zusammenfassung werden einige der wichtigsten Funktionen vorgestellt, die in Amazon DocumentDB 5.0 eingeführt wurden. Eine vollständige Liste der neuen Funktionen finden Sie unterVersionshinweise.

- Das Speicherlimit wurde für alle instanzbasierten Amazon DocumentDB-Cluster und shard-basierten Elastic-Cluster auf 128 TiB erhöht.
- Amazon DocumentDB 5.0 Engine (Version 3.0.775) eingeführt
  - Support für MongoDB 5.0 API-Treiber
  - Support für Client-side Field Level Encryption (FLE). Sie können jetzt Felder auf der Clientseite verschlüsseln, bevor Sie die Daten in den Amazon DocumentDB-Cluster schreiben. Weitere Informationen finden Sie unter Verschlüsselung auf FeldebeneClient-side .
  - Neue Aggregationsoperatoren:`$dateAdd`, `$dateSubtract`
  - Unterstützt Indizes mit `$elemMatch` Operator. Das hat zur Folge, `$elemMatch` dass Abfragen zu Indexscans führen.

Amazon DocumentDB unterstützt nicht jede MongoDB 5.0-Funktion. Bei der Entwicklung von Amazon DocumentDB 5.0 haben wir die Funktionen und Fähigkeiten, nach denen uns unsere Kunden am häufigsten gefragt haben, rückwärts gearbeitet. Wir werden weiterhin zusätzliche MongoDB 5.0-Funktionen hinzufügen, je nachdem, was unsere Kunden von uns erwarten. Die aktuelle Liste der unterstützten APIs finden Sie unterUnterstützte MongoDB-APIs, Operationen und Datentypen in Amazon DocumentDB.

Was ist neu in Amazon DocumentDB 5.0.1

Amazon DocumentDB 5.0.1 ist die erste Nebenversion für die Amazon DocumentDB 5.0-Hauptversion. Nebenversionen enthalten Verbesserungen wie neue Funktionen,

Sicherheitskorrekturen und Fehlerkorrekturen. Sie können mit einem kleineren Versionsupgrade von 5.0.0 auf 5.0.1 aktualisieren. Weitere Informationen finden Sie unter Upgrade der Nebenversion von Amazon DocumentDB.

- Verbesserte Aggregationsfunktionen mit neuen Operatoren (`$rand`,,`$pow`,`$dateToParts`). `$dateFromParts`
- Metrik für aktive Verbindungen zur Überwachung von Instanzen. Die Beschränkungen finden Sie auf unserer Amazon DocumentDB-Seite Kontingente und Beschränkungen.
- Detaillierte Leistungskennzahlen auf Befehlsebene CloudWatch für CRUD-Operationen (`find`,,`insert`,,`findAndModify`,`update`,`delete`,`aggregate`,`count`,`commitTransaction`) `distinct` `getMore` `abortTransaction` `AvgDurationP100Duration`, Offenlegung und `MaxConcurrent` Dimensionen für eine verbesserte Betriebsüberwachung.
- Amazon DocumentDB 5.0.1 unterstützt nur TLS 1.2 und höher für Datenbankverbindungen.
- Es wurde eine `documentFragmentStats` Unterteilung der Messwerte auf Erfassungsebene in `storageSegmentBase` und `storageSegmentExtended` in hinzugefügt`gcRuntimeStats`, `collstats` um mehr Informationen über den allgemeinen Zustand des Garbage-Collection-Prozesses zu erhalten.
- Die regionsübergreifende Resilienz des globalen Clusters wurde verbessert, indem der sekundäre Cluster-Neustart mit Global Survivable Read Only überflüssig wurde.

Erste Schritte mit Amazon DocumentDB 5.0

Informationen zu den ersten Schritten mit Amazon DocumentDB 5.0 finden Sie im Handbuch Erste Schritte. Sie können einen neuen Amazon DocumentDB 5.0-Cluster mit dem AWS-Managementkonsole oder dem AWS SDK, AWS CLI, oder CloudFormation erstellen. Wenn Sie eine Verbindung zu Amazon DocumentDB herstellen, müssen Sie einen MongoDB-Treiber oder ein MongoDB-Tool verwenden, das mit MongoDB 5.0 oder höher kompatibel ist.

> **Note**
>
> Wenn Sie das AWS SDK oder CloudFormation verwenden AWS CLI, wird die Engine-Version standardmäßig auf 5.0.0 gesetzt. Sie müssen den Parameter explizit angeben`engineVersion = 4.0.0`, um einen neuen Amazon DocumentDB 4.0-Cluster oder einen neuen Amazon DocumentDB 3.6-Cluster `engineVersion = 3.6.0` zu erstellen. Für einen bestimmten Amazon DocumentDB-Cluster können Sie die Cluster-Version ermitteln, indem Sie AWS CLI den aufrufen `describe-db-clusters` oder die

Amazon DocumentDB-Managementkonsole verwenden, um die Engine-Versionsnummer für einen bestimmten Cluster anzuzeigen.

Amazon DocumentDB 5.0 und 8.0 unterstützt den Amazon EC2 `r8g` Graviton4-Prozessor und Graviton2-Prozessoren sowie `t4.medium` Instance-Typen für Ihre Cluster `r6g` und ist in allen unterstützten Regionen verfügbar (siehe). Instances Weitere Informationen zur Preisgestaltung finden Sie unter Amazon DocumentDB (mit MongoDB-Kompatibilität) — Preise.

Upgrade oder Migration auf Amazon DocumentDB 5.0

Sie können von MongoDB 3.6 oder MongoDB 4.0 zu Amazon DocumentDB 5.0 migrieren, indem Sie Dienstprogramme wie `mongodump`,`mongorestore`, `mongoimport` und verwenden. AWS DMS`mongoexport` Anweisungen zur Migration finden Sie unter. Aktualisieren Ihres Amazon DocumentDB-Clusters mit AWS Database Migration Service

Funktionelle Unterschiede

Funktionale Unterschiede zwischen Amazon DocumentDB 4.0 und 5.0

Mit der Veröffentlichung von Amazon DocumentDB 5.0 gibt es funktionale Unterschiede zwischen Amazon DocumentDB 4.0 und Amazon DocumentDB 5.0:

- Die integrierte Backup-Rolle unterstützt jetzt. `serverStatus` Aktion — Entwickler und Anwendungen mit Backup-Rolle können Statistiken über den Status des Amazon DocumentDB-Clusters sammeln.
- Das `SecondaryDelaySecs` Feld ersetzt `slaveDelay` in der `replSetGetConfig` Ausgabe.
- Der hello Befehl ersetzt `isMaster` — hello gibt ein Dokument zurück, das die Rolle eines Amazon DocumentDB-Clusters beschreibt.
- Amazon DocumentDB 5.0 unterstützt jetzt Indexscans mit dem `$elemMatch` Operator in der ersten Verschachtelungsebene. Indexscans werden unterstützt, wenn der Filter „Nur Abfrage“ eine Filterebene hat, aber nicht unterstützt, wenn eine verschachtelte `$elemMatch` Abfrage enthalten ist. `$elemMatch`

  Wenn Sie beispielsweise in Amazon DocumentDB 5.0 den `$elemMatch` Operator in die verschachtelte Ebene aufnehmen, gibt er keinen Wert zurück, wie dies in Amazon DocumentDB 4.0 der Fall ist:

```
db.foo.insert(
[
    {a: {b: 5}},
    {a: {b: [5]}},
    {a: {b: [3, 7]}},
    {a: [{b: 5}]},
    {a: [{b: 3}, {b: 7}]},
    {a: [{b: [5]}]},
    {a: [{b: [3, 7]}]},
    {a: [[{b: 5}]]},
    {a: [[{b: 3}, {b: 7}]]},
    {a: [[{b: [5]}]]},
    {a: [[{b: [3, 7]}]]}
]);

// DocumentDB 5.0
> db.foo.find({a: {$elemMatch: {b: {$elemMatch: {$lt: 6, $gt: 4}}}}}, {_id: 0})
{ "a" : [ { "b" : [ 5 ] } ] }

// DocumentDB 4.0
> db.foo.find({a: {$elemMatch: {b: {$elemMatch: {$lt: 6, $gt: 4}}}}}, {_id: 0})
{ "a" : [ { "b" : [ 5 ] } ] }
{ "a" : [ [ { "b" : [ 5 ] } ] ] }
```

- Die Projektion „$“ in Amazon DocumentDB 4.0 gibt alle Dokumente mit allen Feldern zurück. Bei Amazon DocumentDB 5.0 gibt der find Befehl mit einer „$“ -Projektion Dokumente zurück, die dem Abfrageparameter entsprechen und nur das Feld enthalten, das der Projektion „$“ entspricht.
- In Amazon DocumentDB 5.0 geben die find Befehle mit `$regex` und `$options` Abfrageparametern einen Fehler zurück: „Optionen können nicht in beiden `$regex` und festgelegt werden`$options`“.
- In Amazon DocumentDB 5.0 wird `$indexOfCP` jetzt „-1" zurückgegeben, wenn:
  - die Teilzeichenfolge wurde im Zeichenkettenausdruck nicht gefunden, oder
  - Start ist eine Zahl größer als Ende, oder
  - start ist eine Zahl, die größer als die Bytelänge der Zeichenfolge ist.
- Gibt in Amazon DocumentDB 4.0 „0" `$indexOfCP` zurück, wenn die Startposition eine Zahl ist, die größer als das Ende oder die Bytelänge der Zeichenfolge ist.
- Mit Amazon DocumentDB 5.0 geben `_id fields` Projektionsoperationen beispielsweise Dokumente zurück`{"_id.nestedField" : 1}`, die nur das projizierte Feld enthalten. In

Amazon DocumentDB 4.0 hingegen filtern Befehle zur verschachtelten Feldprojektion kein Dokument heraus.

MongoDB 4.0-Kompatibilität

Themen

- Funktionen von Amazon DocumentDB 4.0
- Erste Schritte mit Amazon DocumentDB 4.0
- Upgrade oder Migration zu Amazon DocumentDB 4.0
- Funktionelle Unterschiede

Funktionen von Amazon DocumentDB 4.0

Amazon DocumentDB 4.0 führte viele neue Funktionen und Fähigkeiten ein, darunter ACID-Transaktionen und Verbesserungen bei Change-Streams. Die folgende Zusammenfassung zeigt einige der wichtigsten Funktionen, die in Amazon DocumentDB 4.0 eingeführt wurden. Eine vollständige Liste der Funktionen finden Sie unterVersionshinweise.

- ACID-Transaktionen: Amazon DocumentDB unterstützt jetzt die Möglichkeit, Transaktionen über mehrere Dokumente, Kontoauszüge, Sammlungen und Datenbanken hinweg durchzuführen. Transaktionen vereinfachen die Anwendungsentwicklung, indem sie es Ihnen ermöglichen, atomare, konsistente, isolierte und dauerhafte Operationen (ACID) für ein oder mehrere Dokumente innerhalb eines Amazon DocumentDB-Clusters durchzuführen. Weitere Informationen finden Sie unter Transaktionen in Amazon DocumentDB.
- Streams ändern: Sie haben jetzt die Möglichkeit, einen Change-Stream auf Cluster-Ebene (`client.watch()`odermongo.watch()) und in der Datenbank (`db.watch()`) zu öffnen, Sie können einen Cursor angeben, `startAtOperationTime` um einen Change-Stream zu öffnen, und schließlich können Sie Ihren Change-Stream-Aufbewahrungszeitraum jetzt auf 7 Tage (zuvor 24 Stunden) verlängern. Weitere Informationen finden Sie unter Change-Streams mit Amazon DocumentDB verwenden.
- AWS Database Migration Service(AWS DMS): Sie können jetzt Ihre MongoDB 4.0-Workloads AWS DMS zu Amazon DocumentDB migrieren. AWS DMS unterstützt jetzt eine MongoDB 4.0-Quelle, ein Amazon DocumentDB 4.0-Ziel und eine Amazon DocumentDB 3.6-Quelle für die Durchführung von Upgrades zwischen Amazon DocumentDB 3.6 und 4.0. Weitere Informationen finden Sie in der AWS DMS Dokumentation.

- Leistung und Indizierung: Sie können jetzt einen Index verwenden`$lookup`, Abfragen mit einer Projektion suchen, die ein Feld oder ein Feld enthalten, und das `_id` Feld kann direkt aus dem Index bereitgestellt werden, ohne dass aus der Sammlung gelesen werden muss (abgedeckte Abfrage), die Möglichkeit`findAndModify`, `hint()` mit, Leistungsoptimierungen für `$addToSet` und Verbesserungen zur Reduzierung der Gesamtindexgröße. Weitere Informationen finden Sie unter Versionshinweise.
- Operatoren: Amazon DocumentDB 4.0 unterstützt jetzt eine Reihe neuer Aggregationsoperatoren:`$ifNull`,,`$replaceRoot`,, `$setIsSubset``$setIntersection`,`$setUnion`. `$setEquals` Alle MongoDB-APIs, -Operationen und -Datentypen, die wir unterstützen, finden Sie unterUnterstützte MongoDB-APIs, Operationen und Datentypen in Amazon DocumentDB.
- Rollenbasierte Zugriffskontrolle (RBAC): Bei `ListDatabase` Befehlen sowohl als auch `ListCollection` können Sie jetzt optional die `authorizedDatabases` Parameter `authorizedCollections` und verwenden, damit Benutzer die Sammlungen und Datenbanken auflisten können, auf die sie zugreifen dürfen, ohne dass die `listCollections` `listDatabase` Rollen bzw. Sie haben auch die Möglichkeit, Ihre eigenen Cursor zu beenden, ohne die Rolle zu benötigen. `KillCursor`

Amazon DocumentDB unterstützt nicht alle MongoDB 4.0-Funktionen. Bei der Entwicklung von Amazon DocumentDB 4.0 haben wir die Funktionen und Fähigkeiten, nach denen unsere Kunden uns am häufigsten gefragt haben, rückwärts gearbeitet. Wir werden weiterhin zusätzliche MongoDB 4.0-Funktionen hinzufügen, je nachdem, was unsere Kunden von uns erwarten. Beispielsweise unterstützt Amazon DocumentDB 4.0 derzeit nicht die Typkonvertierungsoperatoren oder Zeichenkettenoperatoren, die in MongoDB 4.0 eingeführt wurden. Die aktuelle Liste der unterstützten APIs finden Sie unter. Unterstützte MongoDB-APIs, Operationen und Datentypen in Amazon DocumentDB

Erste Schritte mit Amazon DocumentDB 4.0

Informationen zu den ersten Schritten mit Amazon DocumentDB 4.0 finden Sie im Handbuch Erste Schritte. Sie können einen neuen Amazon DocumentDB 4.0-Cluster mit dem AWS-Managementkonsole oder dem AWS SDK, AWS CLI, oder CloudFormation erstellen. Wenn Sie eine Verbindung zu Amazon DocumentDB herstellen, müssen Sie einen MongoDB-Treiber oder ein MongoDB-Tool verwenden, das mit MongoDB 4.0 oder höher kompatibel ist.

> **Note**
>
> Wenn Sie das AWS SDK oder CloudFormation verwenden AWS CLI, wird die Engine-Version standardmäßig auf 5.0.0 gesetzt. Sie müssen den Parameter explizit angeben`engineVersion = 4.0.0`, um einen neuen Amazon DocumentDB 4.0-Cluster oder einen neuen Amazon DocumentDB 3.6-Cluster `engineVersion = 3.6.0` zu erstellen. Für einen bestimmten Amazon DocumentDB-Cluster können Sie die Cluster-Version ermitteln, indem Sie AWS CLI den aufrufen `describe-db-clusters` oder die Amazon DocumentDB-Managementkonsole verwenden, um die Engine-Versionsnummer für einen bestimmten Cluster anzuzeigen.

Amazon DocumentDB 4.0 unterstützt `r5r6g`,`t3.medium`, und `t4g.medium` Instance-Typen für Ihre Cluster und ist in allen unterstützten Regionen verfügbar. Für die Nutzung von Amazon DocumentDB 4.0 fallen keine zusätzlichen Kosten an. Weitere Informationen zur Preisgestaltung finden Sie unter Amazon DocumentDB (mit MongoDB-Kompatibilität) — Preise.

Upgrade oder Migration zu Amazon DocumentDB 4.0

Sie können von MongoDB 3.6 oder MongoDB 4.0 zu Amazon DocumentDB 4.0 migrieren, indem Sie Dienstprogramme wie `mongodump`,`mongorestore`, `mongoimport` und verwenden. AWS DMS`mongoexport` Ebenso können Sie dieselben Tools für ein Upgrade von Amazon DocumentDB 3.6 auf Amazon DocumentDB 4.0 verwenden. Anweisungen zur Migration finden Sie unter. Aktualisieren Ihres Amazon DocumentDB-Clusters mit AWS Database Migration Service

Funktionelle Unterschiede

Funktionale Unterschiede zwischen Amazon DocumentDB 3.6 und 4.0

Mit der Veröffentlichung von Amazon DocumentDB 4.0 gibt es funktionale Unterschiede zwischen Amazon DocumentDB 3.6 und Amazon DocumentDB 4.0:

- Projektion für verschachtelte Dokumente: Amazon DocumentDB 3.6 berücksichtigt bei der Anwendung einer Projektion das erste Feld in einem verschachtelten Dokument. Amazon DocumentDB 4.0 analysiert jedoch Unterdokumente und wendet die Projektion auch auf jedes Unterdokument an. Beispiel: Wenn die Projektion ist`"a.b.c": 1`, dann ist das Verhalten in beiden Versionen identisch. Wenn die Projektion jedoch `{a:{b:{c:1}}}` so ist, wendet Amazon DocumentDB 3.6 die Projektion nur auf 'a' und nicht auf 'b' oder 'c' an.

- Verhalten für**`minKey`**, **`maxKey`**: In Amazon DocumentDB 4.0 `{x:{$gt:MaxKey}}` gibt das Verhalten für nichts und für alles `{x:{$lt:MaxKey}}` zurück.
- Unterschiede beim Dokumentenvergleich: Der Vergleich von numerischen Werten verschiedener Typen (Double, Int, Long) in Unterdokumenten (z. B. b in`{"_id" :1, "a" :{"b":1}}`) bietet jetzt eine konsistente Ausgabe für alle numerischen Datentypen und für jede Ebene eines Dokuments.

Funktionale Unterschiede zwischen Amazon DocumentDB 4.0 und MongoDB 4.0

Im Folgenden sind die funktionalen Unterschiede zwischen Amazon DocumentDB 4.0 und MongoDB 4.0 aufgeführt.

- Suche mit leerem Schlüssel im Pfad: Wenn eine Sammlung ein Dokument mit leerem Schlüssel innerhalb des Arrays enthält (z. B.`{"x" : [ { "" : 10 }, { "b" : 20 } ]}`) und wenn der in der Abfrage verwendete Schlüssel mit einer leeren Zeichenfolge endet (z. B.`x.`), gibt Amazon DocumentDB dieses Dokument zurück, da es alle Dokumente im Array durchläuft, während MongoDB dieses Dokument nicht zurückgibt.
- **`$setOnInsert`**zusammen mit **`$`** im Pfad: Der Feldoperator `$setOnInsert` funktioniert nicht in Kombination mit $ im Pfad in Amazon DocumentDB, was auch mit MongoDB 4.0 konsistent ist.

Transaktionen in Amazon DocumentDB

Amazon DocumentDB (mit MongoDB-Kompatibilität) unterstützt Transaktionen in Amazon DocumentDB 4.0 und höher. Sie können Transaktionen für mehrere Dokumente, Kontoauszüge, Sammlungen und Datenbanken durchführen. Transaktionen vereinfachen die Anwendungsentwicklung, indem sie es Ihnen ermöglichen, atomare, konsistente, isolierte und dauerhafte Operationen (ACID) für ein oder mehrere Dokumente innerhalb eines Amazon DocumentDB-Clusters durchzuführen. Zu den häufigsten Anwendungsfällen für Transaktionen gehören die Finanzabwicklung, die Ausführung und Verwaltung von Bestellungen sowie die Entwicklung von Spielen für mehrere Spieler.

Für Transaktionen fallen keine zusätzlichen Kosten an. Sie zahlen nur für die IOs mit Lese- und Schreibzugriff, die Sie im Rahmen der Transaktionen nutzen.

Themen

- Voraussetzungen
- Best Practices
- Einschränkungen
- Überwachung und Diagnose
- Isolationsstufe für Transaktionen
- Anwendungsfälle
- Unterstützte Befehle
- Nicht unterstützte Funktionen
- Sitzungen
- Transaktionsfehler

Voraussetzungen

Um die Transaktionsfunktion nutzen zu können, müssen Sie die folgenden Anforderungen erfüllen:

- Sie müssen Amazon DocumentDB 4.0 oder höher verwenden.
- Sie müssen einen Treiber verwenden, der mit MongoDB 4.0 oder höher kompatibel ist.

Best Practices

Im Folgenden finden Sie einige bewährte Methoden, damit Sie Transaktionen mit Amazon DocumentDB optimal nutzen können.

- Bestätigen oder brechen Sie die Transaktion immer ab, nachdem sie abgeschlossen ist. Wenn eine Transaktion in einem unvollständigen Zustand belassen wird, werden Datenbankressourcen gebunden und es kann zu Schreibkonflikten kommen.
- Es wird empfohlen, Transaktionen auf die geringstmögliche Anzahl von Befehlen zu beschränken. Wenn Sie Transaktionen mit mehreren Kontoauszügen haben, die in mehrere kleinere Transaktionen aufgeteilt werden können, ist es ratsam, dies zu tun, um die Wahrscheinlichkeit eines Timeouts zu verringern. Versuchen Sie immer, kurze Transaktionen und keine lang andauernden Lesevorgänge zu erstellen.

Einschränkungen

- Amazon DocumentDB unterstützt keine Cursor innerhalb einer Transaktion.
- Amazon DocumentDB kann keine neuen Sammlungen in einer Transaktion erstellen und kann auch nicht für nicht existierende query/update Sammlungen verwendet werden.
- Document-level Für Schreibsperren gilt ein Timeout von 1 Minute, das vom Benutzer nicht konfiguriert werden kann.
- Befehle für wiederholbare Schreibvorgänge, wiederholbares Festschreiben und wiederholbares Abbrechen werden in Amazon DocumentDB nicht unterstützt. Wenn Sie eine ältere Mongo-Shell (nicht Mongosh) verwenden, nehmen Sie den Befehl nicht in eine Codezeichenfolge auf. `retryWrites=false` Standardmäßig sind wiederholbare Schreibvorgänge deaktiviert. `retryWrites=false`Das Einschließen kann zu einem Fehler bei normalen Lesebefehlen führen.
- Jede Amazon DocumentDB DocumentDB-Instance hat eine Obergrenze für die Anzahl gleichzeitiger Transaktionen, die gleichzeitig auf der Instance geöffnet sind. Die Grenzwerte finden Sie unter. Instance-Limits
- Für eine bestimmte Transaktion muss die Größe des Transaktionsprotokolls weniger als 32 MB betragen.
- Amazon DocumentDB unterstützt zwar Transaktionen `count()` innerhalb einer Transaktion, aber nicht alle Treiber unterstützen diese Funktion. Eine Alternative ist die Verwendung der `countDocuments()` API, die die Zählabfrage in eine Aggregationsabfrage auf der Clientseite übersetzt.

- Transaktionen haben ein Ausführungslimit von einer Minute und Sitzungen haben ein 30-minütiges Timeout. Wenn bei einer Transaktion das Timeout überschritten wird, wird sie abgebrochen, und alle nachfolgenden Befehle, die innerhalb der Sitzung für die bestehende Transaktion ausgegeben werden, führen zu dem folgenden Fehler:

```
WriteCommandError({
"ok" : 0,
"operationTime" : Timestamp(1603491424, 627726),
"code" : 251,
"errmsg" : "Given transaction number 0 does not match any in-progress transactions."
}
```

Überwachung und Diagnose

Mit der Unterstützung für Transaktionen in Amazon DocumentDB 4.0 wurden zusätzliche CloudWatch Metriken hinzugefügt, die Ihnen helfen, Ihre Transaktionen zu überwachen.

Neue Metriken CloudWatch

- `DatabaseTransactions`: Die Anzahl der offenen Transaktionen, die innerhalb eines Zeitraums von einer Minute getätigt wurden.
- `DatabaseTransactionsAborted`: Die Anzahl der abgebrochenen Transaktionen innerhalb einer Minute.
- `DatabaseTransactionsMax`: Die maximale Anzahl offener Transaktionen in einem Zeitraum von einer Minute.
- `TransactionsAborted`: Die Anzahl der Transaktionen, die auf einer Instance in einem Zeitraum von einer Minute abgebrochen wurden.
- `TransactionsCommitted`: Die Anzahl der Transaktionen, die innerhalb einer Minute auf einer Instance festgeschrieben wurden.
- `TransactionsOpen`: Die Anzahl der offenen Transaktionen auf einer Instance, die innerhalb eines Zeitraums von einer Minute ausgeführt wurden.
- `TransactionsOpenMax`: Die maximale Anzahl von Transaktionen, die innerhalb einer Minute auf einer Instance geöffnet werden.
- `TransactionsStarted`: Die Anzahl der Transaktionen, die innerhalb einer Minute auf einer Instance gestartet wurden.

> **Note**
>
> Weitere CloudWatch Metriken für Amazon DocumentDB finden Sie Überwachen von Amazon DocumentDB mit CloudWatch unter.

Darüber hinaus wurden neue Felder zu `currentOp` `lsidtransactionThreadId`, und ein neuer Status für „`idle transaction`“ und `serverStatus` Transaktionen hinzugefügt:`currentActive`,`currentInactive`,`currentOpen`, `totalAbortedtotalCommitted`, und`totalStarted`.

Isolationsstufe für Transaktionen

Wenn Sie eine Transaktion starten, können Sie sowohl als auch angeben, `writeConcern` wie im folgenden Beispiel gezeigt: `readConcern`

```
mySession.startTransaction({readConcern: {level: 'snapshot'}, writeConcern:
{w: 'majority'}});
```

Denn `readConcern` Amazon DocumentDB unterstützt standardmäßig die Snapshot-Isolierung. Wenn „Lokal“, „Verfügbar“ oder „Mehrheit“ angegeben ist, führt Amazon DocumentDB ein Upgrade der `readConcern` Stufe auf Snapshot durch. `readConcern` Amazon DocumentDB unterstützt das Linearisierbare nicht `readConcern` und die Angabe eines solchen Leseproblems führt zu einem Fehler.

Denn Amazon DocumentDB unterstützt standardmäßig die Mehrheit`writeConcern`, und ein Schreibquorum wird erreicht, wenn vier Kopien der Daten auf drei AZs persistent gespeichert werden. Wenn ein niedrigerer Wert angegeben `writeConcern` wird, führt Amazon DocumentDB ein Upgrade `writeConcern` auf die Mehrheit durch. Darüber hinaus werden alle Amazon DocumentDB DocumentDB-Schreibvorgänge protokolliert und das Journaling kann nicht deaktiviert werden.

Anwendungsfälle

In diesem Abschnitt werden wir uns mit zwei Anwendungsfällen für Transaktionen befassen: Multi-Statement und Multi-Collection.

Multi-Statement Transaktionen

Amazon DocumentDB-Transaktionen bestehen aus mehreren Anweisungen, was bedeutet, dass Sie eine Transaktion schreiben können, die sich über mehrere Anweisungen mit einem expliziten Commit oder Rollback erstreckt. Sie können `findAndModify` Aktionen`insert`, `update``delete`, und als eine einzige atomare Operation gruppieren.

Ein häufiger Anwendungsfall für Transaktionen mit mehreren Kontoauszügen ist eine Debit-/Kredittransaktion. Zum Beispiel: Sie schulden einem Freund Geld für Kleidung. Sie müssen also 500 USD von Ihrem Konto abbuchen (abheben) und dem Konto Ihres Freundes 500 USD (Einzahlung) gutschreiben. Um diesen Vorgang durchzuführen, führen Sie sowohl den Debit- als auch den Kreditvorgang innerhalb einer einzigen Transaktion durch, um die Atomarität sicherzustellen. Dadurch werden Szenarien vermieden, in denen 500$ von Ihrem Konto abgebucht, aber nicht dem Konto Ihres Freundes gutgeschrieben werden. So würde dieser Anwendungsfall aussehen:

```
// *** Transfer $500 from Alice to Bob inside a transaction: Success Scenario***
// Setup bank account for Alice and Bob. Each have $1000 in their account

var databaseName = "bank";
var collectionName = "account";
var amountToTransfer = 500;

var session = db.getMongo().startSession({causalConsistency: false});
var bankDB = session.getDatabase(databaseName);
var accountColl = bankDB[collectionName];
accountColl.drop();

accountColl.insert({name: "Alice", balance: 1000});
accountColl.insert({name: "Bob", balance: 1000});

session.startTransaction();

// deduct $500 from Alice's account
var aliceBalance = accountColl.find({"name": "Alice"}).next().balance;
var newAliceBalance = aliceBalance - amountToTransfer;
accountColl.update({"name": "Alice"},{"$set": {"balance": newAliceBalance}});
var findAliceBalance = accountColl.find({"name": "Alice"}).next().balance;

// add $500 to Bob's account
var bobBalance = accountColl.find({"name": "Bob"}).next().balance;
var newBobBalance = bobBalance + amountToTransfer;
```

```
accountColl.update({"name": "Bob"},{"$set": {"balance": newBobBalance}});
var findBobBalance = accountColl.find({"name": "Bob"}).next().balance;

session.commitTransaction();

accountColl.find();

// *** Transfer $500 from Alice to Bob inside a transaction: Failure Scenario***

// Setup bank account for Alice and Bob. Each have $1000 in their account
var databaseName = "bank";
var collectionName = "account";
var amountToTransfer = 500;

var session = db.getMongo().startSession({causalConsistency: false});
var bankDB = session.getDatabase(databaseName);
var accountColl = bankDB[collectionName];
accountColl.drop();

accountColl.insert({name: "Alice", balance: 1000});
accountColl.insert({name: "Bob", balance: 1000});

session.startTransaction();

// deduct $500 from Alice's account
var aliceBalance = accountColl.find({"name": "Alice"}).next().balance;
var newAliceBalance = aliceBalance - amountToTransfer;
accountColl.update({"name": "Alice"},{"$set": {"balance": newAliceBalance}});
var findAliceBalance = accountColl.find({"name": "Alice"}).next().balance;

session.abortTransaction();
```

Multi-collection Transaktionen

Bei unseren Transaktionen handelt es sich auch um Sammeltransaktionen, was bedeutet, dass sie verwendet werden können, um mehrere Operationen innerhalb einer einzigen Transaktion und über mehrere Sammlungen hinweg durchzuführen. Dies ermöglicht eine konsistente Ansicht der Daten und gewährleistet die Integrität Ihrer Daten. Wenn Sie die Befehle einzeln übergeben<>, handelt es sich bei den Transaktionen um Alles-oder-Nichts-Ausführungen. Sie werden entweder alle erfolgreich ausgeführt oder alle schlagen fehl.

Hier ist ein Beispiel für Transaktionen mit mehreren Sammlungen, wobei dasselbe Szenario und die Daten aus dem Beispiel für Transaktionen mit mehreren Kontoauszügen verwendet werden.

```
// *** Transfer $500 from Alice to Bob inside a transaction: Success Scenario***

// Setup bank account for Alice and Bob. Each have $1000 in their account
var amountToTransfer = 500;
var collectionName = "account";

var session = db.getMongo().startSession({causalConsistency: false});
var accountCollInBankA = session.getDatabase("bankA")[collectionName];
var accountCollInBankB = session.getDatabase("bankB")[collectionName];

accountCollInBankA.drop();
accountCollInBankB.drop();

accountCollInBankA.insert({name: "Alice", balance: 1000});
accountCollInBankB.insert({name: "Bob", balance: 1000});

session.startTransaction();

// deduct $500 from Alice's account
var aliceBalance = accountCollInBankA.find({"name": "Alice"}).next().balance;
var newAliceBalance = aliceBalance - amountToTransfer;
accountCollInBankA.update({"name": "Alice"},{"$set": {"balance": newAliceBalance}});
var findAliceBalance = accountCollInBankA.find({"name": "Alice"}).next().balance;

// add $500 to Bob's account
var bobBalance = accountCollInBankB.find({"name": "Bob"}).next().balance;
var newBobBalance = bobBalance + amountToTransfer;
accountCollInBankB.update({"name": "Bob"},{"$set": {"balance": newBobBalance}});
var findBobBalance = accountCollInBankB.find({"name": "Bob"}).next().balance;

session.commitTransaction();

accountCollInBankA.find(); // Alice holds $500 in bankA
accountCollInBankB.find(); // Bob holds $1500 in bankB

// *** Transfer $500 from Alice to Bob inside a transaction: Failure Scenario***

// Setup bank account for Alice and Bob. Each have $1000 in their account
var collectionName = "account";
```

```
var amountToTransfer = 500;

var session = db.getMongo().startSession({causalConsistency: false});
var accountCollInBankA = session.getDatabase("bankA")[collectionName];
var accountCollInBankB = session.getDatabase("bankB")[collectionName];

accountCollInBankA.drop();
accountCollInBankB.drop();

accountCollInBankA.insert({name: "Alice", balance: 1000});
accountCollInBankB.insert({name: "Bob", balance: 1000});

session.startTransaction();

// deduct $500 from Alice's account
var aliceBalance = accountCollInBankA.find({"name": "Alice"}).next().balance;
var newAliceBalance = aliceBalance - amountToTransfer;
accountCollInBankA.update({"name": "Alice"},{"$set": {"balance": newAliceBalance}});
var findAliceBalance = accountCollInBankA.find({"name": "Alice"}).next().balance;

// add $500 to Bob's account
var bobBalance = accountCollInBankB.find({"name": "Bob"}).next().balance;
var newBobBalance = bobBalance + amountToTransfer;
accountCollInBankB.update({"name": "Bob"},{"$set": {"balance": newBobBalance}});
var findBobBalance = accountCollInBankB.find({"name": "Bob"}).next().balance;

session.abortTransaction();

accountCollInBankA.find(); // Alice holds $1000 in bankA
accountCollInBankB.find(); // Bob holds $1000 in bankB
```

Beispiele für Transaktions-APIs für die Callback-API

Die Callback-API ist nur für Treiber ab Version 4.2 verfügbar.

Javascript

Der folgende Code zeigt, wie die Amazon DocumentDB-Transaktions-API mit Javascript verwendet wird.

```
// *** Transfer $500 from Alice to Bob inside a transaction: Success ***
// Setup bank account for Alice and Bob. Each have $1000 in their account
```

```
var databaseName = "bank";
var collectionName = "account";
var amountToTransfer = 500;

var session = db.getMongo().startSession({causalConsistency: false});
var bankDB = session.getDatabase(databaseName);
var accountColl = bankDB[collectionName];
accountColl.drop();

accountColl.insert({name: "Alice", balance: 1000});
accountColl.insert({name: "Bob", balance: 1000});

session.startTransaction();

// deduct $500 from Alice's account
var aliceBalance = accountColl.find({"name": "Alice"}).next().balance;
assert(aliceBalance >= amountToTransfer);
var newAliceBalance = aliceBalance - amountToTransfer;
accountColl.update({"name": "Alice"},{"$set": {"balance": newAliceBalance}});
var findAliceBalance = accountColl.find({"name": "Alice"}).next().balance;
assert.eq(newAliceBalance, findAliceBalance);

// add $500 to Bob's account
var bobBalance = accountColl.find({"name": "Bob"}).next().balance;
var newBobBalance = bobBalance + amountToTransfer;
accountColl.update({"name": "Bob"},{"$set": {"balance": newBobBalance}});
var findBobBalance = accountColl.find({"name": "Bob"}).next().balance;
assert.eq(newBobBalance, findBobBalance);

session.commitTransaction();

accountColl.find();
```

Node.js

Der folgende Code zeigt, wie Sie die Amazon DocumentDB-Transaktions-API mit Node.js verwenden.

```
// Node.js callback API:

const bankDB = await mongoclient.db("bank");
var accountColl = await bankDB.createCollection("account");
var amountToTransfer = 500;
```

```
const session = mongoclient.startSession({causalConsistency: false});
await accountColl.drop();

await accountColl.insertOne({name: "Alice", balance: 1000}, { session });
await accountColl.insertOne({name: "Bob", balance: 1000}, { session });

const transactionOptions = {
    readConcern: { level: 'snapshot' },
    writeConcern: { w: 'majority' }
    };

// deduct $500 from Alice's account
var aliceBalance = await accountColl.findOne({name: "Alice"}, {session});
assert(aliceBalance.balance >= amountToTransfer);
var newAliceBalance = aliceBalance - amountToTransfer;
session.startTransaction(transactionOptions);
await accountColl.updateOne({name: "Alice"}, {$set: {balance: newAliceBalance}},
 {session });
await session.commitTransaction();
aliceBalance = await accountColl.findOne({name: "Alice"}, {session});
assert(newAliceBalance == aliceBalance.balance);

// add $500 to Bob's account
var bobBalance = await accountColl.findOne({name: "Bob"}, {session});
var newBobBalance = bobBalance.balance + amountToTransfer;
session.startTransaction(transactionOptions);
await accountColl.updateOne({name: "Bob"}, {$set: {balance: newBobBalance}},
 {session });
await session.commitTransaction();
bobBalance = await accountColl.findOne({name: "Bob"}, {session});
assert(newBobBalance == bobBalance.balance);
```

C#

Der folgende Code zeigt, wie die Amazon DocumentDB-Transaktions-API mit C# verwendet wird.

```
// C# Callback API

var dbName = "bank";
var collName = "account";
var amountToTransfer = 500;
```

```
using (var session = client.StartSession(new ClientSessionOptions{CausalConsistency
 = false}))
{
    var bankDB = client.GetDatabase(dbName);
    var accountColl = bankDB.GetCollection<BsonDocument>(collName);
    bankDB.DropCollection(collName);
    accountColl.InsertOne(session, new BsonDocument { {"name", "Alice"}, {"balance",
 1000 } });
    accountColl.InsertOne(session, new BsonDocument { {"name", "Bob"}, {"balance",
 1000 } });

    // start transaction
    var transactionOptions = new TransactionOptions(
            readConcern: ReadConcern.Snapshot,
            writeConcern: WriteConcern.WMajority);
    var result = session.WithTransaction(
        (sess, cancellationtoken) =>
        {
            // deduct $500 from Alice's account
            var aliceBalance = accountColl.Find(sess,
 Builders<BsonDocument>.Filter.Eq("name",
 "Alice")).FirstOrDefault().GetValue("balance");
            Debug.Assert(aliceBalance >= amountToTransfer);
            var newAliceBalance = aliceBalance.AsInt32 - amountToTransfer;
            accountColl.UpdateOne(sess, Builders<BsonDocument>.Filter.Eq("name",
 "Alice"),
                                    Builders<BsonDocument>.Update.Set("balance",
 newAliceBalance));
            aliceBalance = accountColl.Find(sess,
 Builders<BsonDocument>.Filter.Eq("name",
 "Alice")).FirstOrDefault().GetValue("balance");
            Debug.Assert(aliceBalance == newAliceBalance);

            // add $500 from Bob's account
            var bobBalance = accountColl.Find(sess,
 Builders<BsonDocument>.Filter.Eq("name",
 "Bob")).FirstOrDefault().GetValue("balance");
            var newBobBalance = bobBalance.AsInt32 + amountToTransfer;
            accountColl.UpdateOne(sess, Builders<BsonDocument>.Filter.Eq("name",
 "Bob"),
                                    Builders<BsonDocument>.Update.Set("balance",
 newBobBalance));
```

```
            bobBalance = accountColl.Find(sess,
 Builders<BsonDocument>.Filter.Eq("name",
 "Bob")).FirstOrDefault().GetValue("balance");
            Debug.Assert(bobBalance == newBobBalance);

            return "Transaction committed";
        }, transactionOptions);
   // check values outside of transaction
    var aliceNewBalance = accountColl.Find(Builders<BsonDocument>.Filter.Eq("name",
 "Alice")).FirstOrDefault().GetValue("balance");
    var bobNewBalance = accountColl.Find(Builders<BsonDocument>.Filter.Eq("name",
 "Bob")).FirstOrDefault().GetValue("balance");
    Debug.Assert(aliceNewBalance ==  500);
    Debug.Assert(bobNewBalance ==  1500);
}
```

Ruby

Der folgende Code zeigt, wie die Amazon DocumentDB-Transaktions-API mit Ruby verwendet wird.

```
// Ruby Callback API

dbName = "bank"
collName = "account"
amountToTransfer = 500

session = client.start_session(:causal_consistency=> false)
bankDB = Mongo::Database.new(client, dbName)
accountColl = bankDB[collName]
accountColl.drop()

accountColl.insert_one({"name"=>"Alice", "balance"=>1000})
accountColl.insert_one({"name"=>"Bob", "balance"=>1000})

    # start transaction
    session.with_transaction(read_concern: {level: :snapshot}, write_concern:
 {w: :majority}) do
        # deduct $500 from Alice's account
        aliceBalance = accountColl.find({"name"=>"Alice"}, :session=>
 session).first['balance']
        assert aliceBalance >= amountToTransfer
        newAliceBalance = aliceBalance - amountToTransfer
```

```
        accountColl.update_one({"name"=>"Alice"}, { "$set" =>
 {"balance"=>newAliceBalance} }, :session=> session)
        aliceBalance = accountColl.find({"name"=>>"Alice"}, :session=>
 session).first['balance']
        assert_equal(newAliceBalance, aliceBalance)

        # add $500 from Bob's account
        bobBalance = accountColl.find({"name"=>"Bob"}, :session=>
 session).first['balance']
        newBobBalance = bobBalance + amountToTransfer
        accountColl.update_one({"name"=>"Bob"}, { "$set" =>
 {"balance"=>newBobBalance} }, :session=> session)
        bobBalance = accountColl.find({"name"=>"Bob"}, :session=>
 session).first['balance']
        assert_equal(newBobBalance, bobBalance)
    end

   # check results outside of transaction
    aliceBalance = accountColl.find({"name"=>"Alice"}).first['balance']
    bobBalance = accountColl.find({"name"=>"Bob"}).first['balance']
    assert_equal(aliceBalance, 500)
    assert_equal(bobBalance, 1500)

session.end_session
```

Go

Der folgende Code zeigt, wie Sie die Amazon DocumentDB-Transaktions-API mit Go verwenden.

```
// Go - Callback API
type Account struct {
    Name string
    Balance  int
}

ctx := context.TODO()

dbName := "bank"
collName := "account"
amountToTransfer := 500

session, err := client.StartSession(options.Session().SetCausalConsistency(false))
assert.NilError(t, err)
defer session.EndSession(ctx)
```

```
bankDB := client.Database(dbName)
accountColl := bankDB.Collection(collName)
accountColl.Drop(ctx)

_, err = accountColl.InsertOne(ctx, bson.M{"name" : "Alice", "balance":1000})
_, err = accountColl.InsertOne(ctx, bson.M{"name" : "Bob", "balance":1000})

transactionOptions := options.Transaction().SetReadConcern(readconcern.Snapshot()).

 SetWriteConcern(writeconcern.New(writeconcern.WMajority()))
_, err = session.WithTransaction(ctx, func(sessionCtx mongo.SessionContext)
 (interface{}, error) {
    var result Account
    // deduct $500 from Alice's account
    err = accountColl.FindOne(sessionCtx, bson.M{"name": "Alice"}).Decode(&result)
    aliceBalance := result.Balance
    newAliceBalance := aliceBalance - amountToTransfer
    _, err = accountColl.UpdateOne(sessionCtx, bson.M{"name": "Alice"},
 bson.M{"$set": bson.M{"balance": newAliceBalance}})
    err = accountColl.FindOne(sessionCtx, bson.M{"name": "Alice"}).Decode(&result)
    aliceBalance = result.Balance
    assert.Equal(t, aliceBalance, newAliceBalance)

    // add $500 to Bob's account
    err = accountColl.FindOne(sessionCtx, bson.M{"name": "Bob"}).Decode(&result)
    bobBalance := result.Balance
    newBobBalance := bobBalance + amountToTransfer
    _, err = accountColl.UpdateOne(sessionCtx, bson.M{"name": "Bob"}, bson.M{"$set":
 bson.M{"balance": newBobBalance}})
    err = accountColl.FindOne(sessionCtx, bson.M{"name": "Bob"}).Decode(&result)
    bobBalance = result.Balance
    assert.Equal(t, bobBalance, newBobBalance)

    if err != nil {
        return nil, err
    }
    return "transaction committed", err
}, transactionOptions)

// check results outside of transaction
var result Account
err = accountColl.FindOne(ctx, bson.M{"name": "Alice"}).Decode(&result)
aliceNewBalance := result.Balance
```

```
err = accountColl.FindOne(ctx, bson.M{"name": "Bob"}).Decode(&result)
bobNewBalance := result.Balance
assert.Equal(t, aliceNewBalance, 500)
assert.Equal(t, bobNewBalance, 1500)
```

Java

Der folgende Code zeigt, wie die Amazon DocumentDB-Transaktions-API mit Java verwendet wird.

```
// Java (sync) - Callback API
MongoDatabase bankDB = mongoClient.getDatabase("bank");
MongoCollection accountColl = bankDB.getCollection("account");
accountColl.drop();
int amountToTransfer = 500;

// add sample data
accountColl.insertOne(new Document("name", "Alice").append("balance", 1000));
accountColl.insertOne(new Document("name", "Bob").append("balance", 1000));

TransactionOptions txnOptions = TransactionOptions.builder()
        .readConcern(ReadConcern.SNAPSHOT)
        .writeConcern(WriteConcern.MAJORITY)
        .build();
ClientSessionOptions sessionOptions =
 ClientSessionOptions.builder().causallyConsistent(false).build();
try ( ClientSession clientSession = mongoClient.startSession(sessionOptions) ) {
    clientSession.withTransaction(new TransactionBody<Void>() {
        @Override
        public Void execute() {
            // deduct $500 from Alice's account
            List<Document> documentList = new ArrayList<>();
            accountColl.find(clientSession, new Document("name",
 "Alice")).into(documentList);
            int aliceBalance = (int) documentList.get(0).get("balance");
            int newAliceBalance = aliceBalance - amountToTransfer;

            accountColl.updateOne(clientSession, new Document("name", "Alice"), new
 Document("$set", new Document("balance", newAliceBalance)));

            // check Alice's new balance
            documentList = new ArrayList<>();
```

```
            accountColl.find(clientSession, new Document("name",
 "Alice")).into(documentList);
            int updatedBalance = (int) documentList.get(0).get("balance");
            Assert.assertEquals(updatedBalance, newAliceBalance);

            // add $500 to Bob's account
            documentList = new ArrayList<>();
            accountColl.find(clientSession, new Document("name",
 "Bob")).into(documentList);
            int bobBalance = (int) documentList.get(0).get("balance");
            int newBobBalance = bobBalance + amountToTransfer;

            accountColl.updateOne(clientSession, new Document("name", "Bob"), new
 Document("$set", new Document("balance", newBobBalance)));

            // check Bob's new balance
            documentList = new ArrayList<>();
            accountColl.find(clientSession, new Document("name",
 "Bob")).into(documentList);
            updatedBalance = (int) documentList.get(0).get("balance");
            Assert.assertEquals(updatedBalance, newBobBalance);

            return null;
        }
    }, txnOptions);
}
```

C

Der folgende Code zeigt, wie die Amazon DocumentDB-Transaktions-API mit C verwendet wird.

```
// Sample Code for C with Callback

#include <bson.h>
#include <mongoc.h>
#include <stdio.h>
#include <string.h>
#include <assert.h>

typedef struct {
    int64_t balance;
    bson_t *account;
    bson_t *opts;
    mongoc_collection_t *collection;
```

```
} ctx_t;

bool callback_session (mongoc_client_session_t *session, void *ctx, bson_t **reply,
 bson_error_t *error)
{
    bool r = true;
    ctx_t *data = (ctx_t *) ctx;
    bson_t local_reply;
    bson_t *selector = data->account;
    bson_t *update = BCON_NEW ("$set", "{", "balance", BCON_INT64 (data->balance),
 "}");

    mongoc_collection_update_one (data->collection, selector, update, data->opts,
 &local_reply, error);

    *reply = bson_copy (&local_reply);
    bson_destroy (&local_reply);
    bson_destroy (update);
    return r;
}

void test_callback_money_transfer(mongoc_client_t* client, mongoc_collection_t*
 collection, int amount_to_transfer){

    bson_t reply;
    bool r = true;
    const bson_t *doc;
    bson_iter_t iter;
    ctx_t alice_ctx;
    ctx_t bob_ctx;
    bson_error_t error;

    // find query
    bson_t *alice_query = bson_new ();
    BSON_APPEND_UTF8(alice_query, "name", "Alice");

    bson_t *bob_query = bson_new ();
    BSON_APPEND_UTF8(bob_query, "name", "Bob");

    // create session
    // set causal consistency to false
    mongoc_session_opt_t *session_opts = mongoc_session_opts_new ();
    mongoc_session_opts_set_causal_consistency (session_opts, false);
    // start the session
```

```
   mongoc_client_session_t *client_session = mongoc_client_start_session (client,
session_opts, &error);

   // add session to options
   bson_t *opts = bson_new();
   mongoc_client_session_append (client_session, opts, &error);

   // deduct 500 from Alice
   // find account balance of Alice
   mongoc_cursor_t *cursor = mongoc_collection_find_with_opts (collection,
alice_query, NULL, NULL);
   mongoc_cursor_next (cursor, &doc);
   bson_iter_init (&iter, doc);
   bson_iter_find (&iter, "balance");
   int64_t alice_balance = (bson_iter_value (&iter))->value.v_int64;
   assert(alice_balance >= amount_to_transfer);
   int64_t new_alice_balance = alice_balance - amount_to_transfer;

   // set variables which will be used by callback function
   alice_ctx.collection = collection;
   alice_ctx.opts = opts;
   alice_ctx.balance = new_alice_balance;
   alice_ctx.account = alice_query;

   // callback
   r = mongoc_client_session_with_transaction (client_session, &callback_session,
NULL, &alice_ctx, &reply, &error);
   assert(r);

   // find account balance of Alice after transaction
   cursor = mongoc_collection_find_with_opts (collection, alice_query, NULL, NULL);
   mongoc_cursor_next (cursor, &doc);
   bson_iter_init (&iter, doc);
   bson_iter_find (&iter, "balance");
   alice_balance = (bson_iter_value (&iter))->value.v_int64;
   assert(alice_balance == new_alice_balance);
   assert(alice_balance == 500);

       // add 500 to bob's balance
   // find account balance of Bob
   cursor = mongoc_collection_find_with_opts (collection, bob_query, NULL, NULL);
   mongoc_cursor_next (cursor, &doc);
   bson_iter_init (&iter, doc);
   bson_iter_find (&iter, "balance");
```

```
    int64_t bob_balance = (bson_iter_value (&iter))->value.v_int64;
    int64_t new_bob_balance = bob_balance + amount_to_transfer;

    bob_ctx.collection = collection;
    bob_ctx.opts = opts;
    bob_ctx.balance = new_bob_balance;
    bob_ctx.account = bob_query;

    // set read & write concern
    mongoc_read_concern_t *read_concern = mongoc_read_concern_new ();
    mongoc_write_concern_t *write_concern = mongoc_write_concern_new ();
    mongoc_transaction_opt_t *txn_opts = mongoc_transaction_opts_new ();

    mongoc_write_concern_set_w(write_concern, MONGOC_WRITE_CONCERN_W_MAJORITY);
    mongoc_read_concern_set_level(read_concern, MONGOC_READ_CONCERN_LEVEL_SNAPSHOT);
    mongoc_transaction_opts_set_write_concern (txn_opts, write_concern);
    mongoc_transaction_opts_set_read_concern (txn_opts, read_concern);

    // callback
    r = mongoc_client_session_with_transaction (client_session, &callback_session,
 txn_opts, &bob_ctx, &reply, &error);
    assert(r);

 // find account balance of Bob after transaction
    cursor = mongoc_collection_find_with_opts (collection, bob_query, NULL, NULL);
    mongoc_cursor_next (cursor, &doc);
    bson_iter_init (&iter, doc);
    bson_iter_find (&iter, "balance");
    bob_balance = (bson_iter_value (&iter))->value.v_int64;
    assert(bob_balance == new_bob_balance);
    assert(bob_balance == 1500);

    // cleanup
    bson_destroy(alice_query);
    bson_destroy(bob_query);
    mongoc_client_session_destroy(client_session);
    bson_destroy(opts);
    mongoc_transaction_opts_destroy(txn_opts);
    mongoc_read_concern_destroy(read_concern);
    mongoc_write_concern_destroy(write_concern);
    mongoc_cursor_destroy(cursor);
    bson_destroy(doc);
}
int main(int argc, char* argv[]) {
```

```
    mongoc_init ();
    mongoc_client_t* client = mongoc_client_new (<connection uri>);
    bson_error_t error;

    // connect to bank db
    mongoc_database_t *database = mongoc_client_get_database (client, "bank");
    // access account collection
    mongoc_collection_t* collection = mongoc_client_get_collection(client, "bank",
 "account");
    // set amount to transfer
    int64_t amount_to_transfer = 500;
    // delete the collection if already existing
    mongoc_collection_drop(collection, &error);

    // open Alice account
    bson_t *alice_account = bson_new ();
    BSON_APPEND_UTF8(alice_account, "name", "Alice");
    BSON_APPEND_INT64(alice_account, "balance", 1000);

    // open Bob account
    bson_t *bob_account = bson_new ();
    BSON_APPEND_UTF8(bob_account, "name", "Bob");
    BSON_APPEND_INT64(bob_account, "balance", 1000);

    bool r = true;

    r = mongoc_collection_insert_one(collection, alice_account, NULL, NULL, &error);
    if (!r) {printf("Error encountered:%s", error.message);}
    r = mongoc_collection_insert_one(collection, bob_account, NULL, NULL, &error);
    if (!r) {printf("Error encountered:%s", error.message);}

    test_callback_money_transfer(client, collection, amount_to_transfer);

}
```

Python

Der folgende Code zeigt, wie die Amazon DocumentDB-Transaktions-API mit Python verwendet wird.

```
// Sample Python code with callback api

import pymongo
```

```
def callback(session, balance, query):
    collection.update_one(query, {'$set': {"balance": balance}}, session=session)

client = pymongo.MongoClient(<connection uri>)
rc_snapshot = pymongo.read_concern.ReadConcern('snapshot')
wc_majority = pymongo.write_concern.WriteConcern('majority')

# To start, drop and create an account collection and insert balances for both Alice
 and Bob
collection = client.get_database("bank").get_collection("account")
collection.drop()
collection.insert_one({"_id": 1, "name": "Alice", "balance": 1000})
collection.insert_one({"_id": 2, "name": "Bob", "balance": 1000})

amount_to_transfer = 500

# deduct 500 from Alice's account
alice_balance = collection.find_one({"name": "Alice"}).get("balance")
assert alice_balance >= amount_to_transfer
new_alice_balance = alice_balance - amount_to_transfer

with client.start_session({'causalConsistency':False}) as session:
    session.with_transaction(lambda s: callback(s, new_alice_balance, {"name":
 "Alice"}), read_concern=rc_snapshot, write_concern=wc_majority)

updated_alice_balance = collection.find_one({"name": "Alice"}).get("balance")
assert updated_alice_balance == new_alice_balance

# add 500 to Bob's account
bob_balance = collection.find_one({"name": "Bob"}).get("balance")
assert bob_balance >= amount_to_transfer
new_bob_balance = bob_balance + amount_to_transfer

with client.start_session({'causalConsistency':False}) as session:
    session.with_transaction(lambda s: callback(s, new_bob_balance, {"name":
 "Bob"}), read_concern=rc_snapshot, write_concern=wc_majority)

updated_bob_balance = collection.find_one({"name": "Bob"}).get("balance")
assert updated_bob_balance == new_bob_balance
```

Beispiele für Transaktions-APIs für die Kern-API

Javascript

Der folgende Code zeigt, wie die Amazon DocumentDB-Transaktions-API mit Javascript verwendet wird.

```
// *** Transfer $500 from Alice to Bob inside a transaction: Success ***
// Setup bank account for Alice and Bob. Each have $1000 in their account
var databaseName = "bank";
var collectionName = "account";
var amountToTransfer = 500;

var session = db.getMongo().startSession({causalConsistency: false});
var bankDB = session.getDatabase(databaseName);
var accountColl = bankDB[collectionName];
accountColl.drop();

accountColl.insert({name: "Alice", balance: 1000});
accountColl.insert({name: "Bob", balance: 1000});

session.startTransaction();

// deduct $500 from Alice's account
var aliceBalance = accountColl.find({"name": "Alice"}).next().balance;
assert(aliceBalance >= amountToTransfer);
var newAliceBalance = aliceBalance - amountToTransfer;
accountColl.update({"name": "Alice"},{"$set": {"balance": newAliceBalance}});
var findAliceBalance = accountColl.find({"name": "Alice"}).next().balance;
assert.eq(newAliceBalance, findAliceBalance);

// add $500 to Bob's account
var bobBalance = accountColl.find({"name": "Bob"}).next().balance;
var newBobBalance = bobBalance + amountToTransfer;
accountColl.update({"name": "Bob"},{"$set": {"balance": newBobBalance}});
var findBobBalance = accountColl.find({"name": "Bob"}).next().balance;
assert.eq(newBobBalance, findBobBalance);

session.commitTransaction();

accountColl.find();
```

C#

Der folgende Code zeigt, wie die Amazon DocumentDB-Transaktions-API mit C# verwendet wird.

```
// C# Core API

public void TransferMoneyWithRetry(IMongoCollection<bSondocument> accountColl,
 IClientSessionHandle session)
{
    var amountToTransfer = 500;

    // start transaction
   var transactionOptions = new TransactionOptions(
                readConcern: ReadConcern.Snapshot,
                writeConcern: WriteConcern.WMajority);
    session.StartTransaction(transactionOptions);
   try
    {
        // deduct $500 from Alice's account
        var aliceBalance = accountColl.Find(session,
 Builders<bSondocument>.Filter.Eq("name",
 "Alice")).FirstOrDefault().GetValue("balance");
       Debug.Assert(aliceBalance >= amountToTransfer);
       var newAliceBalance = aliceBalance.AsInt32 - amountToTransfer;
       accountColl.UpdateOne(session, Builders<bSondocument>.Filter.Eq("name",
 "Alice"),
                                Builders<bSondocument>.Update.Set("balance",
 newAliceBalance));
       aliceBalance = accountColl.Find(session,
 Builders<bSondocument>.Filter.Eq("name",
 "Alice")).FirstOrDefault().GetValue("balance");
       Debug.Assert(aliceBalance == newAliceBalance);

       // add $500 from Bob's account
       var bobBalance = accountColl.Find(session,
 Builders<bSondocument>.Filter.Eq("name",
 "Bob")).FirstOrDefault().GetValue("balance");
       var newBobBalance = bobBalance.AsInt32 + amountToTransfer;
       accountColl.UpdateOne(session, Builders<bSondocument>.Filter.Eq("name",
 "Bob"),
                                Builders<bSondocument>.Update.Set("balance",
 newBobBalance));
```

```
        bobBalance = accountColl.Find(session,
 Builders<bSondocument>.Filter.Eq("name",
 "Bob")).FirstOrDefault().GetValue("balance");
        Debug.Assert(bobBalance == newBobBalance);

    }
    catch (Exception e)
    {
        session.AbortTransaction();
        throw;
    }

    session.CommitTransaction();
 }

}
public void DoTransactionWithRetry(MongoClient client)
{
    var dbName = "bank";
    var collName = "account";
    using (var session = client.StartSession(new
 ClientSessionOptions{CausalConsistency = false}))
    {
        try
        {
            var bankDB = client.GetDatabase(dbName);
            var accountColl = bankDB.GetCollection<bSondocument>(collName);
            bankDB.DropCollection(collName);
            accountColl.InsertOne(session, new BsonDocument { {"name", "Alice"},
 {"balance", 1000 } });
            accountColl.InsertOne(session, new BsonDocument { {"name", "Bob"},
 {"balance", 1000 } });

            while(true) {
                try
                {
                        TransferMoneyWithRetry(accountColl, session);
                        break;
                }
                catch (MongoException e)
                {
                    if(e.HasErrorLabel("TransientTransactionError"))
                    {
                        continue;
```

```
                    }
                    else
                    {
                        throw;
                    }
                }
            }

            // check values outside of transaction
            var aliceNewBalance =
 accountColl.Find(Builders<bSondocument>.Filter.Eq("name",
 "Alice")).FirstOrDefault().GetValue("balance");
            var bobNewBalance =
 accountColl.Find(Builders<bSondocument>.Filter.Eq("name",
 "Bob")).FirstOrDefault().GetValue("balance");
            Debug.Assert(aliceNewBalance ==  500);
            Debug.Assert(bobNewBalance ==  1500);
        }
        catch (Exception e)
        {
            Console.WriteLine("Error running transaction: " + e.Message);
        }
    }
}
```

Ruby

Der folgende Code zeigt, wie die Amazon DocumentDB-Transaktions-API mit Ruby verwendet wird.

```
# Ruby Core API

def transfer_money_w_retry(session, accountColl)
    amountToTransfer = 500

    session.start_transaction(read_concern: {level: :snapshot}, write_concern:
 {w: :majority})
    # deduct $500 from Alice's account
    aliceBalance = accountColl.find({"name"=>"Alice"}, :session=>
 session).first['balance']
    assert aliceBalance >= amountToTransfer
    newAliceBalance = aliceBalance - amountToTransfer
```

```
    accountColl.update_one({"name"=>"Alice"}, { "$set" =>
 {"balance"=>newAliceBalance} }, :session=> session)
    aliceBalance = accountColl.find({"name"=>"Alice"}, :session=>
 session).first['balance']
    assert_equal(newAliceBalance, aliceBalance)

    # add $500 to Bob's account
    bobBalance = accountColl.find({"name"=>"Bob"}, :session=>
 session).first['balance']
    newBobBalance = bobBalance + amountToTransfer
    accountColl.update_one({"name"=>"Bob"}, { "$set" =>
 {"balance"=>newBobBalance} }, :session=> session)
    bobBalance = accountColl.find({"name"=>"Bob"}, :session=>
 session).first['balance']
    assert_equal(newBobBalance, bobBalance)

    session.commit_transaction

end

def do_txn_w_retry(client)
     dbName = "bank"
    collName = "account"

    session = client.start_session(:causal_consistency=> false)
    bankDB = Mongo::Database.new(client, dbName)
    accountColl = bankDB[collName]
    accountColl.drop()

    accountColl.insert_one({"name"=>"Alice", "balance"=>1000})
    accountColl.insert_one({"name"=>"Bob", "balance"=>1000})

    begin
        transferMoneyWithRetry(session, accountColl)
        puts "transaction committed"
    rescue Mongo::Error => e
        if e.label?('TransientTransactionError')
            retry
        else
            puts "transaction failed"
            raise
        end
    end
```

```
    # check results outside of transaction
    aliceBalance = accountColl.find({"name"=>"Alice"}).first['balance']
    bobBalance = accountColl.find({"name"=>"Bob"}).first['balance']
    assert_equal(aliceBalance, 500)
    assert_equal(bobBalance, 1500)

end
```

Go

Der folgende Code zeigt, wie Sie die Amazon DocumentDB-Transaktions-API mit Go verwenden.

```
// Go - Core API
type Account struct {
    Name string
    Balance  int
}

func transferMoneyWithRetry(sessionContext mongo.SessionContext, accountColl
 *mongo.Collection, t *testing.T) error {
    amountToTransfer := 500

    transactionOptions :=
 options.Transaction().SetReadConcern(readconcern.Snapshot()).

 SetWriteConcern(writeconcern.New(writeconcern.WMajority()))
    if err := sessionContext.StartTransaction(transactionOptions); err != nil {
        panic(err)
    }

    var result Account
    // deduct $500 from Alice's account
    err := accountColl.FindOne(sessionContext, bson.M{"name":
 "Alice"}).Decode(&result)
    aliceBalance := result.Balance
    newAliceBalance := aliceBalance - amountToTransfer
    _, err = accountColl.UpdateOne(sessionContext, bson.M{"name": "Alice"},
 bson.M{"$set": bson.M{"balance": newAliceBalance}})
    if err != nil {
        sessionContext.AbortTransaction(sessionContext)
    }
    err = accountColl.FindOne(sessionContext, bson.M{"name":
 "Alice"}).Decode(&result)
    aliceBalance = result.Balance
```

```
    assert.Equal(t, aliceBalance, newAliceBalance)

    // add $500 to Bob's account
    err = accountColl.FindOne(sessionContext, bson.M{"name": "Bob"}).Decode(&result)
    bobBalance := result.Balance
    newBobBalance := bobBalance + amountToTransfer
    _, err = accountColl.UpdateOne(sessionContext, bson.M{"name": "Bob"},
 bson.M{"$set": bson.M{"balance": newBobBalance}})
    if err != nil {
        sessionContext.AbortTransaction(sessionContext)
    }
    err = accountColl.FindOne(sessionContext, bson.M{"name": "Bob"}).Decode(&result)
    bobBalance = result.Balance
    assert.Equal(t, bobBalance, newBobBalance)

    err = sessionContext.CommitTransaction(sessionContext)
    return err
}

func doTransactionWithRetry(t *testing.T) {
    ctx := context.TODO()

    dbName := "bank"
    collName := "account"
    bankDB := client.Database(dbName)
    accountColl := bankDB.Collection(collName)

    client.UseSessionWithOptions(ctx, options.Session().SetCausalConsistency(false),
 func(sessionContext mongo.SessionContext) error {
        accountColl.Drop(ctx)
        accountColl.InsertOne(sessionContext, bson.M{"name" : "Alice",
 "balance":1000})
        accountColl.InsertOne(sessionContext, bson.M{"name" : "Bob",
 "balance":1000})
        for {
            err := transferMoneyWithRetry(sessionContext, accountColl, t)
            if err == nil {
                println("transaction committed")
                return nil
            }
            if mongoErr := err.(mongo.CommandError);
 mongoErr.HasErrorLabel("TransientTransactionError") {
                continue
            }
```

```
            println("transaction failed")
            return err
        }
    })

    // check results outside of transaction
    var result Account
    accountColl.FindOne(ctx, bson.M{"name": "Alice"}).Decode(&result)
    aliceBalance := result.Balance
    assert.Equal(t, aliceBalance, 500)
    accountColl.FindOne(ctx, bson.M{"name": "Bob"}).Decode(&result)
    bobBalance := result.Balance
    assert.Equal(t, bobBalance, 1500)
}
```

Java

Der folgende Code zeigt, wie die Amazon DocumentDB-Transaktions-API mit Java verwendet wird.

```
// Java (sync) - Core API

public void transferMoneyWithRetry() {
   // connect to server
    MongoClientURI mongoURI = new MongoClientURI(uri);
    MongoClient mongoClient = new MongoClient(mongoURI);

    MongoDatabase bankDB = mongoClient.getDatabase("bank");
    MongoCollection accountColl = bankDB.getCollection("account");
    accountColl.drop();

   // insert some sample data
    accountColl.insertOne(new Document("name", "Alice").append("balance", 1000));
    accountColl.insertOne(new Document("name", "Bob").append("balance", 1000));

    while (true) {
        try {
            doTransferMoneyWithRetry(accountColl, mongoClient);
            break;
        } catch (MongoException e) {
            if (e.hasErrorLabel(MongoException.TRANSIENT_TRANSACTION_ERROR_LABEL)) {
                continue;
            } else {
```

```
                throw e;
            }
        }
    }
}

public void doTransferMoneyWithRetry(MongoCollection accountColl, MongoClient
 mongoClient) {
    int amountToTransfer = 500;

   TransactionOptions txnOptions = TransactionOptions.builder()
      .readConcern(ReadConcern.SNAPSHOT)
      .writeConcern(WriteConcern.MAJORITY)
      .build();
    ClientSessionOptions sessionOptions =
 ClientSessionOptions.builder().causallyConsistent(false).build();
    try ( ClientSession clientSession = mongoClient.startSession(sessionOptions) ) {
        clientSession.startTransaction(txnOptions);

        // deduct $500 from Alice's account
        List<Document> documentList = new ArrayList<>();
        accountColl.find(clientSession, new Document("name",
 "Alice")).into(documentList);
        int aliceBalance = (int) documentList.get(0).get("balance");
        Assert.assertTrue(aliceBalance >= amountToTransfer);
        int newAliceBalance = aliceBalance - amountToTransfer;
        accountColl.updateOne(clientSession, new Document("name", "Alice"), new
 Document("$set", new Document("balance", newAliceBalance)));

        // check Alice's new balance
        documentList = new ArrayList<>();
        accountColl.find(clientSession, new Document("name",
 "Alice")).into(documentList);
        int updatedBalance = (int) documentList.get(0).get("balance");
        Assert.assertEquals(updatedBalance, newAliceBalance);

        // add $500 to Bob's account
        documentList = new ArrayList<>();
        accountColl.find(clientSession, new Document("name",
 "Bob")).into(documentList);
        int bobBalance = (int) documentList.get(0).get("balance");
        int newBobBalance = bobBalance + amountToTransfer;
        accountColl.updateOne(clientSession, new Document("name", "Bob"), new
 Document("$set", new Document("balance", newBobBalance)));
```

```
        // check Bob's new balance
        documentList = new ArrayList<>();
        accountColl.find(clientSession, new Document("name",
 "Bob")).into(documentList);
        updatedBalance = (int) documentList.get(0).get("balance");
        Assert.assertEquals(updatedBalance, newBobBalance);

        // commit transaction
        clientSession.commitTransaction();
    }
}
// Java (async) -- Core API
public void transferMoneyWithRetry() {
    // connect to the server
    MongoClient mongoClient = MongoClients.create(uri);

    MongoDatabase bankDB = mongoClient.getDatabase("bank");
    MongoCollection accountColl = bankDB.getCollection("account");
    SubscriberLatchWrapper<Void> dropCallback = new SubscriberLatchWrapper<>();
    mongoClient.getDatabase("bank").drop().subscribe(dropCallback);
    dropCallback.await();

    // insert some sample data
    SubscriberLatchWrapper<InsertOneResult> insertionCallback = new
 SubscriberLatchWrapper<>();
    accountColl.insertOne(new Document("name", "Alice").append("balance",
 1000)).subscribe(insertionCallback);
    insertionCallback.await();

    insertionCallback = new SubscriberLatchWrapper<>();
    accountColl.insertOne(new Document("name", "Bob").append("balance",
 1000)).subscribe(insertionCallback);;
    insertionCallback.await();

    while (true) {
        try {
            doTransferMoneyWithRetry(accountColl, mongoClient);
            break;
        } catch (MongoException e) {
            if (e.hasErrorLabel(MongoException.TRANSIENT_TRANSACTION_ERROR_LABEL)) {
                continue;
            } else {
                throw e;
```

```
            }
        }
    }
}

public void doTransferMoneyWithRetry(MongoCollection accountColl, MongoClient
 mongoClient) {
    int amountToTransfer = 500;

    // start the transaction
    TransactionOptions txnOptions = TransactionOptions.builder()
            .readConcern(ReadConcern.SNAPSHOT)
            .writeConcern(WriteConcern.MAJORITY)
            .build();
    ClientSessionOptions sessionOptions =
 ClientSessionOptions.builder().causallyConsistent(false).build();

    SubscriberLatchWrapper<ClientSession> sessionCallback = new
 SubscriberLatchWrapper<>();
    mongoClient.startSession(sessionOptions).subscribe(sessionCallback);
    ClientSession session = sessionCallback.get().get(0);
    session.startTransaction(txnOptions);

    // deduct $500 from Alice's account
    SubscriberLatchWrapper<Document> findCallback = new SubscriberLatchWrapper<>();
    accountColl.find(session, new Document("name",
 "Alice")).first().subscribe(findCallback);
    Document documentFound = findCallback.get().get(0);
    int aliceBalance = (int) documentFound.get("balance");
    int newAliceBalance = aliceBalance - amountToTransfer;

    SubscriberLatchWrapper<UpdateResult> updateCallback = new
 SubscriberLatchWrapper<>();
    accountColl.updateOne(session, new Document("name",
 "Alice"), new Document("$set", new Document("balance",
 newAliceBalance))).subscribe(updateCallback);
    updateCallback.await();

    // check Alice's new balance
    findCallback = new SubscriberLatchWrapper<>();
    accountColl.find(session, new Document("name",
 "Alice")).first().subscribe(findCallback);
    documentFound = findCallback.get().get(0);
    int updatedBalance = (int) documentFound.get("balance");
```

```
    Assert.assertEquals(updatedBalance, newAliceBalance);

    // add $500 to Bob's account
    findCallback = new SubscriberLatchWrapper<>();
    accountColl.find(session, new Document("name",
 "Bob")).first().subscribe(findCallback);
    documentFound = findCallback.get().get(0);
    int bobBalance = (int) documentFound.get("balance");
    int newBobBalance = bobBalance + amountToTransfer;

    updateCallback = new SubscriberLatchWrapper<>();
    accountColl.updateOne(session, new Document("name", "Bob"), new Document("$set",
 new Document("balance", newBobBalance))).subscribe(updateCallback);
    updateCallback.await();

    // check Bob's new balance
    findCallback = new SubscriberLatchWrapper<>();
    accountColl.find(session, new Document("name",
 "Bob")).first().subscribe(findCallback);
    documentFound = findCallback.get().get(0);
    updatedBalance = (int) documentFound.get("balance");
    Assert.assertEquals(updatedBalance, newBobBalance);

    // commit the transaction
    SubscriberLatchWrapper<Void> transactionCallback = new
 SubscriberLatchWrapper<>();
    session.commitTransaction().subscribe(transactionCallback);
    transactionCallback.await();
}

public class SubscriberLatchWrapper<T> implements Subscriber<T> {

    /**
     * A Subscriber that stores the publishers results and provides a latch so can
 block on completion.
     *
     * @param <T> The publishers result type
     */
    private final List<T> received;
    private final List<RuntimeException> errors;
    private final CountDownLatch latch;
    private volatile Subscription subscription;
    private volatile boolean completed;
```

```
    /**
     * Construct an instance
     */
    public SubscriberLatchWrapper() {
        this.received = new ArrayList<>();
        this.errors = new ArrayList<>();
        this.latch = new CountDownLatch(1);
    }

    @Override
    public void onSubscribe(final Subscription s) {
        subscription = s;
        subscription.request(Integer.MAX_VALUE);
    }

    @Override
    public void onNext(final T t) {
        received.add(t);
    }

    @Override
    public void onError(final Throwable t) {
        if (t instanceof RuntimeException) {
            errors.add((RuntimeException) t);
        } else {
            errors.add(new RuntimeException("Unexpected exception", t));
        }
        onComplete();
    }

    @Override
    public void onComplete() {
        completed = true;
        subscription.cancel();
        latch.countDown();
    }

    /**
     * Get received elements
     *
     * @return the list of received elements
     */
    public List<T> getReceived() {
        return received;
```

```
    }

    /**
     * Get received elements.
     *
     * @return the list of receive elements
     */
    public List<T> get() {
        return await().getReceived();
    }

    /**
     * Await completion or error
     *
     * @return this
     */
    public SubscriberLatchWrapper<T> await() {
        subscription.request(Integer.MAX_VALUE);
        try {
            if (!latch.await(300, TimeUnit.SECONDS)) {
                throw new MongoTimeoutException("Publisher onComplete timed out for
 300 seconds");
            }
        } catch (InterruptedException e) {
            throw new MongoInterruptedException("Interrupted waiting for
 observeration", e);
        }
        if (!errors.isEmpty()) {
            throw errors.get(0);
        }
        return this;
    }

    public boolean getCompleted() {
        return this.completed;
    }

    public void close() {
        subscription.cancel();
        received.clear();
    }
}
```

C

Der folgende Code zeigt, wie die Amazon DocumentDB-Transaktions-API mit C verwendet wird.

```
// Sample C code with core session

bool core_session(mongoc_client_session_t *client_session, mongoc_collection_t*
 collection, bson_t *selector, int64_t balance){
    bool r = true;
    bson_error_t error;
    bson_t *opts = bson_new();
    bson_t *update = BCON_NEW ("$set", "{", "balance", BCON_INT64 (balance), "}");

    // set read & write concern
    mongoc_read_concern_t *read_concern = mongoc_read_concern_new ();
    mongoc_write_concern_t *write_concern = mongoc_write_concern_new ();
    mongoc_transaction_opt_t *txn_opts = mongoc_transaction_opts_new ();

    mongoc_write_concern_set_w(write_concern, MONGOC_WRITE_CONCERN_W_MAJORITY);
    mongoc_read_concern_set_level(read_concern, MONGOC_READ_CONCERN_LEVEL_SNAPSHOT);
    mongoc_transaction_opts_set_write_concern (txn_opts, write_concern);
    mongoc_transaction_opts_set_read_concern (txn_opts, read_concern);

    mongoc_client_session_start_transaction (client_session, txn_opts, &error);
    mongoc_client_session_append (client_session, opts, &error);

    r = mongoc_collection_update_one (collection, selector, update, opts, NULL,
 &error);

    mongoc_client_session_commit_transaction (client_session, NULL, &error);
    bson_destroy (opts);
    mongoc_transaction_opts_destroy(txn_opts);
    mongoc_read_concern_destroy(read_concern);
    mongoc_write_concern_destroy(write_concern);
    bson_destroy (update);
    return r;
}

void test_core_money_transfer(mongoc_client_t* client, mongoc_collection_t*
 collection, int amount_to_transfer){

    bson_t reply;
    bool r = true;
    const bson_t *doc;
```

```
    bson_iter_t iter;
    bson_error_t error;

    // find query
    bson_t *alice_query = bson_new ();
    BSON_APPEND_UTF8(alice_query, "name", "Alice");

    bson_t *bob_query = bson_new ();
    BSON_APPEND_UTF8(bob_query, "name", "Bob");

    // create session
    // set causal consistency to false
    mongoc_session_opt_t *session_opts = mongoc_session_opts_new ();
    mongoc_session_opts_set_causal_consistency (session_opts, false);
    // start the session
    mongoc_client_session_t *client_session = mongoc_client_start_session (client,
session_opts, &error);

    // add session to options
    bson_t *opts = bson_new();
    mongoc_client_session_append (client_session, opts, &error);

    // deduct 500 from Alice
    // find account balance of Alice
    mongoc_cursor_t *cursor = mongoc_collection_find_with_opts (collection,
alice_query, NULL, NULL);
    mongoc_cursor_next (cursor, &doc);
    bson_iter_init (&iter, doc);
    bson_iter_find (&iter, "balance");
    int64_t alice_balance = (bson_iter_value (&iter))->value.v_int64;
    assert(alice_balance >= amount_to_transfer);
    int64_t new_alice_balance = alice_balance - amount_to_transfer;

    // core
    r = core_session (client_session, collection, alice_query, new_alice_balance);
    assert(r);

    // find account balance of Alice after transaction
    cursor = mongoc_collection_find_with_opts (collection, alice_query, NULL, NULL);
    mongoc_cursor_next (cursor, &doc);
    bson_iter_init (&iter, doc);
    bson_iter_find (&iter, "balance");
    alice_balance = (bson_iter_value (&iter))->value.v_int64;
    assert(alice_balance == new_alice_balance);
```

```
    assert(alice_balance == 500);

    // add 500 to Bob's balance
    // find account balance of Bob
    cursor = mongoc_collection_find_with_opts (collection, bob_query, NULL, NULL);
    mongoc_cursor_next (cursor, &doc);
    bson_iter_init (&iter, doc);
    bson_iter_find (&iter, "balance");
    int64_t bob_balance = (bson_iter_value (&iter))->value.v_int64;
    int64_t new_bob_balance = bob_balance + amount_to_transfer;

    //core
    r = core_session (client_session, collection, bob_query, new_bob_balance);
    assert(r);

    // find account balance of Bob after transaction
    cursor = mongoc_collection_find_with_opts (collection, bob_query, NULL, NULL);
    mongoc_cursor_next (cursor, &doc);
    bson_iter_init (&iter, doc);
    bson_iter_find (&iter, "balance");
    bob_balance = (bson_iter_value (&iter))->value.v_int64;
    assert(bob_balance == new_bob_balance);
    assert(bob_balance == 1500);

    // cleanup
    bson_destroy(alice_query);
    bson_destroy(bob_query);
    mongoc_client_session_destroy(client_session);
    bson_destroy(opts);
    mongoc_cursor_destroy(cursor);
    bson_destroy(doc);
}

int main(int argc, char* argv[]) {
    mongoc_init ();
    mongoc_client_t* client = mongoc_client_new (<connection uri>);
    bson_error_t error;

    // connect to bank db
    mongoc_database_t *database = mongoc_client_get_database (client, "bank");
    // access account collection
    mongoc_collection_t* collection = mongoc_client_get_collection(client, "bank",
 "account");
    // set amount to transfer
```

```
    int64_t amount_to_transfer = 500;
    // delete the collection if already existing
    mongoc_collection_drop(collection, &error);

    // open Alice account
    bson_t *alice_account = bson_new ();
    BSON_APPEND_UTF8(alice_account, "name", "Alice");
    BSON_APPEND_INT64(alice_account, "balance", 1000);

    // open Bob account
    bson_t *bob_account = bson_new ();
    BSON_APPEND_UTF8(bob_account, "name", "Bob");
    BSON_APPEND_INT64(bob_account, "balance", 1000);

    bool r = true;

    r = mongoc_collection_insert_one(collection, alice_account, NULL, NULL, &error);
    if (!r) {printf("Error encountered:%s", error.message);}
    r = mongoc_collection_insert_one(collection, bob_account, NULL, NULL, &error);
    if (!r) {printf("Error encountered:%s", error.message);}

    test_core_money_transfer(client, collection, amount_to_transfer);

}
```

Scala

Der folgende Code zeigt, wie die Amazon DocumentDB-Transaktions-API mit Scala verwendet wird.

```
// Scala Core API
def transferMoneyWithRetry(sessionObservable: SingleObservable[ClientSession] ,
 database: MongoDatabase ): Unit = {
    val accountColl = database.getCollection("account")
    var amountToTransfer = 500

    var transactionObservable: Observable[ClientSession] =
 sessionObservable.map(clientSession => {
    clientSession.startTransaction()

    // deduct $500 from Alice's account
    var aliceBalance = accountColl.find(clientSession, Document("name" ->
 "Alice")).await().head.getInteger("balance")
```

```
    assert(aliceBalance >= amountToTransfer)
    var newAliceBalance = aliceBalance - amountToTransfer
    accountColl.updateOne(clientSession, Document("name" -> "Alice"),
 Document("$set" -> Document("balance" -> newAliceBalance))).await()
    aliceBalance = accountColl.find(clientSession, Document("name" ->
 "Alice")).await().head.getInteger("balance")
    assert(aliceBalance == newAliceBalance)

    // add $500 to Bob's account
    var bobBalance = accountColl.find(clientSession, Document("name" ->
 "Bob")).await().head.getInteger("balance")
    var newBobBalance = bobBalance + amountToTransfer
    accountColl.updateOne(clientSession, Document("name" -> "Bob"), Document("$set"
 -> Document("balance" -> newBobBalance))).await()
    bobBalance = accountColl.find(clientSession, Document("name" ->
 "Bob")).await().head.getInteger("balance")
    assert(bobBalance == newBobBalance)

    clientSession
    })

    transactionObservable.flatMap(clientSession =>
 clientSession.commitTransaction()).await()
}

def doTransactionWithRetry(): Unit = {
    val client: MongoClient = MongoClientWrapper.getMongoClient()
    val database: MongoDatabase = client.getDatabase("bank")
    val accountColl = database.getCollection("account")
    accountColl.drop().await()

    val sessionOptions =
 ClientSessionOptions.builder().causallyConsistent(false).build()
    var  sessionObservable: SingleObservable[ClientSession] =
 client.startSession(sessionOptions)
    accountColl.insertOne(Document("name" -> "Alice", "balance" -> 1000)).await()
    accountColl.insertOne(Document("name" -> "Bob", "balance" -> 1000)).await()

    var retry = true
    while (retry) {
        try {
        transferMoneyWithRetry(sessionObservable, database)
        println("transaction committed")
        retry = false
```

```
        }
        catch {
        case e: MongoException if
 e.hasErrorLabel(MongoException.TRANSIENT_TRANSACTION_ERROR_LABEL) => {
            println("retrying transaction")
        }
        case other: Throwable => {
            println("transaction failed")
            retry = false
            throw other

        }
        }
    }

    // check results outside of transaction
    assert(accountColl.find(Document("name" ->
 "Alice")).results().head.getInteger("balance") == 500)
    assert(accountColl.find(Document("name" ->
 "Bob")).results().head.getInteger("balance") == 1500)

    accountColl.drop().await()

}
```

Python

Der folgende Code zeigt, wie die Amazon DocumentDB-Transaktions-API mit Python verwendet wird.

```
// Sample Python code with Core api

import pymongo

client = pymongo.MongoClient(<connection_string>)
rc_snapshot = pymongo.read_concern.ReadConcern('snapshot')
wc_majority = pymongo.write_concern.WriteConcern('majority')

# To start, drop and create an account collection and insert balances for both Alice
 and Bob
collection = client.get_database("bank").get_collection("account")
collection.drop()
collection.insert_one({"_id": 1, "name": "Alice", "balance": 1000})
```

```
collection.insert_one({"_id": 2, "name": "Bob", "balance": 1000})

amount_to_transfer = 500

# deduct 500 from Alice's account
alice_balance = collection.find_one({"name": "Alice"}).get("balance")
assert alice_balance >= amount_to_transfer
new_alice_balance = alice_balance - amount_to_transfer

with client.start_session({'causalConsistency':False}) as session:
    session.start_transaction(read_concern=rc_snapshot, write_concern=wc_majority)
    collection.update_one({"name": "Alice"}, {'$set': {"balance":
 new_alice_balance}}, session=session)
    session.commit_transaction()

updated_alice_balance = collection.find_one({"name": "Alice"}).get("balance")
assert updated_alice_balance == new_alice_balance

# add 500 to Bob's account
bob_balance = collection.find_one({"name": "Bob"}).get("balance")
assert bob_balance >= amount_to_transfer
new_bob_balance = bob_balance + amount_to_transfer

with client.start_session({'causalConsistency':False}) as session:
    session.start_transaction(read_concern=rc_snapshot, write_concern=wc_majority)
    collection.update_one({"name": "Bob"}, {'$set': {"balance": new_bob_balance}},
 session=session)
    session.commit_transaction()

updated_bob_balance = collection.find_one({"name": "Bob"}).get("balance")
assert updated_bob_balance == new_bob_balance
```

Unterstützte Befehle

Befehl	Unterstützt
abortTransaction	Ja
commitTransaction	Ja
endSessions	Ja

Befehl	Unterstützt
`killSession`	Ja
`killAllSession`	Ja
`killAllSessionsByPattern`	Nein
`refreshSessions`	Nein
`startSession`	Ja

Nicht unterstützte Funktionen

Methoden	Stufen oder Befehle

`db.collection.aggregate()`	`$collStats`
	`$currentOp`
	`$indexStats`
	`$listSessions`
	`$out`

`db.collection.count()`
`db.collection.countDocuments()`
	`$where`
	`$near`
	`$nearSphere`

`db.collection.insert()`	`insert`wird nicht unterstützt, wenn es nicht für eine bestehende Sammlung ausgeführt wird. Diese Methode wird unterstützt, wenn sie auf eine bereits bestehende Sammlung abzielt.

Sitzungen

MongoDB-Sitzungen sind ein Framework, das zur Unterstützung wiederholbarer Schreibvorgänge, kausaler Konsistenz, Transaktionen und zur Verwaltung datenbankübergreifender Operationen verwendet wird. Wenn eine Sitzung erstellt wird, wird vom Client ein logischer Sitzungsbezeichner (LSID) generiert, der verwendet wird, um alle Operationen innerhalb dieser Sitzung zu kennzeichnen, wenn Befehle an den Server gesendet werden.

Amazon DocumentDB unterstützt die Verwendung von Sitzungen, um Transaktionen zu ermöglichen, unterstützt jedoch keine kausale Konsistenz oder wiederholbare Schreibvorgänge.

Bei der Verwendung von Transaktionen innerhalb von Amazon DocumentDB wird eine Transaktion innerhalb einer Sitzung mithilfe der `session.startTransaction()` API initiiert, und eine Sitzung unterstützt jeweils eine einzelne Transaktion. In ähnlicher Weise werden Transaktionen entweder mit den APIs commit (`session.commitTransaction()`) oder abort (`session.abortTransaction()`) abgeschlossen.

Kausale Konsistenz

Die kausale Konsistenz garantiert, dass der Client innerhalb einer einzelnen Clientsitzung die Konsistenz beim Lesen nach dem Schreiben beobachtet, d. h. monoatomisch reads/writes, und dass Schreibvorgänge auf Lesevorgänge folgen. Diese Garantien gelten für alle Instanzen in einem Cluster, nicht nur für die primäre. Amazon DocumentDB unterstützt keine kausale Konsistenz und die folgende Aussage führt zu einem Fehler.

```
var mySession = db.getMongo().startSession();
var mySessionObject = mySession.getDatabase('test').getCollection('account');

mySessionObject.updateOne({"_id": 2}, {"$inc": {"balance": 400}});
//Result:{ "acknowledged" : true, "matchedCount" : 1, "modifiedCount" : 1 }

mySessionObject.find()
//Error: error: {
//         "ok" : 0,
//         "code" : 303,
//         "errmsg" : "Feature not supported: 'causal consistency'",
//         "operationTime" : Timestamp(1603461817, 493214)
//}
```

```
mySession.endSession()
```

Sie können die kausale Konsistenz innerhalb einer Sitzung deaktivieren. Beachten Sie, dass Sie auf diese Weise das Session-Framework nutzen können, aber keine Garantie für kausale Konsistenz bei Lesevorgängen bietet. Wenn Sie Amazon DocumentDB verwenden, werden Lesevorgänge von der Primärinstanz nach dem Schreiben konsistent sein, und die Lesevorgänge von den Replikatinstanzen werden letztendlich konsistent sein. Transaktionen sind der Hauptanwendungsfall für die Nutzung von Sitzungen.

```
var mySession = db.getMongo().startSession({causalConsistency: false});
var mySessionObject = mySession.getDatabase('test').getCollection('account');

mySessionObject.updateOne({"_id": 2}, {"$inc": {"balance": 400}});
//Result:{ "acknowledged" : true, "matchedCount" : 1, "modifiedCount" : 1 }

mySessionObject.find()
//{ "_id" : 1, "name" : "Bob", "balance" : 100 }
//{ "_id" : 2, "name" : "Alice", "balance" : 1700 }
```

Wiederholbare Schreibvorgänge

Wiederholbare Schreibvorgänge sind eine Funktion, bei der der Client versucht, Schreibvorgänge einmal zu wiederholen, wenn Netzwerkfehler auftreten oder wenn der Client den primären Schreibvorgang nicht finden kann. In Amazon DocumentDB werden wiederholbare Schreibvorgänge nicht unterstützt und müssen deaktiviert werden. Sie können es mit dem Befehl (`retryWrites=false`) in der Verbindungszeichenfolge deaktivieren.

> **Note**
>
> Wenn Sie eine ältere Mongo-Shell (nicht Mongosh) verwenden, fügen Sie den `retryWrites=false` Befehl in keine Codezeichenfolge ein. Standardmäßig sind wiederholbare Schreibvorgänge deaktiviert. `retryWrites=false`Das Einschließen kann zu einem Fehler bei normalen Lesebefehlen führen.

Transaktionsfehler

Bei der Verwendung von Transaktionen gibt es Szenarien, in denen ein Fehler auftreten kann, der besagt, dass eine Transaktionsnummer mit keiner laufenden Transaktion übereinstimmt.

Der Fehler kann in mindestens zwei verschiedenen Szenarien generiert werden:

- Nach dem Transaktions-Timeout von einer Minute.
- Nach einem Neustart der Instanz (aufgrund von Patches, Wiederherstellung nach einem Absturz usw.) kann dieser Fehler auch dann auftreten, wenn die Transaktion erfolgreich festgeschrieben wurde. Während eines Instance-Neustarts kann die Datenbank den Unterschied zwischen einer erfolgreich abgeschlossenen Transaktion und einer abgebrochenen Transaktion nicht erkennen. Mit anderen Worten, der Status des Transaktionsabschlusses ist mehrdeutig.

Der beste Weg, diesen Fehler zu beheben, besteht darin, Transaktionsaktualisierungen idempotent zu machen — zum Beispiel, indem Sie den `$set` Mutator anstelle einer Operation verwenden. increment/decrement Siehe unten:

```
{ "ok" : 0,
"operationTime" : Timestamp(1603938167, 1),
"code" : 251,
"errmsg" : "Given transaction number 1 does not match any in-progress transactions."
}
```

Bewährte Methoden für Amazon DocumentDB

Lernen Sie bewährte Methoden für die Arbeit mit Amazon DocumentDB (mit MongoDB-Kompatibilität) kennen. Dieser Abschnitt wird fortlaufend aktualisiert, wenn neue bewährte Methoden identifiziert werden.

Themen

- Grundlegende Anleitungen für den Betrieb
- Dimensionierung der Instanzen
- Arbeiten mit Indizes
- Bewährte Methoden für die Gewährleistung der Sicherheit
- Kostenoptimierung
- Verwendung von Metriken zur Identifizierung von Problemen mit der Leistung
- TTL- und Zeitreihen-Workloads
- Migrationen
- Arbeiten mit Cluster-Parametergruppen
- Abfragen in der Aggregationspipeline
- BatchInsert und BatchUpdate

Grundlegende Anleitungen für den Betrieb

Im Folgenden finden Sie grundlegende Betriebsrichtlinien, die jeder bei der Arbeit mit Amazon DocumentDB beachten sollte. Das Amazon DocumentDB Service Level Agreement verlangt, dass Sie diese Richtlinien befolgen.

- Stellen Sie einen Cluster bereit, der aus zwei oder mehr Amazon DocumentDB DocumentDB-Instances in zwei AWS Availability Zones besteht. Für Produktionsworkloads empfehlen wir die Bereitstellung eines Clusters, der aus drei oder mehr Amazon DocumentDB DocumentDB-Instances in drei Availability Zones besteht.
- Verwenden Sie die Services innerhalb der angegebenen Service Limits. Weitere Informationen finden Sie unter Amazon DocumentDB Kontingente und Beschränkungen.
- Überwachen Sie Speicher, CPU, Verbindungen und Speichernutzung. Um Sie bei der Aufrechterhaltung der Systemleistung und Verfügbarkeit CloudWatch zu unterstützen, richten Sie

Amazon so ein, dass Sie benachrichtigt werden, wenn sich die Nutzungsmuster ändern oder wenn Sie die Kapazität Ihrer Bereitstellung fast erreicht haben.

- Skalieren Sie Ihre Instances, wenn Sie die Grenzen der Speicherkapazität beinahe erreicht haben. Ihre Instances sollten mit genügend Rechenressourcen (d. h. RAM, CPU) ausgestattet sein, um Nachfragesteigerungen seitens Ihrer Anwendungen bewältigen zu können.
- Legen Sie die Aufbewahrungszeitraum für Backups so fest, dass sie zu Ihrem Wiederherstellungsziel passt.
- Testen Sie den Failover für Ihren Cluster, um zu verstehen, wie lange der Vorgang für Ihren Anwendungsfall dauert. Weitere Informationen finden Sie unter Amazon DocumentDB-Failover.
- Stellen Sie mit dem Cluster-Endpunkt (siheAmazon DocumentDB DocumentDB-Endpunkte) und im Replikatsatzmodus (siheAls Replikatsatz eine Verbindung zu Amazon DocumentDB herstellen) eine Connect zu Ihrem Amazon DocumentDB-Cluster her, um die Auswirkungen eines Failovers auf Ihre Anwendung zu minimieren.
- Wählen Sie eine Treibereinstellung für die Leseeinstellung aus, die die Leseskalierung maximiert und gleichzeitig die Anforderungen für die Lesekonsistenz Ihrer Anwendung erfüllt. Die Leseeinstellung `secondaryPreferred` ermöglicht Replica-Lesevorgänge, sodass die primäre Instance produktiver sein kann. Weitere Informationen finden Sie unter Lesen Sie die Einstellungsoptionen.
- Entwerfen Sie Ihre Anwendung so, dass Sie im Falle von Netzwerk- und Datenbankfehlern stabil ist. Unterscheiden Sie mithilfe des Fehlermechanismus des Treibers zwischen vorübergehenden Fehlern und persistenten Fehlern. Wiederholen Sie den Vorgang bei vorübergehenden Fehlern mit einem exponentiellen Backoff-Mechanismus (bei Bedarf). Stellen Sie sicher, dass Ihre Anwendung bei der Implementierung von Logik für Wiederholversuche die Datenkonsistenz berücksichtigt.
- Aktivieren Sie den Cluster-Löschschutz für alle Produktions-Cluster oder Cluster mit wertvollen Daten. Bevor Sie einen Amazon DocumentDB-Cluster löschen, erstellen Sie einen letzten Snapshot. Wenn Sie Ressourcen mit bereitstellen CloudFormation, aktivieren Sie den Kündigungsschutz. Weitere Informationen finden Sie unter Kündigungsschutz und Löschschutz.
- Bei der Erstellung eines Amazon DocumentDB-Clusters `--engine-version` ist dies ein optionaler Parameter, der standardmäßig die neueste Hauptversion der Engine verwendet. Die aktuelle Standard-Engine-Version ist 5.0.0 (Hinweis: Amazon DocumentDB 8.0 ist verfügbar, muss aber explizit angegeben werden). Wenn neue Hauptversionen der Engine veröffentlicht werden, `--engine-version` wird die Standard-Engine-Version für aktualisiert, sodass sie die letzte Hauptversion der Engine widerspiegelt. Daher empfehlen wir für Produktionsworkloads, insbesondere solche, die von Skripten, Automatisierung oder CloudFormation Vorlagen abhängig sind, die Angabe der `--engine-version` beabsichtigten Hauptversion ausdrücklich.

Dimensionierung der Instanzen

Einer der wichtigsten Aspekte bei der Auswahl einer Instance-Größe in Amazon DocumentDB ist die Größe des Arbeitsspeichers für Ihren Cache. Amazon DocumentDB reserviert ein Drittel des RAM für seine eigenen Dienste, was bedeutet, dass nur zwei Drittel des Instance-RAM für den Cache verfügbar sind. Daher ist es eine bewährte Methode von Amazon DocumentDB, einen Instance-Typ auszuwählen, der über ausreichend RAM verfügt, damit Ihr Arbeitssatz (d. h. Daten und Indizes) im Arbeitsspeicher Platz findet. Instances mit der richtigen Größe können Sie die Gesamtleistung optimieren und möglicherweise die Kosten minimieren I/O . Sie können den Amazon DocumentDB DocumentDB-Größenrechner eines Drittanbieters verwenden, um die Instance-Größe für einen bestimmten Workload zu schätzen.

Um festzustellen, ob das Working-Set Ihrer Anwendung in den Arbeitsspeicher passt, überwachen `BufferCacheHitRatio` Sie die Nutzung von Amazon CloudWatch für jede Instance in einem Cluster, die unter Last steht.

Die `BufferCacheHitRatio` CloudWatch Metrik misst den Prozentsatz der Daten und Indizes, die aus dem Speichercache einer Instance bereitgestellt werden (im Vergleich zum Speichervolumen). Im Allgemeinen sollte der Wert von `BufferCacheHitRatio` so hoch wie möglich sein, da das Lesen von Daten aus dem Arbeitssatz-Speicher schneller und kostengünstiger ist als das Lesen vom Speicher-Volume. Obwohl es wünschenswert ist, `BufferCacheHitRatio` möglichst nahe bei 100% zu halten, hängt der beste erreichbare Wert von den Zugriffsmustern und den Leistungsanforderungen Ihrer Anwendung ab. Um das höchstmögliche `BufferCacheHitRatio` beizubehalten, wird empfohlen, dass die Instances in Ihrem Cluster über ausreichend RAM verfügen, damit Ihre Indizes und Arbeitsdatensätze in den Speicher passen.

Wenn Ihre Indizes nicht in den Speicher passen, wird Ihnen ein niedrigeres `BufferCacheHitRatio` angezeigt. Kontinuierliches Lesen von der Festplatte verursacht zusätzliche I/O Kosten und ist nicht besser als das Lesen aus dem Arbeitsspeicher. Wenn Ihr `BufferCacheHitRatio`-Verhältnis niedriger als erwartet ist, skalieren Sie die Instance-Größe für Ihren Cluster, um mehr RAM zur Verfügung zu stellen, damit die Arbeitssatzdaten in den Speicher passen. Wenn das Skalieren der Instance-Klasse zu einem enormen Anstieg im `BufferCacheHitRatio` führt, passte der Arbeitssatz Ihrer Anwendung nicht in den Speicher. Skalieren Sie weiter, bis sich `BufferCacheHitRatio` nach einer Skalierungsoperation nicht mehr drastisch erhöht. Weitere Informationen zur Überwachung von Instance-Metriken finden Sie unter Amazon DocumentDB-Metriken.

Abhängig von Ihren Workload- und Latenzanforderungen kann es akzeptabel sein, dass Ihre Anwendung während der stabilen Zustandsnutzung höhere `BufferCacheHitRatio`-Werte aufweist, das `BufferCacheHitRatio` jedoch periodisch nachlässt, da analytische Abfragen, die eine gesamte Sammlung scannen müssen, auf einer Instance ausgeführt werden. Diese periodischen Einbrüche im `BufferCacheHitRatio` können sich als höhere Latenz für nachfolgende Abfragen manifestieren, die die Arbeitssatzdaten aus dem Speicher-Volume wieder in den Puffercache füllen müssen. Es wird empfohlen, Ihre Workloads zunächst in einer Vorproduktionsumgebung mit einem repräsentativen Produktions-Workload zu testen, um die Leistungsmerkmale und das **`BufferCacheHitRatio`** zu verstehen, bevor Sie den Workload für die Produktion bereitstellen.

Es handelt sich beim `BufferCacheHitRatio` um eine Instance-spezifische Metrik, daher können verschiedene Instances innerhalb desselben Clusters unterschiedliche `BufferCacheHitRatio`-Werte aufweisen, je nachdem, wie Lesevorgänge auf die Primär- und Replikat-Instances verteilt werden. Wenn Ihr betrieblicher Workload nicht mit periodischen Erhöhungen der Latenz durch erneutes Auffüllen des Arbeitssatzcache nach dem Ausführen analytischer Abfragen umgehen kann, sollten Sie versuchen, den Puffercache des regulären Workloads von dem der analytischen Abfragen zu isolieren. Sie können eine vollständige `BufferCacheHitRatio`-Isolation erreichen, indem Sie betriebliche Abfragen an die Primär-Instance und analytische Abfragen nur an die Replikat-Instances weiterleiten. Sie können auch eine partielle Isolation erreichen, indem Sie analytische Abfragen an eine bestimmte Replikat-Instance weiterleiten, mit dem Verständnis, dass ein gewisser Prozentsatz der regulären Abfragen auch auf diesem Replikat ausgeführt wird und möglicherweise betroffen sein könnte.

Angemessene `BufferCacheHitRatio`-Werte hängen von Ihrem Anwendungsfall und Ihren Anwendungsanforderungen ab. Es gibt keinen besten oder minimalen Wert für diese Metrik. Nur Sie können entscheiden, ob der Kompromiss von einem vorübergehend niedrigeren `BufferCacheHitRatio` aus Kosten- und Leistungsperspektive akzeptabel ist.

Arbeiten mit Indizes

Erstellen von Indizes

Wenn Sie Daten in Amazon DocumentDB importieren, sollten Sie Ihre Indizes erstellen, bevor Sie große Datensätze importieren. Sie können das Amazon DocumentDB Index Tool verwenden, um Indizes aus einer laufenden MongoDB-Instance oder einem `mongodump` Verzeichnis zu extrahieren und diese Indizes in einem Amazon DocumentDB-Cluster zu erstellen. Weitere Hinweise zu Migrationen finden Sie unter Migration zu Amazon DocumentDB.

Index-Selektivität

Wir empfehlen Ihnen, die Erstellung von Indizes auf Felder zu beschränken, bei denen die Anzahl der Duplikatwerte weniger als 1 % der Gesamtzahl der Dokumente in der Sammlung beträgt. Wenn Ihre Sammlung beispielsweise 100.000 Dokumente enthält, erstellen Sie Indizes nur für Felder, in denen derselbe Wert 1.000 Mal oder weniger vorkommt.

Die Wahl eines Index mit einer hohen Anzahl von eindeutigen Werten (d. h. einer hohen Kardinalität) gewährleistet, dass Filteroperationen eine geringe Anzahl von Dokumenten zurückgeben, wodurch eine gute Leistung während der Index-Scans erzielt wird. Ein Beispiel für einen Index hoher Kardinalität ist ein einzigartiger Index, der garantiert, dass Gleichheitsprädikate höchstens ein einziges Dokument zurückgeben. Beispiele für niedrige Kardinalität sind ein Index über ein boolesches Feld und ein Index über einen Wochentag. Aufgrund ihrer schlechten Leistung ist es unwahrscheinlich, dass der Abfragenoptimierer der Datenbank Indizes mit niedriger Kardinalität auswählt. Gleichzeitig verbrauchen Indizes mit niedriger Kardinalität weiterhin Ressourcen wie Festplattenspeicher und. I/Os Als Faustregel gilt, dass Sie Indizes für Felder verwenden sollten, bei denen die typische Wertehäufigkeit 1 % der Gesamtsammlungsgröße oder weniger beträgt.

Darüber hinaus wird empfohlen, nur Indizes für Felder zu erstellen, die häufig als Filter verwendet werden, und regelmäßig nach nicht verwendeten Indizes zu suchen. Weitere Informationen finden Sie unter Wie analysiere ich die Indexnutzung und identifiziere ungenutzte Indizes?.

Auswirkung von Indizes auf das Schreiben von Daten

Zwar können Indizes die Abfrageleistung verbessern, da nicht jedes Dokument in einer Sammlung gescannt werden muss, diese Verbesserung erfordert jedoch einen Kompromiss. Für jeden Index einer Sammlung muss die Datenbank jedes Mal, wenn ein Dokument eingefügt, aktualisiert oder gelöscht wird, die Sammlung aktualisieren und die Felder in jeden der Indizes für die Sammlung schreiben. Wenn eine Sammlung beispielsweise über neun Indizes verfügt, muss die Datenbank zehn Schreibvorgänge durchführen, bevor die Operation dem Kunden bestätigt wird. Somit führt jeder zusätzliche Index zu zusätzlicher Schreiblatenz und zu einer Erhöhung des insgesamt genutzten I/O Speichers.

Cluster-Instances müssen über eine angemessene Größe verfügen, um den gesamten Arbeitsspeicher zu erhalten. Dadurch wird vermieden, dass Indexseiten kontinuierlich vom Speichervolumen gelesen werden müssen, was sich negativ auf die Leistung auswirkt und höhere I/O Kosten verursacht. Weitere Informationen finden Sie unter Dimensionierung der Instanzen.

Um eine optimale Leistung zu erzielen, sollten Sie die Anzahl der Indizes in Ihren Sammlungen minimieren und nur die Indizes hinzufügen, die zur Verbesserung der Leistung bei häufigen Abfragen erforderlich sind. Bei variierenden Workloads gilt als gute Richtschnur, die Anzahl der Indizes pro Sammlung auf fünf oder weniger zu beschränken.

Identifizierung fehlender Indizes

Die Identifizierung fehlender Indizes ist eine bewährte Methode, die wir empfehlen, regelmäßig durchzuführen. Weitere Informationen finden Sie unter Wie identifiziere ich fehlende Indizes?.

Identifizieren ungenutzter Indizes

Da das Identifizieren und Löschen fehlender Indizes eine bewährte Vorgehensweise ist, empfiehlt sich eine regelmäßige Durchführung. Weitere Informationen finden Sie unter Wie analysiere ich die Indexnutzung und identifiziere ungenutzte Indizes?.

Bewährte Methoden für die Gewährleistung der Sicherheit

Aus Sicherheitsgründen müssen Sie AWS Identity and Access Management (IAM-) Konten verwenden, um den Zugriff auf Amazon DocumentDB DocumentDB-API-Operationen zu kontrollieren, insbesondere Operationen, die Amazon DocumentDB DocumentDB-Ressourcen erstellen, ändern oder löschen. Zu solchen Ressourcen gehören Cluster, Sicherheitsgruppen und Parametergruppen. Sie müssen IAM auch zur Steuerung von Aktionen verwenden, mit denen allgemeine Verwaltungsaktionen wie das Sichern und Wiederherstellen von Clustern ausgeführt werden. Verwenden Sie bei der Erstellung von IAM-Rollen das Prinzip der geringsten Rechte.

- Erzwingen Sie die geringste Berechtigung mit rollenbasierter Zugriffssteuerung.
- Weisen Sie jeder Person, die Amazon DocumentDB DocumentDB-Ressourcen verwaltet, ein individuelles IAM-Konto zu. Verwenden Sie den AWS-Konto Root-Benutzer nicht zur Verwaltung von Amazon DocumentDB DocumentDB-Ressourcen. Erstellen Sie einen IAM-Benutzer für jede Person einschließlich Sie selbst.
- Erteilen Sie jedem IAM-Benutzer die Mindestberechtigungen, die zur Erfüllung seiner Aufgaben erforderlich sind.
- Verwenden Sie IAM-Gruppen, um Berechtigungen für mehrere Benutzer effektiv zu verwalten. Weitere Informationen zu IAM finden Sie im IAM-Benutzerhandbuch. Weitere Informationen zu bewährten Methoden für IAM finden Sie unter Bewährte Methoden für IAM.

- Wechseln Sie regelmäßig die IAM-Anmeldeinformationen.
- Konfigurieren Sie AWS Secrets Manager so, dass die Secrets für Amazon DocumentDB automatisch rotiert werden. Weitere Informationen finden Sie unter Rotating Your AWS Secrets Manager Secrets und Rotating Secrets for Amazon DocumentDB im AWS Secrets Manager User Guide.
- Erteilen Sie jedem Amazon DocumentDB DocumentDB-Benutzer die Mindestberechtigungen, die zur Erfüllung seiner Aufgaben erforderlich sind. Weitere Informationen finden Sie unter Datenbankzugriff mit Role-Based Access Control.
- Verwenden Sie Transport Layer Security (TLS), um Ihre Daten bei der Übertragung und AWS KMS um Ihre Daten im Ruhezustand zu verschlüsseln.

Kostenoptimierung

Die folgenden bewährten Methoden können Ihnen helfen, Ihre Kosten bei der Verwendung von Amazon DocumentDB zu verwalten und zu minimieren. Preisinformationen finden Sie unter Preise für Amazon DocumentDB (mit MongoDB-Kompatibilität) und häufig gestellte Fragen zu Amazon DocumentDB (mit MongoDB-Kompatibilität).

- Erstellen Sie Gebührenlimit-Warnungen für Schwellenwerte von 50 Prozent und 75 Prozent Ihrer erwarteten Rechnung für den Monat. Weitere Informationen zum Erstellen von Gebührenlimit-Warnungen finden Sie unter Erstellen einer Gebührenlimit-Warnung.
- Die Architektur von Amazon DocumentDB trennt Speicher und Rechenleistung, sodass selbst ein Single-Instance-Cluster äußerst robust ist. Das Cluster-Speicher-Volume repliziert Daten auf sechs Arten in drei Availability Zones und bietet unabhängig von der Anzahl der Instances im Cluster eine extrem hohe Beständigkeit. Ein typischer Produktions-Cluster verfügt über mindestens drei Instances, um eine hohe Verfügbarkeit bereitzustellen. Sie können jedoch die Kosten optimieren, indem Sie einen einzelnen Instance-Entwicklungs-Cluster verwenden, wenn keine hohe Verfügbarkeit erforderlich ist.
- Halten Sie bei Entwicklungs- und Testszenarien einen Cluster an, wenn er nicht mehr benötigt wird, und starten Sie den Cluster, wenn die Entwicklung fortgesetzt wird. Weitere Informationen finden Sie unter Einen Amazon DocumentDB-Cluster stoppen und starten.
- Sowohl TTL- als auch Change-Streams entstehen I/O, wenn Daten geschrieben, gelesen und gelöscht werden. Wenn Sie diese Funktionen aktiviert haben, sie aber in Ihrer Anwendung nicht nutzen, kann die Deaktivierung der Funktionen zur Kostensenkung beitragen.

Verwendung von Metriken zur Identifizierung von Problemen mit der Leistung

Themen

- Anzeigen von Leistungsmetriken
- Einen CloudWatch Alarm einrichten
- Auswerten von Leistungsmetriken
- Auswertung der Nutzung von Amazon DocumentDB DocumentDB-Instances anhand von Metriken CloudWatch
- Optimieren von Abfragen

Um Leistungsprobleme zu identifizieren, die durch unzureichende Ressourcen und andere häufige Engpässe verursacht werden, können Sie die für Ihren Amazon DocumentDB-Cluster verfügbaren Metriken überwachen.

Anzeigen von Leistungsmetriken

Überwachen Sie die Leistungsmetriken regelmäßig, um die Durchschnitts-, Höchst- und Mindestwerte für verschiedene Zeitbereiche anzuzeigen. Auf diese Weise können Sie feststellen, wenn die Leistung nachlässt. Sie können CloudWatch Amazon-Alarme auch für bestimmte Metrik-Schwellenwerte einrichten, sodass Sie benachrichtigt werden, wenn diese erreicht werden.

Um Probleme mit der Leistung zu beheben, müssen Sie die Basisleistung des Systems kennen. Nachdem Sie einen neuen Cluster eingerichtet haben und er mit einer typischen Workload ausgeführt wird, erfassen Sie die Durchschnitts-, Höchst- und Mindestwerte aller Leistungsmetriken in unterschiedlichen Intervallen (z. B. 1 Stunde, 24 Stunden, 1 Woche, 2 Wochen). Auf diese Weise erhalten Sie eine Vorstellung davon, was normal ist. Dies hilft, um Vergleichswerte für Betriebsstunden während und außerhalb von Spitzenbelastungen zu erhalten. Sie können diese Informationen anschließend verwenden, um festzustellen, wann die Leistung unter Standardwerte absinkt.

Sie können Leistungskennzahlen mit dem AWS-Managementkonsole oder anzeigen. AWS CLI Weitere Informationen finden Sie unter CloudWatch Daten anzeigen.

Einen CloudWatch Alarm einrichten

Informationen zum Einstellen eines CloudWatch Alarms finden Sie unter Verwenden von Amazon CloudWatch Alarms im CloudWatch Amazon-Benutzerhandbuch.

Auswerten von Leistungsmetriken

Eine Instance besitzt mehrere unterschiedliche Kategorien von Metriken. Die Art und Weise, wie Sie bestimmen, welche Werte akzeptabel sind, ist von der Metrik abhängig.

CPU

- CPU-Auslastung — Der Prozentsatz der verwendeten Computerverarbeitungskapazität.

Arbeitsspeicher

- Freier Arbeitsspeicher — Wie viel RAM ist auf der Instance verfügbar.
- Swap-Nutzung — Wie viel Swap-Speicherplatz von der Instance verwendet wird, in Megabyte.

Input/output Operationen

- Lese-IOPS, Schreib-IOPS — Die durchschnittliche Anzahl von Festplatten-Lese- oder Schreibvorgängen pro Sekunde.
- Leselatenz, Schreiblatenz — Die durchschnittliche Zeit für einen Lese- oder Schreibvorgang in Millisekunden.
- Lesedurchsatz, Schreibdurchsatz — Die durchschnittliche Anzahl von Megabyte, die pro Sekunde von der Festplatte gelesen oder auf die Festplatte geschrieben werden.
- Tiefe der Festplattenwarteschlange — Die Anzahl der I/O Vorgänge, die darauf warten, auf die Festplatte geschrieben oder von der Festplatte gelesen zu werden.

Netzwerkdatenverkehr

- Netzwerkempfangsdurchsatz, Netzwerkübertragungsdurchsatz — Die Rate des Netzwerkverkehrs zur und von der Instance in Megabyte pro Sekunde.

Datenbankverbindungen

- DB-Verbindungen — Die Anzahl der Client-Sitzungen, die mit der Instance verbunden sind.

Allgemein ausgedrückt, sind die zulässigen Werte für Leistungsmetriken davon abhängig, wie die Basisleistung aussieht und welche Aufgaben von Ihrer Anwendung ausgeführt werden. Prüfen Sie, ob dauerhafte oder tendenzielle Abweichungen von Ihrer Ausgangsbasis vorliegen.

Nachstehend folgen Empfehlungen und Ratschläge zu bestimmten Arten von Metriken:

- Hoher CPU-Verbrauch — Hohe Werte für die CPU-Auslastung können angemessen sein, vorausgesetzt, sie entsprechen Ihren Zielen für Ihre Anwendung (wie Durchsatz oder Parallelität) und werden erwartet. Wenn die CPU-Auslastung konsistent mehr als 80 Prozent beträgt, sollten Sie eine Aufwärtsskalierung Ihrer Instances in Betracht ziehen.
- Hoher RAM-Verbrauch — Wenn Ihre `FreeableMemory` Kennzahl häufig unter 10% des gesamten Instance-Speichers fällt, sollten Sie eine Skalierung Ihrer Instances in Betracht ziehen. Weitere Informationen darüber, was passiert, wenn Ihre DocumentDB-Instance einer hohen Speicherauslastung ausgesetzt ist, finden Sie unter Amazon DocumentDB Resource Governance.
- Swap-Nutzung — Diese Metrik sollte bei oder nahe Null bleiben. Wenn die Swap-Nutzung erheblich ist, sollten Sie eine Aufwärtsskalierung Ihrer Instances in Betracht ziehen.
- Netzwerkverkehr — Wenden Sie sich bezüglich des Netzwerkverkehrs an Ihren Systemadministrator, um zu erfahren, wie hoch der zu erwartende Durchsatz für Ihr Domänennetzwerk und Ihre Internetverbindung ist. Überprüfen Sie den Netzwerkdatenverkehr, wenn der Durchsatz dauerhaft unter dem erwarteten Wert liegt.
- Datenbankverbindungen — Erwägen Sie, Datenbankverbindungen einzuschränken, wenn Sie eine hohe Anzahl von Benutzerverbindungen zusammen mit einer Verringerung der Instanzleistung und Reaktionszeit feststellen. Die optimale Anzahl der Benutzerverbindungen für Ihre Instance ist von der Instance-Klasse und der Komplexität der ausgeführten Operationen abhängig. Bei Problemen mit Leistungsmetriken sollten Sie zunächst die am häufigsten verwendeten und kostspieligsten Abfragen anpassen, um festzustellen, ob dies den Druck auf die Systemressourcen verringert und die Leistung verbessert.

Wenn Ihre Abfragen optimiert sind und ein Problem weiterhin besteht, sollten Sie erwägen, Ihre Amazon DocumentDB DocumentDB-Instance-Klasse auf eine Klasse mit mehr Ressourcen (CPU, RAM, Festplattenspeicher, Netzwerkbandbreite, I/O Kapazität) zu aktualisieren, die mit dem aufgetretenen Problem zusammenhängt.

Auswertung der Nutzung von Amazon DocumentDB DocumentDB-Instances anhand von Metriken CloudWatch

Mithilfe von CloudWatch Metriken können Sie Ihren Instance-Durchsatz beobachten und herausfinden, ob Ihre Instance-Klasse ausreichend Ressourcen für Ihre Anwendungen bereitstellt. Informationen zu Ihren Instance-Klassenlimits finden Sie in den Spezifikationen für Ihre Instance-Klasse, um Ihre Netzwerkleistung zu ermitteln. Instance-Limits

Wenn Ihre Instance-Nutzung nahe dem Instance-Klassenlimit liegt, kann es sein, dass sich die Leistung verlangsamt. Die CloudWatch Metriken können diese Situation bestätigen, sodass Sie planen können, manuell auf eine größere Instance-Klasse hochzuskalieren.

Kombinieren Sie die folgenden CloudWatch Metrikwerte, um herauszufinden, ob Sie sich dem Instance-Klassenlimit nähern:

- NetworkThroughput— Die Menge des Netzwerkdurchsatzes, der von den Clients für jede Instance im Amazon DocumentDB-Cluster empfangen und übertragen wird. Dieser Durchsatzwert beinhaltet nicht den Netzwerkverkehr zwischen Instances im Cluster und dem Cluster-Speichervolumen.
- StorageNetworkThroughput— Die Menge des Netzwerkdurchsatzes, der von jeder Instance im Amazon DocumentDB-Cluster empfangen und an das Amazon DocumentDB-Cluster-Speichervolumen gesendet wurde.

Fügen Sie den hinzu NetworkThroughput, um den Netzwerkdurchsatz StorageNetworkThroughputzu ermitteln, der von jeder Instance in Ihrem Amazon DocumentDB-Cluster vom Amazon DocumentDB-Cluster empfangen und an das Amazon DocumentDB-Cluster gesendet wurde. Das Instance-Klassenlimit für Ihre Instance sollte größer sein als die Summe dieser beiden kombinierten Metriken.

Sie können die folgenden Metriken verwenden, um zusätzliche Details des Netzwerkverkehrs Ihrer Client-Anwendungen beim Senden und Empfangen zu überprüfen:

- NetworkReceiveThroughput— Die Menge des Netzwerkdurchsatzes, den jede Instance im Amazon DocumentDB-Cluster von Clients erhält. Dieser Durchsatz beinhaltet nicht den Netzwerkverkehr zwischen Instances im Cluster und dem Cluster-Speichervolumen.
- NetworkTransmitThroughput— Die Menge des Netzwerkdurchsatzes, der von jeder Instance im Amazon DocumentDB-Cluster an Clients gesendet wird. Dieser Durchsatz beinhaltet nicht den Netzwerkverkehr zwischen Instances im Cluster und dem Cluster-Speichervolumen.

- StorageNetworkReceiveThroughput— Die Menge des Netzwerkdurchsatzes, den jede Instance im Cluster vom Amazon DocumentDB-Cluster-Speichervolumen erhält.
- StorageNetworkTransmitThroughput— Die Menge des Netzwerkdurchsatzes, der von jeder Instance im Cluster an das Amazon DocumentDB-Cluster-Speichervolume gesendet wird.

Addieren Sie all diese Metriken, um zu bewerten, wie Ihre Netzwerknutzung im Vergleich zum Instance-Klassenlimit abschneidet. Das Instance-Klassenlimit sollte größer sein als die Summe dieser kombinierten Metriken.

Die Netzwerklimits und die CPU-Auslastung einer Instance sind wechselseitig. Wenn der Netzwerkdurchsatz steigt, steigt auch die CPU-Auslastung. Die Überwachung der CPU- und Netzwerknutzung gibt Aufschluss darüber, wie und warum die Ressourcen erschöpft werden.

Sie können Folgendes in Betracht ziehen, um die Netzwerknutzung zu minimieren:

- Verwenden einer größeren Instance-Klasse
- Aufteilen der Schreibanforderungen in Batches, um die Gesamttransaktionen zu reduzieren
- Weiterleiten der schreibgeschützten Workload an eine schreibgeschützte Instance
- Löschen aller ungenutzten Indizes

Optimieren von Abfragen

Eine der besten Möglichkeiten zur Verbesserung der Cluster-Leistung besteht darin, die am häufigsten verwendeten und ressourcenintensivsten Abfragen so anzupassen, dass ihre Ausführung weniger aufwändig wird.

Mit dem Profiler (siehe Profilierung von Amazon DocumentDB DocumentDB-Vorgängen) können Sie die Ausführungszeit und Details der Vorgänge protokollieren, die für Ihren Cluster ausgeführt wurden. Profiler ist nützlich für die Überwachung der langsamsten Operationen in Ihrem Cluster, um die Leistung einzelner Abfragen und die allgemeine Cluster-Leistung zu verbessern.

Sie können den Befehl `explain` auch verwenden, um zu erfahren, wie ein Abfrageplan für eine bestimmte Abfrage analysiert wird. Mithilfe dieser Informationen können Sie eine Abfrage oder zugrundeliegende Sammlung ändern, um die Abfrageleistung zu verbessern (z. B. Hinzufügen eines Indexes).

TTL- und Zeitreihen-Workloads

Das Löschen von Dokumenten, das aus dem Ablauf des TTL-Index resultiert, ist ein hochaufwendiges Verfahren. Es wird nicht garantiert, dass Dokumente innerhalb eines bestimmten Zeitraums gelöscht werden. Faktoren wie die Größe der Instance, die Ressourcenauslastung der Instance, die Dokumentgröße, der Gesamtdurchsatz, die Anzahl der Indizes und die Frage, ob die Indizes und der Arbeitssatz in den Speicher passen, können den Zeitpunkt beeinflussen, zu dem abgelaufene Dokumente durch den TTL-Prozess gelöscht werden.

Wenn der TTL-Monitor Ihre Dokumente löscht, fallen bei jedem Löschen I/O Kosten an, was Ihre Rechnung erhöht. Wenn der Durchsatz und die TTL-Löschraten steigen, sollten Sie aufgrund der erhöhten Nutzung mit einer höheren Rechnung rechnen. I/O Wenn Sie jedoch keinen TTL-Index zum Löschen von Dokumenten erstellen, sondern Dokumente anhand der Zeit in Sammlungen unterteilen und diese Sammlungen einfach löschen, wenn sie nicht mehr benötigt werden, fallen Ihnen keine I/O-Kosten an. Dies kann erheblich kostengünstiger sein als die Verwendung eines TTL-Index.

Für Zeitreihen-Workloads können Sie erwägen, statt eines TTL-Index fortlaufende Sammlungen zu erstellen, da rollierende Sammlungen eine bessere und weniger aufwändige Methode zum Löschen von Daten sein können. I/O Wenn Sie über große Sammlungen verfügen (insbesondere Sammlungen mit mehr als 1 TB) oder wenn die I/O Kosten für das Löschen von TTL ein Problem darstellen, empfehlen wir, Dokumente nach Zeit in Sammlungen zu partitionieren und Sammlungen zu löschen, wenn die Dokumente nicht mehr benötigt werden. Sie können eine Sammlung pro Tag oder eine Sammlung pro Woche erstellen, abhängig von der Datenaufnahmerate. Bei je nach Anwendung variierenden Anforderungen gilt als gute Faustregel, besser über mehr kleinere Sammlungen als über einige große Sammlungen zu verfügen. Das Löschen dieser Sammlungen verursacht keine I/O Kosten und kann schneller und kostengünstiger sein als die Verwendung eines TTL-Index.

Migrationen

Als bewährte Methode empfehlen wir, dass Sie bei der Migration von Daten zu Amazon DocumentDB zuerst Ihre Indizes in Amazon DocumentDB erstellen, bevor Sie die Daten migrieren. Indizes zuerst zu erstellen, kann die Gesamtzeit verkürzen und die Geschwindigkeit der Migration erhöhen. Dazu können Sie das Amazon DocumentDB Index Tool verwenden. Weitere Informationen zu Migrationen finden Sie im Amazon DocumentDB-Migrationsleitfaden.

Wir empfehlen außerdem, Ihre Anwendung vor der Migration Ihrer Produktionsdatenbank vollständig auf Amazon DocumentDB zu testen und dabei Funktionalität, Leistung, Betrieb und Kosten zu berücksichtigen.

Arbeiten mit Cluster-Parametergruppen

Es wird empfohlen, Änderungen an Cluster-Parametergruppen zuerst an einem Test-Cluster auszuprobieren, bevor Sie die Änderungen auf Ihre Produktions-Cluster anwenden. Weitere Informationen zum Sichern Ihres Clusters finden Sie unter Sichern und Wiederherstellen in Amazon DocumentDB.

Abfragen in der Aggregationspipeline

Wenn Sie eine Aggregation-Pipeline-Abfrage mit mehreren Stufen erstellen und nur eine Teilmenge der Daten in der Abfrage auswerten, verwenden Sie die `$match`-Stufe als erste Stufe oder am Anfang der Pipeline. Wenn Sie `$match` zuerst verwenden, wird die Anzahl der Dokumente reduziert, die nachfolgende Stufen innerhalb der Aggregation-Pipeline-Abfrage verarbeiten müssen, wodurch die Leistung Ihrer Abfrage verbessert wird.

`BatchInsert und BatchUpdate`

Wenn Sie eine hohe Anzahl gleichzeitiger `batchInsert` and/or `batchUpdate` Operationen ausführen und die Anzahl von `FreeableMemory` (CloudWatch Metric) auf Ihrer primären Instance auf Null sinkt, können Sie entweder die Parallelität der Batch-Insert- oder Aktualisierungs-Workloads reduzieren oder, falls die Parallelität der Workload nicht reduziert werden kann, die Instance-Größe erhöhen, um die Menge von zu erhöhen. `FreeableMemory`

Funktionale Unterschiede: Amazon DocumentDB und MongoDB

Im Folgenden sind die funktionalen Unterschiede zwischen Amazon DocumentDB (mit MongoDB-Kompatibilität) und MongoDB aufgeführt.

Themen

- Funktionale Vorteile von Amazon DocumentDB
- Funktionelle Unterschiede wurden aktualisiert
- Funktionale Unterschiede zu MongoDB

Funktionale Vorteile von Amazon DocumentDB

Implizite Transaktionen

In Amazon DocumentDB garantieren alle CRUD-Anweisungen (`findAndModify`,, `updateinsert`,`delete`) Atomarität und Konsistenz, selbst für Operationen, die mehrere Dokumente ändern. Mit der Einführung von Amazon DocumentDB 4.0 werden jetzt explizite Transaktionen unterstützt, die ACID-Eigenschaften für Operationen mit mehreren Anweisungen und mehreren Sammlungen bereitstellen. Weitere Informationen zur Verwendung von Transaktionen in Amazon DocumentDB finden Sie unterTransaktionen in Amazon DocumentDB.

Im Folgenden finden Sie Beispiele für Operationen in Amazon DocumentDB, bei denen mehrere Dokumente geändert werden, die sowohl atomares als auch konsistentes Verhalten erfüllen.

```
db.miles.update(
    { "credit_card": { $eq: true } },
    { $mul: { "flight_miles.$[]": NumberInt(2) } },
    { multi: true }
)
```

```
db.miles.updateMany(
    { "credit_card": { $eq: true } },
    { $mul: { "flight_miles.$[]": NumberInt(2) } }
)
```

```
db.runCommand({
  update: "miles",
  updates: [
    {
      q: { "credit_card": { $eq: true } },
      u: { $mul: { "flight_miles.$[]": NumberInt(2) } },
      multi: true
    }
  ]
})
```

```
db.products.deleteMany({
  "cost": { $gt: 30.00 }
})
```

```
db.runCommand({
  delete: "products",
  deletes: [{ q: { "cost": { $gt: 30.00 } }, limit: 0 }]
})
```

Die einzelnen Operationen, aus denen die Massenoperationen bestehen, wie `updateMany` und `deleteMany`, sind atomar, aber die Gesamtheit der Massenoperation ist nicht atomar. Zum Beispiel ist die Gesamtheit der `insertMany`-Operation atomar, wenn die einzelnen Einfügeoperationen erfolgreich ohne Fehler ausgeführt werden. Wenn bei einer `insertMany` Operation ein Fehler auftritt, wird jede einzelne Insert-Anweisung innerhalb der `insertMany` Operation als atomare Operation ausgeführt. Wenn Sie ACID-Eigenschaften für `insertManyupdateMany`, und `deleteMany` -Operationen benötigen, wird empfohlen, eine Transaktion zu verwenden.

Funktionelle Unterschiede wurden aktualisiert

Amazon DocumentDB verbessert weiterhin die Kompatibilität mit MongoDB, indem es von den Funktionen, die unsere Kunden uns in Auftrag gegeben haben, abweicht. Dieser Abschnitt enthält die funktionalen Unterschiede, die wir in Amazon DocumentDB entfernt haben, um unseren Kunden Migrationen und die Erstellung von Anwendungen zu erleichtern.

Themen

- Array-Indizierung
- Multi-key Indizes
- Nullzeichen in Zeichenketten
- Role-based Zugriffskontrolle
- $regex-Indizierung
- Projektion für verschachtelte Dokumente

Array-Indizierung

Seit dem 23. April 2020 unterstützt Amazon DocumentDB jetzt die Möglichkeit, Arrays zu indizieren, die größer als 2.048 Byte sind. Das Limit für ein einzelnes Element in einem Array bleibt weiterhin bei 2.048 Byte, was mit MongoDB konsistent ist.

Beim Erstellen eines neuen Index sind keine Maßnahmen erforderlich, um die Vorteile der verbesserten Funktionalität zu nutzen. Wenn Sie über einen vorhandenen Index verfügen, können Sie die verbesserte Funktionalität nutzen, indem Sie den Index löschen und anschließend neu erstellen. Die aktuelle Index-Version mit den verbesserten Fähigkeiten lautet `"v" : 3`.

> **Note**
>
> Bei Produktions-Clustern kann das Entfernen des Index Auswirkungen auf Ihre Anwendungsleistung haben. Wir empfehlen Ihnen, bei Änderungen an einem Produktionssystem zunächst Tests durchzuführen und dann mit Bedacht weiter vorzugehen. Darüber hinaus hängt die Zeit, die für die Neuerstellung des Index benötigt wird, von der Gesamtdatengröße der Sammlung ab.

Mit folgendem Befehl können Sie die Version Ihrer Indizes abfragen.

```
db.collection.getIndexes()
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus. In dieser Ausgabe ist die Indexversion `"v" : 3`, die die aktuellste Indexversion ist.

```
[
```

```
    {
        "v" : 3,
        "key" : {
        "_id" : 1
        },
        "name" : "_id_",
        "ns" : "test.test"
    }
]
```

Multi-key Indizes

Seit dem 23. April 2020 unterstützt Amazon DocumentDB jetzt die Möglichkeit, einen zusammengesetzten Index mit mehreren Schlüsseln im selben Array zu erstellen.

Beim Erstellen eines neuen Index sind keine Maßnahmen erforderlich, um die Vorteile der verbesserten Funktionalität zu nutzen. Wenn Sie über einen vorhandenen Index verfügen, können Sie die verbesserte Funktionalität nutzen, indem Sie den Index löschen und anschließend neu erstellen. Die aktuelle Index-Version mit den verbesserten Fähigkeiten lautet `"v" : 3`.

> **Note**
>
> Bei Produktions-Clustern kann das Entfernen des Index Auswirkungen auf Ihre Anwendungsleistung haben. Wir empfehlen Ihnen, bei Änderungen an einem Produktionssystem zunächst Tests durchzuführen und dann mit Bedacht weiter vorzugehen. Darüber hinaus hängt die Zeit, die für die Neuerstellung des Index benötigt wird, von der Gesamtdatengröße der Sammlung ab.

Mit folgendem Befehl können Sie die Version Ihrer Indizes abfragen.

```
db.collection.getIndexes()
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus. In dieser Ausgabe ist die Indexversion `"v" : 3`, die die aktuellste Indexversion ist.

```
[
    {
        "v" : 3,
```

```
        "key" : {
            "_id" : 1
        },
        "name" : "_id_",
        "ns" : "test.test"
    }
]
```

Nullzeichen in Zeichenketten

Seit dem 22. Juni 2020 unterstützt Amazon DocumentDB jetzt Nullzeichen (`'\0'`) in Zeichenketten.

Role-based Zugriffskontrolle

Seit dem 26. März 2020 unterstützt Amazon DocumentDB die rollenbasierte Zugriffskontrolle (RBAC) für integrierte Rollen. Weitere Informationen hierzu finden Sie unter Role-Based Zugriffskontrolle.

`$regex`-Indizierung

Seit dem 22. Juni 2020 unterstützt Amazon DocumentDB nun die Möglichkeit für `$regex` Betreiber, einen Index zu verwenden.

Um einen Index mit dem `$regex`-Operator zu nutzen, müssen Sie den `hint()`-Befehl verwenden. Bei der Verwendung von `hint()` müssen Sie den Namen des Feldes angeben, auf dem Sie `$regex` anwenden möchten. Wenn Sie beispielsweise einen Index für Feld `product` mit dem Indexnamen `p_1` haben, nutzt `db.foo.find({product: /^x.*/}).hint({product:1})` den `p_1`-Index, aber `db.foo.find({product: /^x.*/}).hint("p_1")` nutzt den Index nicht. Sie können mit dem `explain()`-Befehl überprüfen, ob ein Index ausgewählt wird, oder indem Sie den Profiler zum Protokollieren langsamer Abfragen verwenden. Beispiel, `db.foo.find({product: /^x.*/}).hint("p_1").explain()`.

> **Note**
>
> Die `hint()`-Methode kann nur mit jeweils einem Index verwendet werden.

Die Verwendung eines Index für eine `$regex`-Abfrage ist für regex-Abfragen optimiert, die ein Präfix verwenden und bei denen die regex-Optionen `i`, `m` oder `o` nicht angegeben werden.

Wenn Sie einen Index mit `$regex` verwenden, wird empfohlen, einen Index für hoch selektive Felder zu erstellen, bei denen die Anzahl der doppelten Werte weniger als 1 % der Gesamtzahl der Dokumente in der Sammlung beträgt. Wenn Ihre Sammlung beispielsweise 100.000 Dokumente enthält, erstellen Sie Indizes nur für Felder, in denen derselbe Wert 1.000 Mal oder weniger vorkommt.

Projektion für verschachtelte Dokumente

Es gibt einen funktionalen Unterschied zwischen Amazon DocumentDB und MongoDB in Version 3.6, der in Amazon DocumentDB 4.0 behoben wurde, aber in Amazon DocumentDB 3.6 weiterhin nicht unterstützt wird. `$project`

Amazon DocumentDB 3.6 berücksichtigt bei der Anwendung einer Projektion nur das erste Feld in einem verschachtelten Dokument, wohingegen MongoDB 3.6 Unterdokumente analysiert und die Projektion auch auf jedes Unterdokument anwendet.

Beispiel: Wenn die Projektion ist`"a.b.c": 1`, dann funktioniert das Verhalten sowohl in Amazon DocumentDB als auch in MongoDB erwartungsgemäß. Wenn die Projektion jedoch `{a:{b:{c:1}}}` dann ist, wendet Amazon DocumentDB 3.6 die Projektion nur auf an `a` und nicht auf `b` oder`c`. In Amazon DocumentDB 4.0 `{a:{b:{c:1}}}` wird die Projektion auf `ab`, und `c` angewendet.

Funktionale Unterschiede zu MongoDB

Themen

- $ VectorSearch-Operator
- OpCountersCommand
- Admin-Datenbanken und Sammlungen
- CursorMaxTimeMS
- explain()
- Der Index wird erstellt
- Suche mit leerem Schlüssel im Pfad
- MongoDB-APIs, Operationen und Datentypen
- Dienstprogramme mongodump und mongorestore
- Reihenfolge der Ergebnisse

- Wiederholbare Schreibvorgänge
- Sparse Index
- Verwenden von $elemMatch innerhalb eines $all-Ausdrucks
- Dollar ($) und Punkt (.) in Feldnamen
- $lookup
- $natural und umgekehrte Sortierung

$ VectorSearch-Operator

Amazon DocumentDB unterstützt nicht `$vectorSearch` als unabhängiger Betreiber. Stattdessen unterstützen wir `vectorSearch` innerhalb des `$search` Betreibers. Weitere Informationen finden Sie unter Vektorsuche für Amazon DocumentDB.

OpCountersCommand

Das `OpCountersCommand` Verhalten von Amazon DocumentDB unterscheidet sich wie folgt von MongoDB: `opcounters.command`

- MongoDB `opcounters.command` zählt alle Befehle außer Einfügen, Aktualisieren und Löschen, während Amazon DocumentDB den Befehl `OpCountersCommand` ebenfalls ausschließt. `find`
- Amazon DocumentDB zählt einige interne Befehle zu. `OpCountersCommand`

Admin-Datenbanken und Sammlungen

Amazon DocumentDB unterstützt weder die Admin- oder lokale Datenbank noch MongoDB `system.*` bzw. `startup_log` Sammlungen.

CursorMaxTimeMS

`cursor.maxTimeMS`Setzt in Amazon DocumentDB den Zähler für jede `getMore` Anfrage zurück. Wenn also ein Wert von 3000 MS angegeben `maxTimeMS` ist, die Abfrage 2800 MS und jede nachfolgende `getMore` Anforderung 300 MS benötigt, wird der Cursor kein Timeout haben. Für den Cursor wird nur ein Timeout ausgeführt, wenn eine einzelne Operation, entweder die Abfrage oder eine einzelne `getMore` Anfrage, länger dauert als angegeben. `maxTimeMS` Außerdem läuft der Sweeper, der die Cursor-Ausführungszeit überprüft, mit einer Granularität von fünf (5) Minuten.

explain()

Amazon DocumentDB emuliert die MongoDB-APIs 3.6, 4.0, 5.0 und 8.0 auf einer speziell entwickelten Datenbank-Engine, die ein verteiltes, fehlertolerantes, selbstheilendes Speichersystem verwendet. Daher `explain()` können sich die Abfragepläne und die Ausgabe von zwischen Amazon DocumentDB und MongoDB unterscheiden. Kunden, die die Kontrolle über ihren Abfrageplan wünschen, können den `$hint`-Operator verwenden, um die Auswahl eines bevorzugten Indexes zu erzwingen.

Der Index wird erstellt

Amazon DocumentDB lässt zu, dass jeweils nur ein Index für eine Sammlung erstellt wird. Entweder im Vordergrund oder im Hintergrund. Wenn Vorgänge wie `createIndex()` oder `dropIndex()` für dieselbe Sammlung auftreten, wenn gerade ein Index erstellt wird,, schlägt der neu versuchte Vorgang fehl.

Standardmäßig werden Index-Builds in Amazon DocumentDB und MongoDB Version 4.0 im Vordergrund ausgeführt. MongoDB Version 4.2 und höher ignoriert die Option zum Erstellen des Hintergrundindexes, wenn sie für createIndexes oder seine Shell-Helfer und angegeben wurde. `createIndex()` `createIndexes()`

Bei einem Time to Live (TTL) -Index laufen Dokumente ab, nachdem die Indexerstellung abgeschlossen ist.

Suche mit leerem Schlüssel im Pfad

Wenn Sie mit einem Schlüssel suchen, der eine leere Zeichenfolge als Teil des Pfads enthält (z. B.`x..b`)`x.`, und das Objekt einen leeren Zeichenkettenschlüsselpfad (z. B.`{"x" : [ { "" : 10 }, { "b" : 20 } ]}`) innerhalb eines Arrays hat, gibt Amazon DocumentDB andere Ergebnisse zurück, als wenn Sie dieselbe Suche in MongoDB ausführen würden.

In MongoDB funktioniert die Suche nach einem leeren Schlüsselpfad innerhalb eines Arrays wie erwartet, wenn sich der leere Zeichenkettenschlüssel nicht am Ende der Pfadsuche befindet. Wenn sich der leere Zeichenkettenschlüssel jedoch am Ende der Pfadsuche befindet, schaut er nicht in das Array hinein.

In Amazon DocumentDB wird jedoch nur das erste Element innerhalb des Arrays gelesen, da eine leere Zeichenfolge in eine leere Zeichenfolge `getArrayIndexFromKeyString` konvertiert wird`0`,

sodass die Suche nach Zeichenkettenschlüsseln wie die Suche nach einem Array-Index behandelt wird.

MongoDB-APIs, Operationen und Datentypen

Amazon DocumentDB ist mit den MongoDB-APIs 3.6, 4.0, 5.0 und 8.0 kompatibel. Die aktuelle Liste der unterstützten Funktionen finden Sie unter Unterstützte MongoDB-APIs, Operationen und Datentypen in Amazon DocumentDB.

`Dienstprogramme mongodump und mongorestore`

Amazon DocumentDB unterstützt keine Admin-Datenbank und speichert die Admin-Datenbank daher nicht und stellt sie auch nicht wieder her, wenn Sie die Dienstprogramme `mongodump` oder `mongorestore` verwenden. Wenn Sie mit Amazon DocumentDB eine neue Datenbank erstellen`mongorestore`, müssen Sie zusätzlich zum Wiederherstellungsvorgang auch die Benutzerrollen neu erstellen.

> **Note**
>
> Wir empfehlen MongoDB Database Tools bis einschließlich Version 100.6.1 für Amazon DocumentDB. Sie können hier auf die Downloads der MongoDB Database Tools zugreifen.

Reihenfolge der Ergebnisse

Amazon DocumentDB garantiert nicht die implizite Sortierreihenfolge von Ergebnismengen. Um die Reihenfolge einer Ergebnismenge zu gewährleisten, geben Sie mit `sort()` explizit eine Sortierreihenfolge an.

Das folgende Beispiel sortiert die Artikel in der Inventur in absteigender Reihenfolge basierend auf dem Bestandsfeld.

```
db.inventory.find().sort({ stock: -1 })
```

Bei Verwendung der `$sort` Aggregationsphase wird die Sortierreihenfolge nicht beibehalten, es sei denn, die `$sort` Phase ist die letzte Phase in der Aggregationspipeline. Wenn die `$sort` Aggregationsphase in Kombination mit der Aggregationsphase verwendet wird, wird die `$group`

Aggregationsphase nur auf die `$sort` Akkumulatoren und angewendet. `$first` `$last` In Amazon DocumentDB 4.0 wurde Unterstützung für `$push` die Beibehaltung der Sortierreihenfolge aus der vorherigen `$sort` Phase hinzugefügt.

Wiederholbare Schreibvorgänge

Ab MongoDB 4.2-kompatiblen Treibern sind wiederholbare Schreibvorgänge standardmäßig aktiviert. Amazon DocumentDB unterstützt derzeit jedoch keine wiederholbaren Schreibvorgänge. Der funktionale Unterschied wird sich in einer Fehlermeldung ähnlich der folgenden zeigen.

```
{"ok":0,"errmsg":"Unrecognized field: 'txnNumber'","code":9,"name":"MongoError"}
```

Wiederholbare Schreibvorgänge können über die Verbindungszeichenfolge (z. B.`MongoClient("mongodb://my.mongodb.cluster/db?retryWrites=false")`) oder das Schlüsselwortargument des MongoClient Konstruktors (z. B.) deaktiviert werden. `MongoClient("mongodb://my.mongodb.cluster/db", retryWrites=False)`

Im Folgenden finden Sie ein Python-Beispiel, das wiederholbare Schreibvorgänge in der Verbindungszeichenfolge deaktiviert.

```
client =
 pymongo.MongoClient('mongodb://
<username>:<password>@docdb-2019-03-17-16-49-12.cluster-ccuszbx3pn5e.us-
east-1.docdb.amazonaws.com:27017/?
replicaSet=rs0',w='majority',j=True,retryWrites=False)
```

Sparse Index

Um einen Sparse-Index zu verwenden, den Sie in einer Abfrage erstellt haben, müssen Sie die `$exists`-Bedingungen für die Felder verwenden, die der Index abdecken. Wenn Sie ihn weglassen`$exists`, verwendet Amazon DocumentDB den Sparse-Index nicht.

Im Folgenden wird ein -Beispiel gezeigt.

```
db.inventory.count({ "stock": { $exists: true }})
```

Für spärliche Indizes mit mehreren Schlüsseln unterstützt Amazon DocumentDB keine eindeutige Schlüsseleinschränkung, wenn die Suche nach einem Dokument zu einer Reihe von Werten führt

und nur eine Teilmenge der indizierten Felder fehlt. Beispielsweise wird `createIndex({"a.b" : 1 }, { unique : true, sparse :true })` nicht unterstützt, wenn `"a" : [ { "b" : 2 }, { "c" : 1 } ]` eingegeben wird, da `"a.c"` im Index gespeichert ist.

Verwenden von $elemMatch innerhalb eines $all-Ausdrucks

Amazon DocumentDB unterstützt derzeit nicht die Verwendung des `$elemMatch` Operators innerhalb eines `$all` Ausdrucks. Sie können dies umgehen, indem Sie den Operator `$and` wie folgt mit `$elemMatch` verwenden.

Ursprüngliche Operation:

```
db.col.find({
  qty: {
    $all: [
      { "$elemMatch": { part: "xyz", qty: { $lt: 11 } } },
      { "$elemMatch": { num: 40, size: "XL" } }
    ]
  }
})
```

Aktualisierte Operation:

```
db.col.find({
  $and: [
    { qty: { "$elemMatch": { part: "xyz", qty: { $lt: 11 } } } },
    { qty: { "$elemMatch": { qty: 40, size: "XL" } } }
  ]
})
```

Dollar ($) und Punkt (.) in Feldnamen

Amazon DocumentDB unterstützt nicht die Abfrage von Feldern mit dem Präfix Dollar ($) in $in, $nin und $all in verschachtelten Objekten. Die folgende Abfrage ist beispielsweise in Amazon DocumentDB nicht gültig:

```
coll.find({"field": {"$all": [{ "$a": 1 }]}})
```

$lookup

Amazon DocumentDB unterstützt Gleichheitsabgleiche (z. B. Left Outer Join) und unterstützt auch unkorrelierte Unterabfragen, aber keine korrelierten Unterabfragen.

Verwendung eines Indexes mit $lookup

Sie können jetzt einen Index mit dem `$lookup` Stage-Operator verwenden. Je nach Anwendungsfall gibt es mehrere Indexierungsalgorithmen, mit denen Sie die Leistung optimieren können. In diesem Abschnitt werden die verschiedenen Indexierungsalgorithmen für Sie erläutert `$lookup` und Sie bei der Auswahl des für Ihren Workload am besten geeigneten Algorithmus unterstützt.

Standardmäßig verwendet Amazon DocumentDB den Hash-Algorithmus, wenn `allowDiskUse:false` es verwendet wird, und Sort Merge, wenn `allowDiskUse:true` es verwendet wird.

> **Note**
>
> Die `allowDiskUse` Option wird derzeit für den `find` Befehl nicht unterstützt. Die Option wird nur als Teil der Aggregation unterstützt. Wir empfehlen, das Aggregationsframework mit `allowDiskUse:true` zu verwenden, um große Abfragen zu verarbeiten, die Speicherlimits überschreiten könnten.

In einigen Anwendungsfällen kann es wünschenswert sein, den Abfrageoptimierer zu zwingen, einen anderen Algorithmus zu verwenden. Im Folgenden sind die verschiedenen Indizierungsalgorithmen aufgeführt, die der `$lookup` Aggregationsoperator verwenden kann:

- Verschachtelte Schleife: Ein Plan mit verschachtelter Schleife ist in der Regel für eine Arbeitslast von Vorteil, wenn die ausländische Sammlung weniger als 1 GB groß ist und das Feld in der ausländischen Sammlung über einen Index verfügt. Wenn der Nested-Loop-Algorithmus verwendet wird, zeigt der Explain-Plan die Phase als an. `NESTED_LOOP_LOOKUP`
- Zusammenführung sortieren: Ein Plan zur Zusammenführung von Sortierungen ist in der Regel für eine Arbeitslast von Vorteil, wenn die ausländische Sammlung keinen Index für das bei der Suche verwendete Feld hat und der Arbeitsdatensatz nicht in den Arbeitsspeicher passt. Wenn der Algorithmus zur Sortierung und Zusammenführung verwendet wird, zeigt der Erläuterungsplan die Phase als`SORT_LOOKUP`.

- Hash: Ein Hash-Plan ist in der Regel für eine Arbeitslast von Vorteil, wenn die ausländische Sammlung weniger als 1 GB groß ist und der Arbeitsdatensatz in den Arbeitsspeicher passt. Wenn der Hash-Algorithmus verwendet wird, zeigt der Explain-Plan die Phase als`HASH_LOOKUP`.

Sie können den Indizierungsalgorithmus, der für den `$lookup` Operator verwendet wird, `explain` anhand der Abfrage identifizieren. Im Folgenden finden Sie ein Beispiel:

```
db.localCollection.explain().aggregate(
   [
      {
         $lookup:
            {
               from: "foreignCollection",
               localField: "a",
               foreignField: "b",
               as: "joined"
            }
      }
   ]
)

output
{
    "queryPlanner" : {
        "plannerVersion" : 1,
        "namespace" : "test.localCollection",
        "winningPlan" : {
            "stage" : "SUBSCAN",
            "inputStage" : {
                "stage" : "SORT_AGGREGATE",
                "inputStage" : {
                    "stage" : "SORT",
                    "inputStage" : {
                        "stage" : "NESTED_LOOP_LOOKUP",
                        "inputStages" : [
                            {
                                "stage" : "COLLSCAN"
                            },
                            {
                                "stage" : "FETCH",
                                "inputStage" : {
```

```
                                    "stage" : "COLLSCAN"
                                }
                            }
                        ]
                    }
                }
            }
        }
    },
    "serverInfo" : {
        "host" : "devbox-test",
        "port" : 27317,
        "version" : "3.6.0"
    },
    "ok" : 1
}
```

Als Alternative zur Verwendung der `explain()` Methode können Sie den Profiler verwenden, um den Algorithmus zu überprüfen, der bei Ihrer Verwendung des `$lookup` Operators verwendet wird. Weitere Informationen zum Profiler finden Sie unter. Profilierung von Amazon DocumentDB DocumentDB-Vorgängen

Verwenden eines PlanHints

Wenn Sie den Abfrageoptimierer zwingen möchten, einen anderen Indizierungsalgorithmus zu verwenden`$lookup`, können Sie a verwenden. `planHint` Verwenden Sie dazu den Kommentar in den Optionen der Aggregationsphase, um einen anderen Plan zu erzwingen. Im Folgenden finden Sie ein Beispiel für die Syntax des Kommentars:

```
comment : {
    comment :  "<string>",
    lookupStage : { planHint : "SORT" | "HASH" | "NESTED_LOOP" }
}
```

Im Folgenden finden Sie ein Beispiel für die Verwendung von`planHint`, um den Abfrageoptimierer zur Verwendung des HASH Indexierungsalgorithmus zu zwingen:

```
db.foo.aggregate(
   [
      {
```

```
         $lookup:
            {
               from: "foo",
               localField: "_id",
               foreignField: "_id",
               as: "joined"
            },
      }
   ]
),
{
   comment : "{ \"lookupStage\" : { \"planHint\": \"HASH\" }}"
```

Um zu testen, welcher Algorithmus für Ihre Arbeitslast am besten geeignet ist, können Sie den `executionStats` Parameter der `explain` Methode verwenden, um die Ausführungszeit der `$lookup` Phase zu messen und gleichzeitig den Indizierungsalgorithmus zu ändern (d. h.HASH//SORT). NESTED_LOOP

Das folgende Beispiel zeigt, wie Sie `executionStats` die Ausführungszeit der `$lookup` Phase mithilfe des SORT Algorithmus messen können.

```
db.foo.explain("executionStats").aggregate(
   [
      {
         $lookup:
            {
               from: "foo",
               localField: "_id",
               foreignField: "_id",
               as: "joined"
            },
      }
   ]
),
{
   comment : "{ \"lookupStage\" : { \"planHint\": \"SORT\" }}"
```

$natural und umgekehrte Sortierung

Amazon DocumentDB unterstützt nur `$natural` Forward-Collection-Scans. Rückwärtige Sammelscans ({`$natural: -1`}) führen zu einem`MongoServerError`.

Unterstützte MongoDB-APIs, Operationen und Datentypen in Amazon DocumentDB

Amazon DocumentDB (mit MongoDB-Kompatibilität) ist ein schneller, skalierbarer, hochverfügbarer und vollständig verwalteter Dokumentendatenbankservice, der MongoDB-Workloads unterstützt. Amazon DocumentDB ist mit den MongoDB-APIs 3.6, 4.0, 5.0 und 8.0 kompatibel. In diesem Abschnitt werden die unterstützten Funktionalitäten aufgeführt. Unterstützung bei der Verwendung von MongoDB-APIs und -Treibern finden Sie in den MongoDB-Community-Foren. Wenn Sie Unterstützung bei der Nutzung des Amazon DocumentDB-Services benötigen, wenden Sie sich an das entsprechende AWS Support-Team. Informationen zu den Funktionsunterschieden zwischen Amazon DocumentDB und MongoDB finden Sie unter. Funktionale Unterschiede: Amazon DocumentDB und MongoDB

MongoDB-Befehle und -Operatoren, die nur intern oder nicht auf einen verwalteten Service anwendbar sind, werden nicht unterstützt und sind nicht in der Liste der unterstützten Funktionalität enthalten.

Seit der Markteinführung haben wir mehr als 50 zusätzliche Funktionen hinzugefügt und werden uns weiter an den Anforderungen unserer Kunden ausrichten, um ihnen die benötigten Funktionen bereitzustellen. Informationen zu den neuesten Produkteinführungen finden Sie unter Ankündigungen von Amazon DocumentDB.

Wenn es eine Funktion gibt, die nicht unterstützt wird und die Sie von uns erstellen lassen möchten, teilen Sie uns dies mit, indem Sie eine E-Mail mit Ihrer accountID, den angeforderten Funktionen und dem Anwendungsfall an das Amazon DocumentDB-Serviceteam senden.

Topics

- Befehle für die Datenbank
- Abfrage- und Projektionsoperatoren
- Operatoren aktualisieren
- Geodaten
- Cursor-Methoden
- Operatoren für Aggregationspipelines
- Datentypen
- Indizes

Befehle für die Datenbank

Themen

- Administrative Befehle
- Aggregation
- Authentifizierung
- Diagnosebefehle
- Abfrage- und Schreiboperationen
- Befehle zur Rollenverwaltung
- Befehle für Sitzungen
- Benutzerverwaltung
- Sharding-Befehle

Administrative Befehle

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
Gedeckelte Sammlungen	Nein	Nein	Nein	Nein	Nein
klonen CollectionAsCapped	Nein	Nein	Nein	Nein	Nein
collMod	Teilweise	Teilweise	Teilweise	Teilweise	Teilweise
CollMod: ablaufen AfterSeconds	Ja	Ja	Ja	Ja	Ja
konvertieren ToCapped	Nein	Nein	Nein	Nein	Nein
copydb	Nein	Nein	Nein	Nein	Nein

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
Erstellen	Ja	Ja	Ja	Ja	Ja
createView	Nein	Nein	Nein	Ja	Nein
createIndexes	Ja	Ja	Ja	Ja	Ja
currentOp	Ja	Ja	Ja	Ja	Ja
fallen lassen	Ja	Ja	Ja	Ja	Ja
dropDatabase	Ja	Ja	Ja	Ja	Ja
dropIndexes	Ja	Ja	Ja	Ja	Ja
filemd5	Nein	Nein	Nein	Nein	Nein
erhaltenAuditConfig	Nein	Ja	Ja	Ja	Nein
killCursors	Ja	Ja	Ja	Ja	Ja
killOp	Ja	Ja	Ja	Ja	Ja
listCollectionsauflisten*	Ja	Ja	Ja	Ja	Ja
listDatabases	Ja	Ja	Ja	Ja	Ja
listIndexes	Ja	Ja	Ja	Ja	Ja
reIndex	Nein	Nein	Ja	Ja	Nein
renameCollection	Ja	Ja	Ja	Ja	Nein

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
setzen AuditConfig	Nein	Ja	Ja	Ja	Nein

* Der `type` Schlüssel in der Filteroption wird nicht unterstützt.

Aggregation

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
aggregate	Ja	Ja	Ja	Ja	Ja
count	Ja	Ja	Ja	Ja	Ja
distinct	Ja	Ja	Ja	Ja	Ja
mapReduce	Nein	Nein	Nein	Ja	Nein

Authentifizierung

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
authenticate	Ja	Ja	Ja	Ja	Ja
logout	Ja	Ja	Ja	Ja	Ja

Diagnosebefehle

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
buildInfo	Ja	Ja	Ja	Ja	Ja
collStats	Ja	Ja	Ja	Ja	Ja
Conn PoolStats	Nein	Nein	Nein	Nein	Nein
connectio nStatus	Ja	Ja	Ja	Ja	Ja
dataSize	Ja	Ja	Ja	Ja	Ja
dbHash	Nein	Nein	Nein	Nein	Nein
dbStats	Ja	Ja	Ja	Ja	Ja
explain	Ja	Ja	Ja	Ja	Ja
Erklären: execution Stats	Ja	Ja	Ja	Ja	Ja
features	Nein	Nein	Nein	Nein	Nein
hostInfo	Ja	Ja	Ja	Ja	Ja
listComma nds	Ja	Ja	Ja	Ja	Ja
Profiler	Ja	Ja	Ja	Ja	Nein
serverStatus	Ja	Ja	Ja	Ja	Ja
top	Ja	Ja	Ja	Ja	Ja

Abfrage- und Schreiboperationen

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
Change streams	Ja	Ja	Ja	Ja	Nein
delete	Ja	Ja	Ja	Ja	Ja
find	Ja	Ja	Ja	Ja	Ja
finden AndModify	Ja	Ja	Ja	Ja	Ja
bekommen LastError	Nein	Nein	Nein	Nein	Nein
getMore	Ja	Ja	Ja	Ja	Ja
bekommen PrevError	Nein	Nein	Nein	Nein	Nein
GridFS	Ja	Ja	Ja	Ja	Nein
insert	Ja	Ja	Ja	Ja	Ja
parallel CollectionScan	Nein	Nein	Nein	Nein	Nein
resetError	Nein	Nein	Nein	Nein	Nein
update	Ja	Ja	Ja	Ja	Ja
ReplaceOne	Ja	Ja	Ja	Ja	Ja

Befehle zur Rollenverwaltung

E	3	4	5	8	E e C
c e	Ja	Ja	Ja	Ja	Nein
f l A r s	Ja	Ja	Ja	Ja	Nein
c	Ja	Ja	Ja	Ja	Nein
g F l	Ja	Ja	Ja	Ja	Nein
v n F F	Ja	Ja	Ja	Ja	Nein
v n F s	Ja	Ja	Ja	Ja	Nein
r	Ja	Ja	Ja	Ja	Nein
u e	Ja	Ja	Ja	Ja	Nein

Befehle für Sitzungen

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
Transaktion abbrechen	Nein	Ja	Ja	Ja	Nein
commitTransaction	Nein	Ja	Ja	Ja	Nein
Sitzungen beenden	Nein	Nein	Nein	Nein	Nein
töten AllSessions	Nein	Ja	Ja	Ja	Nein
töten AllSessionsByPattern	Nein	Nein	Nein	Nein	Nein
Sessions beenden	Nein	Ja	Ja	Ja	Nein
Sitzungen aktualisieren	Nein	Nein	Nein	Nein	Nein
Sitzung starten	Nein	Ja	Ja	Ja	Nein

Benutzerverwaltung

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
createUser	Ja	Ja	Ja	Ja	Ja

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
fallen lassen AllUsersFromDatabase	Ja	Ja	Ja	Ja	Ja
dropUser	Ja	Ja	Ja	Ja	Ja
gewähren RolesToUser	Ja	Ja	Ja	Ja	Ja
widerrufen RolesFrom User	Ja	Ja	Ja	Ja	Ja
updateUser	Ja	Ja	Ja	Ja	Ja
Benutzerinformationen	Ja	Ja	Ja	Ja	Ja

Sharding-Befehle

Befehl	Elastischer Cluster
abbrechen ReshardCollection	Nein
Schere hinzufügen	Nein
hinzufügen ShardToZone	Nein
Balancer CollectionStatus	Nein
Balancer starten	Nein
Balancer-Status	Nein
Balancer Stopp	Nein

Befehl	Elastischer Cluster
überprüfen ShardingIndex	Nein
klar JumboFlag	Nein
cleanupOrphaned	Nein
aufräumen ReshardCollection	Nein
verpflichten ReshardCollection	Nein
Sharding aktivieren	Ja
spülen RouterConfig	Nein
bekommen ShardMap	Nein
bekommen ShardVersion	Nein
isdbgrid	Nein
Listet Scherben auf	Nein
Median-Key	Nein
Chunk verschieben	Nein
Primär verschieben	Nein
Blöcke zusammenführen	Nein
verfeinern CollectionShardKey	Nein
Entfernt Schwer	Nein
entfernen ShardFromZone	Nein
Sammlung Reshard	Nein
Satz AllowMigrations	Nein

Befehl	Elastischer Cluster
setzen ShardVersion	Nein
Sammlung Shard	Ja
Status „Sharding“	Nein
split	Nein
Vektor teilen	Nein
Harding deaktivieren	Nein
aktualisieren ZoneKeyRange	Nein

Abfrage- und Projektionsoperatoren

Themen

- Array-Operatoren
- Bitweise Operatoren
- Operator kommentieren
- Vergleichsoperatoren
- Elementoperatoren
- Operatoren für Bewertungsabfragen
- Logische Operatoren
- Projektionsoperatoren

Array-Operatoren

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
$all	Ja	Ja	Ja	Ja	Ja

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
$elemMatch	Ja	Ja	Ja	Ja	Ja
$size	Ja	Ja	Ja	Ja	Ja

Bitweise Operatoren

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
$ Bits AllSet	Ja	Ja	Ja	Ja	Ja
$ Bits AnySet	Ja	Ja	Ja	Ja	Ja
$ Bits AllClear	Ja	Ja	Ja	Ja	Ja
$ Bits AnyClear	Ja	Ja	Ja	Ja	Ja

Operator kommentieren

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
$comment	Ja	Ja	Ja	Ja	Ja

Vergleichsoperatoren

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
$eq	Ja	Ja	Ja	Ja	Ja

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
$gt	Ja	Ja	Ja	Ja	Ja
$gte	Ja	Ja	Ja	Ja	Ja
$in	Ja	Ja	Ja	Ja	Ja
$lt	Ja	Ja	Ja	Ja	Ja
$lte	Ja	Ja	Ja	Ja	Ja
$ne	Ja	Ja	Ja	Ja	Ja
$nin	Ja	Ja	Ja	Ja	Ja

Elementoperatoren

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
$exists	Ja	Ja	Ja	Ja	Ja
$type	Ja	Ja	Ja	Ja	Ja

Operatoren für Bewertungsabfragen

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
$expr	Nein	Ja	Ja	Ja	Nein
$jsonSchema	Nein	Ja	Ja	Ja	Nein
$mod	Ja	Ja	Ja	Ja	Ja

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
$regex	Ja	Ja	Ja	Ja	Ja
$text	Nein	Nein	Ja	Ja	Nein
$where	Nein	Nein	Nein	Nein	Nein

Logische Operatoren

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
$and	Ja	Ja	Ja	Ja	Ja
$nor	Ja	Ja	Ja	Ja	Ja
$not	Ja	Ja	Ja	Ja	Ja
$or	Ja	Ja	Ja	Ja	Ja

Projektionsoperatoren

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
$	Ja	Ja	Ja	Ja	Ja
$elemMatch	Ja	Ja	Ja	Ja	Ja
$meta	Nein	Nein	Ja	Ja	Nein
$slice	Ja	Ja	Ja	Ja	Ja

Operatoren aktualisieren

Themen

- Array-Operatoren
- Bitweise Operatoren
- Feldoperatoren
- Modifikatoren aktualisieren

Array-Operatoren

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
$	Ja	Ja	Ja	Ja	Ja
$[]	Ja	Ja	Ja	Ja	Ja
$ [<Kennung>]	Ja	Ja	Ja	Ja	Ja
$addToSet	Ja	Ja	Ja	Ja	Ja
$pop	Ja	Ja	Ja	Ja	Ja
$pullAll	Ja	Ja	Ja	Ja	Ja
$pull	Ja	Ja	Ja	Ja	Ja
$push	Ja	Ja	Ja	Ja	Ja

Bitweise Operatoren

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
$bit	Ja	Ja	Ja	Ja	Ja

Feldoperatoren

Operator	3.6	4,0	5.0	8.0	Elastischer Cluster
$currentDate	Ja	Ja	Ja	Ja	Ja
$inc	Ja	Ja	Ja	Ja	Ja
$max	Ja	Ja	Ja	Ja	Ja
$min	Ja	Ja	Ja	Ja	Ja
$mul	Ja	Ja	Ja	Ja	Ja
$rename	Ja	Ja	Ja	Ja	Ja
$set	Ja	Ja	Ja	Ja	Ja
$setOnInsert	Ja	Ja	Ja	Ja	Ja
$unset	Ja	Ja	Ja	Ja	Ja

Modifikatoren aktualisieren

Operator	3.6	4,0	5.0	8.0	Elastischer Cluster
$each	Ja	Ja	Ja	Ja	Ja
$position	Ja	Ja	Ja	Ja	Ja
$slice	Ja	Ja	Ja	Ja	Ja
$sort	Ja	Ja	Ja	Ja	Ja

Geodaten

Geometrie-Spezifizierer

Abfrageauswahl	3.6	4,0	5.0	8.0	Elastischer Cluster
$box	Nein	Nein	Nein	Nein	Nein
$center	Nein	Nein	Nein	Nein	Nein
$centerSphere	Nein	Nein	Nein	Nein	Nein
$geometry	Ja	Ja	Ja	Ja	Ja
$maxDistance	Ja	Ja	Ja	Ja	Ja
$minDistance	Ja	Ja	Ja	Ja	Ja
$nearSphere	Ja	Ja	Ja	Ja	Ja
$polygon	Nein	Nein	Nein	Nein	Nein
$uniqueDocs	Nein	Nein	Nein	Nein	Nein

Selektoren abfragen

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
$geoIntersects	Ja	Ja	Ja	Ja	Ja
$geoWithin	Ja	Ja	Ja	Ja	Ja
$near	Ja	Ja	Ja	Ja	Ja

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
$nearSphere	Ja	Ja	Ja	Ja	Ja
$polygon	Nein	Nein	Nein	Nein	Nein
$uniqueDocs	Nein	Nein	Nein	Nein	Nein

Cursor-Methoden

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
cursor.batchSize()	Ja	Ja	Ja	Ja	Ja
cursor.close()	Ja	Ja	Ja	Ja	Ja
cursor.collation()	Nein	Nein	Nein	Ja	Nein
cursor.comment()	Ja	Ja	Ja	Ja	Ja
cursor.count()	Ja	Ja	Ja	Ja	Ja
cursor.explain()	Ja	Ja	Ja	Ja	Nein
cursor.forEach()	Ja	Ja	Ja	Ja	Ja
cursor.hasNext()	Ja	Ja	Ja	Ja	Ja
cursor.hint()	Ja	Ja	Ja	Ja	Ja*

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
cursor.isClosed()	Ja	Ja	Ja	Ja	Ja
cursor.isExhausted()	Ja	Ja	Ja	Ja	Nein
cursor.itcount()	Ja	Ja	Ja	Ja	Nein
cursor.limit()	Ja	Ja	Ja	Ja	Nein
cursor.map()	Ja	Ja	Ja	Ja	Nein
cursor.max()	Nein	Nein	Nein	Nein	Nein
cursor.maxScan()	Ja	Ja	Ja	Ja	Nein
cursor.maxTimeMS()	Ja	Ja	Ja	Ja	Nein
cursor.min()	Nein	Nein	Nein	Nein	Nein
cursor.next()	Ja	Ja	Ja	Ja	Ja
cursor.noCursorTimeout ()	Nein	Nein	Nein	Nein	Nein
cursor.objs () LeftInBatch	Ja	Ja	Ja	Ja	Nein
cursor.pretty()	Ja	Ja	Ja	Ja	Nein
cursor.readConcern()	Ja	Ja	Ja	Ja	Nein

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
cursor.readPref()	Ja	Ja	Ja	Ja	Nein
cursor.returnKey()	Nein	Nein	Nein	Nein	Nein
cursor.showRecordId ()	Nein	Nein	Nein	Nein	Nein
cursor.size()	Ja	Ja	Ja	Ja	Nein
cursor.skip()	Ja	Ja	Ja	Ja	Nein
cursor.sort()	Ja	Ja	Ja	Ja	Nein
cursor.tailable()	Nein	Nein	Nein	Nein	Nein
cursor.toArray()	Ja	Ja	Ja	Ja	Nein

* Index `hint` wird mit Indexausdrücken unterstützt. Beispiel, `db.foo.find().hint({x:1})`.

Operatoren für Aggregationspipelines

Themen

- Akkumulatorausdrücke
- Arithmetische Operatoren
- Array-Operatoren
- Boolesche Operatoren
- Vergleichsoperatoren
- Operatoren für bedingte Ausdrücke
- Datentyp-Operator

- Operator zur Datengröße
- Datumsoperatoren
- Wörtlicher Operator
- Operator zusammenführen
- Natürlicher Operator
- Satzoperatoren
- Betreiber der Bühne
- Zeichenfolgenoperatoren
- Systemvariablen
- Operator für die Textsuche
- Geben Sie Konvertierungsoperatoren ein
- Operatoren für Variablen
- Verschiedene Betreiber

Akkumulatorausdrücke

Expression	3.6	4,0	5.0	8.0	Elastischer Cluster
$Akkumulator	-	-	Nein	Nein	Nein
$ hinzufügen ToSet	Ja	Ja	Ja	Ja	Ja
$avg	Ja	Ja	Ja	Ja	Ja
$count	-	-	Nein	Nein	Nein
$Kovarian zPop	Nein	Nein	Nein	Nein	Nein
$Kovarian zAMP	Nein	Nein	Nein	Nein	Nein
$ DenseRank	Nein	Nein	Nein	Nein	Nein

Expression	3.6	4,0	5.0	8.0	Elastischer Cluster
$ Ableitung	Nein	Nein	Nein	Nein	Nein
$ Nummer des Dokuments	Nein	Nein	Nein	Nein	Nein
$exp MovingAvg	Nein	Nein	Nein	Nein	Nein
$first	Ja	Ja	Ja	Ja	Ja
$ ganzheitlich	Nein	Nein	Nein	Nein	Nein
$last	Ja	Ja	Ja	Ja	Ja
$max	Ja	Ja	Ja	Ja	Ja
$min	Ja	Ja	Ja	Ja	Ja
$push	Ja	Ja	Ja	Ja	Ja
$ Rang	Nein	Nein	Nein	Nein	Nein
$ Schicht	Nein	Nein	Nein	Nein	Nein
$ std DevPop	Nein	Nein	Nein	Nein	Nein
$ std DevSamp	Nein	Nein	Nein	Nein	Nein
$sum	Ja	Ja	Ja	Ja	Ja

Arithmetische Operatoren

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
$abs	Ja	Ja	Ja	Ja	Ja
$add	Ja	Ja	Ja	Ja	Ja
$ceil	Nein	Ja	Ja	Ja	Ja
$divide	Ja	Ja	Ja	Ja	Ja
$exp	Nein	Ja	Ja	Ja	Ja
$floor	Nein	Ja	Ja	Ja	Ja
$ln	Nein	Ja	Ja	Ja	Ja
$log	Nein	Ja	Ja	Ja	Ja
$log10	Nein	Ja	Ja	Ja	Ja
$mod	Ja	Ja	Ja	Ja	Ja
$multiply	Ja	Ja	Ja	Ja	Ja
$pow	Nein	Nein	Ja (5.0.1+)	Ja	Nein
$rund	-	-	Nein	Nein	Nein
$sqrt	Nein	Ja	Ja	Ja	Ja
$subtract	Ja	Ja	Ja	Ja	Ja
$trunc	Nein	Nein	Nein	Nein	Nein

Array-Operatoren

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
$arrayElemAt	Ja	Ja	Ja	Ja	Ja
$arrayToObject	Ja	Ja	Ja	Ja	Ja
$concatArrays	Ja	Ja	Ja	Ja	Ja
$filter	Ja	Ja	Ja	Ja	Ja
$first	-	-	Ja	Ja	Nein
$in	Ja	Ja	Ja	Ja	Ja
$ indexOfArray	Ja	Ja	Ja	Ja	Ja
$isArray	Ja	Ja	Ja	Ja	Ja
$last	-	-	Ja	Ja	Nein
$objektToArray	Ja	Ja	Ja	Ja	Ja
$range	Ja	Ja	Ja	Ja	Ja
$reverseArray	Ja	Ja	Ja	Ja	Ja
$reduce	Ja	Ja	Ja	Ja	Ja
$size	Ja	Ja	Ja	Ja	Ja
$slice	Ja	Ja	Ja	Ja	Ja

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
$zip	Ja	Ja	Ja	Ja	Ja

Boolesche Operatoren

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
$and	Ja	Ja	Ja	Ja	Ja
$not	Ja	Ja	Ja	Ja	Ja
$or	Ja	Ja	Ja	Ja	Ja

Vergleichsoperatoren

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
$cmp	Ja	Ja	Ja	Ja	Ja
$eq	Ja	Ja	Ja	Ja	Ja
$gt	Ja	Ja	Ja	Ja	Ja
$gte	Ja	Ja	Ja	Ja	Ja
$lt	Ja	Ja	Ja	Ja	Ja
$lte	Ja	Ja	Ja	Ja	Ja
$ne	Ja	Ja	Ja	Ja	Ja

Operatoren für bedingte Ausdrücke

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
$cond	Ja	Ja	Ja	Ja	Ja
$ifNull	Ja	Ja	Ja	Ja	Ja
$switch	Nein	Ja	Ja	Ja	Nein

Datentyp-Operator

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
$type	Ja	Ja	Ja	Ja	Ja

Operator zur Datengröße

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
$BinarySize	-	-	Nein	Nein	Nein
$ bsonGröße	-	-	Nein	Nein	Nein

Datumsoperatoren

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
$DateAdd	Nein	Nein	Ja	Ja	Ja
$DateDiff	-	-	Ja	Ja	Nein

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
$datum FromParts	Nein	Nein	Ja (5.0.1+)	Nein	Nein
$datum FromString	Ja	Ja	Ja	Ja	Ja
$DateSubtrahieren	Nein	Nein	Ja	Ja	Ja
$datum ToParts	Nein	Nein	Ja (5.0.1+)	Nein	Nein
$datum ToString	Ja	Ja	Ja	Ja	Ja
$DateTrunc	-	-	Nein	Ja	Nein
$Tag OfMonth	Ja	Ja	Ja	Ja	Ja
$Tag OfWeek	Ja	Ja	Ja	Ja	Ja
$Tag OfYear	Ja	Ja	Ja	Ja	Ja
$hour	Ja	Ja	Ja	Ja	Ja
$ iso DayOfWeek	Ja	Ja	Ja	Ja	Ja
$isoWeek	Ja	Ja	Ja	Ja	Ja
$ iso WeekYear	Ja	Ja	Ja	Ja	Ja
$millisecond	Ja	Ja	Ja	Ja	Ja
$minute	Ja	Ja	Ja	Ja	Ja

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
$month	Ja	Ja	Ja	Ja	Ja
$second	Ja	Ja	Ja	Ja	Ja
$week	Ja	Ja	Ja	Ja	Ja
$year	Ja	Ja	Ja	Ja	Ja

Wörtlicher Operator

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
$literal	Ja	Ja	Ja	Ja	Ja

Operator zusammenführen

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
$mergeObjects	Ja	Ja	Ja	Ja	Ja

Natürlicher Operator

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
$ natürlich	Ja	Ja	Ja	Ja	Ja

Satzoperatoren

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
$ alles ElementsTrue	Nein	Ja	Ja	Ja	Ja
$ beliebig ElementTrue	Nein	Ja	Ja	Ja	Ja
$setDifference	Nein	Ja	Ja	Ja	Ja
$setEquals	Ja	Ja	Ja	Ja	Ja
$setIntersection	Ja	Ja	Ja	Ja	Ja
$ gesetzt IsSubset	Ja	Ja	Ja	Ja	Ja
$setUnion	Ja	Ja	Ja	Ja	Ja
$set WindowFields	Nein	Nein	Nein	Nein	Nein

Betreiber der Bühne

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
$addFields	Ja	Ja	Ja	Ja	Ja
$bucket	Nein	Nein	Nein	Ja	Nein

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
$bucketAuto	Nein	Nein	Nein	Nein	
$ Stream ändern	Ja	Ja	Ja	Ja	Nein
$collStats	Nein	Ja	Ja	Ja	Nein
$count	Ja	Ja	Ja	Ja	Ja
$currentOp	Ja	Ja	Ja	Ja	Ja
$facet	Nein	Nein	Nein	Nein	Nein
$geoNear	Ja	Ja	Ja	Ja	Ja
$graphLookup	Nein	Nein	Nein	Nein	Nein
$group	Ja	Ja	Ja	Ja	Ja
$indexStats	Ja	Ja	Ja	Ja	Ja
$limit	Ja	Ja	Ja	Ja	Ja
$listeLocalSessions	Nein	Nein	Nein	Nein	Nein
$listSessions	Nein	Nein	Nein	Nein	Nein
$lookup	Ja	Ja	Ja	Ja	Ja
$match	Ja	Ja	Ja	Ja	Ja
$ zusammenführen	-	-	Nein	Ja	Nein
$out	Ja	Ja	Ja	Ja	Nein

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
$ planen CacheStats	-	-	Nein	Nein	Nein
$project	Ja	Ja	Ja	Ja	Ja
$redact	Ja	Ja	Ja	Ja	Ja
$replaceRoot	Ja	Ja	Ja	Ja	Ja
$sample	Ja	Ja	Ja	Ja	Ja
$set	-	-	Nein	Ja	Nein
$ festgelegt WindowFields	-	-	Nein	Nein	Nein
$skip	Ja	Ja	Ja	Ja	Ja
$sort	Ja	Ja	Ja	Ja	Ja
$ sortieren ByCount	Nein	Nein	Nein	Nein	Nein
$ Union mit	-	-	Nein	Nein	Nein
$unset	-	-	Nein	Ja	Nein
$unwind	Ja	Ja	Ja	Ja	Ja
$ ersetzend urch	Nein	Nein	Nein	Ja	Nein
$VectorSearch	Nein	Nein	Nein	Ja	Nein

Zeichenfolgenoperatoren

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
$concat	Ja	Ja	Ja	Ja	Ja
$ index OfBytes	Ja	Ja	Ja	Ja	Ja
$indexOfCP	Ja	Ja	Ja	Ja	Ja
$ ltrim	Nein	Ja	Ja	Ja	Nein
$RegexFind	-	-	Ja	Ja	Nein
$ regulärer Ausdruck FindAll	-	-	Ja	Ja	Nein
$RegexMatch	-	-	Ja	Ja	Nein
$ Alles ersetzen	-	-	Ja	Ja	Nein
$ ersetzenEins	-	-	Ja	Ja	Nein
$rtrim	Nein	Ja	Ja	Ja	Nein
$split	Ja	Ja	Ja	Ja	Ja
$strcasecmp	Ja	Ja	Ja	Ja	Ja
$str LenBytes	Ja	Ja	Ja	Ja	Ja
$strLenCP	Ja	Ja	Ja	Ja	Ja
$substr	Ja	Ja	Ja	Ja	Ja
$substrBytes	Ja	Ja	Ja	Ja	Ja

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
$substrCP	Ja	Ja	Ja	Ja	Ja
$toLower	Ja	Ja	Ja	Ja	Ja
$toUpper	Ja	Ja	Ja	Ja	Ja
$trim	Nein	Ja	Ja	Ja	Nein

Systemvariablen

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
$$CURRENT	Nein	Nein	Nein	Nein	Nein
$$DESCEND	Ja	Ja	Ja	Ja	Ja
$$KEEP	Ja	Ja	Ja	Ja	Ja
$$PRUNE	Ja	Ja	Ja	Ja	Ja
$$REMOVE	Nein	Nein	Nein	Nein	Nein
$ WURZEL	Ja	Ja	Ja	Ja	Ja

Operator für die Textsuche

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
$meta	Nein	Nein	Ja	Ja	Nein
$suche	Nein	Nein	Ja	Ja	Nein

Geben Sie Konvertierungsoperatoren ein

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
$ konvertieren	Nein	Ja	Ja	Ja	Ja
$ ist Zahl	-	-	Nein	Nein	Nein
$ zu Bool	Nein	Ja	Ja	Ja	Ja
$ bis Datum	Nein	Ja	Ja	Ja	Ja
$ zu Dezimal	Nein	Ja	Ja	Ja	Ja
$ bis verdoppeln	Nein	Ja	Ja	Ja	Ja
$ zu Int	Nein	Ja	Ja	Ja	Ja
$ zu Long	Nein	Ja	Ja	Ja	Ja
$ bis ObjectId	Nein	Ja	Ja	Ja	Ja
$ toString	Nein	Ja	Ja	Ja	Ja

Operatoren für Variablen

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
$let	Ja	Ja	Ja	Ja	Ja
$map	Ja	Ja	Ja	Ja	Ja

Verschiedene Betreiber

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
$getField	-	-	Nein	Nein	Nein
$ Rand	-	-	Ja (5.0.1+)	Ja	Nein
$ Samplerate	-	-	Nein	Nein	Nein

Datentypen

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
32-Bit-Ganzzahl (int)	Ja	Ja	Ja	Ja	Ja
64-Bit-Ganzzahl (lang)	Ja	Ja	Ja	Ja	Ja
Array	Ja	Ja	Ja	Ja	Ja
Binäre Daten	Ja	Ja	Ja	Ja	Ja
Boolesch	Ja	Ja	Ja	Ja	Ja
Date	Ja	Ja	Ja	Ja	Ja
DBPointer	Nein	Nein	Nein	Nein	Nein
DBRefs	Nein	Nein	Nein	Nein	Nein
Decimal128	Ja	Ja	Ja	Ja	Ja
Double	Ja	Ja	Ja	Ja	Ja
JavaScript	Nein	Nein	Nein	Nein	Nein

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
JavaScript(mit Geltungsbereich)	Nein	Nein	Nein	Nein	Nein
MaxKey	Ja	Ja	Ja	Ja	Ja
MinKey	Ja	Ja	Ja	Ja	Ja
Null	Ja	Ja	Ja	Ja	Ja
Objekt	Ja	Ja	Ja	Ja	Ja
ObjectId	Ja	Ja	Ja	Ja	Ja
Regulärer Ausdruck	Ja	Ja	Ja	Ja	Ja
Zeichenfolge	Ja	Ja	Ja	Ja	Ja
Symbol	Nein	Nein	Nein	Nein	Nein
Zeitstempel	Ja	Ja	Ja	Ja	Ja
Undefined	Nein	Nein	Nein	Nein	Nein

Indizes und Indexeigenschaften

Themen

- Indizes
- Eigenschaften indizieren

Indizes

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
2dsphere	Ja	Ja	Ja	Ja	Ja
2D-Index	Nein	Nein	Nein	Nein	Nein
Verbundindex	Ja	Ja	Ja	Ja	Ja
Hash-Index	Nein	Nein	Nein	Nein	Nein
Multikey-Index	Ja	Ja	Ja	Ja	Ja
Einzelfeldindex	Ja	Ja	Ja	Ja	Ja
Textindex	Nein	Nein	Ja	Ja	Nein
Platzhalter	Nein	Nein	Nein	Nein	Nein

Eigenschaften indizieren

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
Hintergrund	Ja	Ja	Ja	Ja	Ja
Berücksichtigt Groß- und Kleinschreibung nicht	Nein	Nein	Nein	Ja	Nein
Hidden	Nein	Nein	Nein	Nein	Nein
Teilweise	Nein	Nein	Ja	Ja	Nein

Befehl	3.6	4,0	5.0	8.0	Elastischer Cluster
Sparse	Ja	Ja	Ja	Ja	Ja
Text	Nein	Nein	Ja	Ja	Nein
TTL	Ja	Ja	Ja	Ja	Ja
Eindeutig	Ja	Ja	Ja	Ja	Ja
Vektor	Nein	Nein	Ja	Ja	Nein

Ausführliche Informationen zu bestimmten MongoDB-Operatoren finden Sie in den folgenden Themen:

- Betreiber von Aggregationspipelines
- Geodaten
- Projektionsoperatoren
- Operatoren aktualisieren

Betreiber von Aggregationspipelines

Dieser Abschnitt enthält detaillierte Informationen zu Aggregationspipeline-Operatoren, die von Amazon DocumentDB unterstützt werden.

Themen

- $$DESCEND
- $$KEEP
- $$PRUNE
- $ WURZEL
- $abs
- $add
- $ hinzufügen ToSet
- $addFields

- $ alles ElementsTrue
- $and
- $ beliebig ElementTrue
- $array ElemAt
- $array ToObject
- $avg
- $bucket
- $ceil
- $ Stream ändern
- $cmp
- $collStats
- $concat
- $concatArrays
- $cond
- $ konvertieren
- $count
- $currentOp
- $DateAdd
- $DateDiff
- $datum FromString
- $DateSubtrahieren
- $datum ToString
- $DateTrunc
- $Tag OfMonth
- $Tag OfWeek
- $Tag OfYear
- $divide
- $eq
- $exp

- $filter
- $first
- $floor
- $geoNear
- $group
- $gt
- $gte
- $hour
- $ifNull
- $in
- $ index OfArray
- $ index OfBytes
- $indexOfCP
- $indexStats
- $isArray
- $ iso DayOfWeek
- $isoWeek
- $ iso WeekYear
- $last
- $let
- $limit
- $literal
- $ln
- $log
- $log10
- $lt
- $lte
- $lookup
- $ ltrim

- $map
- $match
- $max
- $meta
- $ zusammenführen
- $mergeObjects
- $millisecond
- $min
- $minute
- $mod
- $month
- $multiply
- $ natürlich
- $ne
- $not
- $objekt ToArray
- $or
- $out
- $pow
- $push
- $project
- $ Rand
- $range
- $redact
- $reduce
- $RegexFind
- $ regulärer Ausdruck FindAll
- $RegexMatch
- $ Alles ersetzen

- $ ersetzenEins
- $replaceRoot
- $ ersetzendurch
- $reverseArray
- $rtrim
- $sample
- $suche
- $second
- $set
- $setDifference
- $setEquals
- $setIntersection
- $ gesetzt IsSubset
- $setUnion
- $skip
- $slice
- $size
- $sort
- $split
- $sqrt
- $str LenBytes
- $strLenCP
- $strcasecmp
- $substr
- $substrBytes
- $substrCP
- $subtract
- $sum
- $switch

- $ zu Bool
- $ bis Datum
- $ zu Dezimal
- $ bis verdoppeln
- $ zu Int
- $ zu Long
- $toLower
- $ bis ObjectId
- $ toString
- $toUpper
- $trim
- $type
- $unset
- $unwind
- $VectorSearch
- $week
- $year
- $zip

$$DESCEND

Der `$$DESCEND` Operator in Amazon DocumentDB ist ein spezieller Positions-Array-Operator, der in der `$redact` Pipeline-Phase verwendet wird. Er weist die Aggregationspipeline an, in das aktuelle Dokument abzusteigen und alle Felder zu verarbeiten, unabhängig von ihrer Verschachtelungsebene.

Wenn die `$redact` Phase auf den `$$DESCEND` Operator trifft, bleiben alle Felder im aktuellen Dokument sichtbar und werden weiter unten in der Pipeline verarbeitet. Dies ist nützlich, wenn Sie bestimmte Felder anhand einer Bedingung selektiv schwärzen oder beschneiden und dabei die Struktur des Dokuments beibehalten möchten.

Parameter

Keine.

Beispiel (MongoDB Shell)

In diesem Beispiel verwenden wir den `$redact` Schritt mit dem `$$DESCEND` Operator, um selektiv Dokumente anzuzeigen, bei denen das `code` Feld „Reg“ entspricht.

Erstellen Sie Beispieldokumente

```
db.patient.insertMany([
  { "_id": 1, "code": "Emp", "patient": "John Doe", "DOB": "1/1/1980", "Hospital":
 "Main" },
  { "_id": 2, "code": "Reg", "patient": "Jane Doe", "DOB": "3/27/1989", "Hospital":
 "Cherry Hill" },
  { "_id": 3, "code": "Emp", "patient": "Bob Smith", "DOB": "6/15/1975", "Hospital":
 "Downtown" }
]);
```

Beispiel für eine Abfrage

```
db.patient.aggregate([
  { $redact: {
    $cond: {
      if: { $eq: ["Reg", "$code"] },
      then: "$$DESCEND",
      else: "$$PRUNE"
    }
  }}
]);
```

Ausgabe

```
{
  "_id": 2,
  "code": "Reg",
  "patient": "Jane Doe",
  "DOB": "3/27/1989",
  "Hospital": "Cherry Hill"
}
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$$DESCEND` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function redactPatients() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('patient');

  const result = await collection.aggregate([
    { $redact: {
      $cond: {
        if: { $eq: ["Reg", "$code"] },
        then: "$$DESCEND",
        else: "$$PRUNE"
      }
    }}
  ]).toArray();

  console.log(result);
  client.close();
}

redactPatients();
```

Python

```
from pymongo import MongoClient

def redact_patients():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client.test
    collection = db.patient

    result = list(collection.aggregate([
        { "$redact": {
            "$cond": {
                "if": { "$eq": ["Reg", "$code"] },
                "then": "$$DESCEND",
```

```
                "else": "$$PRUNE"
            }
        }}
    ]))

    print(result)
    client.close()

redact_patients()
```

$$KEEP

Die $$KEEP Systemvariable wird zusammen mit der $redact Phase in der Aggregationspipeline verwendet, um das aktuelle Dokument oder Feld unverändert zu lassen und es in die Ausgabe aufzunehmen.

Parameter

Keine

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt die Verwendung von $$KEEP in einer Amazon DocumentDB-Aggregationspipeline. Dokumente werden nur aufbewahrt, wenn der Zugriff auf „öffentlich“ steht, andernfalls werden sie entfernt.

Erstellen Sie Beispieldokumente

```
db.articles.insertMany([
  { title: "Article A", access: "public", content: "Visible content" },
  { title: "Article B", access: "private", content: "Hidden content" }
]);
```

Beispiel für eine Abfrage

```
db.articles.aggregate([
  {
    $redact: {
      $cond: [
        { $eq: ["$access", "public"] },
        "$$KEEP",
```

```
        "$$PRUNE"
      ]
    }
  }
]);
```

Ausgabe

```
[
  {
    "_id" : ObjectId("..."),
    "title" : "Article A",
    "access" : "public",
    "content" : "Visible content"
  }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des $$KEEP Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function run() {
  const client = new MongoClient(
    'mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-bundle.pem&replicaSet=rs0'
  );

  try {
    await client.connect();
    const db = client.db('test');
    const articles = db.collection('articles');

    const pipeline = [
      {
        $redact: {
          $cond: [
            { $eq: ["$access", "public"] },
            "$$KEEP",
```

```
            "$$PRUNE"
          ]
        }
      }
    ];

    const results = await articles.aggregate(pipeline).toArray();
    console.log(results);
  } finally {
    await client.close();
  }
}

run().catch(console.error);
```

Python

```
from pymongo import MongoClient

client = MongoClient(
    "mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-bundle.pem&replicaSet=rs0"
)

db = client.test
articles = db.articles

pipeline = [
    {
        "$redact": {
            "$cond": [
                {"$eq": ["$access", "public"]},
                "$$KEEP",
                "$$PRUNE"
            ]
        }
    }
]

results = list(articles.aggregate(pipeline))
print(results)

client.close()
```

$$PRUNE

Die $$PRUNE Systemvariable wird zusammen mit der $redact Phase in der Aggregationspipeline verwendet, um Dokumente oder eingebettete Dokumentebenen aus den Ergebnissen auszuschließen. Wenn eine Bedingung als Ergebnis ausgewertet wird$$PRUNE, wird das aktuelle Dokument oder Unterdokument aus der Ausgabe entfernt. Es wird normalerweise zusammen mit $ $DESCEND (um das Dokument zu behalten und zu durchsuchen) oder $$KEEP (um das Dokument auf allen Ebenen beizubehalten) verwendet.

Parameter

Keine. Die $$PRUNE Systemvariable wird ohne Parameter verwendet und muss mit $redact verwendet werden.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie Sie $$PRUNE mit with Benutzer$redact, die älter als 30 Jahre sind, von den Ergebnissen ausschließen können.

Erstellen Sie Beispieldokumente

```
db.users.insert([
  { _id:1, name: "Carlos Salazar", age: 35, address: { street: "123 Main St", city:
 "Anytown", state: "CA" } },
  { _id:2, name: "Saanvi Sarkar", age: 28, address: { street: "456 Oak Rd", city:
 "Someplace", state: "NY" } },
  { _id:3, name: "Li Juan", age: 42, address: { street: "789 Pine Ave", city:
 "Springfield", state: "TX" } }
])
```

Beispiel für eine Abfrage

```
db.users.aggregate([
  {
    $redact: {
      $cond: {
        if: { $gt: ["$age", 30] },
        then: "$$PRUNE",
        else: "$$DESCEND"
      }
```

```
    }
  }
])
```

Ausgabe

```
[
  {
    "_id": 2,
    "name": "Saanvi Sarkar",
    "age": 28,
    "address": {
      "street": "456 Oak Rd",
      "city": "Someplace",
      "state": "NY"
    }
  }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des $$PRUNE Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

const client = new MongoClient('mongodb://<username>:<password>@<cluster-
endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');

async function main() {
  await client.connect();
  const db = client.db('test');
  const users = db.collection('users');

  const result = await users.aggregate([
    {
      $redact: {
        $cond: {
          if: { $gt: ["$age", 30] },
```

```
          then: "$$PRUNE",
          else: "$$DESCEND"
        }
      }
    }
  ]).toArray();

  console.log(result);
  await client.close();
}

main();
```

Python

```
from pymongo import MongoClient

client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
db = client['test']
users = db['users']

result = list(users.aggregate([
    {
        '$redact': {
            '$cond': {
                'if': { '$gt': ['$age', 30] },
                'then': '$$PRUNE',
                'else': '$$DESCEND'
            }
        }
    }
]))

print(result)
client.close()
```

$ WURZEL

Der $R00T Operator in Amazon DocumentDB wird verwendet, um auf das gesamte Eingabedokument innerhalb einer Aggregationspipeline zu verweisen. Damit können Sie auf das

gesamte Dokument zugreifen und es bearbeiten, einschließlich all seiner verschachtelten Felder und Strukturen.

Parameter

Keine

Beispiel (MongoDB Shell)

Dieses Beispiel zeigt, wie $ROOT Sie ein Prüfprotokoll erstellen können, das das vollständige Originaldokument zusammen mit Metadaten darüber, wann es verarbeitet wurde, erfasst.

Erstellen Sie Beispieldokumente

```
db.orders.insertMany([
  {
    _id: 1,
    orderId: "ORD-2024-001",
    customer: "María García",
    email: "maría@example.com",
    items: [
      { product: "Laptop", quantity: 1, price: 1299.99 }
    ],
    totalAmount: 1299.99
  },
  {
    _id: 2,
    orderId: "ORD-2024-002",
    customer: "Arnav Desai",
    email: "arnav@example.com",
    items: [
      { product: "Mouse", quantity: 2, price: 29.99 },
      { product: "Keyboard", quantity: 1, price: 89.99 }
    ],
    totalAmount: 149.97
  }
]);
```

Beispiel für eine Abfrage

```
db.orders.aggregate([
  {
    $project: {
```

```
      processedAt: new Date(),
      originalDocument: "$$ROOT",
      summary: {
        $concat: [
          "Order ",
          "$orderId",
          " for ",
          "$customer",
          " - Total: $",
          { $toString: "$totalAmount" }
        ]
      }
    }
  }
]);
```

Ausgabe

```
[
  {
    _id: 1,
    processedAt: ISODate('2025-11-24T20:43:51.492Z'),
    originalDocument: {
      _id: 1,
      orderId: 'ORD-2024-001',
      customer: 'María García',
      email: 'maría@example.com',
      items: [ { product: 'Laptop', quantity: 1, price: 1299.99 } ],
      totalAmount: 1299.99
    },
    summary: 'Order ORD-2024-001 for María García - Total: $1299.99'
  },
  {
    _id: 2,
    processedAt: ISODate('2025-11-24T20:43:51.492Z'),
    originalDocument: {
      _id: 2,
      orderId: 'ORD-2024-002',
      customer: 'Arnav Desai',
      email: 'arnav@example.com',
      items: [
        { product: 'Mouse', quantity: 2, price: 29.99 },
        { product: 'Keyboard', quantity: 1, price: 89.99 }
```

```
      ],
      totalAmount: 149.97
    },
    summary: 'Order ORD-2024-002 for Arnav Desai - Total: $149.97'
  }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des $ROOT Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function createAuditLog() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const orders = db.collection('orders');

  const result = await orders.aggregate([
    {
      $project: {
        processedAt: new Date(),
        originalDocument: "$$ROOT",
        summary: {
          $concat: [
            "Order ",
            "$orderId",
            " for ",
            "$customer",
            " - Total: $",
            { $toString: "$totalAmount" }
          ]
        }
      }
    }
  ]).toArray();

  console.log(result);
```

```
  await client.close();
}

createAuditLog();
```

Python

```
from pymongo import MongoClient
from datetime import datetime

def create_audit_log():
    client = MongoClient('mongodb://username:password@docdb-
cluster.cluster-123456789.us-east-1.docdb.amazonaws.com:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['orders']

    result = list(collection.aggregate([
        {
            '$project': {
                'processedAt': datetime.now(),
                'originalDocument': '$$ROOT',
                'summary': {
                    '$concat': [
                        "Order ",
                        "$orderId",
                        " for ",
                        "$customer",
                        " - Total: $",
                        { '$toString': "$totalAmount" }
                    ]
                }
            }
        }
    ]))

    print(result)
    client.close()

create_audit_log()
```

$abs

Der `$abs` Operator in Amazon DocumentDB gibt den absoluten Wert einer Zahl zurück. Er kann in der Aggregationspipeline verwendet werden, um mathematische Operationen an numerischen Feldern durchzuführen.

Parameter

- `number`: Der numerische Ausdruck, für den der absolute Wert zurückgegeben wird.

Beispiel (MongoDB Shell)

Dieses Beispiel demonstriert die Verwendung des `$abs` Operators, um den absoluten Wert eines numerischen Feldes zu ermitteln.

Erstellen Sie Beispieldokumente

```
db.numbers.insertMany([
  { "_id": 1, "value": -5 },
  { "_id": 2, "value": 10 },
  { "_id": 3, "value": -3.14 },
  { "_id": 4, "value": 0 }
]);
```

Beispiel für eine Abfrage

```
db.numbers.aggregate([
  { $project: {
    "_id": 1,
    "absolute_value": { $abs: "$value" }
  }}
]);
```

Ausgabe

```
[
  { "_id": 1, "absolute_value": 5 },
  { "_id": 2, "absolute_value": 10 },
  { "_id": 3, "absolute_value": 3.14 },
  { "_id": 4, "absolute_value": 0 }
```

```
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des $abs Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function main() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('numbers');

  const result = await collection.aggregate([
    { $project: {
      "_id": 1,
      "absolute_value": { $abs: "$value" }
    }}
  ]).toArray();

  console.log(result);
  await client.close();
}

main();
```

Python

```
from pymongo import MongoClient

def main():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['numbers']
```

```
    result = list(collection.aggregate([
        { '$project': {
            "_id": 1,
            "absolute_value": { "$abs": "$value" }
        }}
    ]))

    print(result)
    client.close()

if __name__ == "__main__":
    main()
```

$add

Der `$add` Operator in Amazon DocumentDB wird verwendet, um Zahlen oder Daten zu addieren. Er kann verwendet werden, um arithmetische Operationen an numerischen Feldern durchzuführen oder um Datumsarithmetik durchzuführen, indem einem Datumsfeld eine Anzahl von Zeiteinheiten hinzugefügt wird.

Parameter

- `expression1`: Die erste Zahl oder das erste Datum, das hinzugefügt werden soll.
- `expression2`: Die zweite Zahl oder das zweite Datum, das hinzugefügt werden soll.
- `expression3`: (optional) Zusätzliche Zahlen oder Daten, die hinzugefügt werden sollen.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$add` Operator verwendet wird, um zwei Zahlen zu addieren.

Erstellen Sie Beispieldokumente

```
db.numbers.insertMany([
  { _id: 1, a: 5, b: 3 },
  { _id: 2, a: 10, b: 7 },
  { _id: 3, a: 2, b: 8 }
]);
```

Beispiel für eine Abfrage

```
db.numbers.aggregate([
  { $project: {
    _id: 1,
    sum: { $add: ["$a", "$b"] }
  }}
])
```

Ausgabe

```
[
  { "_id" : 1, "sum" : 8 },
  { "_id" : 2, "sum" : 17 },
  { "_id" : 3, "sum" : 10 }
]
```

In diesem Beispiel wird der $add Operator verwendet, um die Werte der b Felder a und für jedes Dokument hinzuzufügen und das Ergebnis im sum Feld zu speichern.

Codebeispiele

Um ein Codebeispiel für die Verwendung des $add Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('numbers');

  const result = await collection.aggregate([
    { $project: {
      _id: 1,
      sum: { $add: ['$a', '$b'] }
    }}
  ]).toArray();
```

```
  console.log(result);
  client.close();
}

example();
```

Python

```
from pymongo import MongoClient

client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
db = client['test']
collection = db['numbers']

result = list(collection.aggregate([
    { '$project': {
        '_id': 1,
        'sum': { '$add': ['$a', '$b'] }
    }}
]))

print(result)
client.close()
```

$ hinzufügen ToSet

Der `$addToSet` Aggregationsoperator gibt für jede Gruppe ein Array mit eindeutigen Werten aus einem angegebenen Ausdruck zurück. Er wird innerhalb der `$group` Phase verwendet, um unterschiedliche Werte zu akkumulieren, wodurch Duplikate automatisch entfernt werden.

Parameter

- `expression`: Der Ausdruck, der für jedes Dokument in der Gruppe ausgewertet werden soll.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$addToSet` Operator verwendet wird, um für jeden Kunden eindeutige Städte zu erfassen, in denen Bestellungen aufgegeben wurden.

Erstellen Sie Beispieldokumente

```
db.orders.insertMany([
  { _id: 1, customer: "Alice", city: "Seattle", amount: 100 },
  { _id: 2, customer: "Alice", city: "Portland", amount: 150 },
  { _id: 3, customer: "Bob", city: "Seattle", amount: 200 },
  { _id: 4, customer: "Alice", city: "Seattle", amount: 75 },
  { _id: 5, customer: "Bob", city: "Boston", amount: 300 }
]);
```

Beispiel für eine Abfrage

```
db.orders.aggregate([
  {
    $group: {
      _id: "$customer",
      cities: { $addToSet: "$city" }
    }
  }
]);
```

Ausgabe

```
[
  { _id: 'Bob', cities: [ 'Seattle', 'Boston' ] },
  { _id: 'Alice', cities: [ 'Seattle', 'Portland' ] }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$addToSet` Aggregationsoperators anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
```

```
  const db = client.db('test');
  const collection = db.collection('orders');

  const result = await collection.aggregate([
    {
      $group: {
        _id: "$customer",
        cities: { $addToSet: "$city" }
      }
    }
  ]).toArray();

  console.log(result);
  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['orders']

    result = list(collection.aggregate([
        {
            '$group': {
                '_id': '$customer',
                'cities': { '$addToSet': '$city' }
            }
        }
    ]))

    print(result)
    client.close()

example()
```

$addFields

Die `$addFields` Phase in der Amazon DocumentDB-Aggregationspipeline ermöglicht es Ihnen, neue berechnete Felder zu Dokumenten hinzuzufügen. Dies kann nützlich sein, um den Dokumenten abgeleitete oder transformierte Daten hinzuzufügen.

Parameter

- `newField`: Der Name des neuen Feldes, das hinzugefügt werden soll.
- `expression`: Ein Ausdruck, der den Wert des neuen Felds ergibt.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie Sie ein neues Feld `$addFields` hinzufügen`TotalInventory`, das den Gesamtbestand auf der Grundlage der Felder `Inventory.OnHand` und `Inventory.OrderQnty` berechnet.

Erstellen Sie Beispieldokumente

```
db.example.insertMany([
  {
    "Item": "Spray Paint",
    "Colors": ["Black", "Red", "Green", "Blue"],
    "Inventory": {
      "OnHand": 47,
      "MinOnHand": 50,
      "OrderQnty": 36
    },
    "UnitPrice": 3.99
  },
  {
    "Item": "Ruler",
    "Colors": ["Red", "Green", "Blue", "Clear", "Yellow"],
    "Inventory": {
      "OnHand": 47,
      "MinOnHand": 40
    },
    "UnitPrice": 0.89
  }
]);
```

Beispiel für eine Abfrage

```
db.example.aggregate([
  {
    $addFields: {
      TotalInventory: { $add: ["$Inventory.OnHand", "$Inventory.OrderQnty"] }
    }
  }
])
```

Ausgabe

```
[
  {
    "_id" : ObjectId("5bedafbcf65ff161707de24f"),
    "Item" : "Ruler",
    "Colors" : [ "Red", "Green", "Blue", "Clear", "Yellow" ],
    "Inventory" : {
      "OnHand" : 47,
      "MinOnHand" : 40
    },
    "UnitPrice" : 0.89,
    "TotalInventory" : 47
  },
  {
    "_id" : ObjectId("5bedafbcf65ff161707de250"),
    "Item" : "Spray Paint",
    "Colors" : [ "Black", "Red", "Green", "Blue" ],
    "Inventory" : {
      "OnHand" : 47,
      "MinOnHand" : 50,
      "OrderQnty" : 36
    },
    "UnitPrice" : 3.99,
    "TotalInventory" : 83
  }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$addFields` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
const db = client.db('test');
const collection = db.collection('example');

const result = await collection.aggregate([
  {
    $addFields: {
      TotalInventory: { $add: ['$Inventory.OnHand', '$Inventory.OrderQnty'] }
    }
  }
]).toArray();

console.log(result);

await client.close();
```

Python

```
from pymongo import MongoClient

client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
db = client['test']
collection = db['example']

result = list(collection.aggregate([
    {
        '$addFields': {
            'TotalInventory': { '$add': ['$Inventory.OnHand',
 '$Inventory.OrderQnty'] }
        }
    }
]))

print(result)
client.close()
```

$ alles ElementsTrue

Neu ab Version 4.0

Der `$allElementsTrue` Operator wird verwendet, um zu überprüfen, ob alle Elemente in einem Array einen wahren Wert ergeben.

Parameter

- `expression`: Ein Ausdruck, der zu einem Array ausgewertet wird.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt die Verwendung von`$allElementsTrue`, um zu überprüfen, ob alle Elemente in einem Array wahr sind.

Erstellen Sie Beispieldokumente

```
db.collection.insert([
  { "name": "John", "scores": [100, 90, 80] },
  { "name": "Jane", "scores": [80, 85, 0] },
  { "name": "Bob", "scores": [90, 95, null] }
])
```

Beispiel für eine Abfrage

```
db.collection.find({
  "scores": { "$allElementsTrue": [{ "$gt": 0 }] }
})
```

Ausgabe

```
[
  { "_id" : ObjectId("..."), "name" : "John", "scores" : [ 100, 90, 80 ] },
  { "_id" : ObjectId("..."), "name" : "Bob", "scores" : [ 90, 95, null ] }
]
```

In diesem Beispiel prüft die Abfrage, ob alle Elemente im `scores` Array größer als 0 sind. Das Dokument mit "name": "Jane" wird ausgeschlossen, weil das `scores` Array eine 0 enthält, was ein falscher Wert ist.

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$allElementsTrue` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('collection');

  const result = await collection.find({
    "scores": { "$allElementsTrue": [{ "$gt": 0 }] }
  }).toArray();

  console.log(result);

  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['collection']

    result = list(collection.find({
        "scores": {"$allElementsTrue": [{"$gt": 0}]}
    }))

    print(result)
```

```
    client.close()

example()
```

$and

Der `$and` Aggregationsoperator wertet mehrere Ausdrücke aus und gibt `true` nur zurück, wenn alle Ausdrücke zu 0 ausgewertet werden. `true` Wenn ein Ausdruck „Ja“ ist`false`, wird er zurückgegeben. `false`

Parameter

- `expressions`: Eine Reihe von Ausdrücken, die ausgewertet werden sollen.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$and` Operator verwendet wird, um zu überprüfen, ob Produkte mehrere Kriterien erfüllen.

Erstellen Sie Beispieldokumente

```
db.products.insertMany([
  { _id: 1, name: "Laptop", price: 1200, inStock: true },
  { _id: 2, name: "Mouse", price: 25, inStock: false },
  { _id: 3, name: "Keyboard", price: 75, inStock: true }
]);
```

Beispiel für eine Abfrage

```
db.products.aggregate([
  {
    $project: {
      name: 1,
      price: 1,
      inStock: 1,
      affordable: {
        $and: [
          { $lt: ["$price", 100] },
```

```
          { $eq: ["$inStock", true] }
        ]
      }
    }
  }
]);
```

Ausgabe

```
[
  { _id: 1, name: 'Laptop', price: 1200, inStock: true, affordable: false },
  { _id: 2, name: 'Mouse', price: 25, inStock: false, affordable: false },
  { _id: 3, name: 'Keyboard', price: 75, inStock: true, affordable: true }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des $and Aggregationsoperators anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('products');

  const result = await collection.aggregate([
    {
      $project: {
        name: 1,
        price: 1,
        inStock: 1,
        affordable: {
          $and: [
            { $lt: ["$price", 100] },
            { $eq: ["$inStock", true] }
          ]
```

```
        }
      }
    }
  ]).toArray();

  console.log(result);
  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['products']

    result = list(collection.aggregate([
        {
            '$project': {
                'name': 1,
                'price': 1,
                'inStock': 1,
                'affordable': {
                    '$and': [
                        { '$lt': ['$price', 100] },
                        { '$eq': ['$inStock', True] }
                    ]
                }
            }
        }
    ]))

    print(result)
    client.close()

example()
```

$ beliebig ElementTrue

Neu ab Version 4.0

Der `$anyElementTrue` Operator wird verwendet, um festzustellen, ob ein Element in einem Array wahr ist.

Parameter

- `field`: Ein auszuwertendes Array-Feld.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt die Verwendung von`$anyElementTrue`, um zu überprüfen, ob ein Element in einem Array wahr ist.

Erstellen Sie Beispieldokumente

```
db.grades.insertMany([
  { _id: 1, student: 'Tim', scores: [false, false, null] },
  { _id: 2, student: 'Bob', scores: [false, 0, false] },
  { _id: 3, student: 'Ivy', scores: [false, true, 0] }
])
```

Beispiel für eine Abfrage

```
db.grades.aggregate([
  {
    $project: {
      student: 1,
      isAnyTrue: { $anyElementTrue: ["$scores"] },
      _id: 0
    }
  }
])
```

Ausgabe

```
[
  { student: 'Tim', isAnyTrue: false },
```

```
  { student: 'Bob', isAnyTrue: false },
  { student: 'Ivy', isAnyTrue: true }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$anyElementTrue` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('grades');

  const result = await collection.aggregate([
    {
      $project: {
        student: 1,
        isAnyTrue: { $anyElementTrue: ["$scores"] },
        _id: 0
      }
    }
  ]).toArray();

  console.log(result);

  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
```

```
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['grades']

    result = list(collection.aggregate([
      {
        "$project": {
          "student": 1,
          "isAnyTrue": { "$anyElementTrue": ["$scores"] },
          "_id": 0
        }
      }
    ]))

    print(result)

    client.close()

example()
```

$array ElemAt

Der `$arrayElemAt` Operator in Amazon DocumentDB ermöglicht es Ihnen, ein Element anhand seiner Indexposition aus einem Array abzurufen. Dies ist besonders nützlich, wenn Sie auf ein bestimmtes Element innerhalb eines Array-Felds in Ihren Dokumenten zugreifen müssen.

Parameter

- `array`: Das Eingabe-Array, aus dem ein Element abgerufen werden soll.
- `index`: Die auf Null basierende Indexposition des abzurufenden Elements. Dieser Wert muss eine nicht negative Ganzzahl sein.

Beispiel (MongoDB Shell)

In diesem Beispiel zeigen wir, wie der `$arrayElemAt` Operator verwendet wird, um bestimmte Elemente aus dem `flight_miles` Array in der `miles` Sammlung abzurufen.

Erstellen Sie Beispieldokumente

```
db.miles.insertMany([
  { "_id" : 1, "member_since" : ISODate("1987-01-01T00:00:00Z"), "credit_card" : false,
 "flight_miles" : [ 1205, 2560, 880 ]},
  { "_id" : 2, "member_since" : ISODate("1982-01-01T00:00:00Z"), "credit_card" : true,
 "flight_miles" : [ 1205, 2560, 890, 2780 ]},
  { "_id" : 3, "member_since" : ISODate("1999-01-01T00:00:00Z"), "credit_card" : true,
 "flight_miles" : [ 1205, 880 ]}
]);
```

Beispiel für eine Abfrage

```
db.miles.aggregate([
  { $project: {
    "_id": 1,
    "first_mile": { $arrayElemAt: [ "$flight_miles", 0 ] },
    "last_mile": { $arrayElemAt: [ "$flight_miles", -1 ] }
  }}
]);
```

Ausgabe

```
{ "_id" : 1, "first_mile" : 1205, "last_mile" : 880 }
{ "_id" : 2, "first_mile" : 1205, "last_mile" : 2780 }
{ "_id" : 3, "first_mile" : 1205, "last_mile" : 880 }
```

In diesem Beispiel verwenden wir den `$arrayElemAt` Operator, um das erste und das letzte Element des `flight_miles` Arrays für jedes Dokument abzurufen.

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$arrayElemAt` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
```

```
  const db = client.db('test');
  const collection = db.collection('miles');

  const result = await collection.aggregate([
    { $project: {
      "_id": 1,
      "first_mile": { $arrayElemAt: [ "$flight_miles", 0 ] },
      "last_mile": { $arrayElemAt: [ "$flight_miles", -1 ] }
    }}
  ]).toArray();

  console.log(result);
  client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client.mydatabase
    collection = db.miles

    result = list(collection.aggregate([
        { "$project": {
            "_id": 1,
            "first_mile": { "$arrayElemAt": [ "$flight_miles", 0 ] },
            "last_mile": { "$arrayElemAt": [ "$flight_miles", -1 ] }
        }}
    ]))

    print(result)
    client.close()

example()
```

$array ToObject

Der `$arrayToObject` Operator in Amazon DocumentDB ist das Gegenteil des `$objectToArray` Operators. Er nimmt ein Array von Dokumenten mit Schlüssel-Wert-Paaren und konvertiert es in ein einzelnes Dokument. Dies ist besonders nützlich, wenn Sie ein Array von Schlüssel-Wert-Paaren wieder in eine Objekt- oder Dokumentstruktur konvertieren müssen.

Parameter

- `array expression`: Ein Ausdruck, der in ein Array aufgelöst wird. Die Array-Elemente müssen Dokumente mit zwei Feldern sein: k (der Schlüssel) und v (der Wert).

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie Sie `$arrayToObject` ein Array von Schlüssel-Wert-Paaren wieder in ein Dokument konvertieren können.

Erstellen Sie Beispieldokumente

```
db.videos.insertMany([
  { "_id": 1, "name": "Live Soft", "inventory": { "Des Moines": 1000, "Ames": 500 } },
  { "_id": 2, "name": "Top Pilot", "inventory": { "Mason City": 250, "Des Moines":
 1000 } },
  { "_id": 3, "name": "Romancing the Rock", "inventory": { "Mason City": 250, "Ames":
 500 } },
  { "_id": 4, "name": "Bravemind", "inventory": { "Mason City": 250, "Des Moines":
 1000, "Ames": 500 } }
]);
```

Beispiel für eine Abfrage

```
db.videos.aggregate([
  { $project: { name: 1, videos: { $objectToArray: "$inventory" } } },
  { $project: { name: 1, inventory: { $arrayToObject: "$videos" } } }
]);
```

Ausgabe

```
{ "_id" : 1, "name" : "Live Soft", "inventory" : { "Des Moines" : 1000, "Ames" :
 500 } }
```

```
{ "_id" : 2, "name" : "Top Pilot", "inventory" : { "Mason City" : 250, "Des Moines" :
 1000 } }
{ "_id" : 3, "name" : "Romancing the Rock", "inventory" : { "Mason City" : 250,
 "Ames" : 500 } }
{ "_id" : 4, "name" : "Bravemind", "inventory" : { "Mason City" : 250, "Des Moines" :
 1000, "Ames" : 500 } }
```

In diesem Beispiel wird der `$objectToArray` Operator verwendet, um das `inventory` Objekt in ein Array von Schlüssel-Wert-Paaren umzuwandeln. Der `$arrayToObject` Operator wird dann verwendet, um das Array wieder in ein Dokument zu konvertieren, wodurch die ursprüngliche Objektstruktur wiederhergestellt wird.

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$arrayToObject` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('videos');

  const result = await collection.aggregate([
    { $project: { name: 1, videos: { $objectToArray: '$inventory' } } },
    { $project: { name: 1, inventory: { $arrayToObject: '$videos' } } }
  ]).toArray();

  console.log(result);
  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient
```

```
def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['videos']

    result = list(collection.aggregate([
        { '$project': { 'name': 1, 'videos': { '$objectToArray': '$inventory' } } },
        { '$project': { 'name': 1, 'inventory': { '$arrayToObject': '$videos' } } }
    ]))

    print(result)
    client.close()

example()
```

$avg

Der `$avg` Aggregationsoperator in Amazon DocumentDB berechnet den Durchschnittswert des angegebenen Ausdrucks für die Dokumente, die in die Phase eingegeben werden. Dieser Operator ist nützlich, um den Durchschnitt eines numerischen Felds oder Ausdrucks in einer Reihe von Dokumenten zu berechnen.

Parameter

- `expression`: Der Ausdruck, der zur Berechnung des Durchschnitts verwendet werden soll. Dies kann ein Feldpfad (z. B.`"$field"`) oder ein Ausdruck (z. B.`{ $multiply: ["$field1", "$field2"] }`) sein.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$avg` Operator verwendet wird, um die durchschnittliche Punktzahl für eine Reihe von Studentendokumenten zu berechnen.

Erstellen Sie Beispieldokumente

```
db.students.insertMany([
  { name: "John", score: 85 },
```

```
  { name: "Jane", score: 92 },
  { name: "Bob", score: 78 },
  { name: "Alice", score: 90 }
]);
```

Beispiel für eine Abfrage

```
db.students.aggregate([
  { $group: {
    _id: null,
    avgScore: { $avg: "$score" }
  }}
]);
```

Ausgabe

```
[
  {
    "_id": null,
    "avgScore": 86.25
  }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des $avg Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function calculateAvgScore() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const result = await db.collection('students').aggregate([
    { $group: {
      _id: null,
      avgScore: { $avg: '$score' }
    }}
```

```
  ]).toArray();
  console.log(result);
  await client.close();
}

calculateAvgScore();
```

Python

```
from pymongo import MongoClient

def calculate_avg_score():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client.test
    result = list(db.students.aggregate([
        { '$group': {
            '_id': None,
            'avgScore': { '$avg': '$score' }
        }}
    ]))
    print(result)
    client.close()

calculate_avg_score()
```

$bucket

Neu ab Version 8.0

Wird von Elastic Cluster nicht unterstützt.

Die `$bucket` Aggregationsphase in Amazon DocumentDB ermöglicht es Ihnen, Eingabedokumente auf der Grundlage eines bestimmten Ausdrucks und der Bucket-Grenzen in Buckets zu gruppieren. Dies kann nützlich sein, um Daten zu analysieren, die in bestimmte Wertebereiche oder Kategorien fallen.

Parameter

- `groupBy`(erforderlich): Der Ausdruck, der den Wert angibt, nach dem gruppiert werden soll.

- `boundaries`(erforderlich): Ein Array mit doppelten Werten, die die Bucket-Grenzen definieren. Dokumente werden Buckets auf der Grundlage des `groupBy` Ausdruckswerts zugewiesen, der innerhalb der angegebenen Grenzen liegt.
- `default`(optional): Ein Literalwert, der für Dokumente ausgegeben wird, deren `groupBy` Ausdruckswert unter keine der angegebenen Grenzen fällt.
- `output`(optional): Ein Objekt, das die Informationen angibt, die für jeden Bucket ausgegeben werden sollen. Sie können Akkumulatoroperatoren wie`$sum`,, und verwenden `$avg``$min`, `$max` um Aggregationen für jeden Bucket zu berechnen.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie die `$bucket` Phase verwendet wird, um Verkaufsdaten nach Preisklassen zu gruppieren.

Erstellen Sie Beispieldokumente

```
db.sales.insertMany([
  { item: "abc", price: 10, quantity: 2, date: new Date("2020-09-01") },
  { item: "def", price: 20, quantity: 1, date: new Date("2020-10-01") },
  { item: "ghi", price: 5, quantity: 3, date: new Date("2020-11-01") },
  { item: "jkl", price: 15, quantity: 2, date: new Date("2020-12-01") },
  { item: "mno", price: 25, quantity: 1, date: new Date("2021-01-01") }
]);
```

Beispiel für eine Abfrage

```
db.sales.aggregate([
  {
    $bucket: {
      groupBy: "$price",
      boundaries: [0, 10, 20, 30],
      default: "Other",
      output: {
        "count": { $sum: 1 },
        "totalQuantity": { $sum: "$quantity" }
      }
    }
  },
  {
```

```
    $sort: { _id: 1 }
  }
])
```

Ausgabe

```
[
  { _id: 0, count: 1, totalQuantity: 3 },
  { _id: 10, count: 2, totalQuantity: 4 },
  { _id: 20, count: 2, totalQuantity: 2 }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$bucket` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const sales = db.collection('sales');

  const result = await sales.aggregate([
    {
      $bucket: {
        groupBy: "$price",
        boundaries: [0, 10, 20, 30],
        default: "Other",
        output: {
          "count": { $sum: 1 },
          "totalQuantity": { $sum: "$quantity" }
        }
      }
    },
    {
      $sort: { _id: 1 }
```

```
    }
  ]).toArray();

  console.log(result);
  client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&lsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    sales = db['sales']

    result = list(sales.aggregate([
        {
            '$bucket': {
                'groupBy': '$price',
                'boundaries': [0, 10, 20, 30],
                'default': 'Other',
                'output': {
                    'count': {'$sum': 1},
                    'totalQuantity': {'$sum': '$quantity'}
                }
            }
        },
        {
            "$sort": { "_id": 1 }
        }
    ]))

    print(result)
    client.close()

example()
```

$ceil

Neu ab Version 4.0

Der `$ceil` Operator in Amazon DocumentDB rundet wie in MongoDB eine Zahl auf die nächste Ganzzahl auf. Dies ist nützlich, wenn Sie mathematische Operationen an numerischen Feldern ausführen und sicherstellen müssen, dass das Ergebnis eine ganze Zahl ist.

Parameter

- `expression`: Der numerische Ausdruck, der aufgerundet werden soll.

Beispiel (MongoDB Shell)

Dieses Beispiel zeigt, wie der `$ceil` Operator verwendet wird, um ein numerisches Feld aufzurunden.

Erstellen Sie Beispieldokumente

```
db.numbers.insertMany([
  { "_id": 1, "value": 3.14 },
  { "_id": 2, "value": -2.7 },
  { "_id": 3, "value": 0 }
])
```

Beispiel für eine Abfrage

```
db.numbers.aggregate([
  { $project: {
    "roundedUp": { $ceil: "$value" }
  }}
])
```

Ausgabe

```
{ "_id": 1, "roundedUp": 4 }
{ "_id": 2, "roundedUp": -2 }
{ "_id": 3, "roundedUp": 0 }
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$ceil` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('numbers');

  const result = await collection.aggregate([
    { $project: {
      "roundedUp": { $ceil: "$value" }
    }}
  ]).toArray();

  console.log(result);
  client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client.test
    collection = db.numbers

    result = list(collection.aggregate([
        { '$project': {
            "roundedUp": { '$ceil': "$value" }
        }}
```

```
    ]))

    print(result)
    client.close()

example()
```

$ Stream ändern

Wird von Elastic Cluster nicht unterstützt.

In der `$changeStream` Aggregationsphase wird ein Change-Stream-Cursor geöffnet, um Änderungen an einer Sammlung in Echtzeit zu überwachen. Sie gibt Änderungsereignisdokumente zurück, wenn Einfüge-, Aktualisierungs-, Ersetzungs- oder Löschvorgänge ausgeführt werden.

Parameter

- `fullDocument`: Gibt an, ob bei Aktualisierungsvorgängen das vollständige Dokument zurückgegeben werden soll. Die Optionen lauten `default` oder `updateLookup`.
- `resumeAfter`: Optional. Setzen Sie das Token fort, um ab einem bestimmten Punkt im Change-Stream fortzufahren.
- `startAtOperationTime`: Optional. Zeitstempel, ab dem der Change-Stream gestartet werden soll.
- `allChangesForCluster`: Optional. Boolescher Wert: Wann`true`, überwacht alle Änderungen im gesamten Cluster (für die Admin-Datenbank). Wenn `false` (Standard), wird nur die angegebene Sammlung überwacht.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie die `$changeStream` Bühne verwendet wird, um Änderungen an einer Sammlung zu überwachen.

Beispiel für eine Abfrage

```
// Open change stream first
const changeStream = db.inventory.aggregate([
  { $changeStream: { fullDocument: "updateLookup" } }
]);
```

```
// In another session, insert a document
db.inventory.insertOne({ _id: 1, item: "Widget", qty: 10 });

// Back in the first session, read the change event
if (changeStream.hasNext()) {
  print(tojson(changeStream.next()));
}
```

Ausgabe

```
{
  _id: { _data: '...' },
  operationType: 'insert',
  clusterTime: Timestamp(1, 1234567890),
  fullDocument: { _id: 1, item: 'Widget', qty: 10 },
  ns: { db: 'test', coll: 'inventory' },
  documentKey: { _id: 1 }
}
```

Codebeispiele

Um ein Codebeispiel für die Verwendung der `$changeStream` Aggregationsphase anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('inventory');

  // Open change stream
  const changeStream = collection.watch([]);

  changeStream.on('change', (change) => {
    console.log('Change detected:', change);
  });
```

```
  // Simulate insert in another operation
  setTimeout(async () => {
    await collection.insertOne({ _id: 1, item: 'Widget', qty: 10 });
  }, 1000);

  // Keep connection open to receive changes
  // In production, handle cleanup appropriately
}

example();
```

Python

```
from pymongo import MongoClient
import threading
import time

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['inventory']

    # Open change stream
    change_stream = collection.watch([])

    # Insert document in separate thread after delay
    def insert_doc():
        time.sleep(1)
        collection.insert_one({'_id': 1, 'item': 'Widget', 'qty': 10})

    threading.Thread(target=insert_doc).start()

    # Watch for changes
    for change in change_stream:
        print('Change detected:', change)
        break  # Exit after first change

    client.close()

example()
```

$cmp

Der `$cmp` Operator in Amazon DocumentDB wird verwendet, um zwei Werte zu vergleichen und einen Ganzzahlwert zurückzugeben, der ihre relative Reihenfolge angibt. Es ist ein Vergleichsoperator, der zwei Ausdrücke vergleicht und einen Ganzzahlwert von -1, 0 oder 1 zurückgibt, je nachdem, ob der erste Wert kleiner, gleich oder größer als der zweite Wert ist.

Parameter

- `expression1`: Der erste Ausdruck, der verglichen werden soll.
- `expression2`: Der zweite zu vergleichende Ausdruck.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt die Verwendung des `$cmp` Operators, um zwei numerische Werte zu vergleichen.

Erstellen Sie Beispieldokumente

```
db.collection.insertMany([
  { _id: 1, value1: 10, value2: 20 },
  { _id: 2, value1: 15, value2: 15 },
  { _id: 3, value1: 20, value2: 10 }
]);
```

Beispiel für eine Abfrage

```
db.collection.find({
  $expr: {
    $cmp: ["$value1", "$value2"]
  }
})
```

Ausgabe

```
[
  { "_id" : 1, "value1" : 10, "value2" : 20 },
  { "_id" : 3, "value1" : 20, "value2" : 10 }
]
```

In diesem Beispiel vergleicht der `$cmp` Operator die `value2` Felder `value1` und für jedes Dokument. Das Ergebnis ist:

```
- `$cmp: ["$value1", "$value2"]` returns -1 for the first document (10 < 20), 0 for the
 second document (15 = 15), and 1 for the third document (20 > 10).
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$cmp` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

Hier ist ein Beispiel für die Verwendung des `$cmp` Operators in einer Node.js Anwendung mit dem `mongodb` Treiber:

```
const { MongoClient } = require('mongodb');

const client = new MongoClient('mongodb://<username>:<password>@<cluster-
endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');

async function main() {
  await client.connect();
  const db = client.db('test');
  const collection = db.collection('mycollection');

  // Insert sample documents
  await collection.insertMany([
    { _id: 1, value1: 10, value2: 20 },
    { _id: 2, value1: 15, value2: 15 },
    { _id: 3, value1: 20, value2: 10 }
  ]);

  // Query using $cmp operator
  const result = await collection.find({
    $expr: {
      $cmp: ['$value1', '$value2']
    }
  }).toArray();

  console.log(result);
```

```
  await client.close();
}

main();
```

Python

Hier ist ein Beispiel für die Verwendung des $cmp Operators in einer Python-Anwendung mit dem pymongo Treiber:

```
from pymongo import MongoClient

client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
db = client['test']
collection = db['mycollection']

# Insert sample documents
collection.insert_many([
    {'_id': 1, 'value1': 10, 'value2': 20},
    {'_id': 2, 'value1': 15, 'value2': 15},
    {'_id': 3, 'value1': 20, 'value2': 10}
])

# Query using $cmp operator
result = list(collection.find({
    '$expr': {
        '$cmp': ['$value1', '$value2']
    }
}))

print(result)

client.close()
```

Die Ausgabe sowohl des Python-Beispiels als auch des Node.js Python-Beispiels entspricht der des MongoDB-Shell-Beispiels:

```
[
  { "_id" : 1, "value1" : 10, "value2" : 20 },
```

```
  { "_id" : 2, "value1" : 15, "value2" : 15 },
  { "_id" : 3, "value1" : 20, "value2" : 10 }
]
```

$collStats

Neu ab Version 4.0

Die `$collStats` Aggregationsphase in Amazon DocumentDB bietet Statistiken über die angegebene Sammlung, ähnlich dem `db.collection.stats()` Befehl in der MongoDB-Shell. In dieser Phase können Informationen über die Sammlung abgerufen werden, z. B. die Anzahl der Dokumente, die Gesamtgröße der Sammlung und verschiedene Leistungskennzahlen.

Parameter

- `latencyStats`: (optional) Ein Dokument, das die Optionen für die Erfassung von Latenzstatistiken spezifiziert. Dieser Parameter wird in Amazon DocumentDB nicht unterstützt.
- `recordStats`: (optional) Ein Dokument, das die Optionen für die Erfassung von Datensatzstatistiken festlegt. Dieser Parameter wird in Amazon DocumentDB nicht unterstützt.
- `queryExecStats`: (optional) Ein Dokument, das die Optionen für die Erfassung von Statistiken zur Abfrageausführung spezifiziert. Dieser Parameter wird in Amazon DocumentDB nicht unterstützt.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie die `$collStats` Aggregationsphase verwendet wird, um Statistiken über eine `test` in der db Datenbank benannte Sammlung abzurufen.

Erstellen Sie Beispieldokumente

```
db.test.insertMany([
  { "name": "John", "age": 30 },
  { "name": "Jane", "age": 25 },
  { "name": "Bob", "age": 35 }
]);
```

Beispiel für eine Abfrage

```
db.test.aggregate([
  { $collStats: {} }
]);
```

Ausgabe

```
{
  "ns" : "db.test",
  "count" : 3,
  "size" : 87,
  "avgObjSize" : 29,
  "storageSize" : 40960,
  "capped" : false,
  "nindexes" : 1,
  "totalIndexSize" : 8192,
  "indexSizes" : {
    "_id_" : 8192
  },
  "collScans" : 0,
  "idxScans" : 0,
  "opCounter" : {
    "numDocsIns" : 3,
    "numDocsUpd" : 0,
    "numDocsDel" : 0
  },
  "cacheStats" : {
    "collBlksHit" : 0,
    "collBlksRead" : 0,
    "collHitRatio" : 0,
    "idxBlksHit" : 0,
    "idxBlksRead" : 0,
    "idxHitRatio" : 0
  },
  "lastReset" : "2023-04-11T12:00:00Z",
  "ok" : 1,
  "operationTime" : Timestamp(1681206000, 1)
}
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$collStats` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

Hier ist ein Beispiel für die Verwendung der `$collStats` Aggregationsphase in einer Node.js Anwendung, die den offiziellen Node.js MongoDB-Treiber verwendet:

```
const { MongoClient } = require('mongodb');

async function runCollStatsExample() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('db');
  const collection = db.collection('test');

  const result = await collection.aggregate([
    { $collStats: {} }
  ]).toArray();

  console.log(result);

  await client.close();
}

runCollStatsExample();
```

Python

Hier ist ein Beispiel für die Verwendung der `$collStats` Aggregationsphase in einer Python-Anwendung mithilfe des PyMongo Treibers:

```
from pymongo import MongoClient

def run_coll_stats_example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['db']
    collection = db['test']

    result = list(collection.aggregate([
        { '$collStats': {} }
    ]))
```

```
    print(result)

    client.close()

run_coll_stats_example()
```

$concat

Der `$concat` Aggregationsoperator in Amazon DocumentDB verkettet (oder kombiniert) mehrere Zeichenketten in einem Dokument, um eine einzige Zeichenfolge zu erzeugen, die an die Anwendung zurückgegeben werden kann. Dies reduziert den Arbeitsaufwand in der Anwendung, da die Bearbeitung der Zeichenfolge auf Datenbankebene erfolgt.

Parameter

- `expression1`: Die erste Zeichenfolge, die verkettet werden soll.
- `expression2`: Die zweite Zeichenfolge, die verkettet werden soll.
- `...`: Zusätzliche Zeichenketten zum Verketten (optional).

Beispiel (MongoDB Shell)

In diesem Beispiel verketten wir die Vor- und Nachnamen der Benutzer, um den vollständigen Namen jeder Person zu erhalten.

Erstellen Sie Beispieldokumente

```
db.people.insertMany([
  { "_id":1, "first_name":"Jane", "last_name":"Doe", "DOB":"2/1/1999", "Desk": "MSP102-
MN"},
  { "_id":2, "first_name":"John", "last_name":"Doe", "DOB":"12/21/1992", "Desk":
 "DSM301-IA"},
  { "_id":3, "first_name":"Steve", "last_name":"Smith", "DOB":"3/21/1981",
 "Desk":"MKE233-WI"}
])
```

Beispiel für eine Abfrage

```
db.people.aggregate([
  { $project: { full_name: { $concat: [ "$first_name", " ", "$last_name"] } } }
```

```
])
```

Ausgabe

```
{ "_id" : 1, "full_name" : "Jane Doe" }
{ "_id" : 2, "full_name" : "John Doe" }
{ "_id" : 3, "full_name" : "Steve Smith" }
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$concat` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function concatenateNames() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');

  const result = await db.collection('people').aggregate([
    { $project: { full_name: { $concat: [ "$first_name", " ", "$last_name"] } } }
  ]).toArray();

  console.log(result);

  await client.close();
}

concatenateNames();
```

Python

```
from pymongo import MongoClient

def concatenate_names():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
```

```
    db = client['test']

    result = list(db.people.aggregate([
        { '$project': { 'full_name': { '$concat': [ '$first_name', ' ',
  '$last_name' ] } } }
    ]))

    print(result)

    client.close()

concatenate_names()
```

$concatArrays

Der `$concatArrays` Aggregationsoperator in Amazon DocumentDB wird verwendet, um zwei oder mehr Arrays zu einem einzigen Array zu verketten. Dies kann nützlich sein, wenn Sie mehrere Datenarrays zur weiteren Verarbeitung oder Analyse zu einem einzigen Array kombinieren müssen.

Parameter

- `array1`: Das erste Array, das verkettet werden soll.
- `array2`: Das zweite Array, das verkettet werden soll.
- `[array3, ...]`: (optional) Zusätzliche Arrays, die verkettet werden sollen.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$concatArrays` Operator verwendet wird, um zwei Arrays zu einem einzigen Array zu kombinieren.

Erstellen Sie Beispieldokumente

```
db.collection.insertMany([
  {
    "_id": 1,
    "name": "John Doe",
    "hobbies": ["reading", "swimming"],
    "skills": ["programming", "design"]
  },
```

```
  {
    "_id": 2,
    "name": "Jane Smith",
    "hobbies": ["hiking", "cooking"],
    "skills": ["marketing", "analysis"]
  }
]);
```

Beispiel für eine Abfrage

```
db.collection.aggregate([
  {
    $project: {
      _id: 0,
      name: 1,
      all_activities: { $concatArrays: ["$hobbies", "$skills"] }
    }
  }
]);
```

Ausgabe

```
[
  {
    "name": "John Doe",
    "all_activities": [
      "reading",
      "swimming",
      "programming",
      "design"
    ]
  },
  {
    "name": "Jane Smith",
    "all_activities": [
      "hiking",
      "cooking",
      "marketing",
      "analysis"
    ]
  }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$concatArrays` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('mydb');
  const collection = db.collection('mycollection');

  const result = await collection.aggregate([
    {
      $project: {
        _id: 0,
        name: 1,
        all_activities: { $concatArrays: ['$hobbies', '$skills'] }
      }
    }
  ]).toArray();

  console.log(result);
  client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['mydb']
    collection = db['mycollection']
```

```
    result = list(collection.aggregate([
        {
            '$project': {
                '_id': 0,
                'name': 1,
                'all_activities': { '$concatArrays': ['$hobbies', '$skills'] }
            }
        }
    ]))

    print(result)
    client.close()

example()
```

$cond

Der `$cond` Operator in Amazon DocumentDB wird verwendet, um einen bedingten Ausdruck auszuwerten und einen von zwei möglichen Ergebnisausdrücken zurückzugeben.

Parameter

- `if`: Der boolesche Ausdruck, der ausgewertet werden soll.
- `then`: Der Ausdruck, der zurückgegeben werden soll, wenn der `if` Ausdruck wahr ist.
- `else`: Der Ausdruck, der zurückgegeben werden soll, wenn der `if` Ausdruck falsch ist.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$cond` Operator verwendet wird, um einen Wert zurückzugeben, der auf dem Alter einer Person basiert.

Erstellen Sie Beispieldokumente

```
db.people.insertMany([
  { _id: 1, name: "John Doe", age: 35 },
  { _id: 2, name: "Jane Doe", age: 25 },
  { _id: 3, name: "Bob Smith", age: 65 }
]);
```

Beispiel für eine Abfrage

```
db.people.aggregate([
  {
    $project: {
      name: 1,
      ageGroup: {
        $cond: {
          if: { $lt: ["$age", 30] },
          then: "young",
          else: {
            $cond: {
              if: { $lt: ["$age", 65] },
              then: "middle-aged",
              else: "elderly"
            }
          }
        }
      }
    }
  }
])
```

Ausgabe

```
[
  { "_id" : 1, "name" : "John Doe", "ageGroup" : "middle-aged" },
  { "_id" : 2, "name" : "Jane Doe", "ageGroup" : "young" },
  { "_id" : 3, "name" : "Bob Smith", "ageGroup" : "elderly" }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des $cond Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
```

```
  const db = client.db('test');
  const collection = db.collection('people');

  const result = await collection.aggregate([
    { $project: {
        name: 1,
        ageGroup: {
            $cond: {
                if: { $lt: ["$age", 30] },
                then: "young",
                else: {
                    $cond: {
                        if: { $lt: ["$age", 65] },
                        then: "middle-aged",
                        else: "elderly"
                    }
                }
            }
        }
      }
    }
  ]).toArray();

  console.log(result);
  client.close();
}

example();
```

Python

```
from pymongo import MongoClient


def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client.test
    collection = db.people

    result = list(collection.aggregate([
        {
```

```
            '$project': {
                'name': 1,
                'ageGroup': {
                    '$cond': {
                        'if': { '$lt': ["$age", 30]},
                        'then': "young",
                        'else': {
                            '$cond': {
                                'if': { '$lt': ["$age", 65]},
                                'then': "middle-aged",
                                'else': "elderly"
                            }
                        }
                    }
                }
            }
        }
    ]))

    print(result)
    client.close()

example()
```

$ konvertieren

Neu ab Version 4.0

Der `$convert` Operator in Amazon DocumentDB wird verwendet, um einen Wert von einem Datentyp in einen anderen zu konvertieren. Dieser Operator ist nützlich, wenn Sie Operationen mit Daten verschiedener Typen ausführen müssen, z. B. die Konvertierung einer Zeichenfolge in eine Zahl oder eines Datums in einen Zeitstempel.

Parameter

- `to`: Der Zieldatentyp, in den der Wert konvertiert werden soll. Unterstützte Werte sind `"string"`, `"double"`, `"long"`, `"int"`, `"date"` und `"boolean"`.
- `from`: Der aktuelle Datentyp des Werts. Falls nicht angegeben, versucht Amazon DocumentDB, den Datentyp automatisch zu erkennen.

- onError: (optional) Der Wert, der zurückgegeben werden soll, wenn die Konvertierung fehlschlägt. Kann ein bestimmter Wert oder einer der folgenden Sonderwerte sein:"null","zerofill", oder"error".
- onNull: (optional) Der Wert, der zurückgegeben werden soll, wenn der Eingabewertnull. Kann ein bestimmter Wert oder einer der folgenden Sonderwerte sein:"null","zerofill", oder"error".

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt die Konvertierung eines Zeichenkettenwerts in ein Datum mithilfe des $convert Operators.

Erstellen Sie Beispieldokumente

```
db.users.insertMany([
  { _id: 1, name: "John Doe", joinedOn: "2022-01-01" },
  { _id: 2, name: "Jane Smith", joinedOn: "2023-02-15" },
  { _id: 3, name: "Bob Johnson", joinedOn: "invalid date" }
]);
```

Beispiel für eine Abfrage

```
db.users.aggregate([
  {
    $project: {
      _id: 1,
      name: 1,
      joinedOn: {
        $convert: {
          input: "$joinedOn",
          to: "date",
          onError: "null",
          onNull: "null"
        }
      }
    }
  }
])
```

Ausgabe

```
[
  { "_id" : 1, "name" : "John Doe", "joinedOn" : ISODate("2022-01-01T00:00:00Z") },
  { "_id" : 2, "name" : "Jane Smith", "joinedOn" : ISODate("2023-02-15T00:00:00Z") },
  { "_id" : 3, "name" : "Bob Johnson", "joinedOn" : null }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$convert` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require("mongodb");

async function example() {
  const client = await MongoClient.connect("mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false");
  const db = client.db("test");
  const users = db.collection("users");

  const results = await users.aggregate([
    {
      $project: {
        _id: 1,
        name: 1,
        joinedOn: {
          $convert: {
            input: "$joinedOn",
            to: "date",
            onError: "null",
            onNull: "null"
          }
        }
      }
    }
  ]).toArray();

  console.log(results);
  client.close();
}
```

```
example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient("mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false")
    db = client["test"]
    users = db["users"]

    results = list(users.aggregate([
        {
            "$project": {
                "_id": 1,
                "name": 1,
                "joinedOn": {
                    "$convert": {
                        "input": "$joinedOn",
                        "to": "date",
                        "onError": "null",
                        "onNull": "null"
                    }
                }
            }
        }
    ]))

    print(results)
    client.close()

example()
```

$count

Die `$count` Aggregationsphase in Amazon DocumentDB wird verwendet, um die Anzahl der Dokumente zu zählen, die in die Phase gelangen. Sie wird häufig als letzte Phase in einer Aggregationspipeline verwendet, um die Gesamtzahl der Dokumente zurückzugeben, die den vorherigen Phasen entsprechen.

Parameter

- `field`: Das zu zählende Feld. Dieser Parameter ist optional. Wenn er nicht angegeben wird, zählt die Phase die Gesamtzahl der Eingabedokumente.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$count` Schritt verwendet wird, um die Gesamtzahl der Dokumente in einer Sammlung abzurufen.

Erstellen Sie Beispieldokumente

```
db.users.insertMany([
  { name: "John", age: 30 },
  { name: "Jane", age: 25 },
  { name: "Bob", age: 35 },
  { name: "Alice", age: 28 }
]);
```

Beispiel für eine Abfrage

```
db.users.aggregate([
  { $count: "total" }
]);
```

Ausgabe

```
{ "total" : 4 }
```

Das Beispiel aggregiert die `users` Sammlung und verwendet die `$count` Phase, um die Gesamtzahl der Dokumente zu zählen.

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$count` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');
```

```
async function countDocuments() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('mydb');
  const collection = db.collection('users');

  const result = await collection.aggregate([
    { $count: "total" }
  ]).toArray();

  console.log(result[0].total);

  await client.close();
}

countDocuments();
```

Python

```
from pymongo import MongoClient

def count_documents():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['mydb']
    collection = db['users']

    result = list(collection.aggregate([
        { '$count': "total" }
    ]))

    print(result[0]['total'])

    client.close()

count_documents()
```

$currentOp

Die `$currentOp` Aggregationsphase gibt Informationen über aktuell ausgeführte Operationen in der Datenbank zurück. Diese Phase ist nützlich für die Überwachung aktiver Abfragen und Operationen in einer Aggregationspipeline.

Parameter

- `allUsers`(optional): Wenn auf gesetzt`true`, werden Operationen für alle Benutzer zurückgegeben. Der Standardwert ist `false`.
- `idleConnections`(optional): Wenn auf gesetzt`true`, schließt dies inaktive Verbindungen ein. Der Standardwert ist `false`.
- `idleCursors`(optional): Wenn auf gesetzt`true`, enthält dies Informationen über Cursor im Leerlauf. Der Standardwert ist `false`.
- `idleSessions`(optional): Wenn auf gesetzt`true`, enthält es Informationen über inaktive Sitzungen. Der Standardwert ist `true`.
- `localOps`(optional): Wenn auf gesetzt`true`, schließt dies lokale Operationen ein. Der Standardwert ist `false`.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie die `$currentOp` Aggregationsphase verwendet wird, um Informationen über aktive Lesevorgänge abzurufen.

Beispiel für eine Abfrage

```
db.aggregate([
  { $currentOp: { allUsers: true, idleConnections: false } },
  { $match: { op: "query" } }
])
```

Ausgabe

```
[
  {
    "opid": "12345",
    "active": true,
    "op": "query",
    "ns": "test.users",
```

```
    "secs_running": 2
  }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$currentOp` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('admin');

  const result = await db.aggregate([
    { $currentOp: { allUsers: true, idleConnections: false } },
    { $match: { op: "query" } }
  ]).toArray();

  console.log(result);
  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['admin']

    result = list(db.aggregate([
        { '$currentOp': { 'allUsers': True, 'idleConnections': False } },
        { '$match': { 'op': 'query' } }
```

```
    ]))

    print(result)
    client.close()

example()
```

$DateAdd

Neu ab Version 5.0

Mit dem `$dateAdd` Aggregationsoperator in Amazon DocumentDB können Sie einem Datums- und Uhrzeitwert eine Dauer hinzufügen.

Parameter

- `date`: Ein Datums- und Uhrzeitwert, dem eine Dauer hinzugefügt werden soll.
- `duration`: Die Dauer, die dem `date` Wert hinzugefügt werden soll. Dies kann als Objekt mit Schlüsseln für`years`,,`months`, `weeks` `days` `hours``minutes`, und angegeben `seconds` werden.
- `timezone`: (optional) Die Zeitzone, die beim Hinzufügen des Datums verwendet werden soll. Falls nicht angegeben, wird die Standardzeitzone des Amazon DocumentDB-Clusters verwendet.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$dateAdd` Operator verwendet wird, um einem Datum 2 Tage und 12 Stunden hinzuzufügen.

Erstellen Sie Beispieldokumente

```
db.events.insertMany([
  { _id: 1, eventDate: ISODate("2023-04-01T10:00:00Z") },
  { _id: 2, eventDate: ISODate("2023-04-02T12:00:00Z") },
  { _id: 3, eventDate: ISODate("2023-04-03T14:00:00Z") }
]);
```

Beispiel für eine Abfrage

```
db.events.aggregate([
  {
    $project: {
```

```
      _id: 1,
      eventDate: 1,
      eventDatePlustwodaysandtwelvehours: {
        $dateAdd: {
          startDate: {
            $dateAdd: {
              startDate: "$eventDate",
              unit: "day",
              amount: 2
            }
          },
          unit: "hour",
          amount: 12
        }
      }
    }
  }
])
```

Ausgabe

```
[
  {
    "_id": 1,
    "eventDate": "2023-04-01T10:00:00Z",
    "eventDatePlustwodaysandtwelvehours": ISODate("2023-04-03T22:00:00Z)"
  },
  {
    "_id": 2,
    "eventDate": "2023-04-02T12:00:00Z",
    "eventDatePlustwodaysandtwelvehours": ISODate("2023-04-05T00:00:00Z)"
  },
  {
    "_id": 3,
    "eventDate": "2023-04-03T14:00:00Z",
    "eventDatePlustwodaysandtwelvehours": ISODate("2023-04-06T02:00:00Z)"
  }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$dateAdd` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('events');

  const result = await collection.aggregate([
    {
      $project: {
        _id: 1,
        eventDate: 1,
        eventDatePlustwodaysandtwelvehours: {
          $dateAdd: {
            startDate: {
              $dateAdd: {
                startDate: "$eventDate",
                unit: "day",
                amount: 2
              }
            },
            unit: "hour",
            amount: 12
          }
        }
      }
    }
  ]).toArray();

  console.log(result);

  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient
```

```
from bson.date_time import datetime

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['events']

    result = list(collection.aggregate([
        {
            '$project': {
                '_id': 1,
                'eventDate': 1,
                'eventDatePlustwodaysandtwelvehours': {
                    '$dateAdd': {
                        'startDate': {
                            '$dateAdd' : {
                                'startDate': '$eventDate',
                                'unit': 'day',
                                'amount': 2,
                            }
                        },
                        'unit': 'hour',
                        'amount': 12,
                    }
                }
            }
        }
    ]))

    print(result)

    client.close()

example()
```

$DateDiff

Neu ab Version 5.0

Wird von Elastic Cluster nicht unterstützt.

Der `$dateDiff` Aggregationsoperator berechnet die Differenz zwischen zwei Daten in angegebenen Einheiten. Er gibt die Anzahl der Einheitengrenzen zurück, die zwischen dem Start- und dem Enddatum überschritten wurden.

Parameter

- `startDate`: Der Ausdruck für das Anfangsdatum.
- `endDate`: Der Ausdruck für das Enddatum.
- `unit`: Die Zeiteinheit für die Differenz. Unterstützte Einheiten sind `year`,`quarter`,`month`,`week`,`day`,`hour`,`minute`,`second`, und`millisecond`.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$dateDiff` Operator verwendet wird, um die Anzahl der Tage zwischen Auftragserteilung und Lieferung zu berechnen.

Erstellen Sie Beispieldokumente

```
db.shipments.insertMany([
  {
    orderId: 1001,
    orderDate: ISODate("2025-01-10T08:00:00Z"),
    deliveryDate: ISODate("2025-01-15T14:30:00Z")
  },
  {
    orderId: 1002,
    orderDate: ISODate("2025-02-05T10:00:00Z"),
    deliveryDate: ISODate("2025-02-12T16:45:00Z")
  }
]);
```

Beispiel für eine Abfrage

```
db.shipments.aggregate([
  {
    $project: {
      orderId: 1,
      orderDate: 1,
      deliveryDate: 1,
      daysToDeliver: {
```

```
        $dateDiff: {
          startDate: "$orderDate",
          endDate: "$deliveryDate",
          unit: "day"
        }
      }
    }
  }
]);
```

Ausgabe

```
[
  {
    _id: ObjectId('6924a5f2d66dcae121d29517'),
    orderId: 1001,
    orderDate: ISODate('2025-01-10T08:00:00.000Z'),
    deliveryDate: ISODate('2025-01-15T14:30:00.000Z'),
    daysToDeliver: 5
  },
  {
    _id: ObjectId('6924a5f2d66dcae121d29518'),
    orderId: 1002,
    orderDate: ISODate('2025-02-05T10:00:00.000Z'),
    deliveryDate: ISODate('2025-02-12T16:45:00.000Z'),
    daysToDeliver: 7
  }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$dateDiff` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
```

```
  const db = client.db('test');
  const shipments = db.collection('shipments');

  const result = await shipments.aggregate([
    {
      $project: {
        orderId: 1,
        orderDate: 1,
        deliveryDate: 1,
        daysToDeliver: {
          $dateDiff: {
            startDate: "$orderDate",
            endDate: "$deliveryDate",
            unit: "day"
          }
        }
      }
    }
  ]).toArray();

  console.log(result);
  client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    shipments = db['shipments']

    result = list(shipments.aggregate([
        {
            "$project": {
                "orderId": 1,
                "orderDate": 1,
                "deliveryDate": 1,
```

```
                "daysToDeliver": {
                    "$dateDiff": {
                        "startDate": "$orderDate",
                        "endDate": "$deliveryDate",
                        "unit": "day"
                    }
                }
            }
        }
    ]))

    print(result)
    client.close()

example()
```

$datum FromString

Der `$dateFromString` Aggregationsoperator in Amazon DocumentDB ermöglicht es Ihnen, eine Datums- und Uhrzeitzeichenfolge in ein Datumsobjekt zu konvertieren. Dies ist nützlich, wenn Ihre Daten als Zeichenketten gespeichert sind, Sie aber datumsbasierte Operationen mit den Daten durchführen müssen.

Parameter

- `dateString`: Eine Zeichenfolge, die ein Datum und eine Uhrzeit darstellt.
- `format`: (optional) Eine Zeichenfolge, die das Format von angibt`dateString`. Falls nicht angegeben, versucht Amazon DocumentDB, die Zeichenfolge im ISO-8601 Format zu analysieren.
- `timezone`: (optional) Eine Zeichenfolge, die die Zeitzone angibt. Falls nicht angegeben, verwendet Amazon DocumentDB die Zeitzone des Servers.
- `onError`: (optional) Gibt die Aktion an, die ausgeführt werden soll, wenn die Konvertierung fehlschlägt. Mögliche Werte sind `'error'` (der Standardwert, der einen Fehler auslöst), `'null'` (Rückgabe`null`) oder `'replace'` (ersetzt den Wert durch die in der `onErrorMessage` Option angegebene Ersatzzeichenfolge).
- `onErrorMessage`: (optional) Wenn auf gesetzt `onError` ist`'replace'`, gibt diese Option die Ersatzzeichenfolge an.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie Sie `$dateFromString` eine Datumszeichenfolge in Amazon DocumentDB in ein Datumsobjekt konvertieren können.

Erstellen Sie Beispieldokumente

```
db.missionLog.insertMany([
{ _id: 1, event: "missionStart", logDate: "2020-03-15T13:41:33"},
{ _id: 2, event: "jumpPoint1", logDate: "2020-03-15T13:45:34"},
{ _id: 3, event: "jumpPoint2", logDate: "2020-03-15T13:48:21"},
{ _id: 4, event: "jumpPoint3", logDate: "2020-03-15T13:52:09"},
{ _id: 5, event: "missionEnd", logDate: "2020-03-15T13:58:44"}
]);
```

Beispiel für eine Abfrage

```
db.missionLog.aggregate([
  {
    $project: {
      event: '$event',
      logDate: {
        $dateFromString: {
          dateString: '$logDate'
        }
      }
    }
  }
]);
```

Ausgabe

```
[
  {
    "_id": 1,
    "event": "missionStart",
    "logDate": ISODate("2020-03-15T13:41:33Z")
  },
  {
    "_id": 2,
    "event": "jumpPoint1",
    "logDate": ISODate("2020-03-15T13:45:34Z")
```

```
  },
  {
    "_id": 3,
    "event": "jumpPoint2",
    "logDate": ISODate("2020-03-15T13:48:21Z")
  },
  {
    "_id": 4,
    "event": "jumpPoint3",
    "logDate": ISODate("2020-03-15T13:52:09Z")
  },
  {
    "_id": 5,
    "event": "missionEnd",
    "logDate": ISODate("2020-03-15T13:58:44Z")
  }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$dateFromString` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('missionLog');

  const result = await collection.aggregate([
    {
      $project: {
        event: '$event',
        logDate: {
          $dateFromString: {
            dateString: '$logDate'
          }
        }
```

```
      }
    }
  ]).toArray();

  console.log(result);
  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['missionLog']

    result = list(collection.aggregate([
        {
            '$project': {
                'event': '$event',
                'logDate': {
                    '$dateFromString': {
                        'dateString': '$logDate'
                    }
                }
            }
        }
    ]))

    print(result)
    client.close()

example()
```

$DateSubtrahieren

Neu ab Version 5.0

Mit dem `$dateSubtract` Aggregationsoperator in Amazon DocumentDB können Sie eine angegebene Dauer von einem Datumswert subtrahieren.

Parameter

- `date`: Ein Datumsausdruck, der in ein Datum oder einen Zeitstempel aufgelöst wird.
- `subtrahend`: Ein Ausdruck für die Dauer, der angibt, wie viel Zeit vom Ausdruck abgezogen werden soll. `date`
- `unit`: Eine Zeichenfolge, die die Zeiteinheit für den `subtrahend` Ausdruck angibt. Unterstützte Einheiten sind „Jahr“, „Quartal“, „Monat“, „Woche“, „Tag“, „Stunde“, „Minute“, „Sekunde“ und „Millisekunde“.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$dateSubtract` Operator verwendet wird, um das Datum vor einem Jahr anhand des aktuellen Datums zu berechnen.

Erstellen Sie Beispieldokumente

```
db.events.insertOne({
  eventName: "Player joined",
  eventTime: ISODate("2023-04-01T12:00:00Z")
});
```

Beispiel für eine Abfrage

```
db.events.aggregate([
  {
    $project: {
      eventName: 1,
      oneYearAgo: {
        $dateSubtract: {
          startDate: "$eventTime",
          amount: 1,
          unit: "year"
        }
      }
    }
  }
])
```

Ausgabe

```
{
  "_id" : ObjectId("64567890abcdef012345678"),
  "eventName" : "Player joined",
  "oneYearAgo" : ISODate("2022-04-01T12:00:00Z")
}
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$dateSubtract` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const events = db.collection('events');

  const result = await events.aggregate([
    {
      $project: {
        eventName: 1,
        oneYearAgo: {
          $dateSubtract: {
            startDate: "$eventTime",
            amount: 1,
            unit: "year"
          }
        }
      }
    }
  ]).toArray();

  console.log(result);
  await client.close();
}
```

```
example();
```

Python

```
from pymongo import MongoClient
from bson.date_time import datetime

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    events = db['events']

    result = list(events.aggregate([
        {
            '$project': {
                'eventName': 1,
                'oneYearAgo': {
                    '$dateSubtract': {
                        'startDate': '$eventTime',
                        'amount': 1,
                        'unit': 'year'
                    }
                }
            }
        }
    ]))

    print(result)
    client.close()

example()
```

$datum ToString

Der `$dateToString` Aggregationsoperator in Amazon DocumentDB wird verwendet, um einen Datums- oder Zeitstempelwert in eine Zeichenkettendarstellung zu konvertieren. Dies ist nützlich, wenn Sie Datum und Uhrzeit für die Anzeige oder Weiterverarbeitung auf eine bestimmte Weise formatieren müssen.

Parameter

- `date`: Der Datums- oder Zeitstempelwert, der in eine Zeichenfolge konvertiert werden soll.
- `format`: Eine Zeichenfolge, die das Format angibt, in dem das Datum dargestellt werden soll. Die Formatzeichenfolge kann verschiedene Formatbezeichner enthalten, z. B. `%Y` für das vierstellige Jahr, `%m` für den zweistelligen Monat, `%d` für den zweistelligen Tag des Monats usw.
- `timezone`: (optional) Die Zeitzone, die für die Konvertierung verwendet werden soll. Falls nicht angegeben, wird die Zeitzone des Servers verwendet, der den Amazon DocumentDB-Cluster hostet.
- `onNull`: (optional) Der Wert, der zurückgegeben werden soll, wenn der `date` Parameter `null`

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt die Verwendung des `$dateToString` Operators zur Formatierung des `logDate` Felds der `missionLog` Sammlung.

Erstellen Sie Beispieldokumente

```
db.missionLog.insertMany([
  { _id: 1, "event":"missionStart", logDate: new Date("2020-03-15T13:41:33Z") },
  { _id: 2, "event":"jumpPoint1", logDate: new Date("2020-03-15T13:45:34Z") },
  { _id: 3, "event":"jumpPoint2", logDate: new Date("2020-03-15T13:48:21Z") },
  { _id: 4, "event":"jumpPoint3", logDate: new Date("2020-03-15T13:52:09Z") },
  { _id: 5, "event":"missionEnd", logDate: new Date("2020-03-15T13:58:44Z") }
]);
```

Beispiel für eine Abfrage

```
db.missionLog.aggregate([
  {
    $project: {
      event: "$event",
      logDateFormatted: {
        $dateToString: {
          format: "%Y-%m-%d %H:%M:%S",
          date: "$logDate"
        }
      }
    }
```

```
  }
])
```

Ausgabe

```
[
  {
    "_id": 1,
    "event": "missionStart",
    "logDateFormatted": "2020-03-15 13:41:33"
  },
  {
    "_id": 2,
    "event": "jumpPoint1",
    "logDateFormatted": "2020-03-15 13:45:34"
  },
  {
    "_id": 3,
    "event": "jumpPoint2",
    "logDateFormatted": "2020-03-15 13:48:21"
  },
  {
    "_id": 4,
    "event": "jumpPoint3",
    "logDateFormatted": "2020-03-15 13:52:09"
  },
  {
    "_id": 5,
    "event": "missionEnd",
    "logDateFormatted": "2020-03-15 13:58:44"
  }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$dateToString` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

Hier ist ein Beispiel für die Verwendung des `$dateToString` Operators in einer Node.js Anwendung:

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('missionLog');

  const result = await collection.aggregate([
    {
      $project: {
        event: "$event",
        logDateFormatted: {
          $dateToString: {
            format: "%Y-%m-%d %H:%M:%S",
            date: "$logDate"
          }
        }
      }
    }
  ]).toArray();

  console.log(result);
  await client.close();
}

example();
```

Python

Hier ist ein Beispiel für die Verwendung des `$dateToString` Operators in einer Python-Anwendung:

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['missionLog']
```

```
    pipeline = [
        {
            '$project': {
                'event': '$event',
                'logDateFormatted': {
                    '$dateToString': {
                        'format': '%Y-%m-%d %H:%M:%S',
                        'date': '$logDate'
                    }
                }
            }
        }
    ]

    result = list(collection.aggregate(pipeline))
    print(result)
    client.close()

example()
```

$DateTrunc

Neu ab Version 8.0

Wird von Elastic Cluster nicht unterstützt.

Der `$dateTrunc` Aggregationsoperator in Amazon DocumentDB kürzt ein Datum auf eine angegebene Einheit.

Parameter

- `date`: Ein Datumsausdruck, der in ein Datum oder einen Zeitstempel aufgelöst wird.
- `unit`: Eine Zeichenfolge, die die Zeiteinheit für den Subtrahend-Ausdruck angibt. Unterstützte Einheiten sind`year`,`quarter`,`month`,`week`,, `day` `hour`, `minute`, `second` und. `millisecond`

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$dateTrunc` Operator verwendet wird, um ein Datum auf die Stunde zu kürzen.

Erstellen Sie Beispieldokumente

```
db.events.insertMany([
  {
    eventName: "Event 1",
    eventTime: ISODate("2025-04-01T12:15:00Z")
  },
  {
    eventName: "Event 2",
    eventTime: ISODate("2025-08-15T14:33:22Z")
  },
]);
```

Beispiel für eine Abfrage

```
db.events.aggregate([
  {
    $project: {
      eventName: 1,
      eventTime: 1,
      truncatedToHour: {
        $dateTrunc: {
          date: "$eventTime",
          unit: "hour"
        }
      }
    }
  }
]);
```

Ausgabe

```
[
  {
    _id: ObjectId('6924a258d66dcae121d29515'),
    eventName: 'Event 1',
    eventTime: ISODate('2025-04-01T12:15:00.000Z'),
    truncatedToHour: ISODate('2025-04-01T12:00:00.000Z')
  },
  {
    _id: ObjectId('6924a258d66dcae121d29516'),
    eventName: 'Event 2',
    eventTime: ISODate('2025-08-15T14:33:22.000Z'),
    truncatedToHour: ISODate('2025-08-15T14:00:00.000Z')
```

```
  }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$dateTrunc` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const events = db.collection('events');

  const result = await events.aggregate([
    {
      $project: {
        eventName: 1,
        eventTime: 1,
        truncatedToHour: {
          $dateTrunc: {
            date: "$eventTime",
            unit: "hour"
          }
        }
      }
    }
  ]).toArray();

  console.log(result);
  client.close();
}

example();
```

Python

```
from pymongo import MongoClient
```

```
def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    events = db['events']

    result = list(events.aggregate([
        {
            "$project": {
                "eventName": 1,
                "eventTime": 1,
                "truncatedToHour": {
                    "$dateTrunc": {
                        "date": "$eventTime",
                        "unit": "hour"
                    }
                }
            }
        }
    ]))

    print(result)
    client.close()

example()
```

$Tag OfMonth

Der `$dayOfMonth` Aggregationsoperator in Amazon DocumentDB ruft den Tag des Monats (von 1 bis 31) für ein bestimmtes Datum ab. Dieser Operator ist nützlich, um den Tag des Monats aus Datumsfeldern in Ihren Dokumenten zu gruppieren, zu filtern oder zu extrahieren.

Parameter

- `date expression`: Der Datumsausdruck kann ein Datumsfeld aus dem Dokument, ein Datumsobjekt oder eine Datumszeichenfolge sein.

Beispiel (MongoDB Shell)

Dieses Beispiel zeigt, wie der `$dayOfMonth` Operator verwendet wird, um den Tag des Monats aus einem Datumsfeld im Dokument zu extrahieren.

Erstellen Sie Beispieldokumente

```
db.events.insertMany([
  { _id: 1, eventDate: new Date("2022-01-15T12:00:00Z") },
  { _id: 2, eventDate: new Date("2022-02-28T15:30:00Z") },
  { _id: 3, eventDate: new Date("2022-03-01T09:45:00Z") },
  { _id: 4, eventDate: new Date("2022-04-30T23:59:59Z") }
]);
```

Beispiel für eine Abfrage

```
db.events.aggregate([
  { $project: {
    eventDay: { $dayOfMonth: "$eventDate" }
  }}
])
```

Ausgabe

```
[
  { "_id" : 1, "eventDay" : 15 },
  { "_id" : 2, "eventDay" : 28 },
  { "_id" : 3, "eventDay" : 1 },
  { "_id" : 4, "eventDay" : 30 }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$dayOfMonth` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');
```

```
async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const events = db.collection('events');

  const result = await events.aggregate([
    { $project: {
      eventDay: { $dayOfMonth: "$eventDate" }
    }}
  ]).toArray();

  console.log(result);
  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client.mydatabase
    events = db.events

    result = list(events.aggregate([
        { "$project": {
            "eventDay": { "$dayOfMonth": "$eventDate" }
        }}
    ]))

    print(result)
    client.close()

example()
```

$Tag OfWeek

Der `$dayOfWeek` Operator in Amazon DocumentDB extrahiert den Wochentag aus einem bestimmten Datumsfeld. Es gibt den Wochentag als Zahl zwischen 1 (Sonntag) und 7 (Samstag) zurück, was dem Verhalten in MongoDB entspricht.

Parameter

- `date field`: Das Datumsfeld, aus dem der Wochentag extrahiert werden soll.

Beispiel (MongoDB Shell)

Dieses Beispiel zeigt, wie der `$dayOfWeek` Operator verwendet wird, um den Wochentag aus dem `date` Feld in der `weather` Sammlung zu extrahieren.

Erstellen Sie Beispieldokumente

```
db.weather.insertMany([
  {
    "temperature": 97.5,
    "humidity": 0.60,
    "date": new Date("2023-04-01")
  },
  {
    "temperature": 95.2,
    "humidity": 0.55,
    "date": new Date("2023-04-02")
  },
  {
    "temperature": 92.8,
    "humidity": 0.65,
    "date": new Date("2023-04-03")
  }
]);
```

Beispiel für eine Abfrage

```
db.weather.aggregate([
  {
    $project: {
      dayOfWeek: { $dayOfWeek: "$date" }
```

```
    }
  }
]).pretty();
```

Ausgabe

```
{ "_id" : ObjectId("64272c6663f4f8ce422c2d91"), "dayOfWeek" : 7 }
{ "_id" : ObjectId("64272c6663f4f8ce422c2d92"), "dayOfWeek" : 1 }
{ "_id" : ObjectId("64272c6663f4f8ce422c2d93"), "dayOfWeek" : 2 }
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$dayOfWeek` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function main() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('weather');

  const result = await collection.aggregate([
    {
      $project: {
        dayOfWeek: { $dayOfWeek: '$date' }
      }
    }
  ]).toArray();

  console.log(result);

  await client.close();
}

main();
```

Python

```
from pymongo import MongoClient

def main():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client.test
    collection = db.weather

    result = list(collection.aggregate([
        {
            '$project': {
                'dayOfWeek': { '$dayOfWeek': '$date' }
            }
        }
    ]))

    print(result)

    client.close()

if __name__ == '__main__':
    main()
```

$Tag OfYear

Der `$dayOfYear` Operator in Amazon DocumentDB gibt den Tag des Jahres für ein Datum als Zahl zwischen 1 und 366 zurück (365 in Nicht-Schaltjahren).

Parameter

- `expression`: Das Datumsfeld oder der Ausdruck, aus dem der Tag des Jahres extrahiert werden soll.

Beispiel (MongoDB Shell)

Dieses Beispiel zeigt, wie der `$dayOfYear` Operator verwendet wird, um den Tag des Jahres aus einem Datumsfeld in einer Amazon DocumentDB-Sammlung zu extrahieren.

Erstellen Sie Beispieldokumente

```
db.weather.insert([
  {
    "temperature" : 97.5,
    "humidity": 0.60,
    "date" : new Date("2023-03-15")
  },
  {
    "temperature" : 82.3,
    "humidity": 0.75,
    "date" : new Date("2023-12-31")
  }
])
```

Beispiel für eine Abfrage

```
db.weather.aggregate([
  {
    $project: {
      dayOfYear: { $dayOfYear: "$date" }
    }
  }
]).pretty()
```

Ausgabe

```
{ "_id" : ObjectId("642b86fc7d8e07af279bbe63"), "dayOfYear" : 74 }
{ "_id" : ObjectId("642b86fc7d8e07af279bbe64"), "dayOfYear" : 365 }
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$dayOfYear` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
```

```
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('weather');

  const result = await collection.aggregate([
    {
      $project: {
        dayOfYear: { $dayOfYear: "$date" }
      }
    }
  ]).toArray();

  console.log(result);

  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['weather']

    result = list(collection.aggregate([
        {
            '$project': {
                'dayOfYear': { '$dayOfYear': '$date' }
            }
        }
    ]))

    print(result)

    client.close()
```

```
example()
```

$divide

Der `$divide` Operator in der Amazon DocumentDB-Aggregationspipeline wird verwendet, um eine Zahl durch eine andere zu dividieren. Es ist ein nützlicher Operator für die Ausführung mathematischer Operationen an numerischen Feldern in Ihren Dokumenten.

Parameter

- `numerator`: Die Dividende oder die Zahl, die geteilt werden soll.
- `denominator`: Der Divisor oder die Zahl, durch die dividiert werden soll.

Beispiel (MongoDB Shell)

Dieses Beispiel zeigt, wie der `$divide` Operator verwendet wird, um den Stundensatz für Mitarbeiter auf der Grundlage ihres Jahresgehalts und der Anzahl der Arbeitsstunden pro Jahr zu berechnen.

Erstellen Sie Beispieldokumente

```
db.employees.insertMany([
  { _id: 1, name: "John Doe", salary: 80000, hoursPerYear: 2080 },
  { _id: 2, name: "Jane Smith", salary: 90000, hoursPerYear: 2080 },
  { _id: 3, name: "Bob Johnson", salary: 75000, hoursPerYear: 2080 }
]);
```

Beispiel für eine Abfrage

```
db.employees.aggregate([
  {
    $project: {
      name: 1,
      hourlyRate: { $divide: ["$salary", "$hoursPerYear"] }
    }
  }
])
```

Ausgabe

```
[
  { "_id" : 1, "name" : "John Doe", "hourlyRate" : 38.46153846153846 },
  { "_id" : 2, "name" : "Jane Smith", "hourlyRate" : 43.26923076923077 },
  { "_id" : 3, "name" : "Bob Johnson", "hourlyRate" : 36.05769230769231 }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$divide` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function calculateHourlyRate() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const employees = db.collection('employees');

  const result = await employees.aggregate([
    {
      $project: {
        name: 1,
        hourlyRate: { $divide: ["$salary", "$hoursPerYear"] }
      }
    }
  ]).toArray();

  console.log(result);
  client.close();
}

calculateHourlyRate();
```

Python

```
from pymongo import MongoClient

def calculate_hourly_rate():
```

```
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client.mydatabase
    employees = db.employees

    result = list(employees.aggregate([
        {
            '$project': {
                'name': 1,
                'hourlyRate': { '$divide': ['$salary', '$hoursPerYear'] }
            }
        }
    ]))

    print(result)
    client.close()

calculate_hourly_rate()
```

$eq

Der `$eq` Aggregationsoperator vergleicht zwei Werte und gibt zurück, `true` wenn sie gleich sind, andernfalls gibt er zurück`false`.

Parameter

- `expression1`: Der erste zu vergleichende Wert.
- `expression2`: Der zweite zu vergleichende Wert.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$eq` Operator verwendet wird, um zu überprüfen, ob die Produktmengen den Zielwerten entsprechen.

Erstellen Sie Beispieldokumente

```
db.inventory.insertMany([
  { _id: 1, item: "Widget", qty: 50, target: 50 },
  { _id: 2, item: "Gadget", qty: 30, target: 50 },
```

```
  { _id: 3, item: "Tool", qty: 50, target: 40 }
]);
```

Beispiel für eine Abfrage

```
db.inventory.aggregate([
  {
    $project: {
      item: 1,
      qty: 1,
      target: 1,
      meetsTarget: { $eq: ["$qty", "$target"] }
    }
  }
]);
```

Ausgabe

```
[
  { _id: 1, item: 'Widget', qty: 50, target: 50, meetsTarget: true },
  { _id: 2, item: 'Gadget', qty: 30, target: 50, meetsTarget: false },
  { _id: 3, item: 'Tool', qty: 50, target: 40, meetsTarget: false }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$eq` Aggregationsoperators anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('inventory');

  const result = await collection.aggregate([
```

```
    {
      $project: {
        item: 1,
        qty: 1,
        target: 1,
        meetsTarget: { $eq: ["$qty", "$target"] }
      }
    }
  ]).toArray();

  console.log(result);
  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['inventory']

    result = list(collection.aggregate([
        {
            '$project': {
                'item': 1,
                'qty': 1,
                'target': 1,
                'meetsTarget': { '$eq': ['$qty', '$target'] }
            }
        }
    ]))

    print(result)
    client.close()

example()
```

$exp

Neu ab Version 4.0

Mit dem `$exp` Operator in Amazon DocumentDB können Sie die Konstante e auf eine bestimmte Zahl erhöhen.

Parameter

- `expression`: Der auszuwertende Ausdruck. Dies kann ein beliebiger gültiger Aggregationsausdruck sein, einschließlich Feldverweise, arithmetischer Operationen und anderer Aggregationsstufen.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$exp` Operator verwendet wird, um alle Dokumente zu finden, bei denen das `quantity` Feld größer als das `price` Feld ist.

Erstellen Sie Beispieldokumente

```
db.items.insertMany([
  { item: "canvas", quantity: 4 },
  { item: "journal", quantity: 2 }
]);
```

Beispiel für eine Abfrage

```
db.items.aggregate([
  { $project: {
    "quantityRaised": {$exp: "$quantity"}}
  }
]);
```

Ausgabe

```
[
  {
    _id: ObjectId('6920b785311cf98b79d2950d'),
    quantityRaised: 54.598150033144236
  },
```

```
  {
    _id: ObjectId('6920b785311cf98b79d2950e'),
    quantityRaised: 7.38905609893065
  }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$exp` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function aggregateExp() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const items = db.collection('items');

  const result = await items.aggregate([
    { $project: {
      "quantityRaised": {$exp: "$quantity"}}
    }
    ]).toArray();

  console.log(result);
  client.close();
}

aggregateExp();
```

Python

```
from pymongo import MongoClient

def aggregate_exp():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
```

```
    db = client.test
    items = db.items

    result = list(items.aggregate([
      { "$project": {
        "quantityRaised": {"$exp": "$quantity"}}
      }
    ]))

    print(result)
    client.close()

aggregate_exp()
```

$filter

Der `$filter` Operator in Amazon DocumentDB wird verwendet, um einen Filterausdruck auf jedes Element eines Arrays anzuwenden und ein Array zurückzugeben, das nur die Elemente enthält, die der angegebenen Bedingung entsprechen. Dieser Operator ist nützlich, wenn Sie komplexe Filteroperationen für Array-Felder in Ihren Dokumenten durchführen müssen.

Parameter

- `input`: Das zu filternde Array-Feld.
- `as`: Der Variablenname, der für jedes Element des `input` Arrays innerhalb des `cond` Ausdrucks verwendet werden soll.
- `cond`: Der boolesche Ausdruck, der bestimmt, ob ein bestimmtes Element in das Ausgabearray aufgenommen werden soll.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$filter` Operator verwendet wird, um den Kunden jeder Bestellung zu projizieren und ein neues Array-Feld PaidItems zu erstellen, das nur die Artikel aus dem Artikelarray enthält, bei denen der Preis höher als 15 ist. Im Wesentlichen werden die Artikel jeder Bestellung so gefiltert, dass sie nur Produkte enthalten, die mehr als 15€ kosten.

Erstellen Sie Beispieldokumente

```
db.orders.insertMany([
```

```
  { _id: 1, customer: "abc123", items: [
    { name: "Product A", price: 10, qty: 2 },
    { name: "Product B", price: 20, qty: 1 }
  ]},
  { _id: 2, customer: "def456", items: [
    { name: "Product C", price: 5, qty: 3 },
    { name: "Product D", price: 15, qty: 4 }
  ]},
  { _id: 3, customer: "ghi789", items: [
    { name: "Product E", price: 8, qty: 3 },
    { name: "Product F", price: 12, qty: 1 }
  ]}
]);
```

Beispiel für eine Abfrage

```
db.orders.aggregate([
  {
    $project: {
      customer: 1,
      paidItems: {
        $filter: {
          input: "$items",
          as: "item",
          cond: { $gt: ["$$item.price", 15] }
        }
      }
    }
  }
]).pretty();
```

Ausgabe

```
[
  {
    _id: 1,
    customer: 'abc123',
    paidItems: [ { name: 'Product B', price: 20, qty: 1 } ]
  },
  { _id: 2, customer: 'def456', paidItems: [] },
  { _id: 3, customer: 'ghi789', paidItems: [] }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$filter` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const uri = 'mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false';
  const client = new MongoClient(uri);

  try {
    await client.connect();

    const db = client.db('test');
    const collection = db.collection('orders');

    const result = await collection.aggregate([
      {
        $project: {
          customer: 1,
          paidItems: {
            $filter: {
              input: "$items",
              as: "item",
              cond: { $gt: ["$$item.price", 15] }
            }
          }
        }
      }
    ]).toArray();

    console.log(JSON.stringify(result, null, 2));

  } catch (error) {
    console.error('Error:', error);
  } finally {
    await client.close();
  }
```

```
}

example();
```

Python

```
from pymongo import MongoClient
from pprint import pprint

def example():
    uri = 'mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false'

    with MongoClient(uri) as client:
        db = client.test
        collection = db.orders

        result = list(collection.aggregate([
            {
                '$project': {
                    'customer': 1,
                    'paidItems': {
                        '$filter': {
                            'input': '$items',
                            'as': 'item',
                            'cond': { '$gt': ['$$item.price', 15] }
                        }
                    }
                }
            }
        ]))

        for doc in result:
            pprint(doc)

example()
```

$first

Neu ab Version 5.0.

Wird von Elastic Cluster nicht unterstützt.

Der `$first` Operator in Amazon DocumentDB gibt das erste Dokument aus einem gruppierten Satz von Dokumenten zurück. Er wird häufig in Aggregationspipelines verwendet, um das erste Dokument abzurufen, das einer bestimmten Bedingung entspricht.

Parameter

- `expression`: Der Ausdruck, der als erster Wert in jeder Gruppe zurückgegeben werden soll.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$first` Operator verwendet wird, um den ersten Elementwert abzurufen, der während der Aggregation für jede Kategorie gefunden wurde.

Hinweis: `$first` Gibt das erste Dokument auf der Grundlage der aktuellen Reihenfolge der Dokumente in der Pipeline zurück. Um eine bestimmte Reihenfolge sicherzustellen (z. B. nach Datum, Preis usw.), sollte vor der `$sort` Phase eine `$group` Stufe verwendet werden.

Erstellen Sie Musterdokumente

```
db.products.insertMany([
  { _id: 1, item: "abc", price: 10, category: "food" },
  { _id: 2, item: "jkl", price: 20, category: "food" },
  { _id: 3, item: "xyz", price: 5, category: "toy" },
  { _id: 4, item: "abc", price: 5, category: "toy" }
]);
```

Beispiel für eine Abfrage

```
db.products.aggregate([
  { $group: { _id: "$category", firstItem: { $first: "$item" } } }
]);
```

Ausgabe

```
[
  { "_id" : "food", "firstItem" : "abc" },
  { "_id" : "toy", "firstItem" : "xyz" }
```

```
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$first` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const uri = 'mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false';
  const client = new MongoClient(uri);

  try {
    await client.connect();

    const db = client.db('test');
    const collection = db.collection('products');

    const result = await collection.aggregate([
      { $group: { _id: "$category", firstItem: { $first: "$item" } } }
    ]).toArray();

    console.log(result);

  } catch (error) {
    console.error('Error:', error);
  } finally {
    await client.close();
  }
}

example();
```

Python

```
from pymongo import MongoClient
from pprint import pprint
```

```
def example():
    client = None
    try:
        client = MongoClient('mongodb://<username>:<password>@<cluster-
endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')

        db = client['test']
        collection = db['products']

        result = list(collection.aggregate([
            { '$group': { '_id': '$category', 'firstItem': { '$first': '$item' } } }
        ]))

        pprint(result)

    except Exception as e:
        print(f"An error occurred: {e}")

    finally:
        if client:
            client.close()

example()
```

$floor

Neu ab Version 4.0.

Der `$floor` Operator in Amazon DocumentDB gibt die größte Ganzzahl zurück, die kleiner oder gleich der angegebenen Zahl ist. Dieser Operator ist nützlich, um numerische Werte abzurunden.

Parameter

- `expression`: Der numerische Ausdruck, der abgerundet werden soll.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$floor` Operator verwendet wird, um einen Dezimalwert auf die nächste Ganzzahl abzurunden.

Erstellen Sie Beispieldokumente

```
db.numbers.insertOne({ value: 3.14 });
```

Beispiel für eine Abfrage

```
db.numbers.aggregate([
  { $project: { _id: 0, floored: { $floor: "$value" } } }
]);
```

Ausgabe

```
{ "floored" : 3 }
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$floor` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const uri = 'mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false';
  const client = new MongoClient(uri);

  try {
    await client.connect();

    const db = client.db('test');
    const collection = db.collection('numbers');

    const result = await collection.aggregate([
      { $project: { _id: 0, floored: { $floor: "$value" } } }
    ]).toArray();

    console.log(result);
```

```
  } catch (error) {
    console.error('Error:', error);
  } finally {
    await client.close();
  }
}

example();
```

Python

```
from pymongo import MongoClient
from pprint import pprint

def example():
    client = None
    try:
        client = MongoClient('mongodb://<username>:<password>@<cluster-
endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')

        db = client.test
        collection = db.numbers

        result = list(collection.aggregate([
            { '$project': { '_id': 0, 'floored': { '$floor': '$value' }}}
        ]))

        pprint(result)

    except Exception as e:
        print(f"An error occurred: {e}")

    finally:
        if client:
            client.close()

example()
```

$geoNear

In der `$geoNear` Aggregationsphase werden Dokumente in der Reihenfolge ihrer Nähe zu einem bestimmten Punkt zurückgegeben. Sie berechnet die Entfernung vom Punkt und bezieht die Entfernung in die Ausgabedokumente ein.

Parameter

- `near`: Der Punkt, von dem aus Entfernungen berechnet werden sollen, angegeben als GeoJSON- oder Legacy-Koordinaten.
- `distanceField`: Der Feldname zum Speichern der berechneten Entfernung.
- `spherical`: Boolescher Wert, der angibt, ob sphärische Geometrie verwendet werden soll (erforderlich für GeoJSON-Punkte).
- `maxDistance`: Optional. Maximaler Abstand vom Mittelpunkt.
- `minDistance`: Optional. Minimaler Abstand vom Mittelpunkt.
- `query`: Optional. Zusätzliche anzuwendende Filterkriterien.
- `limit`: Optional. Maximale Anzahl zurückzugebender Dokumente.
- `key`: Optional. Feld, das für Geodatenabfragen verwendet werden soll, wenn mehrere Geoindizes vorhanden sind.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie die `$geoNear` Bühne verwendet wird, um Geschäfte zu finden, die einem bestimmten Standort am nächsten sind.

Erstellen Sie Beispieldokumente

```
db.stores.createIndex({ location: "2dsphere" });

db.stores.insertMany([
  { _id: 1, name: "Store A", location: { type: "Point", coordinates: [-122.4,
 37.8] } },
  { _id: 2, name: "Store B", location: { type: "Point", coordinates: [-122.5,
 37.7] } },
  { _id: 3, name: "Store C", location: { type: "Point", coordinates: [-122.3, 37.9] } }
]);
```

Beispiel für eine Abfrage

```
db.stores.aggregate([
  {
    $geoNear: {
      near: { type: "Point", coordinates: [-122.4, 37.8] },
      distanceField: "distance",
      spherical: true
    }
  }
]);
```

Ausgabe

```
[
  { _id: 1, name: 'Store A', location: { type: 'Point', coordinates: [ -122.4,
 37.8 ] }, distance: 0 },
  { _id: 3, name: 'Store C', location: { type: 'Point', coordinates: [ -122.3,
 37.9 ] }, distance: 13877.82 },
  { _id: 2, name: 'Store B', location: { type: 'Point', coordinates: [ -122.5,
 37.7 ] }, distance: 15557.89 }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung der `$geoNear` Aggregationsphase anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('stores');

  const result = await collection.aggregate([
    {
      $geoNear: {
        near: { type: "Point", coordinates: [-122.4, 37.8] },
        distanceField: "distance",
```

```
        spherical: true
      }
    }
  ]).toArray();

  console.log(result);
  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['stores']

    result = list(collection.aggregate([
        {
            '$geoNear': {
                'near': { 'type': 'Point', 'coordinates': [-122.4, 37.8] },
                'distanceField': 'distance',
                'spherical': True
            }
        }
    ]))

    print(result)
    client.close()

example()
```

$group

Die `$group` Aggregationsphase in Amazon DocumentDB ermöglicht es Ihnen, Dokumente nach einem bestimmten Ausdruck zu gruppieren und verschiedene kumulative Operationen mit den

gruppierten Daten durchzuführen. Dies kann für Aufgaben wie die Berechnung von Gesamtwerten, Durchschnittswerten oder anderen Statistiken auf der Grundlage der gruppierten Daten nützlich sein.

Parameter

- `_id`: Gibt den Ausdruck an, nach dem die Eingabedokumente gruppiert werden sollen. Dies kann ein Feldname, ein berechneter Ausdruck oder eine Kombination aus beidem sein.
- `accumulator expressions`: (optional) Ein oder mehrere Akkumulatorausdrücke, die auf die gruppierten Daten angewendet werden sollen. Diese Ausdrücke verwenden die oben genannten Akkumulatoroperatoren.

Beispiel (MongoDB Shell)

Im folgenden Beispiel werden Kunden nach ihrer Stadt gruppiert und der Gesamtbestellbetrag für jede Stadt berechnet.

Erstellen Sie Beispieldokumente

```
db.customers.insertMany([
  { name: "John Doe", city: "New York", orders: [{ amount: 100 }, { amount: 200 }] },
  { name: "Jane Smith", city: "Los Angeles", orders: [{ amount: 150 }, { amount:
 300 }] },
  { name: "Bob Johnson", city: "New York", orders: [{ amount: 75 }, { amount: 125 }] },
  { name: "Samantha Lee", city: "Chicago", orders: [{ amount: 50 }, { amount: 100 }] }
]);
```

Beispiel für eine Abfrage

```
db.customers.aggregate([
  {
    $group: {
      _id: "$city",
      totalOrders: { $sum: { $sum: "$orders.amount" } }
    }
  }
]);
```

Ausgabe

```
[
```

```
  { _id: 'Chicago', totalOrders: 150 },
  { _id: 'Los Angeles', totalOrders: 450 },
  { _id: 'New York', totalOrders: 500 }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$group` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function groupByCity() {
  const uri = 'mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false';
  const client = new MongoClient(uri);

  try {
    await client.connect();
    const db = client.db('test');
    const result = await db.collection('customers').aggregate([
      { $unwind: '$orders' },
      {
        $group: {
          _id: '$city',
          totalOrders: { $sum: '$orders.amount' }
        }
      }
    ]).toArray();

    console.log(result);
  } catch (err) {
    console.error('Error during aggregation:', err);
  } finally {
    await client.close();
  }
}

groupByCity();
```

Python

```
from pymongo import MongoClient

def group_by_city():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')

    try:
        db = client.test
        result = list(db.customers.aggregate([
            {'$unwind': '$orders'},
            {
                '$group': {
                    '_id': '$city',
                    'totalOrders': {'$sum': '$orders.amount'}
                }
            }
        ]))
        print(result)
    except Exception as e:
        print(f"Error during aggregation: {e}")
    finally:
        client.close()

group_by_city()
```

$gt

Der `$gt` Aggregationsoperator vergleicht zwei Werte und gibt zurück, `true` wenn der erste Wert größer als der zweite ist, andernfalls kehrt `false` er zurück.

Parameter

- `expression1`: Der erste zu vergleichende Wert.
- `expression2`: Der zweite zu vergleichende Wert.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$gt` Operator verwendet wird, um Produkte zu identifizieren, die einen Preisschwellenwert überschreiten.

Erstellen Sie Beispieldokumente

```
db.products.insertMany([
  { _id: 1, name: "Laptop", price: 1200 },
  { _id: 2, name: "Mouse", price: 25 },
  { _id: 3, name: "Monitor", price: 400 }
]);
```

Beispiel für eine Abfrage

```
db.products.aggregate([
  {
    $project: {
      name: 1,
      price: 1,
      expensive: { $gt: ["$price", 100] }
    }
  }
]);
```

Ausgabe

```
[
  { _id: 1, name: 'Laptop', price: 1200, expensive: true },
  { _id: 2, name: 'Mouse', price: 25, expensive: false },
  { _id: 3, name: 'Monitor', price: 400, expensive: true }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$gt` Aggregationsoperators anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');
```

```
async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('products');

  const result = await collection.aggregate([
    {
      $project: {
        name: 1,
        price: 1,
        expensive: { $gt: ["$price", 100] }
      }
    }
  ]).toArray();

  console.log(result);
  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['products']

    result = list(collection.aggregate([
        {
            '$project': {
                'name': 1,
                'price': 1,
                'expensive': { '$gt': ['$price', 100] }
            }
        }
```

```
    ]))

    print(result)
    client.close()

example()
```

$gte

Der `$gte` Aggregationsoperator vergleicht zwei Werte und gibt zurück, `true` ob der erste Wert größer oder gleich dem zweiten ist, andernfalls kehrt `false` er zurück.

Parameter

- `expression1`: Der erste zu vergleichende Wert.
- `expression2`: Der zweite zu vergleichende Wert.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$gte` Operator verwendet wird, um zu überprüfen, ob Schüler eine Prüfung bestanden haben.

Erstellen Sie Beispieldokumente

```
db.students.insertMany([
  { _id: 1, name: "Alice", score: 85 },
  { _id: 2, name: "Bob", score: 60 },
  { _id: 3, name: "Charlie", score: 72 }
]);
```

Beispiel für eine Abfrage

```
db.students.aggregate([
  {
    $project: {
      name: 1,
      score: 1,
      passed: { $gte: ["$score", 70] }
    }
  }
```

```
]);
```

Ausgabe

```
[
  { _id: 1, name: 'Alice', score: 85, passed: true },
  { _id: 2, name: 'Bob', score: 60, passed: false },
  { _id: 3, name: 'Charlie', score: 72, passed: true }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$gte` Aggregationsoperators anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('students');

  const result = await collection.aggregate([
    {
      $project: {
        name: 1,
        score: 1,
        passed: { $gte: ["$score", 70] }
      }
    }
  ]).toArray();

  console.log(result);
  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['students']

    result = list(collection.aggregate([
        {
            '$project': {
                'name': 1,
                'score': 1,
                'passed': { '$gte': ['$score', 70] }
            }
        }
    ]))

    print(result)
    client.close()

example()
```

$hour

Der $hour Operator extrahiert die Stundenkomponente aus einem Datums- oder Zeitstempelfeld.

Parameter

- dateExpression: Das Datum, auf das der Operator angewendet wird. Dies muss ein gültiges BSON-Datum ergeben (z. B. ein Feld wie $createdAt oder ein Datumsliteral).

Ein Parameter kann auch als Dokument im folgenden Format angegeben werden:

{Datum:<dateExpression>, Zeitzone:<timezoneExpression>}

Dies ermöglicht die Anwendung zeitzonenorientierter Datumsoperationen.

```
- `<tzExpression>`: (optional) The timezone of the operation result. It must be a valid
 expression that resolves to a string formatted as either an Olson Timezone Identifier
 or a UTC Offset. If no timezone is provided, the result is in UTC.
```

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der $hour Operator verwendet wird, um die Stundenkomponente aus einem Datumsfeld zu extrahieren und die Daten entsprechend zu gruppieren.

Erstellen Sie Beispieldokumente

```
db.events.insertMany([
  { timestamp: new Date("2023-04-01T10:30:00Z") },
  { timestamp: new Date("2023-04-01T12:45:00Z") },
  { timestamp: new Date("2023-04-02T08:15:00Z") },
  { timestamp: new Date("2023-04-02T16:20:00Z") },
  { timestamp: new Date("2023-04-03T23:59:00Z") }
]);
```

Beispiel für eine Abfrage

```
db.events.aggregate([
  {
    $project: {
      hour: { $hour: "$timestamp" }
    }
  },
  {
    $group: {
      _id: "$hour",
      count: { $sum: 1 }
    }
  },
  {
    $sort: { _id: 1 }
  }
]);
```

Ausgabe

```
[
```

```
  { "_id": 8, "count": 1 },
  { "_id": 10, "count": 1 },
  { "_id": 12, "count": 1 },
  { "_id": 16, "count": 1 },
  { "_id": 23, "count": 1 }
]
```

Diese Abfrage gruppiert die Ereignisse nach der Stundenkomponente des `timestamp` Felds und zählt die Anzahl der Ereignisse für jede Stunde.

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$hour` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = new MongoClient('mongodb://<username>:<password>@<cluster-
endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');

  try {
    await client.connect();
    const db = client.db('test');
    const collection = db.collection('events');

    const result = await collection.aggregate([
      {
        $project: {
          hour: { $hour: "$timestamp" }
        }
      },
      {
        $group: {
          _id: "$hour",
          count: { $sum: 1 }
        }
      },
      {
        $sort: { _id: 1 }
```

```
      }
    ]).toArray();

    console.log(result);
  } catch (error) {
    console.error('Error occurred:', error);
  } finally {
    await client.close();
  }
}

example();
```

Python

```
from pymongo import MongoClient
from datetime import datetime

def example():
    try:
        client = MongoClient('mongodb://<username>:<password>@<cluster-
endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')

        db = client.test
        collection = db.events

        result = list(collection.aggregate([
            {
                "$project": {
                    "hour": {"$hour": "$timestamp"}
                }
            },
            {
                "$group": {
                    "_id": "$hour",
                    "count": {"$sum": 1}
                }
            },
            {
                "$sort": {"_id": 1}
            }
        ]))
```

```
        print(result)

    except Exception as e:
        print(f"An error occurred: {e}")

    finally:
        client.close()

example()
```

$ifNull

Der `$ifNull` Operator wird verwendet, um einen bestimmten Wert zurückzugeben, wenn der Eingabeausdruck Null oder undefiniert ergibt. Dieser Operator kann in Szenarien nützlich sein, in denen Sie einen Standardwert angeben oder Fälle behandeln null/undefined möchten.

Parameter

- `expression`: Der auszuwertende Ausdruck.
- `replacement`: Der Wert, der zurückgegeben werden soll, wenn die `<expression>` Auswertung Null oder undefiniert ergibt.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt die Verwendung des `$ifNull` Operators zur Bereitstellung eines Standardwerts, wenn das `name` Feld Null oder undefiniert ist.

Erstellen Sie Beispieldokumente

```
db.users.insertMany([
  { _id: 1, name: "John" },
  { _id: 2, name: null },
  { _id: 3 }
]);
```

Beispiel für eine Abfrage

```
db.users.aggregate([
```

```
  {
    $project: {
      _id: 1,
      name: { $ifNull: ["$name", "No Name"] }
    }
  }
]);
```

Ausgabe

```
[
  { "_id": 1, "name": "John" },
  { "_id": 2, "name": "No Name" },
  { "_id": 3, "name": "No Name" }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$ifNull` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');

  const db = client.db('test');

  const collection = db.collection('users');

  const pipeline = [
    {
      $project: {
        _id: 1,
        name: { $ifNull: ["$name", "No Name"] }
      }
    }
  ];
```

```
  const cursor = await collection.aggregate(pipeline);

  await cursor.forEach(doc => {
    console.log(doc);
  });

  await client.close();

}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')

    db = client.test
    collection = db.users

    pipeline = [
        {
            "$project": {
                "_id": 1,
                "name": { "$ifNull": ["$name", "No Name"] }
            }
        }
    ]

    result = collection.aggregate(pipeline)

    for doc in result:
        print(doc)

    client.close()

example()
```

$in

Der `$in` Aggregationsoperator prüft, ob ein bestimmter Wert innerhalb eines Arrays existiert. Er gibt zurück`true`, ob der Wert im Array gefunden wurde, und `false` andernfalls.

Parameter

- `value`: Der Wert, nach dem gesucht werden soll.
- `array`: Das Array, in dem gesucht werden soll.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$in` Operator verwendet wird, um zu überprüfen, ob in den Fähigkeiten jedes Mitarbeiters eine bestimmte Fähigkeit vorhanden ist.

Erstellen Sie Beispieldokumente

```
db.employees.insertMany([
  { _id: 1, name: "Sarah", skills: ["Python", "JavaScript", "SQL"] },
  { _id: 2, name: "Mike", skills: ["Java", "C++", "Go"] },
  { _id: 3, name: "Emma", skills: ["Python", "Ruby", "Rust"] }
]);
```

Beispiel für eine Abfrage

```
db.employees.aggregate([
  {
    $project: {
      name: 1,
      hasPython: { $in: ["Python", "$skills"] }
    }
  }
]);
```

Ausgabe

```
[
  { _id: 1, name: 'Sarah', hasPython: true },
  { _id: 2, name: 'Mike', hasPython: false },
  { _id: 3, name: 'Emma', hasPython: true }
```

```
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$in` Aggregationsoperators anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('employees');

  const result = await collection.aggregate([
    {
      $project: {
        name: 1,
        hasPython: { $in: ["Python", "$skills"] }
      }
    }
  ]).toArray();

  console.log(result);
  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['employees']
```

```
    result = list(collection.aggregate([
        {
            '$project': {
                'name': 1,
                'hasPython': { '$in': ['Python', '$skills'] }
            }
        }
    ]))

    print(result)
    client.close()

example()
```

$ index OfArray

Der `$indexOfArray` Operator in Amazon DocumentDB wird verwendet, um den Index des ersten Vorkommens eines bestimmten Elements in einem Array zu finden. Dieser Operator gibt die auf Null basierende Indexposition des ersten Elements im Array zurück, das dem angegebenen Wert entspricht. Wenn der Wert nicht gefunden wird, gibt er -1 zurück.

Parameter

- `array`: Das zu durchsuchende Array.
- `value`: Der Wert, nach dem im Array gesucht werden soll.
- `start`: (optional) Die Position im Array, von der aus die Suche gestartet werden soll. Der Standardwert lautet 0.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der OfArray $index-Operator verwendet wird, um den Index des ersten Vorkommens des Elements „Mango“ im Array „fruits“ für jedes Dokument zu finden.

Erstellen Sie Beispieldokumente

```
db.collection.insertMany([
  { _id: 1, fruits: ["apple", "banana", "cherry", "durian"] },
  { _id: 2, fruits: ["mango", "orange", "pineapple"] },
  { _id: 3, fruits: ["kiwi", "lemon", "mango"] }
```

```
]);
```

Beispiel für eine Abfrage

```
db.collection.aggregate([
  {
    $project: {
      _id: 1,
      fruitIndex: { $indexOfArray: ["$fruits", "mango"] }
    }
  }
]);
```

Ausgabe

```
{ "_id" : 1, "fruitIndex" : 1 }
{ "_id" : 2, "fruitIndex" : 0 }
{ "_id" : 3, "fruitIndex" : 2 }
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$indexOfArray` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('collection');

  const result = await collection.aggregate([
    {
      $project: {
        _id: 1,
        fruitIndex: { $indexOfArray: ["$fruits", "mango"] }
      }
    }
```

```
  ]).toArray();

  console.log(result);
  client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['collection']

    result = list(collection.aggregate([
        {
            '$project': {
                '_id': 1,
                'fruitIndex': { '$indexOfArray': ["$fruits", "mango"] }
            }
        }
    ]))

    print(result)
    client.close()

example()
```

$ index OfBytes

Der OfBytes $index-Operator in Amazon DocumentDB wird verwendet, um den Startindex einer Teilzeichenfolge innerhalb einer Zeichenfolge auf der Grundlage der Bytepositionen der Zeichen zu finden. Dies kann nützlich sein, wenn Sie mit Textdaten arbeiten, die Mehrbyte-Zeichen enthalten können, wie sie beispielsweise in nicht-lateinischen Schriften vorkommen.

Parameter

- `string`: Die Eingabezeichenfolge, nach der gesucht werden soll.
- `substring`: Die Teilzeichenfolge, nach der innerhalb der Eingabezeichenfolge gesucht werden soll.
- `[<start>]`: (optional) Die Startposition (auf Null basierend) der Suche. Wenn nicht angegeben, beginnt die Suche am Anfang der Zeichenfolge.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt die Verwendung von`$indexOfBytes`, um den Index des ersten Bindestrichs in einer Reihe von Zeichenketten zu finden, die Schreibtischpositionen darstellen.

Erstellen Sie Beispieldokumente

```
db.people.insertMany([
  { "_id": 1, "Desk": "Düsseldorf-BVV-021" },
  { "_id": 2, "Desk": "Munich-HGG-32a" },
  { "_id": 3, "Desk": "Cologne-ayu-892.50" },
  { "_id": 4, "Desk": "Dortmund-Hop-78" }
]);
```

Beispiel für eine Abfrage

```
db.people.aggregate([
  { $project: { stateLocation: { $indexOfBytes: ["$Desk", "-"] } } }
]);
```

Ausgabe

```
{ "_id" : 1, "stateLocation" : 11 }
{ "_id" : 2, "stateLocation" : 6 }
{ "_id" : 3, "stateLocation" : 7 }
{ "_id" : 4, "stateLocation" : 8 }
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$indexOfBytes` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const events = db.collection('people');

  const result = await db.collection('people').aggregate([
    { $project: { stateLocation: { $indexOfBytes: ["$Desk", "-"] } } }
  ]).toArray();
  console.log(result);
  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['people']

    result = list(db.people.aggregate([
        { '$project': { 'stateLocation': { '$indexOfBytes': ['$Desk', '-'] } } }
    ]))
    print(result)
    client.close()

example()
```

$indexOfCP

Der `$indexOfCP` Operator in Amazon DocumentDB wird verwendet, um den Index in Codepunkten (CP) des ersten Vorkommens einer angegebenen Teilzeichenfolge innerhalb eines Zeichenkettenausdrucks zu finden. Dies kann beim Parsen und Extrahieren von Inhalten aus Zeichenkettenfeldern nützlich sein.

Parameter

- `string expression`: Die zu durchsuchende Zeichenfolge.
- `substring`: Die Teilzeichenfolge, nach der gesucht werden soll.
- `[<start>]`: (optional) Die Position, an der die Suche gestartet werden soll (nullbasierter Index). Standard = 0.

Beispiel (MongoDB Shell)

In diesem Beispiel verwenden wir den `$indexOfCP` Operator, um den Index des ersten Vorkommens des Bindestrichs zu ermitteln — im Feld Schreibtisch jedes Dokuments.

Erstellen Sie Beispieldokumente

```
db.people.insertMany([
  { "_id":1, "name":"John Doe", "Manager":"Jane Doe", "Role":"Developer", "Desk":
 "Düsseldorf-BVV-021"},
  { "_id":2, "name":"John Stiles", "Manager":"Jane Doe", "Role":"Manager", "Desk":
 "Munich-HGG-32a"},
  { "_id":3, "name":"Richard Roe", "Manager":"Jorge Souza", "Role":"Product", "Desk":
 "Cologne-ayu-892.50"},
  { "_id":4, "name":"Mary Major", "Manager":"Jane Doe", "Role":"Solution Architect",
 "Desk": "Dortmund-Hop-78"}
])
```

Beispiel für eine Abfrage

```
db.people.aggregate([
  { $project: { stateLocation: { $indexOfCP: [ "$Desk", "-"] } } }
])
```

Ausgabe

```
{ "_id" : 1, "stateLocation" : 10 }
{ "_id" : 2, "stateLocation" : 6 }
{ "_id" : 3, "stateLocation" : 7 }
{ "_id" : 4, "stateLocation" : 8 }
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$indexOfCP` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function main() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('people');

  const result = await collection.aggregate([
    { $project: { stateLocation: { $indexOfCP: [ "$Desk", "-"] } } }
  ]).toArray();

  console.log(result);

  await client.close();
}

main();
```

Python

```
from pymongo import MongoClient

client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
db = client['test']
collection = db['people']
```

```
result = list(collection.aggregate([
    { '$project': { 'stateLocation': { '$indexOfCP': [ '$Desk', '-' ] } } }
]))

print(result)

client.close()
```

$indexStats

Die `$indexStats` Aggregationsphase in Amazon DocumentDB bietet Einblick in die Verwendung von Indizes innerhalb einer Sammlung. Dieser Operator ermöglicht es Ihnen, die Zugriffsmuster Ihrer Indizes zu überwachen, was Ihnen helfen kann, fundierte Entscheidungen über die Indexverwaltung und -optimierung zu treffen.

Parameter

Keine

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$indexStats` Operator verwendet wird, um die Indexnutzung in einer Amazon DocumentDB-Sammlung zu analysieren.

Erstellen Sie Beispieldokumente

```
db.grocery.insertMany([
  { _id: 1, product: "milk", quantity: 10 },
  { _id: 2, product: "eggs", quantity: 20 },
  { _id: 3, product: "bread", quantity: 5 },
  { _id: 4, product: "cheese", quantity: 15 },
  { _id: 5, product: "apple", quantity: 8 }
]);
```

Beispiel für eine Abfrage

```
db.grocery.aggregate([
  { $indexStats: {} }
]);
```

Ausgabe

```
[
  {
    "name": "_id_",
    "key": {
      "_id": 1
    },
    "host": "docdb-cluster-1.cluster-123456789.us-west-2.docdb.amazonaws.com",
    "accesses": {
      "ops": NumberLong(5),
      "since": ISODate("2023-04-06T12:34:56.789Z")
    }
  },
  {
    "name": "product_1",
    "key": {
      "product": 1
    },
    "host": "docdb-cluster-1.cluster-123456789.us-west-2.docdb.amazonaws.com",
    "accesses": {
      "ops": NumberLong(10),
      "since": ISODate("2023-04-06T12:34:56.789Z")
    }
  }
]
```

In diesem Beispiel zeigt der `$indexStats` Operator, dass seit dem `_id_` letzten Reset oder Serverneustart fünfmal auf den `product_1` Index zugegriffen wurde und dass zehnmal auf den Index zugegriffen wurde.

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$indexStats` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function indexStats() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
```

```
  const db = client.db('test');
  const result = await db.collection('grocery').aggregate([
    { $indexStats: {} }
  ]).toArray();
  console.log(result);
  await client.close();
}

indexStats();
```

Python

```
from pymongo import MongoClient

def index_stats():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    result = list(db.grocery.aggregate([
        { '$indexStats': {} }
    ]))
    print(result)
    client.close()

index_stats()
```

$isArray

Der `$isArray` Operator in Amazon DocumentDB wird verwendet, um zu prüfen, ob es sich bei einem Feld in einem Dokument um ein Array handelt. Dieser Operator kann in Aggregationspipelines und bedingten Ausdrücken nützlich sein, um Felder vom Typ Array zu verarbeiten.

Parameter

- `field`: Der Feldpfad, um zu überprüfen, ob es sich um ein Array handelt.

Beispiel (MongoDB Shell)

Dieses Beispiel zeigt, wie der `$isArray` Operator verwendet wird, um Dokumente zu identifizieren, bei denen das Feld „Inventar“ ein Array ist.

Erstellen Sie Beispieldokumente

```
db.videos.insertMany([
  { "_id":1, "name":"Live Soft", "inventory": {"Des Moines": 1000, "Ames" : 500}},
  { "_id":2, "name":"Top Pilot", "inventory": {"Mason City": 250, "Des Moines": 1000}},
  { "_id":3, "name":"Romancing the Rock", "inventory": {"Mason City": 250, "Ames" :
 500}},
  { "_id":4, "name":"Bravemind", "inventory": [{"location": "Mason City", "count":
 250}, {"location": "Des Moines", "count": 1000}, {"location": "Ames", "count": 500}]}
]);
```

Beispiel für eine Abfrage

```
db.videos.aggregate([
  {
    $match: {
      $isArray: "$inventory"
    }
  },
  {
    $project: {
      _id: 1,
      name: 1,
      "inventory.location": 1,
      "inventory.count": 1
    }
  }
]).pretty();
```

Ausgabe

```
{
  "_id": 4,
  "name": "Bravemind",
  "inventory": [
    {
      "location": "Mason City",
      "count": 250
    },
    {
      "location": "Des Moines",
      "count": 1000
    },
```

```
    {
      "location": "Ames",
      "count": 500
    }
  ]
}
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$isArray` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function run() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('videos');

  const result = await collection.aggregate([
    {
      $match: {
        $isArray: '$inventory'
      }
    },
    {
      $project: {
        _id: 1,
        name: 1,
        "inventory.location": 1,
        "inventory.count": 1
      }
    }
  ]).toArray();

  console.log(result);

  await client.close();
}
```

```
run();
```

Python

```
from pymongo import MongoClient

client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
db = client['test']
collection = db['videos']

result = list(collection.aggregate([
    {
        '$match': {
            '$isArray': '$inventory'
        }
    },
    {
        '$project': {
            '_id': 1,
            'name': 1,
            'inventory.location': 1,
            'inventory.count': 1
        }
    }
]))

print(result)

client.close()
```

$ iso DayOfWeek

Der `$isoDayOfWeek` Operator in Amazon DocumentDB gibt den ISO-Wochentag für ein Datum als Ganzzahl zurück. Das ISO-Wochendatumssystem definiert jede Woche, die an einem Montag beginnt und an einem Sonntag endet, wobei Woche 1 die Woche ist, die den ersten Donnerstag des Jahres enthält.

Parameter

- `expression`: Der Datumsausdruck, für den der ISO-Wochentag zurückgegeben werden soll.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$isoDayOfWeek` Operator verwendet wird, um den ISO-Wochentag für eine Reihe von Ereignisdokumenten abzurufen.

Erstellen Sie Beispieldokumente

```
db.events.insertMany([
  { _id: 1, eventDate: ISODate("2023-04-01T12:00:00Z") },
  { _id: 2, eventDate: ISODate("2023-04-02T12:00:00Z") },
  { _id: 3, eventDate: ISODate("2023-04-03T12:00:00Z") },
  { _id: 4, eventDate: ISODate("2023-04-04T12:00:00Z") },
  { _id: 5, eventDate: ISODate("2023-04-05T12:00:00Z") },
  { _id: 6, eventDate: ISODate("2023-04-06T12:00:00Z") },
  { _id: 7, eventDate: ISODate("2023-04-07T12:00:00Z") }
]);
```

Beispiel für eine Abfrage

```
db.events.aggregate([
  { $project: {
    _id: 1,
    eventDate: 1,
    isoDayOfWeek: { $isoDayOfWeek: "$eventDate" }
  }}
]);
```

Ausgabe

```
[
  { "_id": 1, "eventDate": ISODate("2023-04-01T12:00:00Z"), "isoDayOfWeek": 6 },
  { "_id": 2, "eventDate": ISODate("2023-04-02T12:00:00Z"), "isoDayOfWeek": 7 },
  { "_id": 3, "eventDate": ISODate("2023-04-03T12:00:00Z"), "isoDayOfWeek": 1 },
  { "_id": 4, "eventDate": ISODate("2023-04-04T12:00:00Z"), "isoDayOfWeek": 2 },
  { "_id": 5, "eventDate": ISODate("2023-04-05T12:00:00Z"), "isoDayOfWeek": 3 },
  { "_id": 6, "eventDate": ISODate("2023-04-06T12:00:00Z"), "isoDayOfWeek": 4 },
  { "_id": 7, "eventDate": ISODate("2023-04-07T12:00:00Z"), "isoDayOfWeek": 5 }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$isoDayOfWeek` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const events = db.collection('events');

  const result = await events.aggregate([
    {
      $project: {
        _id: 1,
        eventDate: 1,
        isoDayOfWeek: { $isoDayOfWeek: '$eventDate' }
      }
    }
  ]).toArray();

  console.log(result);
  client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client.test
    events = db.events
```

```
    result = list(events.aggregate([
        {
            '$project': {
                '_id': 1,
                'eventDate': 1,
                'isoDayOfWeek': { '$isoDayOfWeek': '$eventDate' }
            }
        }
    ]))

    print(result)
    client.close()

example()
```

$isoWeek

Der `$isoWeek` Operator in Amazon DocumentDB gibt die ISO-Wochennummer für ein Datum zurück. Das ISO-Wochendatumssystem ist eine Methode zur Nummerierung von Wochen in einem Jahr, wobei die erste Woche eines neuen Jahres die Woche ist, die den ersten Donnerstag des Jahres enthält. Dies unterscheidet sich vom gregorianischen Kalender, bei dem die erste Woche eines neuen Jahres die Woche ist, die den 1. Januar enthält.

Parameter

Keine

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$isoWeek` Operator verwendet wird, um die ISO-Wochennummer für ein bestimmtes Datum abzurufen.

Erstellen Sie Beispieldokumente

```
db.dates.insertMany([
  { _id: 1, date: new ISODate("2022-01-01") },
  { _id: 2, date: new ISODate("2022-12-31") },
  { _id: 3, date: new ISODate("2023-01-01") }
])
```

Beispiel für eine Abfrage

```
db.dates.aggregate([
  {
    $project: {
      _id: 1,
      isoWeek: { $isoWeek: "$date" }
    }
  }
])
```

Ausgabe

```
[
  { "_id": 1, "isoWeek": 52 },
  { "_id": 2, "isoWeek": 52 },
  { "_id": 3, "isoWeek": 1 }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$isoWeek` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('dates');

  const result = await collection.aggregate([
    {
      $project: {
        _id: 1,
        isoWeek: { $isoWeek: "$date" }
      }
    }
  ]).toArray();
```

```
  console.log(result);
  client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['dates']

    result = list(collection.aggregate([
        {
            '$project': {
                '_id': 1,
                'isoWeek': { '$isoWeek': '$date' }
            }
        }
    ]))

    print(result)
    client.close()

example()
```

$ iso WeekYear

Der `$isoWeekYear` Operator in Amazon DocumentDB gibt die ISO-8601-Wochenjahreszahl für ein bestimmtes Datum zurück. Die ISO-Wochenjahreszahl unterscheidet sich vom gregorianischen Kalenderjahr dadurch, dass sich das Wochenjahr vom Kalenderjahr unterscheiden kann, insbesondere zu Beginn und Ende des Jahres.

Parameter

- `expression`: Der Datumsausdruck, für den die Jahreszahl der ISO-8601-Woche zurückgegeben werden soll.

Beispiel (MongoDB Shell)

Dieses Beispiel zeigt, wie der `$isoWeekYear` Operator verwendet wird, um das ISO 8601-Wochenjahr für das Datumsfeld jedes Dokuments in der Eventsammlung abzurufen.

Erstellen Sie Beispieldokumente

```
db.events.insertMany([
  { _id: 1, name: "Event 1", date: ISODate("2022-12-31T00:00:00Z") },
  { _id: 2, name: "Event 2", date: ISODate("2023-01-01T00:00:00Z") },
  { _id: 3, name: "Event 3", date: ISODate("2023-01-02T00:00:00Z") }
]);
```

Beispiel für eine Abfrage

```
db.events.aggregate([
  { $project: {
    name: 1,
    isoWeekYear: { $isoWeekYear: "$date" }
  }}
]);
```

Ausgabe

```
[
  { "_id" : 1, "name" : "Event 1", "isoWeekYear" : 2023 },
  { "_id" : 2, "name" : "Event 2", "isoWeekYear" : 2023 },
  { "_id" : 3, "name" : "Event 3", "isoWeekYear" : 2023 }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$isoWeekYear` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');
```

```
async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const events = db.collection('events');

  const result = await events.aggregate([
    { $project: {
      name: 1,
      isoWeekYear: { $isoWeekYear: '$date' }
    }}
  ]).toArray();

  console.log(result);
  client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client.test
    events = db.events

    result = list(events.aggregate([
        { '$project': {
            'name': 1,
            'isoWeekYear': { '$isoWeekYear': '$date' }
        }}
    ]))

    print(result)
    client.close()

example()
```

$last

Der `$last` Operator in Amazon DocumentDB wird verwendet, um das letzte Element in einem Array zurückzugeben, das den Abfragekriterien entspricht. Er ist besonders nützlich, um das neueste oder das letzte Element in einem Array abzurufen, das eine bestimmte Bedingung erfüllt.

Parameter

- `expression`: Der Ausdruck, der den Array-Elementen entspricht.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt die Verwendung des `$last` Operators in Kombination mit dem `$filter` Abrufen des letzten Elements aus einem Array, das eine bestimmte Bedingung erfüllt (z. B. ist subject 'science').

Erstellen Sie Beispieldokumente

```
db.collection.insertMany([
  {
    "_id": 1,
    "name": "John",
    "scores": [
      { "subject": "math", "score": 82 },
      { "subject": "english", "score": 85 },
      { "subject": "science", "score": 90 }
    ]
  },
  {
    "_id": 2,
    "name": "Jane",
    "scores": [
      { "subject": "math", "score": 92 },
      { "subject": "english", "score": 88 },
      { "subject": "science", "score": 87 }
    ]
  },
  {
    "_id": 3,
    "name": "Bob",
    "scores": [
```

```
      { "subject": "math", "score": 75 },
      { "subject": "english", "score": 80 },
      { "subject": "science", "score": 85 }
    ]
  }
]);
```

Beispiel für eine Abfrage

```
db.collection.aggregate([
    { $match: { name: "John" } },
    {
      $project: {
        name: 1,
        lastScienceScore: {
          $last: {
            $filter: {
              input: "$scores",
              as: "score",
              cond: { $eq: ["$$score.subject", "science"] }
            }
          }
        }
      }
    }
  ]);
```

Ausgabe

```
[
  {
    _id: 1,
    name: 'John',
    lastScienceScore: { subject: 'science', score: 90 }
  }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$last` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');

  const db = client.db('test');
  const collection = db.collection('collection');

  const result = await collection.aggregate([
    { $match: { name: "John" } },
    {
      $project: {
        name: 1,
        lastScienceScore: {
          $last: {
            $filter: {
              input: "$scores",
              as: "score",
              cond: { $eq: ["$$score.subject", "science"] }
            }
          }
        }
      }
    }
  ]).toArray();

  console.log(JSON.stringify(result, null, 2));
  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
```

```
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')

    db = client.test
    collection = db.collection

    pipeline = [
        { "$match": { "name": "John" } },
        {
            "$project": {
                "name": 1,
                "lastScienceScore": {
                    "$last": {
                        "$filter": {
                            "input": "$scores",
                            "as": "score",
                            "cond": { "$eq": ["$$score.subject", "science"] }
                        }
                    }
                }
            }
        }
    ]

    result = list(collection.aggregate(pipeline))

    print(result)

    client.close()

example()
```

$let

Der `$let` Operator in Amazon DocumentDB wird verwendet, um Variablen an Werte zu binden und diese Variablen im Ausdruck zu verwenden. Es ermöglicht Ihnen, lokale Variablen zu definieren, die in nachfolgenden Ausdrücken innerhalb derselben Phase der Aggregationspipeline verwendet werden können.

Parameter

- `vars`: Ein Objekt, das die Variablen definiert, die im Ausdruck verwendet werden sollen.
- `in`: Der Ausdruck, in dem die im vars-Parameter definierten Variablen verwendet werden.

Beispiel (MongoDB Shell)

Dieses Beispiel demonstriert die Verwendung des `$let` Operators zur Berechnung der Fläche eines Rechtecks.

Erstellen Sie Beispieldokumente

```
db.shapes.insertMany([
  { name: "Rectangle 1", length: 5, width: 3 },
  { name: "Rectangle 2", length: 7, width: 4 },
  { name: "Rectangle 3", length: 6, width: 2 }
]);
```

Beispiel für eine Abfrage

```
db.shapes.aggregate([
  {
    $project: {
      name: 1,
      area: {
        $let: {
          vars: {
            length: "$length",
            width: "$width"
          },
          in: {
            $multiply: ["$$length", "$$width"]
          }
        }
      }
    }
  }
])
```

Ausgabe

```
[
  {
```

```
    "_id": ObjectId("6161e5b1a3eba3c7f2960d03"),
    "name": "Rectangle 1",
    "area": 15
  },
  {
    "_id": ObjectId("6161e5b1a3eba3c7f2960d04"),
    "name": "Rectangle 2",
    "area": 28
  },
  {
    "_id": ObjectId("6161e5b1a3eba3c7f2960d05"),
    "name": "Rectangle 3",
    "area": 12
  }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$let` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function calculateRectangleAreas() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('shapes');

  const result = await shapes.aggregate([
    {
      $project: {
        name: 1,
        area: {
          $let: {
            vars: {
              length: '$length',
              width: '$width'
            },
            in: {
```

```
              $multiply: ['$$length', '$$width']
            }
          }
        }
      }
    }
  ]).toArray();

  console.log(result);
  client.close();
}

calculateRectangleAreas();
```

Python

```
from pymongo import MongoClient

def calculate_rectangle_areas():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client.test
    collection = db.shapes

    result = list(shapes.aggregate([
        {
            '$project': {
                'name': 1,
                'area': {
                    '$let': {
                        'vars': {
                            'length': '$length',
                            'width': '$width'
                        },
                        'in': {
                            '$multiply': ['$$length', '$$width']
                        }
                    }
                }
            }
        }
    ]))
```

```
    print(result)
    client.close()

calculate_rectangle_areas()
```

$limit

Der `$limit` Operator in Amazon DocumentDB wird verwendet, um die Anzahl der von einer Abfrage zurückgegebenen Dokumente einzuschränken. Er ähnelt dem `$limit` MongoDB-Operator, es gibt jedoch einige spezifische Überlegungen, wenn er mit Amazon DocumentDB verwendet wird.

In Amazon DocumentDB ist der `$limit` Operator nützlich für die Paginierung, bei der Sie eine Teilmenge der gesamten übereinstimmenden Dokumente abrufen möchten. Damit können Sie die Anzahl der Dokumente kontrollieren, die in jeder Antwort zurückgesendet werden, wodurch die Leistung verbessert und die Menge der über das Netzwerk übertragenen Daten reduziert wird.

Parameter

- `limit`: Die maximale Anzahl von Dokumenten, die zurückgegeben werden sollen. Dies muss ein nicht negativer Ganzzahlwert sein.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$limit` Operator verwendet wird, um maximal ein Dokument zurückzugeben, das dem angegebenen Filter entspricht.

Erstellen Sie Beispieldokumente

```
db.test.insertMany([
  { "_id": 1, "star_rating": 4, "comments": "apple is red" },
  { "_id": 2, "star_rating": 5, "comments": "comfortable couch" },
  { "_id": 3, "star_rating": 3, "comments": "apples, oranges - healthy fruit" },
  { "_id": 4, "star_rating": 5, "comments": "this is a great couch" },
  { "_id": 5, "star_rating": 5, "comments": "interesting couch" }
]);
```

Beispiel für eine Abfrage

```
db.test.createIndex({ comments: "text" });
```

```
db.test.find({
  $and: [
    { star_rating: 5 },
    { $text: { $search: "couch" } }
  ]
}).limit(1);
```

Ausgabe

```
[ { _id: 2, star_rating: 5, comments: 'comfortable couch' } ]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$limit` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function limitExample() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');

  try {
      await client.connect();

      const db = client.db('test');
      const collection = db.collection('test');

      await collection.createIndex({ comments: 'text' });

      const query = {
        $and: [
          { star_rating: 5 },
          { $text: { $search: "couch" } }
        ]
      };

      const result = await collection.find(query).limit(1).toArray();
```

```
      console.log(result);

    } catch (err) {
        console.error("Error:", err);
    } finally {
        await client.close();
    }

}

limitExample();
```

Python

```
from pymongo import MongoClient

def limit_example():
    try:
        client = MongoClient('mongodb://<username>:<password>@<cluster-
endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')

        db = client['test']
        collection = db['test']

        collection.create_index([('comments', 'text')])

        query = {
            '$and': [
                {'star_rating': 5},
                {'$text': {'$search': 'couch'}}
            ]
        }

        result = collection.find(query).limit(1)

        for doc in result:
            print(doc)

    except Exception as e:
        print(f"An error occurred: {e}")
```

```
    finally:
        client.close()

limit_example()
```

$literal

Der `$literal` Operator in Amazon DocumentDB wird verwendet, um einen Literalwert innerhalb einer Aggregationspipeline-Phase darzustellen. Er ermöglicht es Ihnen, einen bestimmten Wert einzubeziehen, z. B. eine Zahl, eine Zeichenfolge oder einen booleschen Wert, ohne ihn als Feldverweis oder Ausdruck zu interpretieren.

Dieser Operator ist besonders nützlich, wenn Sie einen Literalwert als Teil einer komplexeren Aggregationspipeline einbeziehen müssen, z. B. beim Erstellen dynamischer Abfragefilter oder beim Durchführen von Berechnungen.

Parameter

Keine

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt die Verwendung des `$literal` Operators, um einen Literalwert in eine Aggregationspipeline aufzunehmen. Der `$literal` Operator wird verwendet, um den Wert 18 als Literalwert in den $gt-Ausdruck aufzunehmen. Auf diese Weise kann die Aggregationspipeline das Altersfeld mit dem Literalwert 18 vergleichen, um festzustellen, ob es sich bei der Person um einen Erwachsenen handelt.

Erstellen Sie Beispieldokumente

```
db.collection.insertMany([
  { "name": "John Doe", "age": 30, "city": "New York" },
  { "name": "Jane Doe", "age": 25, "city": "Los Angeles" },
  { "name": "Bob Smith", "age": 35, "city": "Chicago" }
]);
```

Beispiel für eine Abfrage

```
db.collection.aggregate([
  {
```

```
    $project: {
      name: 1,
      age: 1,
      city: 1,
      isAdult: { $gt: ["$age", { $literal: 18 }] }
    }
  }
]);
```

Ausgabe

```
[
  {
    "_id": ObjectId("601234567890abcdef012345"),
    "name": "John Doe",
    "age": 30,
    "city": "New York",
    "isAdult": true
  },
  {
    "_id": ObjectId("601234567890abcdef012346"),
    "name": "Jane Doe",
    "age": 25,
    "city": "Los Angeles",
    "isAdult": true
  },
  {
    "_id": ObjectId("601234567890abcdef012347"),
    "name": "Bob Smith",
    "age": 35,
    "city": "Chicago",
    "isAdult": true
  }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$literal` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');
```

```
async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('collection');

  const result = await collection.aggregate([
    {
      $project: {
        name: 1,
        age: 1,
        city: 1,
        isAdult: { $gt: ["$age", { $literal: 18 }] }
      }
    }
  ]).toArray();

  console.log(result);
  client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client.test
    collection = db.collection

    result = list(collection.aggregate([
        {
            '$project': {
                'name': 1,
                'age': 1,
                'city': 1,
                'isAdult': { '$gt': ["$age", { '$literal': 18 }] }
```

```
            }
        }
    ]))

    print(result)
    client.close()

example()
```

$ln

Neu ab Version 4.0.

Der `$ln` Operator in Amazon DocumentDB berechnet den natürlichen Logarithmus (Basis e) einer bestimmten Zahl. Er gibt den Logarithmus der Zahl zur Basis e zurück.

Parameter

- `expression`: Die Zahl, für die der natürliche Logarithmus berechnet wird.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt die Verwendung des `$log` Operators zur Berechnung des natürlichen Logarithmus einer Zahl.

Erstellen Sie Beispieldokumente

```
db.numbers.insertMany([
  { _id: 1, value: 10 },
  { _id: 2, value: 100 },
  { _id: 3, value: 1000 }
]);
```

Beispiel für eine Abfrage

```
db.numbers.aggregate([
  { $project: {
    _id: 1,
    naturalLog: { $ln: "$value" }
  }}
```

```
]);
```

Ausgabe

```
[
  { "_id" : 1, "naturalLog" : 2.302585092994046 },
  { "_id" : 2, "naturalLog" : 4.605170185988092 },
  { "_id" : 3, "naturalLog" : 6.907755278982137 }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$ln` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');

  const db = client.db('test');
  const collection = db.collection('numbers');

  const result = await collection.aggregate([
    { $project: {
      _id: 1,
      naturalLog: { $ln: "$value" }
    }}
  ]).toArray();

  console.log(result);
  client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():

    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')

    db = client.test
    collection = db.numbers

    result = list(collection.aggregate([
        { "$project": {
            "_id": 1,
            "naturalLog": { "$ln": "$value" }
        }}
    ]))

    print(result)
    client.close()

example()
```

$log

Neu ab Version 4.0.

Der `$log` Operator in Amazon DocumentDB berechnet den natürlichen Logarithmus einer Zahl. Er gibt den Logarithmus zur Basis E der angegebenen Zahl zurück.

Parameter

- `expression`: Die Zahl, für die der natürliche Logarithmus berechnet wird.
- `base`: Basiswert für die Log-Berechnung.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt die Verwendung des `$log` Operators zur Berechnung des natürlichen Logarithmus einer Zahl.

Erstellen Sie Beispieldokumente

```
db.numbers.insertMany([
  { _id: 1, value: 10 },
  { _id: 2, value: 100 },
  { _id: 3, value: 1000 }
]);
```

Beispiel für eine Abfrage

```
db.numbers.aggregate([
  { $project: {
    _id: 1,
    naturalLog: { $log: ["$value", 10] }
  }}
]);
```

Ausgabe

```
[
  { "_id" : 1, "naturalLog" : 1 },
  { "_id" : 2, "naturalLog" : 2 },
  { "_id" : 3, "naturalLog" : 2.9999999999999996 }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$log` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');

  const db = client.db('test');
  const collection = db.collection('numbers');
```

```
  const result = await collection.aggregate([
    { $project: {
      _id: 1,
      naturalLog: { $log: ["$value", 10] }
    }}
  ]).toArray();

  console.log(result);
  client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')

    db = client.test
    collection = db.numbers

    result = list(collection.aggregate([
        { "$project": {
            "_id": 1,
            "naturalLog": { "$log": ["$value", 10] }
        }}
    ]))

    print(result)
    client.close()

example()
```

$log10

Neu ab Version 4.0.

Der `$log10` Operator in Amazon DocumentDB wird verwendet, um den Logarithmus einer Zahl zur Basis 10 zu berechnen. Er ist nützlich, um logarithmische Berechnungen für numerische Felder innerhalb der Aggregationspipeline durchzuführen.

Parameter

- `expression`: Der numerische Ausdruck, für den der Logarithmus zur Basis 10 berechnet werden soll.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$log10` Operator verwendet wird, um den Logarithmus zur Basis 10 eines numerischen Feldes zu berechnen.

Erstellen Sie Beispieldokumente

```
db.numbers.insertMany([
  { _id: 1, value: 1 },
  { _id: 2, value: 10 },
  { _id: 3, value: 100 },
  { _id: 4, value: 1000 }
]);
```

Beispiel für eine Abfrage

```
db.numbers.aggregate([
  {
    $project: {
      _id: 1,
      log10Value: { $log10: "$value" }
    }
  }
]);
```

Ausgabe

```
[
  { "_id": 1, "log10Value": 0 },
  { "_id": 2, "log10Value": 1 },
  { "_id": 3, "log10Value": 2 },
```

```
  { "_id": 4, "log10Value": 3 }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$log10` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  let client;

  try {
    client = await MongoClient.connect('mongodb://<username>:<password>@<cluster-
endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');

    const db = client.db('test');
    const collection = db.collection('numbers');

    const result = await collection.aggregate([
      {
        $project: {
          _id: 1,
          log10Value: { $log10: "$value" }
        }
      }
    ]).toArray();

    console.log(result);
  } catch (error) {
    console.error("An error occurred:", error);
  } finally {
    if (client) {
      await client.close();
    }
  }
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = None
    try:
        client = MongoClient('mongodb://<username>:<password>@<cluster-
endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')

        db = client.test
        collection = db.numbers

        result = list(collection.aggregate([
            {
                '$project': {
                    '_id': 1,
                    'log10Value': { '$log10': '$value' }
                }
            }
        ]))

        print(result)

    except Exception as e:
        print(f"An error occurred: {e}")

    finally:
        if client:
            client.close()

example()
```

$lt

Der `$lt` Aggregationsoperator vergleicht zwei Werte und gibt zurück, `true` wenn der erste Wert kleiner als der zweite ist, andernfalls kehrt `false` er zurück.

Parameter

- `expression1`: Der erste zu vergleichende Wert.

- `expression2`: Der zweite zu vergleichende Wert.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$lt` Operator verwendet wird, um Artikel mit geringem Lagerbestand zu identifizieren.

Erstellen Sie Beispieldokumente

```
db.warehouse.insertMany([
  { _id: 1, item: "Bolts", stock: 5 },
  { _id: 2, item: "Nuts", stock: 25 },
  { _id: 3, item: "Screws", stock: 8 }
]);
```

Beispiel für eine Abfrage

```
db.warehouse.aggregate([
  {
    $project: {
      item: 1,
      stock: 1,
      lowStock: { $lt: ["$stock", 10] }
    }
  }
]);
```

Ausgabe

```
[
  { _id: 1, item: 'Bolts', stock: 5, lowStock: true },
  { _id: 2, item: 'Nuts', stock: 25, lowStock: false },
  { _id: 3, item: 'Screws', stock: 8, lowStock: true }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$lt` Aggregationsoperators anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('warehouse');

  const result = await collection.aggregate([
    {
      $project: {
        item: 1,
        stock: 1,
        lowStock: { $lt: ["$stock", 10] }
      }
    }
  ]).toArray();

  console.log(result);
  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['warehouse']

    result = list(collection.aggregate([
        {
            '$project': {
                'item': 1,
                'stock': 1,
```

```
                'lowStock': { '$lt': ['$stock', 10] }
            }
        }
    ]))

    print(result)
    client.close()

example()
```

$lte

Der `$lte` Aggregationsoperator vergleicht zwei Werte und gibt zurück, `true` ob der erste Wert kleiner oder gleich dem zweiten ist, andernfalls kehrt `false` er zurück.

Parameter

- `expression1`: Der erste zu vergleichende Wert.
- `expression2`: Der zweite zu vergleichende Wert.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$lte` Operator verwendet wird, um budgetfreundliche Artikel zu identifizieren.

Erstellen Sie Beispieldokumente

```
db.menu.insertMany([
  { _id: 1, dish: "Salad", price: 8 },
  { _id: 2, dish: "Pasta", price: 12 },
  { _id: 3, dish: "Soup", price: 6 }
]);
```

Beispiel für eine Abfrage

```
db.menu.aggregate([
  {
    $project: {
      dish: 1,
      price: 1,
```

```
      affordable: { $lte: ["$price", 10] }
    }
  }
]);
```

Ausgabe

```
[
  { _id: 1, dish: 'Salad', price: 8, affordable: true },
  { _id: 2, dish: 'Pasta', price: 12, affordable: false },
  { _id: 3, dish: 'Soup', price: 6, affordable: true }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$lte` Aggregationsoperators anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('menu');

  const result = await collection.aggregate([
    {
      $project: {
        dish: 1,
        price: 1,
        affordable: { $lte: ["$price", 10] }
      }
    }
  ]).toArray();

  console.log(result);
  await client.close();
}
```

```
example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['menu']

    result = list(collection.aggregate([
        {
            '$project': {
                'dish': 1,
                'price': 1,
                'affordable': { '$lte': ['$price', 10] }
            }
        }
    ]))

    print(result)
    client.close()

example()
```

$lookup

Die `$lookup` Aggregationsphase in Amazon DocumentDB ermöglicht es Ihnen, einen Left Outer Join zwischen zwei Sammlungen durchzuführen. Mit diesem Vorgang können Sie Daten aus mehreren Sammlungen auf der Grundlage übereinstimmender Feldwerte kombinieren. Dies ist besonders nützlich, wenn Sie Daten aus verwandten Sammlungen in Ihre Abfrageergebnisse integrieren müssen.

Parameter

- `from`: Der Name der Sammlung, mit der die Verknüpfung durchgeführt werden soll.
- `localField`: Das Feld aus den Eingabedokumenten, das mit dem abgeglichen werden soll`foreignField`.

- `foreignField`: Das Feld aus den Dokumenten in der `from` Sammlung, mit dem abgeglichen werden soll`localField`.
- `as`: Der Name des neuen Felds, das zu den Ausgabedokumenten hinzugefügt werden soll, die die passenden Dokumente aus der `from` Sammlung enthalten.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt einen einfachen `$lookup` Vorgang, bei dem Daten aus der `orders` Sammlung mit der `customers` Sammlung verknüpft werden.

Erstellen Sie Beispieldokumente

```
db.customers.insertMany([
  { _id: 1, name: "Alice" },
  { _id: 2, name: "Bob" },
  { _id: 3, name: "Charlie" }
]);

db.orders.insertMany([
  { _id: 1, customer_id: 1, total: 50 },
  { _id: 2, customer_id: 1, total: 100 },
  { _id: 3, customer_id: 2, total: 75 }
]);
```

Beispiel für eine Abfrage

```
db.customers.aggregate([
  {
    $lookup: {
      from: "orders",
      localField: "_id",
      foreignField: "customer_id",
      as: "orders"
    }
  }
]);
```

Ausgabe

```
[
  {
```

```
    _id: 1,
    name: 'Alice',
    orders: [
      { _id: 2, customer_id: 1, total: 100 },
      { _id: 1, customer_id: 1, total: 50 }
    ]
  },
  { _id: 3, name: 'Charlie', orders: [] },
  {
    _id: 2,
    name: 'Bob',
    orders: [ { _id: 3, customer_id: 2, total: 75 } ]
  }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$lookup` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');

  await client.connect();

  const db = client.db('test');

  const result = await db.collection('customers').aggregate([
    {
      $lookup: {
        from: 'orders',
        localField: '_id',
        foreignField: 'customer_id',
        as: 'orders'
      }
    }
  ]).toArray();
```

```
  console.log(JSON.stringify(result, null, 2));
  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')

    db = client.test

    collection = db.customers

    pipeline = [
        {
            "$lookup": {
                "from": "orders",
                "localField": "_id",
                "foreignField": "customer_id",
                "as": "orders"
            }
        }
    ]

    result = collection.aggregate(pipeline)

    for doc in result:
        print(doc)

    client.close()

example()
```

$ ltrim

Neu ab Version 4.0.

Wird von Elastic Cluster nicht unterstützt.

Der `$ltrim` Operator in Amazon DocumentDB wird verwendet, um führende Zeichen aus einer Zeichenfolge zu entfernen. Standardmäßig entfernt er führende Leerzeichen, aber Sie können auch eine Reihe von Zeichen angeben, die entfernt werden sollen, indem Sie das Argument chars übergeben.

Parameter

- `input`: Die Eingabezeichenfolge, aus der führende Leerzeichen entfernt werden sollen.
- `chars`: (optional) Um bestimmte Zeichen zu entfernen.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt die Verwendung von`$ltrim`, um bestimmte Zeichen (“ *“) am Anfang einer Zeichenfolge zu entfernen.

Erstellen Sie Beispieldokumente

```
db.collection.insertMany([
  { name: " *John Doe", age: 30 },
  { name: "Jane Doe*", age: 25 },
  { name: "  Bob Smith  ", age: 35 }
]);
```

Beispiel für eine Abfrage

```
db.collection.aggregate([
  {
    $project: {
      _id: 0,
      name: {
        $ltrim: { input: "$name", chars: " *" }
      },
      age: 1
    }
```

```
  }
]);
```

Ausgabe

```
[
  { "name": "John Doe", "age": 30 },
  { "name": "Jane Doe ", "age": 25 },
  { "name": "Bob Smith  ", "age": 35 }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$ltrim` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');

  try {
    await client.connect();

    const db = client.db('test');
    const collection = db.collection('collection');

    const pipeline = [
      {
        $project: {
          _id: 0,
          name: {
            $ltrim: {
              input: '$name',
              chars: ' *'
            }
          },
          age: 1
```

```
        }
      }
    ];

    const result = await collection.aggregate(pipeline).toArray();

    console.dir(result, { depth: null });

  } finally {
    await client.close();
  }
}

example().catch(console.error);
```

Python

```
from pymongo import MongoClient

def example():
    try:
        client = MongoClient('mongodb://<username>:<password>@<cluster-
endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')

        db = client.test
        collection = db.collection

        pipeline = [
            {
                "$project": {
                    "_id": 0,
                    "name": {
                        "$ltrim": {
                            "input": "$name",
                            "chars": " *"
                        }
                    },
                    "age": 1
                }
            }
        ]
```

```
        results = collection.aggregate(pipeline)

        for doc in results:
            print(doc)

    except Exception as e:
        print(f"An error occurred: {e}")

    finally:
        client.close()

example()
```

$map

Der `$map` Operator in Amazon DocumentDB ermöglicht es Ihnen, einen bestimmten Ausdruck auf jedes Element in einem Array anzuwenden und ein neues Array mit den transformierten Elementen zurückzugeben. Dieser Operator ist besonders nützlich für die Manipulation und Transformation von Daten innerhalb von Arrays. Er kann dazu beitragen, Ihren Anwendungscode zu vereinfachen und die Abfrageleistung zu verbessern, indem die Array-Verarbeitung auf Datenbankebene verlagert wird.

Parameter

- `input`: Das Array, das transformiert werden soll.
- `as`: (optional) Der Name der Variablen, die innerhalb des in-Ausdrucks verwendet werden soll, um das aktuelle Element darzustellen, das gerade verarbeitet wird.
- `in`: Der Ausdruck, der auf jedes Element im Eingabearray angewendet werden soll.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der $map-Operator verwendet wird, um ein Zahlenarray zu transformieren, wobei jeder Wert verdoppelt wird.

Erstellen Sie Beispieldokumente

```
db.collection.insertMany([
  { _id: 1, numbers: [1, 2, 3, 4, 5] },
  { _id: 2, numbers: [10, 20, 30, 40, 50] }
])
```

Beispiel für eine Abfrage

```
db.collection.aggregate([
  {
    $project: {
      doubledNumbers: { $map: { input: "$numbers", as: "num", in: { $multiply: ["$
$num", 2] } } }
    }
  }
])
```

Ausgabe

```
[
  { _id: 1, doubledNumbers: [2, 4, 6, 8, 10] },
  { _id: 2, doubledNumbers: [20, 40, 60, 80, 100] }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des $map Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('collection');

  const result = await collection.aggregate([
    {
      $project: {
        doubledNumbers: { $map: { input: "$numbers", as: "num", in: { $multiply: ["$
$num", 2] } } }
      }
    }
  ]).toArray();
```

```
  console.log(result);
  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client.test
    collection = db.collection

    result = list(collection.aggregate([
        {
            '$project': {
                'doubledNumbers': { '$map': { 'input': '$numbers', 'as': 'num',
 'in': { '$multiply': ['$$num', 2] } } }
            }
        }
    ]))

    print(result)
    client.close()

example()
```

$match

Die `$match` Pipeline-Phase in Amazon DocumentDB wird verwendet, um die Eingabedokumente nur so zu filtern, dass sie den angegebenen Abfragekriterien entsprechen. Sie ist eine der am häufigsten verwendeten Pipeline-Phasen bei Aggregationsvorgängen. Die `$match` Phase wird vor allen anderen Pipeline-Phasen angewendet, sodass Sie die Anzahl der Dokumente, die in den nachfolgenden Phasen verarbeitet werden müssen, effizient reduzieren können.

Parameter

- `query`: Ein Dokument, das die Auswahlkriterien für die Operation zum Ausdruck bringt. Das Abfragedokument verwendet dieselbe Syntax wie die `find()` Methode.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt die Verwendung des `$match` Stagingbereichs zum Filtern von Dokumenten auf der Grundlage eines bestimmten Feldwerts.

Erstellen Sie Beispieldokumente

```
db.collection.insertMany([
  { _id: 1, name: "John", age: 25, city: "New York" },
  { _id: 2, name: "Jane", age: 30, city: "Los Angeles" },
  { _id: 3, name: "Bob", age: 35, city: "Chicago" },
  { _id: 4, name: "Alice", age: 40, city: "Miami" }
]);
```

Beispiel für eine Abfrage

```
db.collection.aggregate([
  { $match: { age: { $gt: 30 } } },
  { $project: { _id: 1, name: 1, city: 1 } }
]);
```

Ausgabe

```
[
  { "_id": 3, "name": "Bob", "city": "Chicago" },
  { "_id": 4, "name": "Alice", "city": "Miami" }
]
```

`$match`In der Phase werden die Dokumente so gefiltert, dass sie nur diejenigen enthalten, bei denen das `age` Feld größer als 30 ist.

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$match` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');

  const db = client.db('test');
  const collection = db.collection('collection');

  const result = await collection.aggregate([
    { $match: { age: { $gt: 30 } } },
    { $project: { _id: 1, name: 1, city: 1 } }
  ]).toArray();

  console.log(result);
  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')

    db = client['test']
    collection = db['collection']

    result = list(collection.aggregate([
        { '$match': { 'age': { '$gt': 30 } } },
        { '$project': { '_id': 1, 'name': 1, 'city': 1 } }
    ]))

    print(result)
    client.close()
```

```
example()
```

$max

Die `$max` Aggregationsphase wird verwendet, um den Maximalwert eines angegebenen Felds für alle Dokumente in einer Pipeline-Phase zurückzugeben. Dieser Operator ist nützlich, um den höchsten Wert in einer Reihe von Dokumenten zu finden.

Parameter

- `expression`: Der Ausdruck, der zur Berechnung des Maximalwerts verwendet werden soll.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$max` Operator verwendet wird, um die maximale Punktzahl in einer Sammlung von Studentendokumenten zu ermitteln. `$group`In der Phase werden alle Dokumente gruppiert, und der `$max` Operator wird verwendet, um den Maximalwert des `score` Feldes für alle Dokumente zu berechnen.

Erstellen Sie Beispieldokumente

```
db.students.insertMany([
  { name: "John", score: 85 },
  { name: "Jane", score: 92 },
  { name: "Bob", score: 78 },
  { name: "Alice", score: 90 }
])
```

Beispiel für eine Abfrage

```
db.students.aggregate([
  { $group: { _id: null, maxScore: { $max: "$score" } } },
  { $project: { _id: 0, maxScore: 1 } }
])
```

Ausgabe

```
[ { maxScore: 92 } ]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$max` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function findMaxScore() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const students = db.collection('students');

  const result = await students.aggregate([
    { $group: { _id: null, maxScore: { $max: "$score" } } }
  ]).toArray();

  console.log(result);
  await client.close();
}

findMaxScore();
```

Python

```
from pymongo import MongoClient

def find_max_score():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    students = db.students

    result = list(students.aggregate([
        { "$group": { "_id": None, "maxScore": { "$max": "$score" } } }
    ]))

    print(result)
    client.close()
```

```
find_max_score()
```

$meta

Der `$meta` Aggregationsoperator greift auf Metadaten zu, die Dokumenten in einer Aggregationspipeline zugeordnet sind. Er wird häufig verwendet, um Ergebnisse der Textsuche abzurufen und Ergebnisse nach Relevanz zu sortieren.

Parameter

- `textScore`: Ruft das Ergebnis der Textsuche ab, das die Relevanz des Dokuments für die Suchabfrage angibt.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt die Verwendung des `$meta` Operators in einer Aggregationspipeline zum Abrufen und Sortieren nach Textsuchergebnissen.

Erstellen Sie Beispieldokumente

```
db.articles.createIndex({ content: "text" });

db.articles.insertMany([
  { _id: 1, title: "Python Programming", content: "Python is a versatile programming
 language used for web development." },
  { _id: 2, title: "Python Guide", content: "Learn Python programming with Python
 tutorials and Python examples." },
  { _id: 3, title: "Java Basics", content: "Java is another popular programming
 language." }
]);
```

Beispiel für eine Abfrage

```
db.articles.aggregate([
  { $match: { $text: { $search: "Python" } } },
  { $addFields: { score: { $meta: "textScore" } } },
  { $sort: { score: -1 } }
]);
```

Ausgabe

```
[
  {
    _id: 2,
    title: 'Python Guide',
    content: 'Learn Python programming with Python tutorials and Python examples.',
    score: 1.5
  },
  {
    _id: 1,
    title: 'Python Programming',
    content: 'Python is a versatile programming language used for web development.',
    score: 0.75
  }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des $meta Aggregationsoperators anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('articles');

  const result = await collection.aggregate([
    { $match: { $text: { $search: "Python" } } },
    { $addFields: { score: { $meta: "textScore" } } },
    { $sort: { score: -1 } }
  ]).toArray();

  console.log(result);
  await client.close();
}
```

```
example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['articles']

    result = list(collection.aggregate([
        { '$match': { '$text': { '$search': 'Python' } } },
        { '$addFields': { 'score': { '$meta': 'textScore' } } },
        { '$sort': { 'score': -1 } }
    ]))

    print(result)
    client.close()

example()
```

$ zusammenführen

In 8.0 eingeführt

Die `$merge` Aggregationsphase in Amazon DocumentDB wird verwendet, um die Ergebnisse der vorherigen Pipeline-Phase in einer Zielsammlung zusammenzuführen. Dies ist nützlich, um Dokumente auf der Grundlage der Daten aus den Eingabedokumenten zu aktualisieren oder in eine Zielsammlung einzufügen.

In dieser `$merge` Phase können Sie verschiedene Aktionen ausführen, die auf der Übereinstimmungsbedingung zwischen den Eingabedokumenten und der Zielsammlung basieren, z. B.:

```
- Insert new documents
- Update existing documents
- Delete documents
- Fail the operation if there are any conflicts
```

Parameter

- `into`: (erforderlich) Der Name der Zielsammlung, zu der die Eingabedokumente zusammengeführt werden sollen.
- on: (erforderlich) Die Felder, die als Vergleichsbedingung zwischen den Eingabedokumenten und der Zielsammlung verwendet werden sollen.
- `whenMatched`: (optional) Die Aktion, die ausgeführt werden soll, wenn das Eingabedokument mit einem vorhandenen Dokument in der Zielsammlung übereinstimmt. Unterstützte Werte sind `"merge"`, `"replace"`, `"keepExisting"` und `"fail"`.
- `whenNotMatched`: (optional) Die Aktion, die ausgeführt werden soll, wenn das Eingabedokument mit keinem Dokument in der Zielsammlung übereinstimmt. Unterstützte Werte sind: `"insert"` und`"fail"`.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$merge` Stagingbereich verwendet wird, um eine `users` Sammlung mit neuen Daten aus einer Eingabepipeline zu aktualisieren.

Erstellen Sie Beispieldokumente

```
db.users.insertMany([
  { _id: 1, name: "John Doe", email: "john@example.com" },
  { _id: 2, name: "Jane Smith", email: "jane@example.com" }
]);

db.inputData.insertMany([
  { _id: 1, name: "John Doe", email: "john@example.com", phone: "123-456-7890" },
  { _id: 3, name: "Bob Johnson", email: "bob@example.com", phone: "987-654-3210" }
]);
```

Beispiel für eine Abfrage

```
db.inputData.aggregate([
  {
    $merge: {
      into: "users",
      on: "_id",
      whenMatched: "merge",
      whenNotMatched: "insert"
    }
```

```
  }
])
```

Ausgabe

Nach dem Ausführen der `$merge` Pipeline wird die `users` Sammlung die folgenden Dokumente enthalten:

```
[
  { _id: 1, name: "John Doe", email: "john@example.com", phone: "123-456-7890" },
  { _id: 2, name: "Jane Smith", email: "jane@example.com" },
  { _id: 3, name: "Bob Johnson", email: "bob@example.com", phone: "987-654-3210" }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$merge` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

Hier ist ein Beispiel für die Verwendung des $merge-Operators in einer Node.js Anwendung:

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');

  await db.collection('inputData').aggregate([
    {
      $merge: {
        into: 'users',
        on: '_id',
        whenMatched: 'merge',
        whenNotMatched: 'insert'
      }
    }
  ]).toArray();

  const users = await db.collection('users').find({}).toArray();
```

```
  console.log(users);

  await client.close();
}

example();
```

Python

Hier ist ein Beispiel für die Verwendung des $merge-Operators in einer Python-Anwendung:

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']

    # Assumes collections 'users' and 'inputData' already exist with sample data
    db.inputData.aggregate([
        {
            '$merge': {
                'into': 'users',
                'on': '_id',
                'whenMatched': 'merge',
                'whenNotMatched': 'insert'
            }
        }
    ])

    users = list(db.users.find({}))
    print(users)

    client.close()

example()
```

$mergeObjects

Der `$mergeObjects` Operator in Amazon DocumentDB wird verwendet, um mehrere Dokumente oder Objekte zu einem einzigen Dokument zu kombinieren. Dieser Operator ist besonders nützlich,

wenn Sie den Inhalt von zwei oder mehr Dokumenten oder Objekten zusammenführen müssen und dabei möglicherweise Werte aus einem Objekt mit denen eines anderen überschreiben müssen.

Parameter

- `expression1`: Das erste Objekt, das zusammengeführt werden soll.
- `expression2`: (optional) Das zweite Objekt, das zusammengeführt werden soll.
- `expression3`: (optional) Zusätzliche Objekte, die zusammengeführt werden sollen.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$mergeObjects` Operator verwendet wird, um zwei Objekte zu kombinieren.

Erstellen Sie Beispieldokumente

```
db.collection.insertMany([
  { "_id": 1, "name": "John", "address": { "city": "New York", "state": "NY" } },
  { "_id": 2, "name": "Jane", "address": { "city": "Los Angeles", "state": "CA" } }
]);
```

Beispiel für eine Abfrage

```
db.collection.aggregate([
  {
    $project: {
      "combinedAddress": {
        $mergeObjects: ["$address", { "country": "USA" }]
      }
    }
  }
])
```

Ausgabe

```
[
  {
    "_id": 1,
    "combinedAddress": {
      "city": "New York",
```

```
      "state": "NY",
      "country": "USA"
    }
  },
  {
    "_id": 2,
    "combinedAddress": {
      "city": "Los Angeles",
      "state": "CA",
      "country": "USA"
    }
  }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$mergeObjects` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('collection');

  const result = await collection.aggregate([
    {
      $project: {
        "combinedAddress": {
          $mergeObjects: ["$address", { "country": "USA" }]
        }
      }
    }
  ]).toArray();

  console.log(result);
  await client.close();
}
```

```
example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['collection']

    result = list(collection.aggregate([
        {
            '$project': {
                "combinedAddress": {
                    "$mergeObjects": ["$address", { "country": "USA" }]
                }
            }
        }
    ]))

    print(result)
    client.close()

example()
```

$millisecond

Der `$millisecond` Operator in Amazon DocumentDB wird verwendet, um den Millisekundenanteil eines Datumswerts zu extrahieren.

Parameter

Keine

Beispiel (MongoDB Shell)

Dieses Beispiel zeigt, wie der `$millisecond` Operator verwendet wird, um den Millisekundenanteil eines Datumswerts zu extrahieren.

Erstellen Sie Beispieldokumente

```
db.events.insert([
  {
    "name": "Event 1",
    "timestamp": ISODate("2023-04-21T10:30:15.123Z")
  },
  {
    "name": "Event 2",
    "timestamp": ISODate("2023-04-21T10:30:15.456Z")
  },
  {
    "name": "Event 3",
    "timestamp": ISODate("2023-04-21T10:30:15.789Z")
  }
])
```

Beispiel für eine Abfrage

```
db.events.aggregate([
  {
    $project: {
      name: 1,
      milliseconds: { $millisecond: "$timestamp" }
    }
  }
])
```

Ausgabe

```
[
  {
    "_id": ObjectId("644332a42054ed1b0d15f0c1"),
    "name": "Event 1",
    "milliseconds": 123
  },
  {
    "_id": ObjectId("644332a42054ed1b0d15f0c2"),
    "name": "Event 2",
    "milliseconds": 456
  },
  {
```

```
    "_id": ObjectId("644332a42054ed1b0d15f0c3"),
    "name": "Event 3",
    "milliseconds": 789
  }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$millisecond` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function main() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const events = db.collection('events');

  const result = await events.aggregate([
    {
      $project: {
        name: 1,
        milliseconds: { $millisecond: '$timestamp' }
      }
    }
  ]).toArray();

  console.log(result);

  await client.close();
}

main();
```

Python

```
from pymongo import MongoClient
```

```
client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
db = client['test']
events = db['events']

result = list(events.aggregate([
    {
        '$project': {
            'name': 1,
            'milliseconds': { '$millisecond': '$timestamp' }
        }
    }
]))

print(result)

client.close()
```

$min

Der `$min` Operator gibt den Minimalwert aus einer Reihe von Werten zurück. Er kann in Aggregationsphasen verwendet werden, um den Mindestwert für ein bestimmtes Feld in mehreren Dokumenten zu ermitteln.

Parameter

- `expression`: Der auszuwertende Ausdruck. Dies kann ein Feldpfad, eine Variable oder ein beliebiger Ausdruck sein, der in einen Wert aufgelöst wird.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$min` Operator verwendet wird, um den Mindestwert des `age` Felds in mehreren Dokumenten zu ermitteln.

Erstellen Sie Beispieldokumente

```
db.users.insertMany([
  { name: "John", age: 35 },
  { name: "Jane", age: 28 },
  { name: "Bob", age: 42 },
```

```
  { name: "Alice", age: 31 }
]);
```

Beispiel für eine Abfrage

```
db.users.aggregate([
  { $group: { _id: null, minAge: { $min: "$age" } } },
  { $project: { _id: 0, minAge: 1 } }
])
```

Ausgabe

```
[ { minAge: 28 } ]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des $min Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function findMinAge() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const users = db.collection('users');

  const result = await users.aggregate([
    { $group: {
        _id: null,
        minAge: { $min: "$age" }
      }}
  ]).toArray();

  console.log(result);
  client.close();
}

findMinAge();
```

Python

```
from pymongo import MongoClient

def find_min_age():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    users = db.users

    result = list(users.aggregate([
        { "$group": {
            "_id": None,
            "minAge": { "$min": "$age" }
        }}
    ]))

    print(result)
    client.close()

find_min_age()
```

$minute

Die `$minute` Aggregationspipeline-Phase in Amazon DocumentDB extrahiert den Minutenwert aus einem Datums- oder Zeitstempelfeld.

Dieser Operator ist nützlich, wenn Sie datums- und zeitbasierte Berechnungen oder Gruppierungen innerhalb Ihrer Aggregationspipeline durchführen müssen.

Parameter

- `expression`: Das Datums- oder Zeitstempelfeld, aus dem der Minutenwert extrahiert werden soll.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$minute` Operator verwendet wird, um die Dokumente nach dem aus dem Zeitstempelfeld extrahierten Minutenwert zu gruppieren und die Anzahl der Dokumente in jeder Gruppe zu zählen.

Erstellen Sie Beispieldokumente

```
db.events.insertMany([
  { timestamp: new Date("2023-04-15T10:30:25.000Z") },
  { timestamp: new Date("2023-04-15T10:30:35.000Z") },
  { timestamp: new Date("2023-04-15T10:31:05.000Z") },
  { timestamp: new Date("2023-04-15T10:31:45.000Z") },
  { timestamp: new Date("2023-04-15T10:32:15.000Z") }
]);
```

Beispiel für eine Abfrage

```
db.events.aggregate([
  {
    $group: {
      _id: {
        minute: { $minute: "$timestamp" }
      },
      count: { $count: {} }
    }
  },
  { $sort: { "_id.minute": 1 } }
]);
```

Ausgabe

```
[
  { "_id": { "minute": 30 }, "count": 2 },
  { "_id": { "minute": 31 }, "count": 2 },
  { "_id": { "minute": 32 }, "count": 1 }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$minute` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');
```

```
async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('events');

  await collection.insertMany([
    { timestamp: new Date("2023-04-15T10:30:25.000Z") },
    { timestamp: new Date("2023-04-15T10:30:35.000Z") },
    { timestamp: new Date("2023-04-15T10:31:05.000Z") },
    { timestamp: new Date("2023-04-15T10:31:45.000Z") },
    { timestamp: new Date("2023-04-15T10:32:15.000Z") }
  ]);

  const result = await collection.aggregate([
    {
      $group: {
        _id: {
          minute: { $minute: "$timestamp" }
        },
        count: { $count: {} }
      }
    },
    { $sort: { "_id.minute": 1 } }
  ]).toArray();

  console.log(result);
  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient
from datetime import datetime

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
```

```
    collection = db['events']

    collection.insert_many([
        {'timestamp': datetime(2023, 4, 15, 10, 30, 25)},
        {'timestamp': datetime(2023, 4, 15, 10, 30, 35)},
        {'timestamp': datetime(2023, 4, 15, 10, 31, 5)},
        {'timestamp': datetime(2023, 4, 15, 10, 31, 45)},
        {'timestamp': datetime(2023, 4, 15, 10, 32, 15)}
    ])

    result = list(collection.aggregate([
        {
            '$group': {
                '_id': {
                    'minute': {'$minute': '$timestamp'}
                },
                'count': {'$count': {}}
            }
        },
        {'$sort': {'_id.minute': 1}}
    ]))

    print(result)
    client.close()

example()
```

$mod

Der $mod Operator ist ein arithmetischer Operator, der eine Modulo-Operation für eine Zahl ausführt. Er gibt den Rest der Division einer Zahl durch eine andere zurück. Dieser Operator wird häufig verwendet, um zu bestimmen, ob eine Zahl ungerade oder gerade ist, oder um Elemente in eine endliche Anzahl von Gruppen zu verteilen.

Parameter

- `expression1`: Der Dividendenausdruck.
- `expression2`: Der Divisor-Ausdruck.

Beispiel (MongoDB Shell)

Dieses Beispiel zeigt, wie der $mod Operator verwendet wird, um die Anzahl der übrig gebliebenen Widgets zu ermitteln, wenn Pakete mit 100 Stück versendet werden.

Erstellen Sie Beispieldokumente

```
db.widgets.insertMany([
  { "_id" : 1, "widget" : "A", "count" : 80372 },
  { "_id" : 2, "widget" : "B", "count" : 409282 },
  { "_id" : 3, "widget" : "C", "count" : 60739 }
])
```

Beispiel für eine Abfrage

```
db.widgets.aggregate([
  { $addFields: { leftOver: { $mod: [ "$count", 100 ] } } }
])
```

Ausgabe

```
[
  { "_id" : 1, "widget" : "A", "count" : 80372, "leftOver" : 72 },
  { "_id" : 2, "widget" : "B", "count" : 409282, "leftOver" : 82 },
  { "_id" : 3, "widget" : "C", "count" : 60739, "leftOver" : 39 }
]
```

Die Ausgabe zeigt den Rest `count` geteilt durch 100 für jedes Dokument. Dies entspricht der Anzahl der übrig gebliebenen Widgets beim Versand in Paketen mit 100 Stück.

Codebeispiele

Um ein Codebeispiel für die Verwendung des $mod Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function main() {
```

```
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const widgets = db.collection('widgets');

  await widgets.insertMany([
    { "_id" : 1, "widget" : "A", "count" : 80372 },
    { "_id" : 2, "widget" : "B", "count" : 409282 },
    { "_id" : 3, "widget" : "C", "count" : 60739 }
  ]);

  const result = await widgets.aggregate([
    { $addFields: { leftOver: { $mod: [ "$count", 100 ] } } }
  ]).toArray();

  console.log(result);
  client.close();
}

main();
```

Python

```
from pymongo import MongoClient

client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
db = client['test']
widgets = db['widgets']

widgets.insert_many([
    { "_id" : 1, "widget" : "A", "count" : 80372 },
    { "_id" : 2, "widget" : "B", "count" : 409282 },
    { "_id" : 3, "widget" : "C", "count" : 60739 }
])

result = list(widgets.aggregate([
    { "$addFields": { "leftOver": { "$mod": [ "$count", 100 ] } } }
]))

print(result)
```

```
client.close()
```

$month

Der `$month` Operator in Amazon DocumentDB gibt den Monat eines Datums als Zahl zwischen 1 und 12 zurück. Dieser Operator ist nützlich, um die Monatskomponente aus einem Datumsfeld zu extrahieren und datumsbasierte Aggregationen und Analysen durchzuführen.

Parameter

- `date_expression`: Dies ist der Ausdruck oder das Feld, das das Datum oder den Zeitstempel enthält, aus dem Sie den Monat extrahieren möchten.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$month` Operator verwendet wird, um den Monat aus einem Datumsfeld zu extrahieren und die Daten nach Monat zu gruppieren.

Erstellen Sie Beispieldokumente

```
db.sales.insert([
  { product: "abc123", price: 10.99, date: new Date("2022-01-15") },
  { product: "def456", price: 15.50, date: new Date("2022-02-28") },
  { product: "ghi789", price: 8.25, date: new Date("2022-03-10") },
  { product: "jkl012", price: 12.75, date: new Date("2022-04-05") },
  { product: "mno345", price: 18.99, date: new Date("2022-05-20") }
]);
```

Beispiel für eine Abfrage

```
db.sales.aggregate([
  { $group: {
      _id: { month: { $month: "$date" } },
      totalSales: { $sum: "$price" }
    }},
  { $sort: { "_id.month": 1 } }
]);
```

Ausgabe

```
[
  { _id: { month: 1 }, totalSales: 10.99 },
  { _id: { month: 2 }, totalSales: 15.5 },
  { _id: { month: 3 }, totalSales: 8.25 },
  { _id: { month: 4 }, totalSales: 12.75 },
  { _id: { month: 5 }, totalSales: 18.99 }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$month` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function groupSalesByMonth() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');

  try {
    await client.connect();
    const db = client.db('test');
    const collection = db.collection('sales');

    const pipeline = [
      {
        $group: {
          _id: { month: { $month: "$date" } },
          totalSales: { $sum: "$price" }
        }
      },
      {
        $sort: { "_id.month": 1 }
      }
    ];

    const results = await collection.aggregate(pipeline).toArray();

    console.dir(results, { depth: null });
```

```
  } finally {
    await client.close();
  }
}

groupSalesByMonth().catch(console.error);
```

Python

```
from pymongo import MongoClient

def group_sales_by_month():

    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')

    try:
        db = client.test
        collection = db.sales

        pipeline = [
            {
                "$group": {
                    "_id": { "$month": "$date" },
                    "totalSales": { "$sum": "$price" }
                }
            },
            {
                "$sort": { "_id": 1 }
            }
        ]

        results = collection.aggregate(pipeline)

        for doc in results:
            print(doc)

    except Exception as e:
        print(f"An error occurred: {e}")

    finally:
        client.close()
```

```
group_sales_by_month()
```

$multiply

Der `$multiply` Operator in Amazon DocumentDB wird verwendet, um die Werte von zwei oder mehr Feldern oder Ausdrücken zu multiplizieren. Dieser Operator ist besonders nützlich, um arithmetische Operationen an numerischen Feldern in Dokumenten durchzuführen. Er kann in verschiedenen Phasen der Aggregationspipeline eingesetzt werden, z. B. bei `$project` und`$addFields`, um neue Felder zu erstellen oder bestehende zu ändern.

Parameter

- `expression1`: Der erste numerische Ausdruck, der multipliziert werden soll.
- `expression2`: Der zweite numerische Ausdruck, der multipliziert werden soll.
- `[expression3, ...]`: (optional) Zusätzliche numerische Ausdrücke, die multipliziert werden sollen.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt die Verwendung `$multiply` zur Berechnung `bonus_miles` durch Multiplikation `base_miles` und `bonus_rate` für Kunden, die für die Reise eine Kreditkarte verwendet haben.

Beispieldokumente

```
db.miles.insertMany([
{ "_id": 1, "customer_name": "Arnav Desai", "member_since":
 ISODate("1997-03-01T00:00:00Z"), "base_miles": 2500, "bonus_rate": 1.8, "credit_card":
 true, "trip_cost": 250 },
{ "_id": 2, "customer_name": "Jorge Souza", "member_since":
 ISODate("2004-01-10T00:00:00Z"), "base_miles": 1890, "bonus_rate": 1.4, "credit_card":
 true, "trip_cost": 189 },
{ "_id": 3, "customer_name": "Saanvi Sarkar", "member_since":
 ISODate("1999-11-22T00:00:00Z"), "base_miles": 3250, "bonus_rate": 1.8, "credit_card":
 false, "trip_cost": 325 },
{ "_id": 4, "customer_name": "Paulo Santos", "member_since":
 ISODate("2021-06-19T00:00:00Z"), "base_miles": 2980, "bonus_rate": 1.2, "credit_card":
 true, "trip_cost": 298 },
```

```
{ "_id": 5, "customer_name": "Wang Xiulan", "member_since":
 ISODate("1995-12-04T00:00:00Z"), "base_miles": 1350, "bonus_rate": 1.9, "credit_card":
 false, "trip_cost": 135 }
]);
```

Beispiel für eine Abfrage

```
db.miles.aggregate([
  {
    $match: { credit_card: true }
  },
  {
    $project: {
      customer_name: 1,
      base_miles: 1,
      bonus_rate:1,
      credit_card: 1,
      total_miles: {
        $multiply: ["$base_miles", "$bonus_rate"]
      }
    }
  }
]);
```

Ausgabe

```
[
  { _id: 1, customer_name: 'Arnav Desai', base_miles: 12500, bonus_rate: 1.8,
 credit_card: true, total_miles: 22500 },
  { _id: 3, customer_name: 'Saanvi Sarkar',base_miles: 15200, bonus_rate: 1.8,
 credit_card: true, total_miles: 27360 },
  { _id: 4, customer_name: 'Paulo Santos', base_miles: 3400, bonus_rate: 1.1,
 credit_card: true, total_miles: 3740 }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$multiply` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function multiplyBonusMiles() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('miles');

  const result = await collection.aggregate([
    { $match: { credit_card: true } },
    {
      $project: {
        customer_name: 1,
        base_miles: 1,
        bonus_rate: 1,
        credit_card: 1,
        total_miles: {
          $multiply: ["$base_miles", "$bonus_rate"]
        }
      }
    }
  ]).toArray();

  console.log(result);
  await client.close();
}

multiplyBonusMiles();
```

Python

```
from pymongo import MongoClient

def multiply_bonus_miles():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['miles']
```

```
    result = list(collection.aggregate([
        {'$match': {'credit_card': True}},
        {
            '$project': {
                'customer_name': 1,
                'base_miles': 1,
                'bonus_rate': 1,
                'credit_card': 1,
                'total_miles': {
                    '$multiply': ['$base_miles', '$bonus_rate']
                }
            }
        }
    ]))

    print(result)
    client.close()

multiply_bonus_miles()
```

$ natürlich

Der `$natural` Operator in Amazon DocumentDB wird verwendet, um die Dokumente in ihrer natürlichen Reihenfolge zu sortieren, d. h. der Reihenfolge, in der sie in die Sammlung eingefügt wurden. Dies steht im Gegensatz zum Standard-Sortierverhalten, bei dem die Dokumente anhand der Werte der angegebenen Felder sortiert werden.

Parameter

Keine

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$natural` Operator verwendet wird, um die Dokumente in einer Sammlung in ihrer natürlichen Reihenfolge zu sortieren.

Erstellen Sie Beispieldokumente

```
db.people.insertMany([
  { "_id": 1, "name": "María García", "age": 28 },
  { "_id": 2, "name": "Arnav Desai", "age": 32 },
  { "_id": 3, "name": "Li Juan", "age": 25 },
```

```
  { "_id": 4, "name": "Carlos Salazar", "age": 41 },
  { "_id": 5, "name": "Sofia Martínez", "age": 35 }
]);
```

Beispiel für eine Abfrage

```
db.people.find({}, { "_id": 1, "name": 1 }).sort({ "$natural": 1 });
```

Ausgabe

```
[
  { "_id": 1, "name": "María García" },
  { "_id": 2, "name": "Arnav Desai" },
  { "_id": 3, "name": "Li Juan" },
  { "_id": 4, "name": "Carlos Salazar" },
  { "_id": 5, "name": "Sofia Martínez" }
]
```

Die Abfrage sortiert die Dokumente in der Sammlung in ihrer natürlichen Reihenfolge, d. h. der Reihenfolge, in der sie eingefügt wurden.

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$natural` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('people');

  const documents = await collection.find({}, { projection: { _id: 1, name: 1 } })
    .sort({ $natural: 1 })
    .toArray();

  console.log(documents);
```

```
  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['people']

    documents = list(collection.find({}, {'_id': 1, 'name': 1}).sort('$natural', 1))
    print(documents)

    client.close()

example()
```

$ne

Der `$ne` Aggregationsoperator vergleicht zwei Werte und gibt zurück, `true` wenn sie nicht gleich sind, andernfalls gibt er zurück`false`.

Parameter

- `expression1`: Der erste Wert, der verglichen werden soll.
- `expression2`: Der zweite zu vergleichende Wert.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$ne` Operator verwendet wird, um Bestellungen mit Statusänderungen zu identifizieren.

Erstellen Sie Beispieldokumente

```
db.orders.insertMany([
  { _id: 1, orderId: "A123", status: "shipped", expectedStatus: "shipped" },
  { _id: 2, orderId: "B456", status: "pending", expectedStatus: "shipped" },
  { _id: 3, orderId: "C789", status: "delivered", expectedStatus: "delivered" }
]);
```

Beispiel für eine Abfrage

```
db.orders.aggregate([
  {
    $project: {
      orderId: 1,
      status: 1,
      expectedStatus: 1,
      needsAttention: { $ne: ["$status", "$expectedStatus"] }
    }
  }
]);
```

Ausgabe

```
[
  { _id: 1, orderId: 'A123', status: 'shipped', expectedStatus: 'shipped',
 needsAttention: false },
  { _id: 2, orderId: 'B456', status: 'pending', expectedStatus: 'shipped',
 needsAttention: true },
  { _id: 3, orderId: 'C789', status: 'delivered', expectedStatus: 'delivered',
 needsAttention: false }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des $ne Aggregationsoperators anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
```

```
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('orders');

  const result = await collection.aggregate([
    {
      $project: {
        orderId: 1,
        status: 1,
        expectedStatus: 1,
        needsAttention: { $ne: ["$status", "$expectedStatus"] }
      }
    }
  ]).toArray();

  console.log(result);
  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['orders']

    result = list(collection.aggregate([
        {
            '$project': {
                'orderId': 1,
                'status': 1,
                'expectedStatus': 1,
                'needsAttention': { '$ne': ['$status', '$expectedStatus'] }
            }
        }
```

```
    ]))

    print(result)
    client.close()

example()
```

$not

Der `$not` Aggregationsoperator führt eine logische NOT-Operation für einen Ausdruck aus. Er gibt zurück`true`, ob der Ausdruck zu `false` ausgewertet wird und `false` ob der Ausdruck zu ausgewertet wird. `true`

Parameter

- `expression`: Der Ausdruck, der negiert werden soll.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$not` Operator verwendet wird, um boolesche Werte umzukehren.

Erstellen Sie Beispieldokumente

```
db.users.insertMany([
  { _id: 1, name: "Alice", active: true },
  { _id: 2, name: "Bob", active: false },
  { _id: 3, name: "Charlie", active: true }
]);
```

Beispiel für eine Abfrage

```
db.users.aggregate([
  {
    $project: {
      name: 1,
      active: 1,
      inactive: { $not: ["$active"] }
    }
  }
```

```
]);
```

Ausgabe

```
[
  { _id: 1, name: 'Alice', active: true, inactive: false },
  { _id: 2, name: 'Bob', active: false, inactive: true },
  { _id: 3, name: 'Charlie', active: true, inactive: false }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des $not Aggregationsoperators anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('users');

  const result = await collection.aggregate([
    {
      $project: {
        name: 1,
        active: 1,
        inactive: { $not: ["$active"] }
      }
    }
  ]).toArray();

  console.log(result);
  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['users']

    result = list(collection.aggregate([
        {
            '$project': {
                'name': 1,
                'active': 1,
                'inactive': { '$not': ['$active'] }
            }
        }
    ]))

    print(result)
    client.close()

example()
```

$objekt ToArray

Der `$objectToArray` Aggregationsoperator in Amazon DocumentDB konvertiert ein Objekt (oder Dokument) in ein Array. Die Eingabe für den Operator ist ein Dokument, und die Ausgabe besteht aus einem Array-Element für jedes Feld-Wert-Paar im Eingabedokument. Dieser Operator ist nützlich, wenn Sie mit den einzelnen Feldern eines Dokuments als Array arbeiten müssen, z. B. wenn Sie das Dokument mit dem Höchst- oder Minimalwert für ein bestimmtes Feld suchen möchten.

Parameter

- `expression`: Der Dokumentausdruck, der in ein Array konvertiert werden soll.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$objectToArray` Operator verwendet werden kann, um das Dokument mit dem maximalen Inventar für eine Videoverleihkette zu finden.

Erstellen Sie Beispieldokumente

```
db.videos.insertMany([
  {
    "_id": 1,
    "name": "Live Soft",
    "inventory": {
      "Des Moines": 1000,
      "Ames": 500
    }
  },
  {
    "_id": 2,
    "name": "Top Pilot",
    "inventory": {
      "Mason City": 250,
      "Des Moines": 1000
    }
  },
  {
    "_id": 3,
    "name": "Romancing the Rock",
    "inventory": {
      "Mason City": 250,
      "Ames": 500
    }
  },
  {
    "_id": 4,
    "name": "Bravemind",
    "inventory": {
      "Mason City": 250,
      "Des Moines": 1000,
      "Ames": 500
    }
  }
]);
```

Beispiel für eine Abfrage

```
db.videos.aggregate([
  {
    $project: {
      name: 1,
      videos: {
        $objectToArray: "$inventory"
      }
    }
  },
  {
    $unwind: "$videos"
  },
  {
    $group: {
      _id: "$name",
      maxInventory: {
        $max: "$videos.v"
      }
    }
  }
]);
```

Ausgabe

```
[
  {
    "_id": "Bravemind",
    "maxInventory": 1000
  },
  {
    "_id": "Live Soft",
    "maxInventory": 1000
  },
  {
    "_id": "Romancing the Rock",
    "maxInventory": 500
  },
  {
    "_id": "Top Pilot",
    "maxInventory": 1000
  }
```

```
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$objectToArray` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function findMaxInventory() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const videos = db.collection('videos');

  const result = await videos.aggregate([
    {
      $project: {
        name: 1,
        videos: {
          $objectToArray: "$inventory"
        }
      }
    },
    {
      $unwind: "$videos"
    },
    {
      $group: {
        _id: "$name",
        maxInventory: {
          $max: "$videos.v"
        }
      }
    }
  ]).toArray();

  console.log(result);
  client.close();
}
```

```
findMaxInventory();
```

Python

```
from pymongo import MongoClient

def find_max_inventory():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    videos = db['videos']

    result = list(videos.aggregate([
        {
            '$project': {
                'name': 1,
                'videos': {
                    '$objectToArray': '$inventory'
                }
            }
        },
        {
            '$unwind': '$videos'
        },
        {
            '$group': {
                '_id': '$name',
                'maxInventory': {
                    '$max': '$videos.v'
                }
            }
        }
    ]))

    print(result)
    client.close()

find_max_inventory()
```

$or

Der `$or` Aggregationsoperator wertet mehrere Ausdrücke aus und gibt zurück, `true` ob mindestens ein Ausdruck zu ausgewertet wird. `true` Er gibt `false` nur zurück, wenn es bei allen Ausdrücken der Fall ist. `false`

Parameter

- `expressions`: Eine Reihe von Ausdrücken, die ausgewertet werden sollen.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$or` Operator verwendet wird, um zu überprüfen, ob Produkte eines von mehreren Kriterien erfüllen.

Erstellen Sie Beispieldokumente

```
db.items.insertMany([
  { _id: 1, name: "Widget", price: 150, onSale: false },
  { _id: 2, name: "Gadget", price: 45, onSale: false },
  { _id: 3, name: "Tool", price: 200, onSale: true }
]);
```

Beispiel für eine Abfrage

```
db.items.aggregate([
  {
    $project: {
      name: 1,
      price: 1,
      onSale: 1,
      goodDeal: {
        $or: [
          { $lt: ["$price", 50] },
          { $eq: ["$onSale", true] }
        ]
      }
    }
  }
]);
```

Ausgabe

```
[
  { _id: 1, name: 'Widget', price: 150, onSale: false, goodDeal: false },
  { _id: 2, name: 'Gadget', price: 45, onSale: false, goodDeal: true },
  { _id: 3, name: 'Tool', price: 200, onSale: true, goodDeal: true }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$or` Aggregationsoperators anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('items');

  const result = await collection.aggregate([
    {
      $project: {
        name: 1,
        price: 1,
        onSale: 1,
        goodDeal: {
          $or: [
            { $lt: ["$price", 50] },
            { $eq: ["$onSale", true] }
          ]
        }
      }
    }
  ]).toArray();

  console.log(result);
  await client.close();
}
```

```
example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['items']

    result = list(collection.aggregate([
        {
            '$project': {
                'name': 1,
                'price': 1,
                'onSale': 1,
                'goodDeal': {
                    '$or': [
                        { '$lt': ['$price', 50] },
                        { '$eq': ['$onSale', True] }
                    ]
                }
            }
        }
    ]))

    print(result)
    client.close()

example()
```

$out

Der `$out` Operator in Amazon DocumentDB wird verwendet, um das Ergebnis einer Aggregationspipeline in eine angegebene Sammlung zu schreiben.

`$out`sollte die letzte Phase in der Pipeline sein.

Parameter

- `output_collection`: Der Name der Ausgabesammlung, in die die Aggregationsergebnisse geschrieben werden sollen.

Hinweis: Wenn die Sammlung bereits existiert, wird sie durch die Ergebnisse der Aggregationsphase ersetzt.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$out` Operator in Amazon DocumentDB verwendet wird, um die Ergebnisse einer Aggregationspipeline in eine neue Sammlung zu schreiben.

Erstellen Sie Beispieldokumente

```
db.products.insertMany([
  { _id: 1, name: "Wireless Headphones", category: "Electronics", price: 100.0 },
  { _id: 2, name: "Smartphone", category: "Electronics", price: 200.0 },
  { _id: 3, name: "JavaScript Guide", category: "Books", price: 50.0 },
  { _id: 4, name: "Database Design Handbook", category: "Books", price: 75.0 }
]);
```

Beispiel für eine Abfrage

```
db.products.aggregate([
  { $group: { _id: "$category", totalPrice: { $sum: "$price" } } },
  { $out: "product_categories" }
])
```

Ausgabe

Keine (die Ergebnisse werden in die Ausgabesammlung geschrieben).

Die Aggregationspipeline gruppiert die Produkte nach Kategorien und berechnet den Gesamtpreis der Artikel für jede Kategorie. Der `$out` Operator schreibt die Ergebnisse in eine neue Sammlung mit dem Namen „product_categories“.

So zeigen Sie die Ergebnisse in der Ausgabesammlung an:

```
db.product_categories.find()
```

```
[
{ "_id" : "Books", "totalPrice" : 125 },
{ "_id" : "Electronics", "totalPrice" : 300 }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des $out Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function demo_out_operator() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const products = db.collection('products');

  // Execute aggregation with $out - results are stored in 'product_categories'
 collection
  await products.aggregate([
    { $group: { _id: "$category", totalPrice: { $sum: "$price" } } },
    { $out: "product_categories" }
  ]).toArray();

  // Retrieve the results from the output collection (limited to 20 records)
  const productCategories = db.collection('product_categories');
  const results = await productCategories.find({}).limit(20).toArray();

  console.log('Results stored in product_categories collection:', results);
  await client.close();
}

demo_out_operator();
```

Python

```
from pymongo import MongoClient
```

```
def demo_out_operator():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    products = db['products']

    # Execute aggregation with $out - results are stored in 'product_categories'
 collection
    list(products.aggregate([
        { '$group': { '_id': '$category', 'totalPrice': { '$sum': '$price' } } },
        { '$out': 'product_categories' }
    ]))

    # Retrieve the results from the output collection (limited to 20 records)
    product_categories = db['product_categories']
    results = list(product_categories.find({}).limit(20))

    print('Results stored in product_categories collection:', results)
    client.close()

demo_out_operator()
```

$pow

Eingeführt in 8.0

Mit dem $pow Operator in Amazon DocumentDB können Sie eine Zahl potenzieren. Dies kann nützlich sein, um exponentielle Berechnungen innerhalb Ihrer Aggregationspipeline durchzuführen.

Parameter

- <number>(erforderlich): Die Zahl, die potenziert werden soll.
- <exponent>(erforderlich): Die Potenz, auf die die Zahl erhöht werden soll.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der $pow Operator verwendet wird, um das Quadrat einer Zahl zu berechnen.

Erstellen Sie Beispieldokumente

```
db.numbers.insertMany([
  { "_id": 1, "value": 2 },
  { "_id": 2, "value": 3 },
  { "_id": 3, "value": 4 }
]);
```

Beispiel für eine Abfrage

```
db.numbers.aggregate([
  { $addFields: { "square": { $pow: ["$value", 2] } } }
])
```

Ausgabe

```
[
  { "_id": 1, "value": 2, "square": 4 },
  { "_id": 2, "value": 3, "square": 9 },
  { "_id": 3, "value": 4, "square": 16 }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des $pow Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

Hier ist ein Beispiel für die Verwendung des $pow-Operators in einer Node.js Anwendung:

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('numbers');

  const result = await collection.aggregate([
    { $addFields: { "square": { $pow: ["$value", 2] } } }
```

```
  ]).toArray();

  console.log(result);
  await client.close();
}

example();
```

Python

Hier ist ein Beispiel für die Verwendung des $pow-Operators in einer Python-Anwendung:

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['numbers']

    result = list(collection.aggregate([
        { "$addFields": { "square": { "$pow": ["$value", 2] } } }
    ]))

    print(result)
    client.close()

example()
```

$push

Der `$push` Aggregationsoperator gibt für jede Gruppe ein Array mit allen Werten aus einem angegebenen Ausdruck zurück. Er wird normalerweise innerhalb der `$group` Phase verwendet, um Werte in einem Array zu akkumulieren.

Parameter

- `expression`: Der Ausdruck, der für jedes Dokument in der Gruppe ausgewertet werden soll.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der $push Operator verwendet wird, um alle Produktnamen für jede Kategorie zu sammeln.

Erstellen Sie Beispieldokumente

```
db.sales.insertMany([
  { _id: 1, category: "Electronics", product: "Laptop", amount: 1200 },
  { _id: 2, category: "Electronics", product: "Mouse", amount: 25 },
  { _id: 3, category: "Furniture", product: "Desk", amount: 350 },
  { _id: 4, category: "Furniture", product: "Chair", amount: 150 },
  { _id: 5, category: "Electronics", product: "Keyboard", amount: 75 }
]);
```

Beispiel für eine Abfrage

```
db.sales.aggregate([
  {
    $group: {
      _id: "$category",
      products: { $push: "$product" }
    }
  }
]);
```

Ausgabe

```
[
  { _id: 'Furniture', products: [ 'Desk', 'Chair' ] },
  { _id: 'Electronics', products: [ 'Laptop', 'Mouse', 'Keyboard' ] }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des $push Aggregationsoperators anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');
```

```
async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('sales');

  const result = await collection.aggregate([
    {
      $group: {
        _id: "$category",
        products: { $push: "$product" }
      }
    }
  ]).toArray();

  console.log(result);
  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['sales']

    result = list(collection.aggregate([
        {
            '$group': {
                '_id': '$category',
                'products': { '$push': '$product' }
            }
        }
    ]))
```

```
    print(result)
    client.close()

example()
```

$project

Mit dem `$project` Operator in Amazon DocumentDB können Sie Felder selektiv in Ausgabedokumente ein- oder ausschließen, Werte an die nächste Pipeline-Phase übergeben und neue Felder aus Eingabedokumentwerten berechnen.

Parameter

- `field`: Das Feld, das in die Ausgabedokumente ein- oder ausgeschlossen werden soll. Dabei kann es sich um einen Feldpfad handeln (z. B. „a.b.c“).
- `1`oder`true`: Schließt das Feld in die Ausgabe ein.
- `0`oder`false`: Schließt das Feld von der Ausgabe aus.

Beispiel (MongoDB Shell)

Das folgende Beispiel demonstriert die Verwendung des `$project` Operators bei der Erfassung von Studenten

Erstellen Sie Beispieldokumente

```
db.students.insertMany([
  { "_id": 1, "name": "Alejandro Rosalez", "math": 85, "science": 92, "grade": "A" },
  { "_id": 2, "name": "Carlos Salazar", "math": 78, "science": 84, "grade": "B" },
  { "_id": 3, "name": "Nikhil Jayashankar", "math": 95, "science": 89, "grade": "A" },
  { "_id": 4, "name": "Shirley Rodriguez", "math": 72, "science": 76, "grade": "B" }
  ]);
```

Diese Abfrage umfasst nur die `math` Felder `name` und in der Ausgabe. Das `_id` Feld ist standardmäßig enthalten, sofern es nicht ausdrücklich ausgeschlossen ist.

```
db.students.aggregate([
  { $project: { "name": 1, "math": 1 } }
])
```

Ausgabe

```
{ _id: 1, name: "Alejandro Rosalez", math: 85 }
{ _id: 2, name: "Carlos Salazar", math: 78 }
{ _id: 3, name: "Nikhil Jayashankar", math: 95 }
{ _id: 4, name: "Shirley Rodriguez", math: 72 }
```

Diese Abfrage schließt die `_id` Felder `grade` und aus der Ausgabe aus und zeigt alle anderen Felder (`name`,`math`,`science`) an.

```
db.students.aggregate([
  { $project: { "grade": 0, "_id": 0 } }
])
```

Ausgabe

```
{ name: "Alejandro Rosalez", math: 85, science: 92 }
{ name: "Carlos Salazar", math: 78, science: 84 }
{ name: "Nikhil Jayashankar", math: 95, science: 89 }
{ name: "Shirley Rodriguez", math: 72, science: 76 }
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$project` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('students');

  const result = await collection.aggregate([
    { $project: { "name": 1, "math": 1 } }
  ]).toArray();
  console.log(result);
```

```
  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['students']

    result = list(collection.aggregate([
        { '$project': { 'name': 1, 'math': 1 } }
    ]))
    print(result)

    client.close()

example()
```

$ Rand

Neu ab Version 8.0

Der `$rand` Operator in Amazon DocumentDB wird verwendet, um eine Zufallszahl zwischen 0 und 1 zu generieren.

Parameter

Keine

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$rand` Operator verwendet wird, um nach dem Zufallsprinzip zwei Dokumente aus der `temp` Sammlung auszuwählen.

Erstellen Sie Beispieldokumente

```
db.items.insertMany([
  { "name": "pencil", "quantity": 110 },
  { "name": "pen", "quantity": 159 }
])
```

Beispiel für eine Abfrage

```
db.items.aggregate([
  {
    $project: {
      randomValue: { $rand: {} }
    }
  }
])
```

Ausgabe

```
[
  {
    _id: ObjectId('6924a5edd66dcae121d29517'),
    randomValue: 0.8615243955294392
  },
  {
    _id: ObjectId('6924a5edd66dcae121d29518'),
    randomValue: 0.22815483022099903
  }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$rand` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
```

```
  const db = client.db('test');
  const collection = db.collection('items');

  const result = await collection.aggregate([
    {
      $project: {
        randomValue: { $rand: {} }
      }
    }
  ]).toArray();

  console.log(result);

  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
  client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
  db = client['test']
  collection = db['items']

  result = list(collection.aggregate([
      {
        "$project": {
          "randomValue": { "$rand": {} }
        }
      }
  ]))

  print(result)

  client.close()

example()
```

$range

Der `$range` Aggregationsoperator in Amazon DocumentDB wird verwendet, um ein Array von aufeinanderfolgenden Zahlen innerhalb eines bestimmten Bereichs zu erstellen. Dieser Operator ist besonders nützlich für die Generierung von Zahlenfolgen, wie z. B. Meilenmarkierungen für Verpflegungsstationen in einem Rennen, wie in den folgenden Beispielen gezeigt.

Parameter

- `start`: Der Startwert für den Bereich.
- `end`: Der Endwert für den Bereich.
- `step`: (optional) Der Schrittwert, der beim Generieren des Bereichs verwendet werden soll. Wenn nicht angegeben, ist der Standard-Schrittwert 1.

Beispiel (MongoDB Shell)

In diesem Beispiel verwenden wir den `$range` Operator, um die Meilenmarkierungen für Wasserstationen in einem Radrennen zu generieren.

Erstellen Sie Beispieldokumente

```
db.races.insertMany([
  { _id: 0, race: "STP", distance: 206 },
  { _id: 1, race: "RSVP", distance: 160 },
  { _id: 2, race: "Chilly Hilly", distance: 33 },
  { _id: 3, race: "Flying Wheels", distance: 100 }
]);
```

Beispiel für eine Abfrage

```
db.races.aggregate([
  {
    $project: {
      race: 1,
      "waterStations": { $range: [20, "$distance", 20] }
    }
  }
]);
```

Ausgabe

```
[
  {
    _id: 0,
    race: 'STP',
    waterStations: [
       20,  40,  60,  80,
      100, 120, 140, 160,
      180, 200
    ]
  },
  {
    _id: 1,
    race: 'RSVP',
    waterStations: [
       20,  40,  60, 80,
      100, 120, 140
    ]
  },
  { _id: 2, race: 'Chilly Hilly', waterStations: [ 20 ] },
  { _id: 3, race: 'Flying Wheels', waterStations: [ 20, 40, 60, 80 ] }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$range` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');

  try {
    await client.connect();
    const db = client.db('test');
    const collection = db.collection('races');

    const pipeline = [
      {
```

```
        $project: {
          race: 1,
          waterStations: { $range: [20, "$distance", 20] }
        }
      }
    ];

    const results = await collection.aggregate(pipeline).toArray();

    console.dir(results, { depth: null });

  } finally {
    await client.close();
  }
}

example().catch(console.error);
```

Python

```
from pymongo import MongoClient

def example():

  client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')

  try:
      db = client.test
      collection = db.races

      pipeline = [
          {
              "$project": {
                  "race": 1,
                  "waterStations": { "$range": [20, "$distance", 20] }
              }
          }
      ]

      results = collection.aggregate(pipeline)
```

```
        for doc in results:
            print(doc)

    except Exception as e:
        print(f"An error occurred: {e}")

    finally:
        client.close()

example()
```

$redact

Die `$redact` Aggregationsphase in Amazon DocumentDB wird verwendet, um Inhalte anhand der Werte der angegebenen Felder selektiv in die Ausgabedokumente ein- oder auszuschließen. Dies ist besonders nützlich in Szenarien, in denen Sie die Sichtbarkeit sensibler Daten auf der Grundlage von Zugriffsebenen oder Benutzerberechtigungen kontrollieren müssen.

Parameter

- `$cond`: Ein Ausdruck, der entweder `$$KEEP``$$PRUNE`, oder `$$DESCEND` für jedes Feld im Dokument ausgewertet wird.
- `$$KEEP`: Behält das aktuelle Feld im Ausgabedokument bei.
- `$$PRUNE`: Entfernt das aktuelle Feld aus dem Ausgabedokument.
- `$$DESCEND`: Wendet den `$redact` Schritt rekursiv auf das aktuelle Feld an, bei dem es sich um ein Objekt oder ein Array handelt.

Beispiel (MongoDB Shell)

In diesem Beispiel verwenden wir die `$redact` Phase, um Bestellungen nach ihrem Status zu filtern und nur Bestellungen mit bestimmten Statuswerten anzuzeigen.

Erstellen Sie Beispieldokumente

```
db.orders.insert([
  { "_id": 1, "status": "shipped", "customer": "Carlos Salazar", "total": 150.00,
 "date": "2025-01-15" },
  { "_id": 2, "status": "processing", "customer": "Saanvi Sarkar", "total": 89.99,
 "date": "2025-01-20" },
```

```
  { "_id": 3, "status": "cancelled", "customer": "Zhang Wei", "total": 220.50, "date":
 "2025-01-18" }
])
```

Beispiel für eine Abfrage

```
db.orders.aggregate([
  {
    $redact: {
      $cond: {
        if: { $in: ["$status", ["shipped", "processing"]] },
        then: "$$KEEP",
        else: "$$PRUNE"
      }
    }
  }
])
```

Ausgabe

```
[
  { _id: 1, status: 'shipped', customer: 'Carlos Salazar', total: 150, date:
 '2025-01-15' },
  { _id: 2, status: 'processing', customer: 'Saanvi Sarkar', total: 89.99, date:
 '2025-01-20' }
]
```

In diesem Beispiel überprüft die `$redact` Phase den Wert des `status` Felds in jedem Dokument. Wenn `status` es sich um „Versand“ oder „Bearbeitung“ handelt, wird das Dokument aufbewahrt (`$$KEEP`). Andernfalls wird das Dokument beschnitten ()`$$PRUNE`.

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$redact` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
```

```
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('orders');

  const result = await collection.aggregate([
    {
      $redact: {
        $cond: {
          if: { $in: ['$status', ['shipped', 'processing']] },
          then: '$$KEEP',
          else: '$$PRUNE'
        }
      }
    }
  ]).toArray();

  console.log(result);
  client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['orders']

    result = list(collection.aggregate([
        {
            '$redact': {
                '$cond': {
                    'if': { '$in': ['$status', ['shipped', 'processing']] },
                    'then': '$$KEEP',
                    'else': '$$PRUNE'
                }
```

```
            }
        }
    ]))

    print(result)
    client.close()

example()
```

$reduce

Der `$reduce` Aggregationsoperator in Amazon DocumentDB wird verwendet, um eine Funktion mit zwei Argumenten kumulativ auf die Elemente eines Arrays anzuwenden, um das Array auf einen einzigen Wert zu reduzieren. Dieser Operator ist besonders nützlich für die Durchführung komplexer Berechnungen oder Transformationen von Array-Daten innerhalb der Aggregationspipeline.

Parameter

- `input`: Das Array, das reduziert werden soll.
- `initialValue`: Der Anfangswert, der bei der Reduktionsoperation verwendet werden soll.
- `in`: Der Ausdruck, der für jedes Element des `input` Arrays ausgewertet werden soll. Dieser Ausdruck sollte einen Wert zurückgeben, der in der nächsten Iteration der Reduktion verwendet wird.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$reduce` Operator verwendet wird, um die Summe aller Elemente in einem Array zu berechnen.

Erstellen Sie Beispieldokumente

```
db.orders.insertMany([
  { "_id": 1, "items": [1, 2, 3, 4, 5] },
  { "_id": 2, "items": [10, 20, 30] },
  { "_id": 3, "items": [5, 15, 25, 35] },
  { "_id": 4, "items": [100, 200] }
])
```

Beispiel für eine Abfrage

```
db.orders.aggregate([
  {
    $project: {
      total: {
        $reduce: {
          input: "$items",
          initialValue: 0,
          in: { $add: ["$$value", "$$this"] }
        }
      }
    }
  }
])
```

Ausgabe

```
[
  { "_id": 1, "total": 15 },
  { "_id": 2, "total": 60 },
  { "_id": 3, "total": 80 },
  { "_id": 4, "total": 300 }
]
```

Der `$reduce` Operator iteriert über das `items` Array und fügt jedes Element dem `initialValue` Wert 0 hinzu. Das Ergebnis ist die Summe aller Elemente im Array.

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$reduce` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

Hier ist ein Beispiel für die Verwendung des `$reduce` Operators in einer Node.js Anwendung:

```
const { MongoClient } = require("mongodb");

async function main() {
  const client = await MongoClient.connect("mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false");
  const db = client.db("test");
```

```
  const orders = db.collection("orders");

  const result = await orders.aggregate([
    {
      $project: {
        total: {
          $reduce: {
            input: "$items",
            initialValue: 0,
            in: { $add: ["$$value", "$$this"] }
          }
        }
      }
    }
  ]).toArray();

  console.log(result);
  await client.close();
}

main();
```

Python

Hier ist ein Beispiel für die Verwendung des `$reduce` Operators in einer Python-Anwendung:

```
from pymongo import MongoClient

def main():
    client = MongoClient("mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false")
    db = client["test"]
    orders = db["orders"]

    result = list(orders.aggregate([
        {
            "$project": {
                "total": {
                    "$reduce": {
                        "input": "$items",
                        "initialValue": 0,
                        "in": { "$add": ["$$value", "$$this"] }
                    }
```

```
                }
            }
        }
    ]))

    print(result)
    client.close()

if __name__ == "__main__":
    main()
```

$RegexFind

Neu ab Version 5.0.

Wird von Elastic Cluster nicht unterstützt.

Der `$regexFind` Operator in Amazon DocumentDB wird verwendet, um den Abgleich regulärer Ausdrücke für Zeichenkettenfelder in Dokumenten durchzuführen. Es ermöglicht Ihnen, nach bestimmten Teilzeichenfolgen zu suchen und diese zu extrahieren, die einem bestimmten Muster für reguläre Ausdrücke entsprechen.

Parameter

- `input`: Das Zeichenkettenfeld oder der Ausdruck, nach dem gesucht werden soll.
- `regex`: Das Muster für reguläre Ausdrücke, nach dem gesucht werden soll.
- `options`: (optional) Ein Objekt, das optionale Parameter für den regulären Ausdruck angibt, z. B. Berücksichtigung von Groß- und Kleinschreibung und mehrzeiliger Abgleich. Unterstützte Optionen sind `i` (ohne Berücksichtigung der Groß-/Kleinschreibung) und `m` (mehrzeilig).

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$regexFind` Operator verwendet wird, um nach Dokumenten zu suchen, bei denen das `name` Feld einem bestimmten Muster für reguläre Ausdrücke entspricht.

Erstellen Sie Beispieldokumente

```
db.users.insertMany([
  { "_id": 1, name: "John Doe", email: "john@example.com" },
```

```
  { "_id": 2, name: "Diego Ramirez", email: "diego@example.com" },
  { "_id": 3, name: "Alejandro Rosalez", email: "alejandro@example.com" },
  { "_id": 4, name: "Shirley Rodriguez", email: "shirley@example.com" }
]);
```

Beispiel für eine Abfrage

```
db.users.aggregate([
  {
    $project: {
      names: {
        $regexFind: { input: '$name', regex: 'j', options: 'i' }
      }
    }
  },
  { $match: {names: {$ne: null}}}
])
```

Diese Abfrage gibt alle Dokumente zurück, in denen das name Feld den Buchstaben „j“ enthält (Groß- und Kleinschreibung wird nicht beachtet).

Ausgabe

```
[
  { _id: 1, names: { match: 'J', idx: 0, captures: [] } }
]
```

Hinweis: Wenn Ihre Abfrage Amazon DocumentDB Planner Version 1 verwendet, müssen Sie einen Hinweis verwenden, um einen Index zu verwenden. Ohne einen Hinweis führt die Abfrage möglicherweise einen Sammlungsscan durch. Um Ihre Planer-Version zu überprüfen und mehr über die Verwendung von Hinweisen zu erfahren, lesen Sie die [Amazon DocumentDB Query Planner-Dokumentation] (https://docs.aws.amazon.com/documentdb/latest/devguide/query-planner.html).

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$regexFind` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');
```

```
async function main() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const users = db.collection('users');

  const results = await users.aggregate([
    { $project: { names: { $regexFind: { input: "$name", regex: "john", options:
 "i" }}}},
    { $match: {names: {$ne: null}}}
  ]).toArray();


  console.log(results);

  await client.close();
}

main();
```

Python

```
from pymongo import MongoClient

client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
db = client['test']
users = db['users']

results = list(users.aggregate([
    { "$project": { "names": { "$regexFind": { "input": "$name", "regex": "john",
 "options": "i" }}}},
    { "$match": {"names": {"$ne": None}}}
]))

print(results)

client.close()
```

$ regulärer Ausdruck FindAll

In 5.0 eingeführt

Der `$regexFindAll` Operator in Amazon DocumentDB wird verwendet, um den Abgleich regulärer Ausdrücke für Zeichenkettenfelder in Dokumenten durchzuführen. Es ermöglicht Ihnen, nach bestimmten Teilzeichenfolgen zu suchen und diese zu extrahieren, die einem bestimmten Muster für reguläre Ausdrücke entsprechen. Dabei werden alle Treffer des regulären Ausdrucks zurückgegeben.

Parameter

- `input`: Das Zeichenkettenfeld oder der Ausdruck, nach dem gesucht werden soll.
- `regex`: Das Muster für reguläre Ausdrücke, nach dem gesucht werden soll.
- `options`: (optional) Ein Objekt, das optionale Parameter für den regulären Ausdruck angibt, z. B. Berücksichtigung von Groß- und Kleinschreibung und mehrzeiliger Abgleich. Unterstützte Optionen sind `i` (ohne Berücksichtigung der Groß-/Kleinschreibung) und `m` (mehrzeilig).

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$regexFindAll` Operator verwendet wird, um alle Buchstabenfolgen aus dem `email` Feld zu extrahieren.

Erstellen Sie Beispieldokumente

```
db.users.insertMany([
  { _id: 1, name: "John Doe", email: "john@example.com", phone: "555-1234" },
  { _id: 2, name: "Jane Roe", email: "jane@example.com", phone: "555-5678" },
  { _id: 3, name: "Carlos Salazar", email: "carlos@example.com", phone: "555-3456" },
  { _id: 4, name: "Saanvi Sarkar", email: "saanvi@example.com", phone: "555-7890" }

]);
```

Beispiel für eine Abfrage

```
db.users.aggregate([
  {
    $project: {
      name: 1,
      emailMatches: {
        $regexFindAll: { input: '$email', regex: '[a-z]+', options: 'i' }
```

```
      }
    }
  }
])
```

Ausgabe

```
[
  {
    _id: 1,
    name: 'John Doe',
    emailMatches: [
      { match: 'john', idx: 0, captures: [] },
      { match: 'example', idx: 5, captures: [] },
      { match: 'com', idx: 13, captures: [] }
    ]
  },
  {
    _id: 2,
    name: 'Jane Roe',
    emailMatches: [
      { match: 'jane', idx: 0, captures: [] },
      { match: 'example', idx: 5, captures: [] },
      { match: 'com', idx: 13, captures: [] }
    ]
  },
  {
    _id: 3,
    name: 'Carlos Salazar',
    emailMatches: [
      { match: 'carlos', idx: 0, captures: [] },
      { match: 'example', idx: 7, captures: [] },
      { match: 'com', idx: 15, captures: [] }
    ]
  },
  {
    _id: 4,
    name: 'Saanvi Sarkar',
    emailMatches: [
      { match: 'saanvi', idx: 0, captures: [] },
      { match: 'example', idx: 7, captures: [] },
      { match: 'com', idx: 15, captures: [] }
    ]
```

```
  }
]
```

Hinweis: Wenn Ihre Abfrage Amazon DocumentDB Planner Version 1 verwendet, müssen Sie einen Hinweis verwenden, um einen Index zu verwenden. Ohne einen Hinweis führt die Abfrage möglicherweise einen Sammlungsscan durch. Um Ihre Planer-Version zu überprüfen und mehr über die Verwendung von Hinweisen zu erfahren, lesen Sie die [Amazon DocumentDB Query Planner-Dokumentation] (https://docs.aws.amazon.com/documentdb/latest/devguide/query-planner.html).

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$regexFindAll` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

Hier ist ein Beispiel für die Verwendung des `$regexFind` Operators in einer Node.js Anwendung:

```
const { MongoClient } = require('mongodb');

async function main() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const users = db.collection('users');

  const results = await users.aggregate([
    {
      $project: {
        name: 1,
        emailMatches: {
          $regexFindAll: { input: "$email", regex: "[a-z]+", options: "i" }
        }
      }
    }
  ]).toArray();

  console.log(JSON.stringify(results, null, 2));

  await client.close();
}
```

```
main();
```

Python

Hier ist ein Beispiel für die Verwendung des `$regexFind` Operators in einer Python-Anwendung:

```
from pymongo import MongoClient

client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
db = client['test']
users = db['users']

results = list(users.aggregate([
    {
        "$project": {
            "name": 1,
            "emailMatches": {
                "$regexFindAll": {
                    "input": "$email",
                    "regex": "[a-z]+",
                    "options": "i"
                }
            }
        }
    }
]))

print(results)

client.close()
```

$RegexMatch

Neu ab Version 5.0. Wird von Elastic Cluster nicht unterstützt.

Der `$regexMatch` Operator in Amazon DocumentDB wird verwendet, um den Abgleich regulärer Ausdrücke für Zeichenkettenfelder durchzuführen. Er gibt einen booleschen Wert (`true`oder`false`) zurück, der angibt, ob die Eingabezeichenfolge dem angegebenen Muster entspricht.

Parameter

- `input`: Die Zeichenfolge, die anhand des regulären Ausdrucks getestet werden soll.
- `regex`: Das Muster für reguläre Ausdrücke, das abgeglichen werden soll.
- `options`: (Optional) Markierungen zur Änderung des Verhaltens regulärer Ausdrücke, z. B. beim Abgleich ohne Berücksichtigung der Groß- und Kleinschreibung (`i`) oder beim mehrzeiligen Abgleich (). `m`

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$regexMatch` Operator verwendet wird, um zu überprüfen, ob Namen mit dem Buchstaben 'M' beginnen. Der Operator gibt `false` für jedes `true` Dokument oder zurück.

Erstellen Sie Beispieldokumente

```
db.users.insertMany([
  { "_id":1, name: "María García", email: "maría@example.com" },
  { "_id":2, name: "Arnav Desai", email: "arnav@example.com" },
  { "_id":3, name: "Martha Rivera", email: "martha@example.com" },
  { "_id":4, name: "Richard Roe", email: "richard@example.com" },

]);
```

Beispiel für eine Abfrage

```
db.users.aggregate([
  {
    $project: {
      name: 1,
      startsWithM: {
        $regexMatch: {
          input: "$name",
          regex: "^M",
          options: "i"
        }
      }
    }
  }
]);
```

Ausgabe

```
{ _id: 1, name: 'María García', startsWithM: true },
{ _id: 2, name: 'Arnav Desai', startsWithM: false },
{ _id: 3, name: 'Martha Rivera', startsWithM: true },
{ _id: 4, name: 'Richard Roe', startsWithM: false }
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$regexMatch` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function checkNamePattern() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('users');

  const result = await collection.aggregate([
    {
      $project: {
        name: 1,
        startsWithM: {
          $regexMatch: {
            input: "$name",
            regex: "^M",
            options: "i"
          }
        }
      }
    }
  ]).toArray();

  console.log(result);

  await client.close();
}

checkNamePattern();
```

Python

```
from pymongo import MongoClient

def check_name_pattern():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client.test
    collection = db.users

    result = list(collection.aggregate([
        {
            '$project': {
                'name': 1,
                'startsWithM': {
                    '$regexMatch': {
                        'input': '$name',
                        'regex': '^M',
                        'options': 'i'
                    }
                }
            }
        }
    ]))

    print(result)

    client.close()

check_name_pattern()
```

$ Alles ersetzen

In 5.0 eingeführt

Der `$replaceAll` Operator in Amazon DocumentDB wird verwendet, um alle Vorkommen eines bestimmten Zeichenkettenmusters in einem Feld durch eine neue Zeichenfolge zu ersetzen. Dieser Operator kann für Aufgaben wie Datennormalisierung, Textreinigung und Zeichenkettenmanipulation nützlich sein.

Parameter

- `input`: Das Feld oder der Ausdruck, der die zu ersetzende Zeichenfolge enthält.
- `find`: Das Zeichenkettenmuster, nach dem gesucht und ersetzt werden soll.
- `replacement`: Die Zeichenfolge, durch die die übereinstimmenden Vorkommen ersetzt werden sollen.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$replaceAll` Operator in einer Aggregationspipeline verwendet wird, um alle Vorkommen der Zeichenfolge „Chocolatier“ durch „Chocolate Co“ zu ersetzen. im Feld „BrandName“ einer Kollektion „Produkte“.

Erstellen Sie Beispieldokumente

```
db.products.insertMany([
  {
    "_id": 1,
    "productId": "PROD-0Y9GL0",
    "brandName": "Gordon's Chocolatier",
    "category": "CPG",
    "rating": {
      "average": 4.8
    }
  },
  {
    "_id": 2,
    "productId": "PROD-1X2YZ3",
    "brandName": "Premium Chocolatier",
    "category": "CPG",
    "rating": {
      "average": 4.5
    }
  },
  {
    "_id": 3,
    "productId": "PROD-Y2E9H5",
    "name": "Nutrition Co. - Original Corn Flakes Cereal",
    "category": "Breakfast Cereals",
    "price": 8.5
  }
]);
```

Beispiel für eine Abfrage

```
db.products.aggregate([
  {
    $addFields: {
      "brandName": {
        $replaceAll: {
          input: "$brandName",
          find: "Chocolatier",
          replacement: "Chocolate Co."
        }
      }
    }
  }
])
```

Ausgabe

```
[
  {
    _id: 1,
    productId: 'PROD-0Y9GL0',
    brandName: "Gordon's Chocolate Co.",
    category: 'CPG',
    rating: { average: 4.8 }
  },
  {
    _id: 2,
    productId: 'PROD-1X2YZ3',
    brandName: 'Premium Chocolate Co.',
    category: 'CPG',
    rating: { average: 4.5 }
  },
  {
    _id: 3,
    productId: 'PROD-Y2E9H5',
    name: 'Nutrition Co. - Original Corn Flakes Cereal',
    category: 'Breakfast Cereals',
    price: 8.5,
    brandName: null
  }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$replaceAll` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function replaceAll() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('products');

  const results = await collection.aggregate([
    {
      $addFields: {
        "brandName": {
          $replaceAll: {
            input: "$brandName",
            find: "Chocolatier",
            replacement: "Chocolate Co."
          }
        }
      }
    }
  ]).toArray();

  console.log(results);

  await client.close();
}

replaceAll();
```

Python

```
from pymongo import MongoClient

def replace_all():
```

```
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client.test
    collection = db.products

    results = list(collection.aggregate([
        {
            "$addFields": {
                "brandName": {
                    "$replaceAll": {
                        "input": "$brandName",
                        "find": "Chocolatier",
                        "replacement": "Chocolate Co."
                    }
                }
            }
        }
    ]))

    print(results)

    client.close()

replace_all()
```

$ ersetzenEins

In 5.0 eingeführt

Der `$replaceOne` Operator in Amazon DocumentDB ist ein Operator für Zeichenkettenausdrücke, der innerhalb von Aggregationspipelines verwendet wird, um das erste Vorkommen einer angegebenen Teilzeichenfolge innerhalb einer Zeichenfolge durch eine Ersatzzeichenfolge zu ersetzen. Dieser Operator unterscheidet Groß- und Kleinschreibung und ersetzt nur die erste gefundene Übereinstimmung.

Parameter

- `input`: Die Zeichenfolge (das Feld), nach der die Suche durchgeführt werden soll.
- `find`: Die Zeichenfolge, nach der in der Eingabe gesucht werden soll.

- `replacement`: Die Zeichenfolge, die das erste Vorkommen des Suchbegriffs in der Eingabe (Feld) ersetzen soll.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$replaceOne` Operator innerhalb einer Aggregationspipeline verwendet wird, um Teilzeichenfolgen in Produktnamen zu ersetzen.

Erstellen Sie Beispieldokumente

```
db.products.insertMany([
  { "_id":1, "productId": "PROD-0Y9GL0", "name": "Gordon's Extra Creamy Milk Chocolate
 - Pack of 4", "category": "Confectionery", "price": 24.99 },
  { "_id":2, "productId": "PROD-Y2E9H5", "name": "Nutrition Co. - Original Corn Flakes
 Cereal", "category": "Breakfast Cereals", "price": 8.50 },
  { "_id":3, "productId": "PROD-Z3F8K2", "name": "Gordon's Dark Chocolate (90% Cocoa)
 Pack - Pack of 4", "category": "Confectionery", "price": 28.99 }
]);
```

Beispiel für eine Aggregation

```
db.products.aggregate([
  {
    $addFields: {
      standardizedName: {
        $replaceOne: {
          input: "$name",
          find: "Pack",
          replacement: "Package"
        }
      }
    }
  }
]);
```

Ausgabe

Die Ausgabe zeigt, dass nur das erste Vorkommen von „Pack“ in jedem Produktnamen durch „Package“ ersetzt wurde.

```
[
```

```
{
  _id: 1,
  productId: 'PROD-0Y9GL0',
  name: "Gordon's Extra Creamy Milk Chocolate - Pack of 4",
  category: 'Confectionery',
  price: 24.99,
  standardizedName: "Gordon's Extra Creamy Milk Chocolate - Package of 4"
},
{
  _id: 2,
  productId: 'PROD-Y2E9H5',
  name: 'Nutrition Co. - Original Corn Flakes Cereal',
  category: 'Breakfast Cereals',
  price: 8.5,
  standardizedName: 'Nutrition Co. - Original Corn Flakes Cereal'
},
{
  _id: 3,
  productId: 'PROD-Z3F8K2',
  name: "Gordon's Dark Chocolate (90% Cocoa) Pack - Pack of 4",
  category: 'Confectionery',
  price: 28.99,
  standardizedName: "Gordon's Dark Chocolate (90% Cocoa) Package - Pack of 4"
}
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$replaceOne` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function replaceOne() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('products');

  const pipeline = [
    {
```

```
      $addFields: {
        standardizedName: {
          $replaceOne: {
            input: '$name',
            find: 'Pack',
            replacement: 'Package'
          }
        }
      }
    }
  ];

  const result = await collection.aggregate(pipeline).toArray();
  console.log(result);

  await client.close();
}

replaceOne();
```

Python

```
from pymongo import MongoClient

def replaceOne():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['products']

    pipeline = [
        {
            '$addFields': {
                'standardizedName': {
                    '$replaceOne': {
                        'input': '$name',
                        'find': 'Pack',
                        'replacement': 'Package'
                    }
                }
            }
        }
```

```
    ]

    result = list(collection.aggregate(pipeline))
    print(result)

    client.close()

replaceOne()
```

$replaceRoot

Der `$replaceRoot` Operator wird verwendet, um das Stammdokument durch das angegebene eingebettete Dokument zu ersetzen. Dies ist nützlich, wenn Sie ein verschachteltes Dokument auf die oberste Ebene hochstufen oder Ihre Datenausgabe neu strukturieren möchten.

Parameter

- `newRoot`: Das neue Stammdokument, das das bestehende Stammdokument ersetzen wird.

Beispiel (MongoDB Shell)

Dieses Beispiel zeigt, wie Lieferadressinformationen aus Kundenbestellungen extrahiert werden, was für die Generierung von Versandetiketten oder Adresslisten nützlich ist.

Erstellen Sie Beispieldokumente

```
db.orders.insertMany([
  {
    "_id":1, "orderId": "ORD-2024-001", "customerId": "CUST-12345", "orderDate":
 "2024-01-15", "shippingAddress": { "name": "María García", "street": "123
 Main St", "city": "Seattle", "state": "WA", "zipCode": "98101", "country":
 "USA" },"totalAmount": 149.99 },
  { "_id":2, "orderId": "ORD-2024-002", "customerId": "CUST-67890", "orderDate":
 "2024-01-16", "shippingAddress": { "name": "Arnav Desai", "street": "456 Oak
 Ave", "city": "Portland", "state": "OR", "zipCode": "97201", "country": "USA" },
 "totalAmount": 89.50 } ])
```

Beispiel für eine Abfrage

```
db.orders.aggregate([
```

```
  {
    $replaceRoot: {
      newRoot: "$shippingAddress"
    }
  }
])
```

Ausgabe

```
{
    name: 'María García',
    street: '123 Main St',
    city: 'Seattle',
    state: 'WA',
    zipCode: '98101',
    country: 'USA'
  },
  {
    name: 'Arnav Desai',
    street: '456 Oak Ave',
    city: 'Portland',
    state: 'OR',
    zipCode: '97201',
    country: 'USA'
  }
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$replaceRoot` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function extractShippingAddresses() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('orders');

  const result = await collection.aggregate([
```

```
    {
      $replaceRoot: {
        newRoot: "$shippingAddress"
      }
    }
  ]).toArray();

  console.log(result);

  await client.close();
}

extractShippingAddresses();
```

Python

```
from pymongo import MongoClient

def extract_shipping_addresses():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['orders']

    result = list(collection.aggregate([
        {
            "$replaceRoot": {
                "newRoot": "$shippingAddress"
            }
        }
    ]))

    print(result)

    client.close()

extract_shipping_addresses()
```

$ ersetzendurch

Neu ab Version 8.0

Wird von Elastic Cluster nicht unterstützt.

Die `$replaceWith` Aggregationsphase in Amazon DocumentDB wird verwendet, um das Eingabedokument durch ein neues Dokument zu ersetzen. Alle vorhandenen Felder im Eingabedokument, einschließlich des Felds _id, werden durch das neue Dokument ersetzt. `$replaceWith`wird häufig verwendet, um Dokumente zu vereinfachen oder ein eingebettetes Dokument auf die oberste Ebene heraufzustufen.

Parameter

- `<replacement>`(erforderlich): Das neue Dokument, das das bestehende Dokument ersetzen wird.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$replaceWith` Operator verwendet wird, um ein vorhandenes Dokument in einer Amazon DocumentDB-Sammlung zu ersetzen.

Erstellen Sie Beispieldokumente

```
db.restaurants.insertMany([
  {
    "restaurantId": "REST-0Y9GL0",
    "name": "Biryani Adda",
    "cuisine": "Indian",
    "ratings": [ 3, 4, 3, 2, 2, 4, 1, 5, 5, 5 ]
  },
  {
    "restaurantId": "REST-8L2PX9",
    "name": "The Burger Spot",
    "cuisine": "American",
    "ratings": [ 2, 3, 4, 5, 3, 1, 1, 2, 4 ]
  }
]);
```

Beispiel für eine Abfrage

```
db.restaurants.aggregate([
  { $replaceWith: {
      name: "$name",
      cuisine: "$cuisine",
```

```
      rating: { $avg: "$ratings" }
    }
  }
]);
```

Ausgabe

```
[
  {
    name: 'Biryani Adda',
    cuisine: 'Indian',
    rating: 3.4
  },
  {
    name: 'The Burger Spot',
    cuisine: 'American',
    rating: 2.7777777777777777
  }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$replaceWith` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function replaceDoc() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('restaurants');

  const result = await collection.aggregate([
    { $replaceWith: {
        name: "description_index",
        cuisine: 2,
        rating: { $avg: "$ratings" }
      }
    }
```

```
  ]).toArray();

  console.log(result);
  client.close();
}

replaceDoc();
```

Python

```
from pymongo import MongoClient


def replace_document():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client.test
    collection = db.restaurants

    result = list(collection.aggregate([
        {
            '$replaceWith': {
                'name': "$name",
                'cuisine': "$cuisine",
                'rating': { '$avg': "$ratings"}
            }
        }
    ]))

    print(result)
    client.close()

replace_document()
```

$reverseArray

Der `$reverseArray` Operator in Amazon DocumentDB wird verwendet, um die Elemente eines Arrays in der angegebenen Reihenfolge umzukehren. Dieser Operator ist nützlich, wenn Sie die Elemente eines Arrays in umgekehrter Richtung neu anordnen müssen.

Parameter

- `expression`: Der Array-Ausdruck, der umgekehrt werden soll.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$reverseArray` Operator verwendet wird, um die Reihenfolge der Elemente in einem Array umzukehren.

Erstellen Sie Beispieldokumente

```
db.miles.insertMany([
  { "_id" : 1, "member_since" : ISODate("1987-01-01T00:00:00Z"), "credit_card" : false,
 "flight_miles" : [ 1205, 2560, 880 ]},
  { "_id" : 2, "member_since" : ISODate("1982-01-01T00:00:00Z"), "credit_card" : true,
 "flight_miles" : [ 1205, 2560, 890, 2780]},
  { "_id" : 3, "member_since" : ISODate("1999-01-01T00:00:00Z"), "credit_card" : true,
 "flight_miles" : [ 1205, 880]}
]);
```

Beispiel für eine Abfrage

```
db.miles.aggregate([
  {
    $project: {
      _id: 1,
      member_since: 1,
      credit_card: 1,
      reversed_flight_miles: { $reverseArray: "$flight_miles" }
    }
  }
]);
```

Ausgabe

```
{ "_id" : 1, "member_since" : ISODate("1987-01-01T00:00:00Z"), "credit_card" : false,
 "reversed_flight_miles" : [ 880, 2560, 1205 ] }
{ "_id" : 2, "member_since" : ISODate("1982-01-01T00:00:00Z"), "credit_card" : true,
 "reversed_flight_miles" : [ 2780, 890, 2560, 1205 ] }
{ "_id" : 3, "member_since" : ISODate("1999-01-01T00:00:00Z"), "credit_card" : true,
 "reversed_flight_miles" : [ 880, 1205 ] }
```

In diesem Beispiel wird der `$reverseArray` Operator verwendet, um die Reihenfolge des `flight_miles` Arrays umzukehren. Das resultierende `reversed_flight_miles` Feld in der Ausgabe zeigt die Elemente des Arrays in umgekehrter Reihenfolge.

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$reverseArray` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

Hier ist ein Beispiel für die Verwendung des `$reverseArray` Operators in einer Node.js Anwendung:

```
const { MongoClient } = require('mongodb');

async function reverseArray() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('miles');

  const result = await collection.aggregate([
    {
      $project: {
        _id: 1,
        member_since: 1,
        credit_card: 1,
        reversed_flight_miles: { $reverseArray: '$flight_miles' }
      }
    }
  ]).toArray();

  console.log(result);
  client.close();
}

reverseArray();
```

Python

Hier ist ein Beispiel für die Verwendung des `$reverseArray` Operators in einer Python-Anwendung:

```
from pymongo import MongoClient

def reverse_array():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client.test
    collection = db.miles

    result = list(collection.aggregate([
        {
            '$project': {
                '_id': 1,
                'member_since': 1,
                'credit_card': 1,
                'reversed_flight_miles': { '$reverseArray': '$flight_miles' }
            }
        }
    ]))

    print(result)
    client.close()

reverse_array()
```

$rtrim

Neu ab Version 4.0.

Wird von Elastic Cluster nicht unterstützt.

Der `$rtrim` Operator in Amazon DocumentDB wird verwendet, um nachfolgende Zeichen aus einer Zeichenfolge zu entfernen. Standardmäßig entfernt er abschließende Leerzeichen, aber Sie können auch eine Reihe von Zeichen angeben, die entfernt werden sollen, indem Sie das Argument chars übergeben.

Parameter

- `input`: Die Eingabezeichenfolge, aus der nachfolgende Leerzeichen entfernt werden sollen.
- `chars`: (optional) Um bestimmte Zeichen zu entfernen.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$rtrim` Operator verwendet wird, um nachfolgende angegebene Zeichen (“ *“) aus einer Zeichenfolge zu entfernen.

Erstellen Sie Beispieldokumente

```
db.collection.insert([
  { "name": "John Doe*  ", "age": 30 },
  { "name": "Jane Smith  ", "age": 25 },
  { "name": "Bob Johnson", "age": 35 }
]);
```

Beispiel für eine Abfrage

```
db.collection.aggregate([
  {
    $project: {
      _id: 0,
      name: { $rtrim: { input: "$name", chars: " *" } },
      age: 1
    }
  }
]);
```

Ausgabe

```
[
  { age: 30, name: 'John Doe' },
  { age: 25, name: 'Jane Smith' },
  { age: 35, name: 'Bob Johnson' }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$rtrim` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient, Bson } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');

  try {

    const db = client.db('test');
    const collection = db.collection('collection');

    const pipeline = [
      {
        $project: {
          _id: 0,
          name: { $rtrim: { input: "$name", chars: " *" } },
          age: 1
        }
      }
    ];

    const results = await collection.aggregate(pipeline).toArray();
    console.dir(results, { depth: null });

  } catch (err) {
    console.error('Error occurred:', err);
  } finally {
    await client.close();
  }
}

example().catch(console.error);
```

Python

```
from pymongo import MongoClient

def example():
```

```
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')

    try:

        db = client.test
        collection = db.collection

        pipeline = [
            {
                "$project": {
                    "_id": 0,
                    "name": { "$rtrim": { "input": "$name", "chars": " *" } },
                    "age": 1
                }
            }
        ]

        results = collection.aggregate(pipeline)

        for doc in results:
            print(doc)

    except Exception as e:
        print(f"An error occurred: {e}")

    finally:
        client.close()

example()
```

$sample

Die `$sample` Aggregationsphase in Amazon DocumentDB wird verwendet, um nach dem Zufallsprinzip eine bestimmte Anzahl von Dokumenten aus einer Sammlung auszuwählen. Dies ist nützlich für Aufgaben wie Datenanalyse, Tests und Generierung von Stichproben für die weitere Verarbeitung.

Parameter

- `size`: Die Anzahl der Dokumente, die nach dem Zufallsprinzip ausgewählt werden sollen.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$sample` Stagingbereich verwendet wird, um nach dem Zufallsprinzip zwei Dokumente aus der `temp` Sammlung auszuwählen.

Erstellen Sie Beispieldokumente

```
db.temp.insertMany([
  { "_id": 1, "temperature": 97.1, "humidity": 0.60, "timestamp":
 ISODate("2019-03-21T21:17:22.425Z") },
  { "_id": 2, "temperature": 98.2, "humidity": 0.59, "timestamp":
 ISODate("2019-03-21T21:17:22.425Z") },
  { "_id": 3, "temperature": 96.8, "humidity": 0.61, "timestamp":
 ISODate("2019-03-21T21:17:22.425Z") },
  { "_id": 4, "temperature": 97.9, "humidity": 0.61, "timestamp":
 ISODate("2019-03-21T21:17:22.425Z") },
  { "_id": 5, "temperature": 97.5, "humidity": 0.60, "timestamp":
 ISODate("2019-03-21T21:17:22.425Z") },
  { "_id": 6, "temperature": 98.0, "humidity": 0.59, "timestamp":
 ISODate("2019-03-21T21:17:22.425Z") },
  { "_id": 7, "temperature": 97.2, "humidity": 0.60, "timestamp":
 ISODate("2019-03-21T21:17:22.425Z") },
  { "_id": 8, "temperature": 98.1, "humidity": 0.59, "timestamp":
 ISODate("2019-03-21T21:17:22.425Z") },
  { "_id": 9, "temperature": 96.9, "humidity": 0.62, "timestamp":
 ISODate("2019-03-21T21:17:22.425Z") },
  { "_id": 10, "temperature": 97.7, "humidity": 0.60, "timestamp":
 ISODate("2019-03-21T21:17:22.425Z") }
]);
```

Beispiel für eine Abfrage

```
db.temp.aggregate([
   { $sample: { size: 2 } }
])
```

Ausgabe

```
{ "_id" : 4, "temperature" : 97.9, "humidity" : 0.61, "timestamp" :
 ISODate("2019-03-21T21:17:22.425Z") }
{ "_id" : 9, "temperature" : 96.9, "humidity" : 0.62, "timestamp" :
 ISODate("2019-03-21T21:17:22.425Z") }
```

Wie die Ergebnisse zeigen, wurden 2 der 10 Dokumente nach dem Zufallsprinzip ausgewählt. Sie können diese Dokumente nun verwenden, um einen Durchschnitt zu ermitteln oder min/max Berechnungen durchzuführen.

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$sample` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function sampleDocuments() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('temp');

  const result = await collection.aggregate([
    { $sample: { size: 2 } }
  ]).toArray();

  console.log(result);
  await client.close();
}

sampleDocuments();
```

Python

```
from pymongo import MongoClient

def sample_documents():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['temp']

    result = list(collection.aggregate([
        { '$sample': { 'size': 2 } }
```

```
    ]))

    print(result)
    client.close()

sample_documents()
```

$suche

Neu ab Version 5.0.

Der `$search` Operator in Amazon DocumentDB wird verwendet, um Textsuchfunktionen bereitzustellen.

Parameter

Keine

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$search` Operator verwendet wird, um eine Textsuchabfrage durchzuführen.

Erstellen Sie Beispieldokumente

```
db.textcollection.createIndex({"description": "text"});

db.textcollection.insertMany([
  { _id: 1, name: "John Doe", description: "This is a sample document about John
 Doe." },
  { _id: 2, name: "Jane Smith", description: "This is a sample document about Jane
 Smith." },
  { _id: 3, name: "Bob Johnson", description: "This is a sample document about Bob
 Johnson." },
  { _id: 4, name: "Jon Jeffries", description: "This is a sample document about Jon
 Jeffries." }
]);
```

Beispiel für eine Abfrage

```
db.textcollection.find(
  { $text: { $search: "John" } }
```

```
);
```

Ausgabe

```
[
  {
    _id: 1,
    name: 'John Doe',
    description: 'This is a sample document about John Doe.'
  }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$search` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function findWithText() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('textcollection');

  const result = await collection.find(
    { $text: { $search: "John" } }
  ).sort({ score: { $meta: "textScore" } }).toArray();

  console.log(result);
  client.close();
}

findWithText();
```

Python

```
from pymongo import MongoClient
```

```
def find_with_text():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['textcollection']

    result = list(collection.find(
        { '$text': { '$search': 'John' } }
    ))

    print(result)
    client.close()

find_with_text()
```

$second

Der `$second` Operator in Amazon DocumentDB extrahiert die Sekundenkomponente aus einem Datum oder Zeitstempel. Er wird verwendet, um den Sekundenwert aus einem Datums- oder Zeitstempelfeld abzurufen.

Parameter

- `expression`: Das Datums- oder Zeitstempelfeld, aus dem der Sekundenwert extrahiert werden soll. Dieser Ausdruck kann ein Feldpfad oder ein beliebiger gültiger Ausdruck sein, der in ein Datum oder einen Zeitstempel aufgelöst wird.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$second` Operator verwendet wird, um die Sekundenkomponente aus einem Datumsfeld zu extrahieren.

Erstellen Sie Beispieldokumente

```
db.users.insertMany([
  { name: "John", dob: new Date("1990-05-15T12:30:45Z") },
  { name: "Jane", dob: new Date("1985-09-20T23:59:59Z") },
  { name: "Bob", dob: new Date("2000-01-01T00:00:00Z") }
]);
```

Beispiel für eine Abfrage

```
db.users.aggregate([{ $project: { name: 1, dobSeconds: { $second: "$dob" } } }])
```

Ausgabe

```
[
  { "_id" : ObjectId("6089a9c306a829d1f8b456a1"), "name" : "John", "dobSeconds" : 45 },
  { "_id" : ObjectId("6089a9c306a829d1f8b456a2"), "name" : "Jane", "dobSeconds" : 59 },
  { "_id" : ObjectId("6089a9c306a829d1f8b456a3"), "name" : "Bob", "dobSeconds" : 0 }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$second` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const users = db.collection('users');

  const result = await users.aggregate([{ $project: { name: 1, dobSeconds:
 { $second: '$dob' } } }]).toArray();
  console.log(result);

  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient
```

```
def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    users = db['users']

    result = list(users.aggregate([{'$project': {'name': 1, 'dobSeconds':
 {'$second': '$dob'}}}]))
    print(result)

    client.close()

example ()
```

$set

Neu ab Version 8.0

Wird von Elastic Cluster nicht unterstützt.

Die `$set` Aggregationsphase in Amazon DocumentDB ermöglicht es Ihnen, während einer Aggregationspipeline neue Felder hinzuzufügen oder bestehende Feldwerte in der Dokumentation zu aktualisieren.

Parameter

- `expression`: Der auszuwertende Ausdruck. Dies kann ein beliebiger gültiger Aggregationsausdruck sein, einschließlich Feldverweise und arithmetischer Operationen.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt die Verwendung der `$set` Aggregationsphase zur Berechnung von Summen durch Multiplikation des Felds mit dem `quantity` Feld. `price`

Erstellen Sie Beispieldokumente

```
db.inventory.insertMany([
  { item: "pencil", quantity: 100, price: 0.24},
  { item: "pen", quantity: 204, price: 1.78 }
```

```
]);
```

Beispiel für eine Aggregation

```
db.inventory.aggregate([
  {
    $set: {
      total: { $multiply: ["$quantity", "$price"] }
    }
  }
])
```

Ausgabe

```
[
  {
    _id: ObjectId('69248951d66dcae121d2950d'),
    item: 'pencil',
    quantity: 100,
    price: 0.24,
    total: 24
  },
  {
    _id: ObjectId('69248951d66dcae121d2950e'),
    item: 'pen',
    quantity: 204,
    price: 1.78,
    total: 363.12
  }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$set` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
```

```
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const inventory = db.collection('inventory');

  const result = await inventory.aggregate([
      {
        $set: {
          total: { $multiply: ["$quantity", "$price"] }
        }
      }
  ]).toArray();

  console.log(result);
  client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    inventory = db['inventory']

    result = list(inventory.aggregate([
      {
        "$set": {
          "total": { "$multiply": ["$quantity", "$price"] }
        }
      }
    ]))

    print(result)
    client.close()

example()
```

$setDifference

Neu ab Version 4.0.

Der `$setDifference` Operator in Amazon DocumentDB wird verwendet, um zwei Sätze zu vergleichen und die Elemente zurückzugeben, die sich in der ersten Gruppe, aber nicht in der zweiten Gruppe befinden. Dieser Operator ist nützlich, um die eindeutigen Elemente zwischen zwei Sätzen zu finden.

Parameter

- `firstSet`: Der erste Satz, der verglichen werden soll.
- `secondSet`: Der zweite zu vergleichende Satz.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$setDifference` Operator verwendet wird, um die eindeutigen Elemente zwischen zwei Sätzen zu finden.

Erstellen Sie Beispieldokumente

```
db.collection.insertMany([
  { _id: 1, fruits: ["apple", "banana", "cherry", "date"] },
  { _id: 2, fruits: ["banana", "cherry", "date", "elderberry"] }
]);
```

Beispiel für eine Abfrage

```
db.collection.aggregate([
  {
    $project: {
      uniqueFruits: { $setDifference: ["$fruits", ["banana", "cherry", "date"]] }
    }
  }
]);
```

Ausgabe

```
[
  { "_id": 1, "uniqueFruits": ["apple"] },
  { "_id": 2, "uniqueFruits": ["elderberry"] }
```

```
]
```

Die Abfrage führt die folgenden Schritte aus:

1. Sie verwendet die `$project` Phase, um `uniqueFruits` für jedes Dokument ein neues Feld zu erstellen.

2. Der `$setDifference` Operator vergleicht das `fruits` Array mit dem Array `["banana", "cherry", "date"]` und gibt die eindeutigen Elemente im `fruits` Array zurück.

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$setDifference` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

Hier ist ein Beispiel für die Verwendung des `$setDifference` Operators in einer Node.js Anwendung:

```
const { MongoClient } = require('mongodb');

async function main() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('mycollection');

  // Insert sample documents
  await collection.insertMany([
    { _id: 1, fruits: ["apple", "banana", "cherry", "date"] },
    { _id: 2, fruits: ["banana", "cherry", "date", "elderberry"] }
  ]);

 // Query using $setDifference
  const result = await collection.aggregate([
    {
      $project: {
        uniqueFruits: { $setDifference: ["$fruits", ["banana", "cherry", "date"]] }
      }
    }
```

```
  ]).toArray();

  console.log(result);
  await client.close();
}

main();
```

Python

Hier ist ein Beispiel für die Verwendung des `$setDifference` Operators in einer Python-Anwendung:

```
from pymongo import MongoClient

def main():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['mycollection']

    # Insert sample documents
    collection.insert_many([
        {'_id': 1, 'fruits': ["apple", "banana", "cherry", "date"]},
        {'_id': 2, 'fruits': ["banana", "cherry", "date", "elderberry"]}
    ])

    # Query using $setDifference
    result = list(collection.aggregate([
        {
            '$project': {
                'uniqueFruits': {'$setDifference': ['$fruits', ["banana", "cherry",
 "date"]]}
            }
        }
    ]))

    print(result)
    client.close()

if __name__ == '__main__':
    main()
```

$setEquals

Der `$setEquals` Operator in Amazon DocumentDB wird verwendet, um festzustellen, ob zwei Sätze gleich sind. Er vergleicht zwei Arrays und gibt zurück, `true` ob sie dieselben unterschiedlichen Elemente enthalten, unabhängig von ihrer Reihenfolge.

Parameter

- `expression1`: Das erste Array, das verglichen werden soll.
- `expression2`: Das zweite Array, das verglichen werden soll.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$setEquals` Operator verwendet wird, um zwei Wertesätze zu vergleichen.

Erstellen Sie Beispieldokumente

```
db.collection.insertMany([
  { _id: 1, fruits: ["apple", "banana", "cherry"] },
  { _id: 2, fruits: ["banana", "apple", "cherry"] },
  { _id: 3, fruits: ["apple", "banana", "orange"] }
])
```

Beispiel für eine Abfrage

```
db.collection.find({
  $expr: {
    $setEquals: ["$fruits", ["apple", "banana", "cherry"]]
  }
})
```

Ausgabe

```
{ "_id" : 1, "fruits" : [ "apple", "banana", "cherry" ] }
{ "_id" : 2, "fruits" : [ "banana", "apple", "cherry" ] }
```

Die Abfrage verwendet den `$setEquals` Operator, um das `fruits` Feld jedes Dokuments mit dem Array zu vergleichen`["apple", "banana", "cherry"]`.

Die Dokumente, bei denen das `fruits` Feld dem Vergleichsarray entspricht, werden zurückgegeben.

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$setEquals` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('mycollection');

  // Insert sample documents
  await collection.insertMany([
    { _id: 1, fruits: ["apple", "banana", "cherry"] },
    { _id: 2, fruits: ["banana", "apple", "cherry"] },
    { _id: 3, fruits: ["apple", "banana", "orange"] }
  ]);

  // Query using $setEquals
  const result = await collection.find({
    $expr: {
      $setEquals: ["$fruits", ["apple", "banana", "cherry"]]
    }
  }).toArray();

  console.log(result);
  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient
```

```
def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['mycollection']

    # Insert sample documents
    collection.insert_many([
        {"_id": 1, "fruits": ["apple", "banana", "cherry"]},
        {"_id": 2, "fruits": ["banana", "apple", "cherry"]},
        {"_id": 3, "fruits": ["apple", "banana", "orange"]}
    ])

    # Query using $setEquals
    result = list(collection.find({
        "$expr": {
            "$setEquals": ["$fruits", ["apple", "banana", "cherry"]]
        }
    }))

    print(result)
    client.close()

example()
```

$setIntersection

Der `$setIntersection` Operator in Amazon DocumentDB wird verwendet, um die gemeinsamen Elemente zwischen zwei oder mehr Arrays zurückzugeben. Dieser Operator ist besonders nützlich, wenn Sie mit Datensätzen arbeiten. Er ermöglicht es Ihnen, die Schnittmenge mehrerer Datensätze zu ermitteln.

Parameter

- `array1`: Das erste Array, das sich überschneidet.
- `array2`: Das zweite Array, das sich überschneiden soll.
- `arrayN`: (optional) Zusätzliche Arrays, die sich überschneiden sollen.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$setIntersection` Operator verwendet wird, um die gemeinsamen Elemente zwischen zwei Arrays zu finden.

Erstellen Sie Beispieldokumente

```
db.collection.insertMany([
  { _id: 1, colors: ["red", "blue", "green"] },
  { _id: 2, colors: ["blue", "yellow", "orange"] },
  { _id: 3, colors: ["red", "green", "purple"] }
])
```

Beispiel für eine Abfrage

```
db.collection.aggregate([
  { $project: {
      _id: 1,
      commonColors: { $setIntersection: ["$colors", ["red", "blue", "green"]] }
    }
  }
])
```

Ausgabe

```
[
  { "_id": 1, "commonColors": ["red", "blue", "green"] },
  { "_id": 2, "commonColors": ["blue"] },
  { "_id": 3, "commonColors": ["red", "green"] }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$setIntersection` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
```

```
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('mycollection');

  const result = await collection.aggregate([
    {
      $project: {
        _id: 1,
        commonColors: { $setIntersection: ["$colors", ["red", "blue", "green"]] }
      }
    }
  ]).toArray();

  console.log(result);
  client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['mycollection']

    result = list(collection.aggregate([
        {
            '$project': {
                '_id': 1,
                'commonColors': { '$setIntersection': ["$colors", ["red", "blue",
 "green"]] }
            }
        }
    ]))

    print(result)
```

```
    client.close()

example()
```

$ gesetzt IsSubset

Der `$setIsSubset` Operator in Amazon DocumentDB wird verwendet, um festzustellen, ob eine Gruppe von Werten eine Teilmenge einer anderen Menge ist. Er ist nützlich, um mengenbasierte Vergleiche und Operationen mit Array-Feldern durchzuführen.

Parameter

- `field`: Das Feld, auf das der `$setIsSubset` Operator angewendet werden soll.
- `set`: Das Set, mit dem das Feld verglichen werden soll.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$setIsSubset` Operator verwendet wird, um zu überprüfen, ob das `tags` Feld eine Teilmenge der angegebenen Menge ist.

Erstellen Sie Beispieldokumente

```
db.products.insertMany([
  { _id: 1, name: "Product A", tags: ["tag1", "tag2", "tag3"] },
  { _id: 2, name: "Product B", tags: ["tag1", "tag2"] },
  { _id: 3, name: "Product C", tags: ["tag2", "tag3"] }
]);
```

Beispiel für eine Abfrage

```
db.products.find({
  $expr: { $setIsSubset: [["tag1", "tag2"], "$tags"] }
})
```

*Hinweis: * `$setIsSubset` ist ein Aggregationsoperator und kann nicht direkt in find () -Abfragen verwendet werden. In diesem Beispiel `$expr` wird mit verwendet, `find()` um die Lücke zwischen Abfrageoperatoren und Aggregationsausdrücken zu schließen.

Ausgabe

```
[
  { "_id" : 1, "name" : "Product A", "tags" : [ "tag1", "tag2", "tag3" ] },
  { "_id" : 2, "name" : "Product B", "tags" : [ "tag1", "tag2" ] }
]
```

Die Abfrage gibt die Dokumente zurück, bei denen das `tags` Feld eine Teilmenge der Menge ist. `["tag1", "tag2"]`

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$setIsSubset` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('products');

  const result = await collection.find({
    $expr: { $setIsSubset: [["tag1", "tag2"], "$tags"] }
  }).toArray();

  console.log(result);

  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
```

```
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['products']

    result = list(collection.find({
        '$expr': {'$setIsSubset': [['tag1', 'tag2'], '$tags']}
    }))

    print(result)

    client.close()

example()
```

$setUnion

Der `$setUnion` Aggregationsoperator in Amazon DocumentDB wird verwendet, um zwei oder mehr Wertesätze zu kombinieren und eine Menge zurückzugeben, die alle eindeutigen Elemente aus den Eingabesätzen enthält. Dieser Operator ist nützlich, wenn Sie mengenbasierte Operationen für Array-Felder in Ihren Dokumenten ausführen müssen.

Parameter

- `expression1`: Ein Ausdruck, der in ein Array aufgelöst wird.
- `expression2`: Ein Ausdruck, der in ein Array aufgelöst wird.
- `expressionN`: Zusätzliche Ausdrücke, die in Arrays aufgelöst werden (optional).

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$setUnion` Operator verwendet wird, um die eindeutigen Elemente aus zwei Array-Feldern in einer Sammlung zu kombinieren.

Erstellen Sie Beispieldokumente

```
db.users.insertMany([
  { _id: 1, name: "Alice", hobbies: ["reading", "swimming"], skills: ["coding",
 "writing"] },
```

```
  { _id: 2, name: "Bob", hobbies: ["cooking", "gardening"], skills: ["coding",
 "photography"] },
  { _id: 3, name: "Charlie", hobbies: ["reading", "painting"], skills: ["gardening",
 "music"] }
]);
```

Beispiel für eine Abfrage

```
db.users.aggregate([
  {
    $project: {
      name: 1,
      allInterests: { $setUnion: ["$hobbies", "$skills"] }
    }
  }
]);
```

Ausgabe

```
[
  { "_id" : 1, "name" : "Alice", "allInterests" : [ "coding", "reading", "swimming",
 "writing" ] },
  { "_id" : 2, "name" : "Bob", "allInterests" : [ "coding", "cooking", "gardening",
 "photography" ] },
  { "_id" : 3, "name" : "Charlie", "allInterests" : [ "gardening", "music", "painting",
 "reading" ] }
]
```

In diesem Beispiel wird der `$setUnion` Operator verwendet, um die eindeutigen Elemente aus den Feldern `hobbies` und `skills` Array für jedes Benutzerdokument zu kombinieren. Das resultierende `allInterests` Feld enthält die Zusammenfassung aller einzigartigen Hobbys und Fähigkeiten für jeden Benutzer.

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$setUnion` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');
```

```
async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const users = db.collection('users');

  const result = await users.aggregate([
    {
      $project: {
        _id: 1,
        name: 1,
        allInterests: { $setUnion: ["$hobbies", "$skills"] }
      }
    }
  ]).toArray();

  console.log(result);
  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    users = db['users']

    result = list(users.aggregate([
        {
            '$project': {
                '_id': 1,
                'name': 1,
                'allInterests': { '$setUnion': ["$hobbies", "$skills"] }
            }
        }
```

```
    ]))

    print(result)
    client.close()

example()
```

$skip

In Amazon DocumentDB wird der `$skip` Operator verwendet, um den Startpunkt der Abfrageergebnisse zu verschieben, sodass Sie eine bestimmte Teilmenge der passenden Dokumente abrufen können. Dies ist besonders nützlich in Paginierungsszenarien, in denen Sie nachfolgende Ergebnisseiten abrufen möchten.

Parameter

- `skip`: Die Anzahl der Dokumente, die übersprungen werden sollen, bevor die verbleibenden Dokumente zurückgegeben werden.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$skip` Operator verwendet wird, um die zweite Ergebnisseite (Dokumente 11-20) aus einer Sammlung abzurufen.

Erstellen Sie Beispieldokumente

```
db.collection.insert([
  { "name": "Document 1" },
  { "name": "Document 2" },
  { "name": "Document 3" },
  { "name": "Document 4" },
  { "name": "Document 5" },
  { "name": "Document 6" },
  { "name": "Document 7" },
  { "name": "Document 8" },
  { "name": "Document 9" },
  { "name": "Document 10" },
  { "name": "Document 11" },
  { "name": "Document 12" },
  { "name": "Document 13" },
  { "name": "Document 14" },
```

```
  { "name": "Document 15" },
  { "name": "Document 16" },
  { "name": "Document 17" },
  { "name": "Document 18" },
  { "name": "Document 19" },
  { "name": "Document 20" }
]);
```

Beispiel für eine Abfrage

```
db.collection.find({}, { "name": 1 })
             .skip(10)
             .limit(10);
```

Ausgabe

```
[
  { "_id" : ObjectId("..."), "name" : "Document 11" },
  { "_id" : ObjectId("..."), "name" : "Document 12" },
  { "_id" : ObjectId("..."), "name" : "Document 13" },
  { "_id" : ObjectId("..."), "name" : "Document 14" },
  { "_id" : ObjectId("..."), "name" : "Document 15" },
  { "_id" : ObjectId("..."), "name" : "Document 16" },
  { "_id" : ObjectId("..."), "name" : "Document 17" },
  { "_id" : ObjectId("..."), "name" : "Document 18" },
  { "_id" : ObjectId("..."), "name" : "Document 19" },
  { "_id" : ObjectId("..."), "name" : "Document 20" }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$skip` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function main() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
```

```
  const db = client.db('test');
  const collection = db.collection('collection');

  const results = await collection.find({}, { projection: { name: 1 } })
                                  .skip(10)
                                  .limit(10)
                                  .toArray();

  console.log(results);

  await client.close();
}

main();
```

Python

```
from pymongo import MongoClient

def main():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client.mydatabase
    collection = db.collection

    results = list(collection.find({}, {'name': 1})
                   .skip(10)
                   .limit(10))

    print(results)

    client.close()

if __name__ == '__main__':
    main()
```

$slice

Mit dem `$slice` Aggregationsoperator können Sie eine Teilmenge eines Arrays zurückgeben, indem Sie das Array entweder vom Anfang oder vom Ende des Arrays durchqueren. Dies wird verwendet,

um eine begrenzte Anzahl von Elementen aus einem Array-Feld anzuzeigen, z. B. die obersten oder untersten N Elemente.

Parameter

- `array`: Das Array-Feld, das aufgeteilt werden soll.
- n: Eine Ganzzahl, die die Anzahl der zurückzugebenden Elemente angibt. Ein positiver Wert beginnt am Anfang des Arrays, während ein negativer Wert am Ende des Arrays beginnt.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie Sie `$slice` jedem Koch die ersten beiden Lieblingssüßigkeiten zurückgeben können.

Erstellen Sie Beispieldokumente

```
db.sweets.insertMany([
  { "_id" : 1, "name" : "Alvin", "favorites": [ "chocolate", "cake", "toffee",
 "beignets" ] },
  { "_id" : 2, "name" : "Tom", "favorites": [ "donuts", "pudding", "pie" ] },
  { "_id" : 3, "name" : "Jessica", "favorites": [ "fudge", "smores", "pudding",
 "cupcakes" ] },
  { "_id" : 4, "name" : "Rachel", "favorites": [ "ice cream" ] }
]);
```

Beispiel für eine Abfrage

```
db.sweets.aggregate([
  { $project: { _id: 0, name: 1, topTwoFavorites: { $slice: [ "$favorites", 2 ] } } }
]);
```

Ausgabe

```
[
  { name: 'Alvin', topTwoFavorites: [ 'chocolate', 'cake' ] },
  { name: 'Tom', topTwoFavorites: [ 'donuts', 'pudding' ] },
  { name: 'Jessica', topTwoFavorites: [ 'fudge', 'smores' ] },
  { name: 'Rachel', topTwoFavorites: [ 'ice cream' ] }
]
```

In diesem Beispiel wird der `$slice` Operator verwendet, um die ersten beiden Elemente aus dem `favorites` Array für jedes Dokument zu extrahieren.

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$slice` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('sweets');

  const result = await collection.aggregate([
    { $project: { name: 1, topTwoFavorites: { $slice: ['$favorites', 2] } } }
  ]).toArray();

  console.log(result);
  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['sweets']

    result = list(collection.aggregate([
        { '$project': { 'name': 1, 'topTwoFavorites': { '$slice': ['$favorites',
 2] } } }
```

```
    ]))

    print(result)
    client.close()

example()
```

$size

Der `$size` Operator wird verwendet, um die Anzahl der Elemente in einem Array-Feld zurückzugeben. Dies kann verwendet werden, um die Anzahl der Elemente in einem Array zu bestimmen, das in einem Dokument gespeichert ist.

Parameter

- `field`: Der Feldpfad, dessen Array-Größe Sie zurückgeben möchten.

Beispiel (MongoDB Shell)

Dieses Beispiel zeigt, wie der `$size` Operator verwendet wird, um die Anzahl der Teams zurückzugeben, denen jeder Benutzer folgt.

Erstellen Sie Beispieldokumente

```
db.profiles.insertMany([
  { _id: 1, name: "John Doe", teams: ["Acme", "Widgets", "Gadgets"] },
  { _id: 2, name: "Jane Smith", teams: ["Acme", "Gadgets"] },
  { _id: 3, name: "Bob Johnson", teams: ["Acme", "Widgets", "Gadgets"] }
]);
```

Beispiel für eine Abfrage

```
db.profiles.aggregate([
  {
    $project: {
      _id: 0,
      name: 1,
      "numberOfTeams": { $size: "$teams" }
    }
```

```
  }
])
```

Ausgabe

```
[
  { name: 'John Doe', numberOfTeams: 3 },
  { name: 'Jane Smith', numberOfTeams: 2 },
  { name: 'Bob Johnson', numberOfTeams: 3 }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$size` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function main() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const profiles = db.collection('profiles');

  const result = await profiles.aggregate([
    {
      $project: {
        item: 1,
        "numberOfTeams": { $size: "$teams" }
      }
    }
  ]).toArray();

  console.log(result);
  await client.close();
}

main();
```

Python

```
from pymongo import MongoClient

def main():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    profiles = db.profiles

    result = list(profiles.aggregate([
        {
            '$project': {
                'item': 1,
                'numberOfTeams': { '$size': '$teams' }
            }
        }
    ]))

    print(result)
    client.close()

if __name__ == "__main__":
    main()
```

$sort

In der `$sort` Aggregationsphase werden Dokumente in der Pipeline auf der Grundlage der angegebenen Feldwerte sortiert. Dokumente werden gemäß den angegebenen Sortierkriterien in aufsteigender oder absteigender Reihenfolge angeordnet.

Parameter

- `field`: Der Feldname, nach dem sortiert werden soll.
- `order`: Wird 1 für aufsteigende oder `-1` absteigende Reihenfolge verwendet.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie die `$sort` Phase verwendet wird, um Produkte nach Preis in absteigender Reihenfolge zu bestellen.

Erstellen Sie Beispieldokumente

```
db.products.insertMany([
  { _id: 1, name: "Laptop", category: "Electronics", price: 1200 },
  { _id: 2, name: "Mouse", category: "Electronics", price: 25 },
  { _id: 3, name: "Desk", category: "Furniture", price: 350 },
  { _id: 4, name: "Chair", category: "Furniture", price: 150 },
  { _id: 5, name: "Monitor", category: "Electronics", price: 400 }
]);
```

Beispiel für eine Abfrage

```
db.products.aggregate([
  { $sort: { price: -1 } }
]);
```

Ausgabe

```
[
  { _id: 1, name: 'Laptop', category: 'Electronics', price: 1200 },
  { _id: 5, name: 'Monitor', category: 'Electronics', price: 400 },
  { _id: 3, name: 'Desk', category: 'Furniture', price: 350 },
  { _id: 4, name: 'Chair', category: 'Furniture', price: 150 },
  { _id: 2, name: 'Mouse', category: 'Electronics', price: 25 }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung der `$sort` Aggregationsphase anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');
```

```
async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('products');

  const result = await collection.aggregate([
    { $sort: { price: -1 } }
  ]).toArray();

  console.log(result);
  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['products']

    result = list(collection.aggregate([
        { '$sort': { 'price': -1 } }
    ]))

    print(result)
    client.close()

example()
```

$split

Der `$split` Aggregationsoperator in Amazon DocumentDB wird verwendet, um eine Zeichenfolge auf der Grundlage eines angegebenen Trennzeichens in ein Array von Teilzeichenfolgen aufzuteilen.

Dies kann nützlich sein, um komplexe Zeichenkettenfelder zu analysieren und einzelne Komponenten für die weitere Verarbeitung zu extrahieren.

Parameter

- `string`: Die Zeichenfolge, die aufgeteilt werden soll.
- `delimiter`: Das Zeichen oder die Zeichenfolge, das zum Teilen der Eingabezeichenfolge verwendet wurde.

Beispiel (MongoDB Shell)

In diesem Beispiel trennen wir `$split` die Komponenten eines Feldes „Desk“ in ein Array, um die Verarbeitung der Daten zu vereinfachen.

Erstellen Sie Beispieldokumente

```
db.people.insertMany([
  { "_id": 1, "Desk": "Düsseldorf-BVV-021" },
  { "_id": 2, "Desk": "Munich-HGG-32a" },
  { "_id": 3, "Desk": "Cologne-ayu-892.50" },
  { "_id": 4, "Desk": "Dortmund-Hop-78" }
]);
```

Beispiel für eine Abfrage

```
db.people.aggregate([
  { $project: { parts: { $split: ["$Desk", "-"] } } }
]);
```

Ausgabe

```
{ "_id" : 1, "parts" : [ "Düsseldorf", "BVV", "021" ] }
{ "_id" : 2, "parts" : [ "Munich", "HGG", "32a" ] }
{ "_id" : 3, "parts" : [ "Cologne", "ayu", "892.50" ] }
{ "_id" : 4, "parts" : [ "Dortmund", "Hop", "78" ] }
```

Die Ausgabe von `$split` erstellt ein Array, das in der Anwendung verwendet werden kann, um die Informationen für die Mitarbeiter anzuzeigen.

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$split` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const result = await db.collection('people').aggregate([
    { $project: { parts: { $split: ['$Desk', '-'] } } }
  ]).toArray();
  console.log(result);
  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client.test
    result = list(db.people.aggregate([
        { '$project': { 'parts': { '$split': ['$Desk', '-'] } } }
    ]))
    print(result)
    client.close()

example()
```

$sqrt

Neu ab Version 4.0.

Der `$sqrt` Operator in Amazon DocumentDB wird verwendet, um die Quadratwurzel einer Zahl zu berechnen.

Parameter

- `expression`: Das Argument kann ein beliebiger gültiger Ausdruck sein, solange es zu einer nicht negativen Zahl aufgelöst wird.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt die Verwendung des `$sqrt` Operators zur Berechnung der Quadratwurzel einer Zahl.

Erstellen Sie Beispieldokumente

```
db.numbers.insertMany([
  { "_id": 1, "number": 16 },
  { "_id": 2, "number": 36 },
  { "_id": 3, "number": 64 }
]);
```

Beispiel für eine Abfrage

```
db.numbers.aggregate([
  { $project: {
    "_id": 1,
    "square_root": { $sqrt: "$number" }
  }}
]);
```

Ausgabe

```
[
  { _id: 1, square_root: 4 },
  { _id: 2, square_root: 6 },
  { _id: 3, square_root: 8 }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$sqrt` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');

  try {
      await client.connect();

      const db = client.db('test');
      const collection = db.collection('numbers');

      const pipeline = [
        {
          $project: {
            _id: 1,
            square_root: { $sqrt: '$number' }
          }
        }
      ];

      const results = await collection.aggregate(pipeline).toArray();

      console.dir(results, { depth: null });

    } finally {
      await client.close();
    }
}

example().catch(console.error);
```

Python

```
from pymongo import MongoClient
```

```
def example():

  client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')

  try:
      db = client.test
      collection = db.numbers

      pipeline = [
          {
              "$project": {
                  "_id": 1,
                  "square_root": {
                    "$sqrt": "$number"
                  }
              }
          }
      ]

      results = collection.aggregate(pipeline)

      for doc in results:
          print(doc)

  except Exception as e:
      print(f"An error occurred: {e}")

  finally:
      client.close()

example()
```

$str LenBytes

Der `$strLenBytes` Operator in Amazon DocumentDB wird verwendet, um die Länge einer Zeichenfolge in Byte zu bestimmen. Dies ist nützlich, wenn Sie die Speichergröße eines Zeichenkettenfeldes verstehen müssen, insbesondere wenn Sie es mit Unicode-Zeichen zu tun haben, die mehr als ein Byte pro Zeichen verwenden können.

Parameter

- `expression`: Der Zeichenkettenausdruck, dessen Länge berechnet werden soll.

Beispiel (MongoDB Shell)

Dieses Beispiel zeigt, wie der `$strLenBytes` Operator verwendet wird, um die Länge von Zeichenkettenfeldern in Byte zu berechnen.

Erstellen Sie Beispieldokumente

```
db.people.insertMany([
  { "_id": 1, "Desk": "Düsseldorf-BVV-021" },
  { "_id": 2, "Desk": "Munich-HGG-32a" },
  { "_id": 3, "Desk": "Cologne-ayu-892.50" },
  { "_id": 4, "Desk": "Dortmund-Hop-78" }
]);
```

Beispiel für eine Abfrage

```
db.people.aggregate([
  {
    $project: {
      "Desk": 1,
      "length": { $strLenBytes: "$Desk" }
    }
  }
])
```

Ausgabe

```
{ "_id" : 1, "Desk" : "Düsseldorf-BVV-021", "length" : 19 }
{ "_id" : 2, "Desk" : "Munich-HGG-32a", "length" : 14 }
{ "_id" : 3, "Desk" : "Cologne-ayu-892.50", "length" : 18 }
{ "_id" : 4, "Desk" : "Dortmund-Hop-78", "length" : 15 }
```

Beachten Sie, dass die Länge der Zeichenfolge „Düsseldorf-BVV-021“ 19 Byte beträgt, was sich von der Anzahl der Codepunkte (18) unterscheidet, da das Unicode-Zeichen „Ü“ 2 Byte belegt.

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$strLenBytes` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('people');

  const result = await collection.aggregate([
    {
      $project: {
        "Desk": 1,
        "length": { $strLenBytes: "$Desk" }
      }
    }
  ]).toArray();

  console.log(result);
  client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client.test
    collection = db.people

    result = list(collection.aggregate([
```

```
        {
            '$project': {
                "Desk": 1,
                "length": { "$strLenBytes": "$Desk" }
            }
        }
    ]))

    print(result)
    client.close()

example()
```

$strLenCP

Der `$strLenCP` Operator in Amazon DocumentDB wird verwendet, um die Länge eines Zeichenkettenausdrucks in Codepunkten (Unicode-Zeichen) zu bestimmen. Dies ist nützlich, wenn Sie die Anzahl der Zeichen in einer Zeichenfolge und nicht die Anzahl der Byte kennen müssen.

Parameter

- `expression`: Der Zeichenkettenausdruck, für den die Länge in Codepunkten zurückgegeben werden soll.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt die Verwendung des `$strLenCP` Operators zur Bestimmung der Länge von Zeichenketten mit Unicode-Zeichen.

Erstellen Sie Beispieldokumente

```
db.people.insertMany([
  { "_id": 1, "Desk": "Düsseldorf-BVV-021" },
  { "_id": 2, "Desk": "Munich-HGG-32a" },
  { "_id": 3, "Desk": "Cologne-ayu-892.50" },
  { "_id": 4, "Desk": "Dortmund-Hop-78" }
])
```

Beispiel für eine Abfrage

```
db.people.aggregate([
  {
    $project: {
      "Desk": 1,
      "length": { $strLenCP: "$Desk" }
    }
  }
])
```

Ausgabe

```
{ "_id" : 1, "Desk" : "Düsseldorf-BVV-021", "length" : 18 }
{ "_id" : 2, "Desk" : "Munich-HGG-32a", "length" : 14 }
{ "_id" : 3, "Desk" : "Cologne-ayu-892.50", "length" : 18 }
{ "_id" : 4, "Desk" : "Dortmund-Hop-78", "length" : 15 }
```

Beachten Sie den Unterschied in der Längenmessung für die Zeichenfolge „Düsseldorf-BVV-021“, die ein Unicode-Zeichen (Ü) enthält. Der `$strLenCP` Operator zählt die Anzahl der Unicode-Zeichen korrekt, während der `$strLenBytes` Operator die Anzahl der Byte zählt.

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$strLenCP` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

Hier ist ein Beispiel für die Verwendung des `$strLenCP` Operators in einer Node.js Anwendung mit dem MongoDB-Treiber:

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('people');

  const result = await collection.aggregate([
    {
```

```
      $project: {
        "Desk": 1,
        "length": { $strLenCP: "$Desk" }
      }
    }
  ]).toArray();

  console.log(result);
  await client.close();
}

example();
```

Python

Hier ist ein Beispiel für die Verwendung des `$strLenCP` Operators in einer Python-Anwendung mit dem PyMongo Treiber:

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client.test
    collection = db.people

    result = list(collection.aggregate([
        {
            '$project': {
                "Desk": 1,
                "length": { "$strLenCP": "$Desk" }
            }
        }
    ]))

    print(result)
    client.close()

example()
```

$strcasecmp

Der `$strcasecmp` Operator in Amazon DocumentDB führt einen Vergleich zwischen zwei Zeichenketten durch, bei dem die Groß- und Kleinschreibung nicht beachtet wird. Er gibt einen Integer-Wert zurück, der den lexikografischen Vergleich der beiden Eingabezeichenfolgen angibt, wobei Unterschiede zwischen Groß- und Kleinschreibung ignoriert werden.

Parameter

- `string1`: Die erste Zeichenfolge, die verglichen werden soll.
- `string2`: Die zweite zu vergleichende Zeichenfolge.

Beispiel (MongoDB Shell)

Dieses Beispiel zeigt, wie der `$strcasecmp` Operator verwendet wird, um Zeichenketten mit Schreibtischstandorten in einer `people` Sammlung zu vergleichen, wobei Unterschiede zwischen Groß- und Kleinschreibung ignoriert werden.

Erstellen Sie Beispieldokumente

```
db.people.insertMany([
  { "_id": 1, "Desk": "mke233-wi" },
  { "_id": 2, "Desk": "MKE233-WI" },
  { "_id": 3, "Desk": "mke233-wi" }
]);
```

Beispiel für eine Abfrage

```
db.people.aggregate([
  {
    $project: {
      item: 1,
      compare: { $strcasecmp: ["$Desk", "mke233-wi"] }
    }
  }
]);
```

Ausgabe

```
{ "_id" : 1, "compare" : 0 }
```

```
{ "_id" : 2, "compare" : 0 }
{ "_id" : 3, "compare" : 0 }
```

Die Ausgabe zeigt, dass der Vergleich zwischen dem "Desk" Feld und der Zeichenfolge `0` für alle drei Dokumente "mke233-wi" zurückgegeben wird, was bedeutet, dass die Zeichenketten identisch sind, wenn die Groß- und Kleinschreibung ignoriert wird.

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$strcasecmp` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('people');

  const result = await collection.aggregate([
    {
      $project: {
        item: 1,
        compare: { $strcasecmp: ["$Desk", "mke233-wi"] }
      }
    }
  ]).toArray();

  console.log(result);

  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient
```

```
def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client.test
    collection = db.people

    result = list(collection.aggregate([
        {
            '$project': {
                'item': 1,
                'compare': { '$strcasecmp': ['$Desk', 'mke233-wi'] }
            }
        }
    ]))

    print(result)

    client.close()

example()
```

$substr

Der `$substr` Operator in Amazon DocumentDB wird verwendet, um eine Teilzeichenfolge aus einer bestimmten Zeichenfolge zu extrahieren. Dies ist besonders nützlich, wenn Sie Teilzeichenfolgen definieren müssen, die auf einem Zeichenbereich und nicht auf einem Bytebereich basieren. Dies ist besonders wichtig, wenn es sich um Unicode-Zeichenketten handelt, bei denen die Anzahl der zur Darstellung eines Zeichens verwendeten Byte variieren kann.

Parameter

- `string`: Die Eingabezeichenfolge, aus der die Teilzeichenfolge extrahiert werden soll.
- `start`: Die Startposition (auf Null basierend) der Teilzeichenfolge, die extrahiert werden soll. Kann ein nicht negativer Integer-Ausdruck sein.
- `length`: Die Anzahl der Zeichen in der extrahierten Teilzeichenfolge. Kann ein nicht negativer Integer-Ausdruck sein.

Beispiel (MongoDB Shell)

In diesem Beispiel demonstrieren wir die Verwendung von, `$substr` um die Abkürzung des Bundesstaates aus dem Schreibtischstandort eines Mitarbeiters zu extrahieren.

Erstellen Sie Beispieldokumente

```
db.people.insertMany([
  { "_id": 1, "Desk": "Düsseldorf-NRW-021" },
  { "_id": 2, "Desk": "Bremerhaven-HBB-32a" },
  { "_id": 3, "Desk": "Norderstedt-SHH-892.50" },
  { "_id": 4, "Desk": "Brandenburg-BBB-78" }
]);
```

Beispiel für eine Abfrage

```
db.people.aggregate([
  {
    $project: {
      "state": { $substr: ["$Desk", 12, 3] }
    }
  }
])
```

Ausgabe

```
{ "_id": 1, "state": "NRW" },
{ "_id": 2, "state": "HBB" },
{ "_id": 3, "state": "SHH" },
{ "_id": 4, "state": "BBB" }
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$substr` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require("mongodb");

async function example() {
```

```
  const client = await MongoClient.connect("mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false");
  const db = client.db("test");
  const collection = db.collection("people");

  const result = await collection.aggregate([
    {
      $project: {
        "state": { $substrCP: ["$Desk", 12, 3] }
      }
    }
  ]).toArray();

  console.log(result);
  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient("mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false")
    db = client["test"]
    collection = db["people"]

    result = list(collection.aggregate([
        {
            "$project": {
                "state": { "$substrCP": ["$Desk", 12, 3] }
            }
        }
    ]))

    print(result)
    client.close()

example()
```

$substrBytes

Der `$substrBytes` Operator in Amazon DocumentDB wird verwendet, um eine Teilzeichenfolge aus einer Zeichenfolge zu extrahieren, die auf einem bestimmten Bytebereich basiert. Dieser Operator ist nützlich, wenn Sie eine Teilzeichenfolge aus einer Zeichenfolge extrahieren müssen und die Anzahl der Byte, die für die Darstellung der einzelnen Zeichen in der Zeichenfolge erforderlich sind, wichtig ist.

Unlike`$substrCP`, der auf der Anzahl der Unicode-Codepunkte basiert, `$substrBytes` arbeitet mit der Anzahl der Byte, die zur Darstellung der Zeichen in der Zeichenfolge erforderlich sind. Dies kann besonders nützlich sein, wenn Sie mit Zeichenketten arbeiten, die Nicht-ASCII-Zeichen enthalten, da für die Darstellung dieser Zeichen möglicherweise mehr als ein Byte erforderlich ist.

*Hinweis: * `$substr` ist seit Version 3.4 veraltet. `$substr`ist jetzt ein Alias für. `$substrBytes`

Parameter

- `string`: Die Eingabezeichenfolge, aus der die Teilzeichenfolge extrahiert wird.
- `startByte`: Die auf Null basierende Start-Byte-Position der zu extrahierenden Teilzeichenfolge. Ein negativer Wert kann verwendet werden, um eine Position am Ende der Zeichenfolge anzugeben.
- `length`: Die Anzahl der Bytes in der Teilzeichenfolge, die extrahiert werden sollen.

Beispiel (MongoDB Shell)

In diesem Beispiel verwenden wir, `$substrBytes` um eine Teilzeichenfolge aus einer Zeichenfolge zu extrahieren, die Nicht-ASCII-Zeichen enthält.

Erstellen Sie Beispieldokumente

```
db.people.insertMany([
  { "_id": 1, "Desk": "Düsseldorf-NRW-021" },
  { "_id": 2, "Desk": "Bremerhaven-HBB-32a" },
  { "_id": 3, "Desk": "Norderstedt-SHH-892.50" },
  { "_id": 4, "Desk": "Brandenburg-BBB-78" }
]);
```

Beispiel für eine Abfrage

```
db.people.aggregate([
  {
    $project: {
      "state": { $substrBytes: [ "$Desk", 12, 3] }
    }
  }
])
```

Ausgabe

```
{ "_id": 1, "state": "NRW" },
{ "_id": 2, "state": "HBB" },
{ "_id": 3, "state": "SHH" },
{ "_id": 4, "state": "BBB" }
```

In diesem Beispiel verwenden wir, `$substrBytes` um eine 3-Byte-Teilzeichenfolge zu extrahieren, beginnend mit dem 12. Byte des Feldes`Desk`. Auf diese Weise können wir die zweistellige Abkürzung für den Bundesstaat extrahieren, auch wenn die Zeichenfolge Nicht-ASCII-Zeichen enthalten kann.

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$substrBytes` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const people = db.collection('people');

  const result = await people.aggregate([
    {
      $project: {
        "state": { $substrBytes: ["$Desk", 12, 3] }
      }
    }
  ]).toArray();
```

```
  console.log(result);
  client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client.test
    people = db.people

    result = list(people.aggregate([
        {
            '$project': {
                "state": { '$substrBytes': ["$Desk", 12, 3] }
            }
        }
    ]))

    print(result)
    client.close()

example()
```

$substrCP

Der `$substrCP` Operator in Amazon DocumentDB wird verwendet, um eine Teilzeichenfolge aus einer Zeichenfolge zu extrahieren, wobei die Teilzeichenfolge als Bereich von UTF-8 Codepunkten (CP) angegeben ist. Dieser Operator ist besonders nützlich, wenn Sie mit Unicode-Zeichenketten arbeiten, da Sie damit Teilzeichenfolgen extrahieren können, ohne sich Gedanken über die zugrunde liegende Byte-Darstellung der Zeichen machen zu müssen.

Im Gegensatz zum `$substrBytes` Operator, der mit Bytepositionen arbeitet, arbeitet der `$substrCP` Operator mit Codepunktpositionen. Dies erleichtert die Arbeit mit Zeichenfolgen, die

Nicht-ASCII-Zeichen enthalten, da die Anzahl der Codepunkte möglicherweise nicht der Anzahl der Byte oder Zeichen entspricht.

Parameter

- `string`: Die Eingabezeichenfolge, aus der die Teilzeichenfolge extrahiert werden soll.
- `start`: Die Startposition des Codepunkts (auf Null basierend), aus der die Teilzeichenfolge extrahiert werden soll.
- `length`: Die Anzahl der zu extrahierenden Codepunkte.

Beispiel (MongoDB Shell)

In diesem Beispiel verwenden wir den `$substrCP` Operator, um die Abkürzung für das Bundesland aus einer Zeichenfolge zu extrahieren, die den Schreibtischstandort des Mitarbeiters enthält.

Erstellen Sie Beispieldokumente

```
db.people.insert([
  { "_id": 1, "first_name": "Jane", "last_name": "Doe", "Desk": "12 Main St,
 Minneapolis, MN 55401" },
  { "_id": 2, "first_name": "John", "last_name": "Doe", "Desk": "456 Oak Rd, New
 Orleans, LA 70032" },
  { "_id": 3, "first_name": "Steve", "last_name": "Smith", "Desk": "789 Elm Ln,
 Bakersfield, CA 93263" }
]);
```

Beispiel für eine Abfrage

```
db.people.aggregate([
  {
    $project: {
      "state": { $substrCP: ["$Desk", 25, 2] }
    }
  }
]);
```

Ausgabe

```
{ "_id" : 1, "state" : "MN" }
{ "_id" : 2, "state" : "LA" }
```

```
{ "_id" : 3, "state" : "CA" }
```

In diesem Beispiel wissen wir, dass die Abkürzung für das Bundesland am 25. Codepunkt im `Desk` Feld beginnt und 2 Codepunkte lang ist. Mithilfe des `$substrCP` Operators können wir die Abkürzung des Bundesstaates extrahieren, ohne uns um die zugrunde liegende Byte-Darstellung der Zeichenfolge kümmern zu müssen.

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$substrCP` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function findStates() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const result = await db.collection('people').aggregate([
    {
      $project: {
        "state": { $substrCP: ["$Desk", 25, 2] }
      }
    }
  ]).toArray();
  console.log(result);
  client.close();
}

findStates();
```

Python

```
from pymongo import MongoClient

def find_states():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
```

```
    db = client.test
    result = list(db.people.aggregate([
        {
            '$project': {
                'state': { '$substrCP': ['$Desk', 25, 2] }
            }
        }
    ]))
    print(result)
    client.close()

find_states()
```

Sowohl im Beispiel als auch im Node.js Python-Beispiel verwenden wir den `$substrCP` Operator, um die Abkürzung des Bundesstaates aus dem `Desk` Feld zu extrahieren, ähnlich dem MongoDB-Shell-Beispiel.

$subtract

Der `$subtract` Operator in Amazon DocumentDB wird verwendet, um Werte zu subtrahieren. Er kann verwendet werden, um Daten, Zahlen oder eine Kombination aus beidem zu subtrahieren. Dieser Operator ist nützlich, um die Differenz zwischen zwei Daten zu berechnen oder einen Wert von einer Zahl zu subtrahieren.

Parameter

- `expression1`: Der erste Wert, der subtrahiert werden soll.
- `expression2`: Der zweite Wert, von dem subtrahiert werden soll. `<expression1>`

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$subtract` Operator verwendet wird, um die Differenz zwischen zwei Daten zu berechnen.

Erstellen Sie ein Beispieldokument

```
db.dates.insert([
  {
  "_id": 1,
  "startDate": ISODate("2023-01-01T00:00:00Z"),
```

```
  "endDate": ISODate("2023-01-05T12:00:00Z")
  }
]);
```

Beispiel für eine Abfrage

```
db.dates.aggregate([
  {
    $project: {
      _id: 1,
      durationDays: {
        $divide: [
          { $subtract: ["$endDate", "$startDate"] },
          1000 * 60 * 60 * 24  // milliseconds in a day
        ]
      }
    }
  }
]);
```

Ausgabe

```
[ { _id: 1, durationDays: 4.5 } ]
```

In diesem Beispiel wird der `$subtract` Operator verwendet, um die Differenz zwischen `$endDate` und `$startDate` in Tagen zu berechnen.

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$subtract` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
```

```
  try {
    await client.connect();
    const db = client.db('test');
    const collection = db.collection('dates');

    const pipeline = [
      {
        $project: {
          _id: 1,
          durationDays: {
            $divide: [
              { $subtract: ["$endDate", "$startDate"] },
              1000 * 60 * 60 * 24  // Convert milliseconds to days
            ]
          }
        }
      }
    ];

    const results = await collection.aggregate(pipeline).toArray();

    console.dir(results, { depth: null });

  } finally {
    await client.close();
  }
}

example().catch(console.error);
```

Python

```
from datetime import datetime, timedelta
from pymongo import MongoClient

def example():

    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')

    try:
        db = client.test
```

```
        collection = db.dates

        pipeline = [
            {
                "$project": {
                    "_id": 1,
                    "durationDays": {
                        "$divide": [
                            { "$subtract": ["$endDate", "$startDate"] },
                            1000 * 60 * 60 * 24  # Convert milliseconds to days
                        ]
                    }
                }
            }
        ]

        results = collection.aggregate(pipeline)

        for doc in results:
            print(doc)

    except Exception as e:
        print(f"An error occurred: {e}")

    finally:
        client.close()

example()
```

$sum

Der `$sum` Operator in Amazon DocumentDB gibt die Summe des angegebenen Ausdrucks für jedes Dokument in einer Gruppe zurück. Es handelt sich um einen Gruppenakkumulatoroperator, der typischerweise in der $group-Phase einer Aggregationspipeline verwendet wird, um Summenberechnungen durchzuführen.

Parameter

- `expression`: Der numerische Ausdruck, der summiert werden soll. Dies kann ein Feldpfad, ein Ausdruck oder eine Konstante sein.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der $sum Operator verwendet wird, um den Gesamtumsatz für jedes Produkt zu berechnen.

Erstellen Sie Beispieldokumente

```
db.sales.insertMany([
  { product: "abc", price: 10, quantity: 2 },
  { product: "abc", price: 10, quantity: 3 },
  { product: "xyz", price: 20, quantity: 1 },
  { product: "xyz", price: 20, quantity: 5 }
]);
```

Beispiel für eine Abfrage

```
db.sales.aggregate([
  { $group: {
      _id: "$product",
      totalSales: { $sum: { $multiply: [ "$price", "$quantity" ] } }
    }}
]);
```

Ausgabe

```
[
  { "_id": "abc", "totalSales": 50 },
  { "_id": "xyz", "totalSales": 120 }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des $sum Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
```

```
  const uri = 'mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false';
  const client = new MongoClient(uri);

  try {
    await client.connect();

    const db = client.db('test');
    const collection = db.collection('sales');

    const result = await collection.aggregate([
      { $group: {
          _id: "$product",
          totalSales: { $sum: { $multiply: [ "$price", "$quantity" ] } }
        }}
    ]).toArray();

    console.log(result);

  } catch (error) {
    console.error('Error:', error);
  } finally {
    await client.close();
  }
}

example();
```

Python

```
from pymongo import MongoClient
from pprint import pprint

def example():
    client = None
    try:
        client = MongoClient('mongodb://<username>:<password>@<cluster-
endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')

        db = client.test
        collection = db.sales
```

```
        result = list(collection.aggregate([
            { '$group': {
                '_id': '$product',
                'totalSales': { '$sum': { '$multiply': [ '$price', '$quantity' ] } } }
            }}
        ]))

        pprint(result)

    except Exception as e:
        print(f"An error occurred: {e}")

    finally:
        if client:
            client.close()

example()
```

$switch

Neu ab Version 4.0.

Wird von Elastic Cluster nicht unterstützt.

Der `$switch` Operator ist ein Operator für bedingte Ausdrücke in Amazon DocumentDB, der es Ihnen ermöglicht, eine Liste von Groß- und Kleinschreibung auszuwerten und den Wert des ersten Falls zurückzugeben, der als wahr ausgewertet wird, oder einen Standardwert, wenn kein Groß-/Kleinschreibung wahr ist.

Parameter

- `branches`: Ein Array von Dokumenten, von denen jedes ein Fallfeld hat, das den auszuwertenden booleschen Ausdruck enthält, und ein Then-Feld, das den Wert enthält, der zurückgegeben werden soll, wenn der Groß-/Kleinschreibung wahr ist.
- `default`: (optional) Der Wert, der zurückgegeben werden soll, wenn keiner der Groß- und Kleinschreibung zutrifft.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$switch` Operator verwendet wird, um die Versandkosten für eine Bestellung anhand der Gesamtsumme der Bestellung zu ermitteln.

Erstellen Sie Beispieldokumente

```
db.orders.insertMany([
  { _id: 1, total: 50 },
  { _id: 2, total: 150 },
  { _id: 3, total: 250 }
]);
```

Beispiel für eine Abfrage

```
db.orders.aggregate([
  {
    $project: {
      _id: 1,
      total: 1,
      shippingCost: {
        $switch: {
          branches: [
            { case: { $lte: ["$total", 100] }, then: 5 },
            { case: { $lte: ["$total", 200] }, then: 10 },
            { case: { $gt: ["$total", 200] }, then: 15 }
          ],
          default: 0
        }
      }
    }
  }
])
```

Ausgabe

```
[
  {
    "_id": 1,
    "total": 50,
    "shippingCost": 5
  },
  {
```

```
    "_id": 2,
    "total": 150,
    "shippingCost": 10
  },
  {
    "_id": 3,
    "total": 250,
    "shippingCost": 15
  }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$switch` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function main() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('orders');

  const result = await collection.aggregate([
    {
      $project: {
        _id: 1,
        total: 1,
        shippingCost: {
          $switch: {
            branches: [
              { case: { $lte: ['$total', 100] }, then: 5 },
              { case: { $lte: ['$total', 200] }, then: 10 },
              { case: { $gt: ['$total', 200] }, then: 15 }
            ],
            default: 0
          }
        }
      }
```

```
    }
  ]).toArray();

  console.log(result);
  await client.close();
}

main();
```

Python

```
from pymongo import MongoClient

def main():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client.test
    collection = db.orders

    result = list(collection.aggregate([
        {
            '$project': {
                '_id': 1,
                'total': 1,
                'shippingCost': {
                    '$switch': {
                        'branches': [
                            { 'case': { '$lte': ['$total', 100] }, 'then': 5 },
                            { 'case': { '$lte': ['$total', 200] }, 'then': 10 },
                            { 'case': { '$gt': ['$total', 200] }, 'then': 15 }
                        ],
                        'default': 0
                    }
                }
            }
        }
    ]))

    print(result)
    client.close()

if __name__ == '__main__':
```

```
    main()
```

$ zu Bool

Der `$toBool` Operator in Amazon DocumentDB konvertiert einen Ausdruck in einen booleschen Wert.

Parameter

- `expression`: Der Ausdruck, der in einen booleschen Wert umgewandelt werden soll.

Hinweis: Jede Zeichenfolge wird konvertiert in. `true`

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$toBool` Operator verwendet wird, um Gerätestatuswerte aus verschiedenen Datentypen zu normalisieren.

Erstellen Sie Beispieldokumente

```
db.deviceStates.insertMany([
  { _id: 1, deviceId: "sensor-001", status: true },
  { _id: 2, deviceId: "camera-002", status: 1 },
  { _id: 3, deviceId: "thermostat-003", status: "active" },
  { _id: 4, deviceId: "doorlock-004", status: 0 }
]);
```

Beispiel für eine Abfrage

```
db.deviceStates.aggregate([
  {
    $project: {
      _id: 1,
      deviceId: 1,
      isActive: { $toBool: "$status" }
    }
  }
]);
```

Ausgabe

```
[
  { "_id": 1, "deviceId": "sensor-001", "isActive": true },
  { "_id": 2, "deviceId": "camera-002", "isActive": true },
  { "_id": 3, "deviceId": "thermostat-003", "isActive": true },
  { "_id": 4, "deviceId": "doorlock-004", "isActive": false }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$toBool` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function main() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('deviceStates');

  const result = await collection.aggregate([
    {
      $project: {
        _id: 1,
        deviceId: 1,
        isActive: { $toBool: '$status' }
      }
    }
  ]).toArray();

  console.log(result);

  await client.close();
}

main();
```

Python

```
from pymongo import MongoClient

def main():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['deviceStates']

    result = list(collection.aggregate([
        {
            '$project': {
                '_id': 1,
                'deviceId': 1,
                'isActive': { '$toBool': '$status' }
            }
        }
    ]))

    print(result)

    client.close()

if __name__ == '__main__':
    main()
```

$ bis Datum

Neu ab Version 4.0

Der `$toDate` Aggregationsoperator in Amazon DocumentDB wird verwendet, um eine Datums- oder Datums- und Uhrzeitzeichenfolge in einen BSON-Datumstyp zu konvertieren. Dies ist die umgekehrte Operation des Operators. `$dateToString`

Parameter

- `dateString`: Eine Zeichenkettendarstellung eines Datums oder eines Datums und einer Uhrzeit, das in einen BSON-Datumstyp konvertiert werden soll.

- `format`: (optional) Eine Zeichenfolge, die das Format von angibt. `dateString` Falls nicht angegeben, versucht der Operator, das `dateString` in verschiedenen standardmäßigen Datums- und Uhrzeitformaten zu analysieren.
- `timezone`: (optional) Eine Zeichenfolge, die die Zeitzone darstellt, die für die Konvertierung verwendet werden soll. Falls nicht angegeben, wird die lokale Zeitzone verwendet.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$toDate` Operator verwendet wird, um eine Datumszeichenfolge in einen BSON-Datumstyp zu konvertieren.

Erstellen Sie Beispieldokumente

```
db.events.insertMany([
  { _id: 1, eventName: "Mission Start", eventTime: "2023-04-15T10:30:00Z" },
  { _id: 2, eventName: "Checkpoint Reached", eventTime: "2023-04-15T11:15:00Z" },
  { _id: 3, eventName: "Mission End", eventTime: "2023-04-15T12:00:00Z" }
]);
```

Beispiel für eine Abfrage

```
db.events.aggregate([
  {
    $project: {
      eventName: 1,
      eventTimeDate: { $toDate: "$eventTime" }
    }
  }
]);
```

Ausgabe

```
[
  {
    "_id": 1,
    "eventName": "Mission Start",
    "eventTimeDate": ISODate("2023-04-15T10:30:00Z")
  },
  {
    "_id": 2,
    "eventName": "Checkpoint Reached",
```

```
    "eventTimeDate": ISODate("2023-04-15T11:15:00Z")
  },
  {
    "_id": 3,
    "eventName": "Mission End",
    "eventTimeDate": ISODate("2023-04-15T12:00:00Z")
  }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$toDate` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('events');

  const result = await collection.aggregate([
    {
      $project: {
        eventName: 1,
        eventTimeDate: { $toDate: '$eventTime' }
      }
    }
  ]).toArray();

  console.log(result);
  client.close();
}

example();
```

Python

```
from pymongo import MongoClient
```

```
def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['events']

    result = list(collection.aggregate([
        {
            '$project': {
                'eventName': 1,
                'eventTimeDate': { '$toDate': '$eventTime' }
            }
        }
    ]))

    print(result)
    client.close()

example()
```

$ zu Dezimal

Neu ab Version 4.0

Der `$toDecimal` Operator in Amazon DocumentDB wird verwendet, um einen Wert in den Decimal128-Datentyp zu konvertieren. Dies ist nützlich, wenn Sie präzise Dezimalarithmetik durchführen oder große Dezimalwerte verarbeiten müssen, die mit dem Double-Datentyp nicht genau dargestellt werden können.

Parameter

- `expression`: Der Ausdruck, der in den Decimal128-Datentyp konvertiert werden soll.

Beispiel (MongoDB Shell)

Dieses Beispiel zeigt, wie der `$toDecimal` Operator verwendet wird, um einen Zeichenkettenwert in einen Decimal128-Datentyp zu konvertieren.

Erstellen Sie Beispieldokumente

```
db.numbers.insertOne({ _id: 1, value: "3.14" });
db.numbers.insertOne({ _id: 2, value: "2.71" });
```

Beispiel für eine Abfrage

```
db.numbers.aggregate([
  { $project: {
    _id: 1,
    decimalValue: { $toDecimal: "$value" }
  }}
])
```

Ausgabe

```
[
  { "_id" : 1, "decimalValue" : Decimal128("3.14") },
  { "_id" : 2, "decimalValue" : Decimal128("2.71") }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$toDecimal` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('numbers');

  const result = await collection.aggregate([
    { $project: {
      _id: 1,
      decimalValue: { $toDecimal: "$value" }
    }}
  ]).toArray();
```

```
  console.log(result);
  client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client.test
    collection = db.numbers

    result = list(collection.aggregate([
        {'$project': {
            '_id': 1,
            'decimalValue': {'$toDecimal': '$value'}
        }}
    ]))

    print(result)
    client.close()

example()
```

$ bis verdoppeln

Neu ab Version 4.0

Der `$toDouble` Operator in Amazon DocumentDB wird verwendet, um einen Wert in eine 64-Bit-Gleitkommazahl mit doppelter Genauigkeit umzuwandeln. Dies kann nützlich sein, wenn Sie arithmetische Operationen mit Werten durchführen müssen, die ursprünglich nicht in einem numerischen Format vorliegen.

Parameter

<expression>: Der Ausdruck, der in einen doppelten Wert umgewandelt werden soll. Dies kann ein beliebiger gültiger Ausdruck sein, der in einen numerischen Wert, eine Zeichenfolge oder einen booleschen Wert aufgelöst wird.

Beispiel (MongoDB Shell)

Dieses Beispiel zeigt, wie der `$toDouble` Operator verwendet wird, um einen Zeichenkettenwert in einen numerischen Wert umzuwandeln, um eine mathematische Berechnung durchzuführen.

Erstellen Sie Beispieldokumente

```
db.numbers.insertMany([
  { _id: 1, value: "10.5" },
  { _id: 2, value: "20.25" },
  { _id: 3, value: "7" }
])
```

Beispiel für eine Abfrage

```
db.numbers.aggregate([
  {
    $project: {
      _id: 1,
      value: 1,
      double_value: { $toDouble: "$value" },
      double_plus_five: { $add: [{ $toDouble: "$value" }, 5] }
    }
  }
])
```

Ausgabe

```
[
  { "_id" : 1, "value" : "10.5", "double_value" : 10.5, "double_plus_five" : 15.5 },
  { "_id" : 2, "value" : "20.25", "double_value" : 20.25, "double_plus_five" : 25.25 },
  { "_id" : 3, "value" : "7", "double_value" : 7.0, "double_plus_five" : 12.0 }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$toDouble` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('numbers');

  const result = await collection.aggregate([
    {
      $project: {
        _id: 1,
        value: 1,
        double_value: { $toDouble: "$value" },
        double_plus_five: { $add: [{ $toDouble: "$value" }, 5] }
      }
    }
  ]).toArray();

  console.log(result);
  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['numbers']

    result = list(collection.aggregate([
        {
            '$project': {
                '_id': 1,
```

```
                'value': 1,
                'double_value': { '$toDouble': '$value' },
                'double_plus_five': { '$add': [{ '$toDouble': '$value' }, 5] }
            }
        }
    ]))

    print(result)
    client.close()

example()
```

$ zu Int

Neu ab Version 4.0

Der `$toInt` Operator in Amazon DocumentDB wird verwendet, um einen Eingabewert in einen Integer-Datentyp zu konvertieren. Dieser Operator ist nützlich, wenn Sie sicherstellen müssen, dass ein Feld oder ein Ausdruck als Ganzzahl dargestellt wird, was für bestimmte Operationen oder Datenverarbeitungsaufgaben wichtig sein kann.

Parameter

- `expression`: Der Ausdruck, der in eine Ganzzahl umgewandelt werden soll.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$toInt` Operator verwendet wird, um einen Zeichenkettenwert in eine Ganzzahl umzuwandeln.

Erstellen Sie Beispieldokumente

```
db.numbers.insertMany([
  { "name": "one", "value": "1" },
  { "name": "hundred", "value": "100" }
]);
```

Beispiel für eine Abfrage

```
db.numbers.aggregate([
```

```
  { $project: {
    "_id": 0,
    "name": 1,
    "intValue": { $toInt: "$value" }
  }}
]);
```

Ausgabe

```
{ "name": "one", "intValue": 1 }
{ "name": "hundred", "intValue": 100 }
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$toInt` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('numbers');

  const result = await collection.aggregate([
    { $project: {
      "_id": 0,
      "name": 1,
      "intValue": { $toInt: "$value" }
    }}
  ]).toArray();

  console.log(result);
  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['numbers']

    result = list(collection.aggregate([
        { "$project": {
            "_id": 0,
            "name": 1,
            "intValue": { "$toInt": "$value" }
        }}
    ]))

    print(result)
    client.close()

example()
```

$ zu Long

Neu ab Version 4.0

Der `$toLong` Operator in Amazon DocumentDB wird verwendet, um einen Wert in einen 64-Bit-Datentyp vom Typ Integer (Long) zu konvertieren. Dies kann nützlich sein, wenn Sie arithmetische Operationen oder Vergleiche mit numerischen Werten durchführen müssen, die als Zeichenketten oder andere Datentypen gespeichert werden können.

Parameter

- `expression`: Der Ausdruck, der in eine 64-Bit-Ganzzahl konvertiert werden soll.

Beispiel (MongoDB Shell)

Dieses Beispiel zeigt, wie der `$toLong` Operator verwendet wird, um einen Zeichenkettenwert in eine 64-Bit-Ganzzahl zu konvertieren.

Erstellen Sie Beispieldokumente

```
db.numbers.insertMany([
  { _id: 1, value: "42" },
  { _id: 3, value: "92233720368547758O7" }
]);
```

Beispiel für eine Abfrage

```
db.numbers.aggregate([
  {
    $project: {
      _id: 1,
      longValue: { $toLong: "$value" }
    }
  }
])
```

Ausgabe

```
[
  { "_id" : 1, "longValue" : 42 },
  { "_id" : 3, "longValue" : 9223372036854775807 }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$toLong` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const numbers = db.collection('numbers');
```

```
  const result = await numbers.aggregate([
    {
      $project: {
        _id: 1,
        longValue: { $toLong: "$value" }
      }
    }
  ]).toArray();

  console.log(result);
  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client.test
    numbers = db.numbers

    result = list(numbers.aggregate([
        {
            '$project': {
                '_id': 1,
                'longValue': { '$toLong': '$value' }
            }
        }
    ]))

    print(result)
    client.close()

example()
```

$toLower

Der `$toLower` Operator in Amazon DocumentDB wird verwendet, um eine Zeichenfolge in Kleinbuchstaben umzuwandeln.

Parameter

- `expression`: Der Zeichenkettenausdruck, der in Kleinbuchstaben umgewandelt werden soll.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$toLower` Operator verwendet wird, um das `Desk` Feld in Kleinbuchstaben umzuwandeln.

Erstellen Sie Beispieldokumente

```
db.locations.insertMany([
  { "_id": 1, "Desk": "Düsseldorf-BVV-021" },
  { "_id": 2, "Desk": "Munich-HGG-32a" }
]);
```

Beispiel für eine Abfrage

```
db.locations.aggregate([
  { $project: { item: { $toLower: "$Desk" } } }
]);
```

Ausgabe

```
{ "_id" : 1, "item" : "düsseldorf-bvv-021" }
{ "_id" : 2, "item" : "munich-hgg-32a" }
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$toLower` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require("mongodb");
```

```
async function main() {
  const client = await MongoClient.connect("mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false");
  const db = client.db("test");
  const collection = db.collection("locations");

  const result = await collection.aggregate([
    { $project: { item: { $toLower: "$Desk" } } }
  ]).toArray();

  console.log(result);

  await client.close();
}

main();
```

Python

```
from pymongo import MongoClient

def main():
    client = MongoClient("mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false")
    db = client["test"]
    collection = db["locations"]

    result = list(collection.aggregate([
        { "$project": { "item": { "$toLower": "$Desk" } } }
    ]))

    print(result)

    client.close()

if __name__ == "__main__":
    main()
```

$ bis ObjectId

Neu ab Version 4.0

Der `$toObjectId` Operator in Amazon DocumentDB wird verwendet, um eine Zeichenkettendarstellung eines in einen tatsächlichen ObjectId Datentyp ObjectId zu konvertieren. Dies kann nützlich sein, wenn Sie mit Daten arbeiten, die als Zeichenkettendarstellungen von gespeichert wurden ObjectIds, da Sie damit Operationen ausführen können, für die der ObjectId Datentyp erforderlich ist.

Parameter

- `expression`: Ein Zeichenkettenausdruck, der einen gültigen Wert darstellt ObjectId.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$toObjectId` Operator verwendet wird, um eine Zeichenkettendarstellung von an in den ObjectId Datentyp ObjectId zu konvertieren.

Erstellen Sie Beispieldokumente

```
db.employees.insertMany([
  { _id: 1, empId:"64e5f8886218c620cf0e8f8a", name: "Carol Smith", employeeId:
 "c720a" },
  { _id: 2, empId:"64e5f94e6218c620cf0e8f8c", name: "Bill Taylor", employeeId:
 "c721a" }
]);
```

Beispiel für eine Abfrage

```
db.employees.aggregate([
  { $project: {
    "empIdAsObjectId": {$toObjectId: "$empId"}}
  }
]);
```

Ausgabe

```
[
```

```
  { _id: 1, empIdAsObjectId: ObjectId('64e5f8886218c620cf0e8f8a') },
  { _id: 2, empIdAsObjectId: ObjectId('64e5f94e6218c620cf0e8f8c') }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$toObjectId` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('employees');

  const result = await collection.aggregate([
    { $project: {
      "empIdAsObjectId": {$toObjectId: "$empId"}}
    }
  ]).toArray();

  console.log(result);
  client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['employees']
```

```
    result = list(collection.aggregate([
      { "$project": {
        "empIdAsObjectId": {"$toObjectId": "$empId"}}
      }
    ]))

    print(result)
    client.close()

example()
```

$ toString

Neu ab Version 4.0

Der `$toString` Operator in Amazon DocumentDB wird verwendet, um einen Wert eines beliebigen Typs (außer Null) in eine Zeichenkettendarstellung zu konvertieren. Dies kann nützlich sein, wenn Sie Zeichenkettenoperationen mit Werten durchführen müssen, die ursprünglich nicht im Zeichenkettenformat vorliegen.

Parameter

- `expression`: Der Ausdruck, der in eine Zeichenfolge konvertiert werden soll.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$toString` Operator verwendet wird, um numerische Werte in Zeichenketten umzuwandeln.

Erstellen Sie Beispieldokumente

```
db.numbers.insertMany([
  { "_id": 1, "value": 42 },
  { "_id": 2, "value": 3.14 }
]);
```

Beispiel für eine Abfrage

```
db.numbers.aggregate([
  { $project: {
```

```
    _id: 1,
    valueAsString: { $toString: "$value" }
  }}
]);
```

Ausgabe

```
{ "_id": 1, "valueAsString": "42" }
{ "_id": 2, "valueAsString": "3.14" }
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$toString` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('numbers');

  const result = await collection.aggregate([
    { $project: {
      _id: 1,
      valueAsString: { $toString: '$value' }
    }}
  ]).toArray();

  console.log(result);
  client.close();
}

example();
```

Python

```
from pymongo import MongoClient
```

```
def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['numbers']

    result = list(collection.aggregate([
        { '$project': {
            '_id': 1,
            'valueAsString': { '$toString': '$value' }
        }}
    ]))

    print(result)
    client.close()

example()
```

$toUpper

Der `$toUpper` Operator in Amazon DocumentDB wird verwendet, um eine Zeichenfolge in Großbuchstaben umzuwandeln.

Parameter

- `expression`: Der Zeichenkettenausdruck, der in Großbuchstaben umgewandelt werden soll.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt die Verwendung des `$toUpper` Operators, um das `Desk` Feld in Großbuchstaben umzuwandeln.

Erstellen Sie Beispieldokumente

```
db.locations.insertMany([
  { "_id": 1, "Desk": "düsseldorf-bvv-021" },
  { "_id": 2, "Desk": "munich-hgg-32a" }
]);
```

Beispiel für eine Abfrage

```
db.locations.aggregate([
  { $project: { item: { $toUpper: "$Desk" } } }
]);
```

Ausgabe

```
{ "_id" : 1, "item" : "DüSSELDORF-BVV-021" }
{ "_id" : 2, "item" : "MUNICH-HGG-32A" }
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$toUpper` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('locations');

  const result = await collection.aggregate([
    { $project: { item: { $toUpper: '$Desk' } } }
  ]).toArray();

  console.log(result);

  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient
```

```
def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['locations']

    result = list(collection.aggregate([
        { '$project': { 'item': { '$toUpper': '$Desk' } } }
    ]))

    print(result)

    client.close()

example()
```

$trim

Neu ab Version 4.0

Der `$trim` Operator in Amazon DocumentDB wird verwendet, um führende and/or abschließende Leerzeichen aus einer Zeichenfolge zu entfernen.

Parameter

- `input`: Der Zeichenkettenausdruck, der gekürzt werden soll.
- `chars`: (optional) Gibt die Zeichen an, die am Anfang und Ende der Eingabe gekürzt werden sollen. Die Standardeinstellung ist Leerzeichen.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$trim` Operator verwendet wird, um führende und nachfolgende Leerzeichen aus einer Zeichenfolge zu entfernen.

Erstellen Sie Beispieldokumente

```
db.people.insertMany([
  { "name": "   John Doe   " },
```

```
  { "name": "   Bob Johnson   " }
])
```

Beispiel für eine Abfrage

```
db.people.aggregate([
  { $project: {
    "name": { $trim: {input: "$name"}}
  }}
])
```

Ausgabe

```
[
  { "name": "John Doe" },
  { "name": "Bob Johnson" }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$trim` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('people');

  const result = await collection.aggregate([
    { $project: {
      "name": { $trim: {input: "$name" }}
    }}
  ]).toArray();

  console.log(result);
  client.close();
```

```
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['people']

    result = list(collection.aggregate([
        {"$project": {
            "name": {"$trim": {"input": "$name"}}
        }}
    ]))

    print(result)
    client.close()

example()
```

$type

Der `$type` Aggregationsoperator gibt den BSON-Datentyp eines angegebenen Felds zurück. Dies ist nützlich, um den Datentyp von Feldwerten bei Aggregationsvorgängen zu identifizieren.

Parameter

- `expression`: Das Feld oder der Ausdruck, dessen Typ zurückgegeben werden soll.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$type` Operator verwendet wird, um den Datentyp des Preisfeldes für jedes Produkt zu identifizieren.

Erstellen Sie Beispieldokumente

```
db.inventory.insertMany([
  { _id: 1, item: "Notebook", price: 15.99 },
  { _id: 2, item: "Pen", price: "2.50" },
  { _id: 3, item: "Eraser", price: 1 },
  { _id: 4, item: "Ruler", price: null }
]);
```

Beispiel für eine Abfrage

```
db.inventory.aggregate([
  {
    $project: {
      item: 1,
      price: 1,
      priceType: { $type: "$price" }
    }
  }
]);
```

Ausgabe

```
[
  { _id: 1, item: 'Notebook', price: 15.99, priceType: 'double' },
  { _id: 2, item: 'Pen', price: '2.50', priceType: 'string' },
  { _id: 3, item: 'Eraser', price: 1, priceType: 'int' },
  { _id: 4, item: 'Ruler', price: null, priceType: 'null' }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$type` Aggregationsoperators anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
```

```
  const collection = db.collection('inventory');

  const result = await collection.aggregate([
    {
      $project: {
        item: 1,
        price: 1,
        priceType: { $type: "$price" }
      }
    }
  ]).toArray();

  console.log(result);
  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['inventory']

    result = list(collection.aggregate([
        {
            '$project': {
                'item': 1,
                'price': 1,
                'priceType': { '$type': '$price' }
            }
        }
    ]))

    print(result)
    client.close()

example()
```

$unset

Neu ab Version 8.0

Wird von Elastic Cluster nicht unterstützt.

Die `$unset` Aggregationsphase in Amazon DocumentDB ermöglicht es Ihnen, Felder aus Dokumenten zu entfernen.

Parameter

- `expression`: Feldname oder Liste mit mehreren Feldnamen.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie das Feld mithilfe der `$unset` Aggregationsphase entfernt wird`price`.

Erstellen Sie Beispieldokumente

```
db.inventory.insertMany([
  { item: "pencil", quantity: 100, price: 0.24},
  { item: "pen", quantity: 204, price: 1.78 }
]);
```

Beispiel für eine Aggregation

```
db.inventory.aggregate([
  {
    $unset: "price"
  }
])
```

Ausgabe

```
[
  {
    _id: ObjectId('69248951d66dcae121d2950d'),
    item: 'pencil',
```

```
    quantity: 100
  },
  {
    _id: ObjectId('69248951d66dcae121d2950e'),
    item: 'pen',
    quantity: 204
  }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des $unset Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const inventory = db.collection('inventory');

  const result = await inventory.aggregate([
      {
        $unset: "price"
      }
  ]).toArray();

  console.log(result);
  client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
```

```
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    inventory = db['inventory']

    result = list(inventory.aggregate([
      {
        "$unset": "price"
      }
    ]))

    print(result)
    client.close()

example()
```

$unwind

Der `$unwind` Operator wird verwendet, um ein Array-Feld aus den Eingabedokumenten zu dekonstruieren, um für jedes Element ein Dokument auszugeben. Dies kann nützlich sein, wenn Sie Operationen an den einzelnen Elementen eines Arrays ausführen möchten, z. B. das Filtern, Sortieren oder Transformieren der Daten.

Parameter

- `path`: Der Pfad zu dem Array-Feld, das rückgängig gemacht werden soll.
- `includeArrayIndex`: (optional) Gibt den Namen des neuen Felds an, das den Index des Array-Elements enthalten soll.
- `preserveNullAndEmptyArrays`: (optional) Bestimmt, ob bei der Operation das Originaldokument beibehalten wird, wenn das Array-Feld Null oder ein leeres Array ist.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$unwind` Operator verwendet wird, um ein Array-Feld zu dekonstruieren und weitere Operationen an den einzelnen Elementen durchzuführen.

Erstellen Sie Beispieldokumente

```
db.people.insertMany([
```

```
  { _id: 1, name: "jon", hobbies: ["painting", "dancing", "singing"] },
  { _id: 2, name: "jane", hobbies: ["reading", "swimming"] },
  { _id: 3, name: "jack", hobbies: [] }
])
```

Beispiel für eine Abfrage

```
db.people.aggregate([
  { $unwind: "$hobbies" }
])
```

Ausgabe

```
[
  { _id: 1, name: 'jon', hobbies: 'painting' },
  { _id: 1, name: 'jon', hobbies: 'dancing' },
  { _id: 1, name: 'jon', hobbies: 'singing' },
  { _id: 2, name: 'jane', hobbies: 'reading' },
  { _id: 2, name: 'jane', hobbies: 'swimming' }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$unwind` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('people');

  const result = await collection.aggregate([
    { $unwind: '$hobbies' }
  ]).toArray();
```

```
  console.log(result);
  client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['people']

    result = list(collection.aggregate([
        { '$unwind': '$hobbies' }
    ]))

    print(result)
    client.close()

example()
```

$VectorSearch

Neu ab Version 8.0

Wird von Elastic Cluster nicht unterstützt.

Der `$vectorSearch` Operator in Amazon DocumentDB ermöglicht Ihnen die Vektorsuche, eine Methode, die beim maschinellen Lernen verwendet wird, um ähnliche Datenpunkte zu finden, indem ihre Vektordarstellungen anhand von Entfernungs- oder Ähnlichkeitsmetriken verglichen werden. Diese Funktion kombiniert die Flexibilität und die umfassenden Abfragen einer JSON-based Dokumentendatenbank mit der Leistungsfähigkeit der Vektorsuche und ermöglicht es Ihnen, Anwendungsfälle für maschinelles Lernen und generative KI wie semantische Suche, Produktempfehlungen und mehr zu entwickeln.

Parameter

- <exact>(optional): Markierung, die angibt, ob die Suche nach dem exakten nächsten Nachbarn (ENN) oder dem ungefähren nächsten Nachbarn (ANN) ausgeführt werden soll. Der Wert kann einer der folgenden sein:
- false — um eine ANN-Suche auszuführen
- true — um die ENN-Suche auszuführen

Wenn es weggelassen oder auf False gesetzt numCandidates ist, ist es erforderlich.

```
- `<index>` : Name of the Vector Search index to use.
- `<limit>` : Number of documents to return in the results.
- `<numCandidates>` (optional): This field is required if 'exact' is false or omitted.
 Number of nearest neighbors to use during the search. Value must be less than or equal
 to (<=) 1000. You can't specify a number less than the number of documents to return
 ('limit').
- `<path>` : Indexed vector type field to search.
- `<queryVector>` : Array of numbers that represent the query vector.
```

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der $vectorSearch Operator verwendet werden kann, um ähnliche Produktbeschreibungen auf der Grundlage ihrer Vektordarstellungen zu finden.

Erstellen Sie Beispieldokumente

```
db.products.insertMany([
  {
    _id: 1,
    name: "Product A",
    description: "A high-quality, eco-friendly product for your home.",
    description_vector: [ 0.2, 0.5, 0.8 ]
  },
  {
    _id: 2,
    name: "Product B",
    description: "An innovative and modern kitchen appliance.",
    description_vector: [0.7, 0.3, 0.9]
  },
  {
    _id: 3,
    name: "Product C",
```

```
    description: "A comfortable and stylish piece of furniture.",
    description_vector: [0.1, 0.2, 0.4]
  }
]);
```

Vektor-Suchindex erstellen

```
db.runCommand(
    {
        createIndexes: "products",
        indexes: [{
            key: {
                "description_vector": "vector"
            },
            vectorOptions: {
                type: "hnsw",
                dimensions: 3,
                similarity: "cosine",
                m: 16,
                efConstruction: 64
            },
            name: "description_index"
        }]
    }
);
```

Beispiel für eine Abfrage

```
db.products.aggregate([
  { $vectorSearch: {
      index: "description_index",
      limit: 2,
      numCandidates: 10,
      path: "description_vector",
      queryVector: [0.1, 0.2, 0.3]
    }
  }
]);
```

Ausgabe

```
[
```

```
  {
    "_id": 1,
    "name": "Product A",
    "description": "A high-quality, eco-friendly product for your home.",
    "description_vector": [ 0.2, 0.5, 0.8 ]
  },
  {
    "_id": 3,
    "name": "Product C",
    "description": "A comfortable and stylish piece of furniture.",
    "description_vector": [ 0.1, 0.2, 0.4 ]
  }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$vectorSearch` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function findSimilarProducts(queryVector) {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('products');

  const result = await collection.aggregate([
    { $vectorSearch: {
        index: "description_index",
        limit: 2,
        numCandidates: 10,
        path: "description_vector",
        queryVector: queryVector
      }
    }
  ]).toArray();

  console.log(result);
  client.close();
```

```
}

findSimilarProducts([0.1, 0.2, 0.3]);
```

Python

```
from pymongo import MongoClient


def find_similar_products(query_vector):
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client.test
    collection = db.products

    result = list(collection.aggregate([
        {
            '$vectorSearch': {
                'index': "description_index",
                'limit': 2,
                'numCandidates': 10,
                'path': "description_vector",
                'queryVector': query_vector
            }
        }
    ]))

    print(result)
    client.close()

find_similar_products([0.1, 0.2, 0.3])
```

$week

Der `$week` Operator in Amazon DocumentDB gibt die Wochennummer eines Datums (0-53) auf der Grundlage des ISO 8601-Standards zurück. Die Wochennummer wird auf der Grundlage des Jahres und des Wochentags berechnet, wobei Montag der erste Tag der Woche ist.

Parameter

Keine

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der $week Operator verwendet wird, um die Wochennummer eines bestimmten Datums abzurufen.

Erstellen Sie Beispieldokumente

```
db.events.insertMany([
  { _id: 1, date: new Date("2023-01-01") },
  { _id: 2, date: new Date("2023-01-08") },
  { _id: 3, date: new Date("2023-12-31") }
]);
```

Beispiel für eine Abfrage

```
db.events.aggregate([
  { $project: {
    _id: 1,
    week: { $week: "$date" }
  }}
]);
```

Ausgabe

```
[
  { "_id": 1, "week": 1 },
  { "_id": 2, "week": 2 },
  { "_id": 3, "week": 53 }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des $week Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
```

```
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const events = db.collection('events');

  const result = await events.aggregate([
    { $project: {
      _id: 1,
      week: { $week: "$date" }
    }}
  ]).toArray();

  console.log(result);
  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
  client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
  db = client['test']
  events = db['events']

  result = list(events.aggregate([
      {'$project': {
          '_id': 1,
          'week': {'$week': '$date'}
      }}
  ]))

  print(result)

  client.close()

example()
```

$year

Der `$year` Operator in Amazon DocumentDB extrahiert die Jahreskomponente aus einem Datum oder Zeitstempel.

Parameter

- `expression`: Der Datums- oder Zeitstempelausdruck, aus dem die Jahreskomponente extrahiert werden soll.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$year` Operator verwendet wird, um die Jahreskomponente aus einem Datumsfeld zu extrahieren.

Erstellen Sie Beispieldokumente

```
db.events.insertMany([
  { "_id": 1, "date": ISODate("2023-04-15T00:00:00Z") },
  { "_id": 3, "date": ISODate("2021-12-31T00:00:00Z") }
]);
```

Beispiel für eine Abfrage

```
db.events.aggregate([
  { $project: { year: { $year: "$date" } } }
]);
```

Ausgabe

```
[
  { "_id": 1, "year": 2023 },
  { "_id": 3, "year": 2021 }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$year` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('events');

  const result = await collection.aggregate([
    { $project: { year: { $year: "$date" } } }
  ]).toArray();

  console.log(result);

  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['events']

    result = list(collection.aggregate([
        {'$project': {'year': {'$year': '$date'}}}
    ]))

    print(result)

    client.close()

example()
```

$zip

Der `$zip` Operator in Amazon DocumentDB ermöglicht es Ihnen, mehrere Arrays zu einem einzigen Array von Tupeln (Schlüssel-Wert-Paare) zu kombinieren. Dies ist nützlich, wenn Sie neue Dokumente oder Objekte erstellen müssen, indem Sie Daten aus verschiedenen Quellen oder Arrays innerhalb eines Dokuments kombinieren.

Parameter

- `inputs`: Eine Reihe von Ausdrücken, die in Arrays aufgelöst werden. Diese Arrays werden zu einem einzigen Array von Tupeln kombiniert.
- `useLongestLength`: (optional) Falls`true`, hat das Ausgabe-Array die Länge des längsten Eingabe-Arrays und füllt kürzere Arrays mit Werten auf. `null` Falls`false`, hat das Ausgabe-Array die Länge des kürzesten Eingabe-Arrays.
- `defaults`: (optional) Ein Array von Standardwerten, das für die Tupel verwendet werden soll, wenn das entsprechende Eingabearray kürzer als das längste Eingabearray `useLongestLength` ist und es ist`true`.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$zip` Operator verwendet wird, um zwei Arrays zu einem einzigen Array von Tupeln zu kombinieren.

Erstellen Sie Beispieldokumente

```
db.grades.insert([
  {
    "_id": 1,
    "name": "John",
    "scores": [90, 85, 92],
    "classes": ["Math", "English", "Science"]
  },
  {
    "_id": 2,
    "name": "Jane",
    "scores": [88, 91, 90, 85],
    "classes": ["Math", "English", "Science", "History"]
  }
])
```

Beispiel für eine Abfrage

```
db.grades.aggregate([
  {
    $project: {
      "name": 1,
      "scoredClasses": {
        $zip: {
          inputs: ["$scores", "$classes"],
          useLongestLength: true,
          defaults: [null, null]
        }
      }
    }
  }
])
```

Ausgabe

```
[
  {
    "_id": 1,
    "name": "John",
    "scoredClasses": [
      [90, "Math"],
      [85, "English"],
      [92, "Science"],
      [null, null]
    ]
  },
  {
    "_id": 2,
    "name": "Jane",
    "scoredClasses": [
      [88, "Math"],
      [91, "English"],
      [90, "Science"],
      [85, "History"]
    ]
  }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$zip` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('grades');

  const result = await collection.aggregate([
    {
      $project: {
        "name": 1,
        "scoredClasses": {
          $zip: {
            inputs: ["$scores", "$classes"],
            useLongestLength: true,
            defaults: [null, null]
          }
        }
      }
    }
  ]).toArray();

  console.log(result);
  client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
```

```
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['grades']

    result = list(collection.aggregate([
        {
            '$project': {
                'name': 1,
                'scoredClasses': {
                    '$zip': {
                        'inputs': ['$scores', '$classes'],
                        'useLongestLength': True,
                        'defaults': [None, None]
                    }
                }
            }
        }
    ]))

    print(result)
    client.close()

example()
```

Geodaten

Dieser Abschnitt enthält detaillierte Informationen zu Geodatenoperatoren, die von Amazon DocumentDB unterstützt werden.

Themen

- $geometry
- $geoIntersects
- $geoWithin
- $maxDistance
- $minDistance
- $near
- $nearSphere

$geometry

Der `$geometry` Operator in Amazon DocumentDB wird verwendet, um ein GeoJSON-Geometrieobjekt als Teil einer Geodatenabfrage anzugeben. Dieser Operator wird in Verbindung mit anderen Operatoren für Geodatenabfragen wie `$geoWithin` und `$geoIntersects` zur Durchführung räumlicher Abfragen Ihrer Daten verwendet.

In Amazon DocumentDB unterstützt der `$geometry` Operator die folgenden GeoJSON-Geometrietypen:

- Point
- LineString
- Polygon
- MultiPoint
- MultiLineString
- MultiPolygon
- GeometryCollection

Parameter

- `type`: Der Typ des GeoJSON-Geometrieobjekts, z. B.`Point`,`Polygon`, usw.
- `coordinates`: Ein Array von Koordinaten, das die Geometrie darstellt. Die Struktur des Koordinatenarrays hängt vom Geometrietyp ab.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$geometry` Operator verwendet wird, um eine `$geoIntersects` Abfrage in Amazon DocumentDB durchzuführen.

Erstellen Sie Beispieldokumente

```
db.locations.insertMany([
  {
    "_id": 1,
    "name": "Location 1",
    "location": {
      "type": "Point",
      "coordinates": [-73.983253, 40.753941]
```

```
    }
  },
  {
    "_id": 2,
    "name": "Location 2",
    "location": {
      "type": "Polygon",
      "coordinates": [[
        [-73.998427, 40.730309],
        [-73.954348, 40.730309],
        [-73.954348, 40.780816],
        [-73.998427, 40.780816],
        [-73.998427, 40.730309]
      ]]
    }
  }
]);
```

Beispiel für eine Abfrage

```
db.locations.find({
  "location": {
    "$geoIntersects": {
      "$geometry": {
        "type": "Polygon",
        "coordinates": [[
          [-73.998, 40.730],
          [-73.954, 40.730],
          [-73.954, 40.781],
          [-73.998, 40.781],
          [-73.998, 40.730]
        ]]
      }
    }
  }
})
```

Ausgabe

```
[
  {
    "_id": 2,
    "name": "Location 2",
```

```
    "location": {
      "type": "Polygon",
      "coordinates": [
        [
          [-73.998427, 40.730309],
          [-73.954348, 40.730309],
          [-73.954348, 40.780816],
          [-73.998427, 40.780816],
          [-73.998427, 40.730309]
        ]
      ]
    }
  }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$geometry` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('locations');

  const query = {
    "location": {
      "$geoIntersects": {
        "$geometry": {
          "type": "Polygon",
          "coordinates": [[
            [-73.998, 40.730],
            [-73.954, 40.730],
            [-73.954, 40.781],
            [-73.998, 40.781],
            [-73.998, 40.730]
          ]]
```

```
        }
      }
    }
  };

  const result = await collection.find(query).toArray();
  console.log(result);

  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['locations']

    query = {
        "location": {
            "$geoIntersects": {
                "$geometry": {
                    "type": "Polygon",
                    "coordinates": [[
                        [-73.998, 40.730],
                        [-73.954, 40.730],
                        [-73.954, 40.781],
                        [-73.998, 40.781],
                        [-73.998, 40.730]
                    ]]
                }
            }
        }
    }

    result = list(collection.find(query))
    print(result)
```

```
    client.close()

example()
```

$geoIntersects

Der `$geoIntersects` Operator in Amazon DocumentDB wird verwendet, um Dokumente zu finden, deren Geodaten sich mit einem bestimmten GeoJSON-Objekt überschneiden. Dieser Operator ist nützlich für Anwendungen, bei denen Dokumente anhand ihrer räumlichen Beziehung zu einer bestimmten geographischen Form, wie z. B. einem Polygon oder Multipolygon, identifiziert werden müssen.

Parameter

- `$geometry`: Ein GeoJSON-Objekt, das die Form darstellt, bei der nach Überschneidungen gesucht werden soll. Die unterstützten GeoJSON-Objekttypen sind`Point`, `LineStringPolygon`, und`MultiPolygon`.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$geoIntersects` Operator verwendet wird, um den Namen des Bundesstaates für einen bestimmten Satz von Koordinaten in Amazon DocumentDB zu finden.

Erstellen Sie Beispieldokumente

```
db.states.insertMany([
  {
    "name": "New York",
    "loc": {
      "type": "Polygon",
      "coordinates": [[
        [-74.25909423828125, 40.47556838210948],
        [-73.70819091796875, 40.47556838210948],
        [-73.70819091796875, 41.31342607582222],
        [-74.25909423828125, 41.31342607582222],
        [-74.25909423828125, 40.47556838210948]
      ]]
    }
  },
```

```
  {
    "name": "California",
    "loc": {
      "type": "Polygon",
      "coordinates": [[
        [-124.4091796875, 32.56456771381587],
        [-114.5458984375, 32.56456771381587],
        [-114.5458984375, 42.00964153424558],
        [-124.4091796875, 42.00964153424558],
        [-124.4091796875, 32.56456771381587]
      ]]
    }
  }
]);
```

Beispiel für eine Abfrage

```
var location = [-73.965355, 40.782865];

db.states.find({
  "loc": {
    "$geoIntersects": {
      "$geometry": {
        "type": "Point",
        "coordinates": location
      }
    }
  }
}, {
  "name": 1
});
```

Ausgabe

```
{ "_id" : ObjectId("536b0a143004b15885c91a2c"), "name" : "New York" }
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$geoIntersects` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function findStateByGeoIntersects(longitude, latitude) {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('states');

  const query = {
    loc: {
      $geoIntersects: {
        $geometry: {
          type: 'Point',
          coordinates: [longitude, latitude]
        }
      }
    }
  };

  const projection = {
    _id: 0,
    name: 1
  };

  const document = await collection.findOne(query, { projection });

  await client.close();

  if (document) {
    return document.name;
  } else {
    throw new Error('The geo location you entered was not found in the United
 States!');
  }
}
```

Python

```
from pymongo import MongoClient
```

```
def find_state_by_geointersects(longitude, latitude):
    try:
        client = MongoClient('mongodb://<username>:<password>@<cluster-
endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
        db = client.test
        collection_states = db.states

        query_geointersects = {
            "loc": {
                "$geoIntersects": {
                    "$geometry": {
                        "type": "Point",
                        "coordinates": [longitude, latitude]
                    }
                }
            }
        }

        document = collection_states.find_one(query_geointersects,
                                              projection={
                                                  "_id": 0,
                                                  "name": 1
                                              })
        if document is not None:
            state_name = document['name']
            return state_name
        else:
            raise Exception("The geo location you entered was not found in the
 United States!")
    except Exception as e:
        print('Exception in geoIntersects: {}'.format(e))
        raise
    finally:
        if client is not None:
            client.close()
```

$geoWithin

Der `$geoWithin` Operator in Amazon DocumentDB wird verwendet, um Dokumente zu finden, deren Standortdaten (dargestellt als GeoJSON-Objekte) vollständig in einer bestimmten Form

enthalten sind, z. B. einem Polygon oder Multipolygon. Dies ist nützlich für die Abfrage von Objekten, die sich in einer bestimmten geografischen Region befinden.

Parameter

- `$geometry`: Ein GeoJSON-Objekt, das die Form darstellt, nach der abgefragt werden soll.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$geoWithin` Operator verwendet werden kann, um alle Flughäfen im Bundesstaat New York zu finden.

Erstellen Sie Beispieldokumente

```
// Insert state document
db.states.insert({
    "name": "New York",
    "loc": {
        "type": "Polygon",
        "coordinates": [[
            [-79.76278, 45.0],
            [-73.94, 45.0],
            [-73.94, 40.5],
            [-79.76278, 40.5],
            [-79.76278, 45.0]
        ]]
    }
});

// Insert airport documents
db.airports.insert([
    {
        "name": "John F. Kennedy International Airport",
        "type": "airport",
        "code": "JFK",
        "loc": {
            "type": "Point",
            "coordinates": [-73.7781, 40.6413]
        }
    },
    {
        "name": "LaGuardia Airport",
        "type": "airport",
```

```
        "code": "LGA",
        "loc": {
            "type": "Point",
            "coordinates": [-73.8772, 40.7769]
        }
    },
    {
        "name": "Buffalo Niagara International Airport",
        "type": "airport",
        "code": "BUF",
        "loc": {
            "type": "Point",
            "coordinates": [-78.7322, 42.9403]
        }
    }
]);
```

Beispiel für eine Abfrage

```
var state = db.states.findOne({"name": "New York"});

db.airports.find({
    "loc": {
        "$geoWithin": {
            "$geometry": state.loc
        }
    }
}, {
    "name": 1,
    "type": 1,
    "code": 1,
    "_id": 0
});
```

Ausgabe

```
[
  {
    "name": "John F. Kennedy International Airport",
    "type": "airport",
    "code": "JFK"
  },
  {
```

```
    "name": "LaGuardia Airport",
    "type": "airport",
    "code": "LGA"
  }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$geoWithin` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function findAirportsWithinState(stateName) {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');

  const stateDoc = await db.collection('states').findOne({ name: stateName },
 { projection: { _id: 0, loc: 1 } });
  const airportDocs = await db.collection('airports').find({
    loc: {
      $geoWithin: {
        $geometry: stateDoc.loc
      }
    }
  }, { projection: { name: 1, type: 1, code: 1, _id: 0 } }).toArray();

  console.log(airportDocs);

  await client.close();
}

findAirportsWithinState('New York');
```

Python

```
from pymongo import MongoClient

def find_airports_within_state(state_name):
```

```
    try:
        client = MongoClient('mongodb://<username>:<password>@<cluster-
endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
        db = client['test']
        state_doc = db.states.find_one({'name': state_name}, {'_id': 0, 'loc': 1})
        airport_docs = db.airports.find({
            'loc': {
                '$geoWithin': {
                    '$geometry': state_doc['loc']
                }
            }
        }, {'name': 1, 'type': 1, 'code': 1, '_id': 0})

        return list(airport_docs)
    except Exception as e:
        print(f'Error: {e}')
    finally:
        client.close()

airports = find_airports_within_state('New York')
print(airports)
```

$maxDistance

Der `$maxDistance` Operator in Amazon DocumentDB wird verwendet, um die maximale Entfernung (in Metern) von einem GeoJSON-Punkt anzugeben, innerhalb derer sich Dokumente befinden müssen, um in die Abfrageergebnisse aufgenommen zu werden. Dieser Operator wird in Verbindung mit dem `$nearSphere` Operator verwendet, um Geodatenabfragen durchzuführen.

Parameter

- `$maxDistance`: Die maximale Entfernung (in Metern) vom Referenzpunkt, innerhalb derer sich Dokumente befinden müssen, um in die Abfrageergebnisse aufgenommen zu werden.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$maxDistance` Operator in Amazon DocumentDB verwendet wird, um alle Hauptstädte der Bundesstaaten im Umkreis von 100 Kilometern von Boston zu finden.

Erstellen Sie Beispieldokumente

```
db.capitals.insert([
  { state: "Massachusetts", city: "Boston", location: { type: "Point", coordinates:
 [-71.0589, 42.3601] } },
  { state: "Rhode Island", city: "Providence", location: { type: "Point", coordinates:
 [-71.4128, 41.8239] } },
  { state: "New Hampshire", city: "Concord", location: { type: "Point", coordinates:
 [-71.5383, 43.2067] } },
  { state: "Vermont", city: "Montpelier", location: { type: "Point", coordinates:
 [-72.5751, 44.2604] } }
]);
```

Beispiel für eine Abfrage

```
db.capitals.find(
  {
    location: {
      $nearSphere: {
        $geometry: { type: "Point", coordinates: [-71.0589, 42.3601] },
        $maxDistance: 100000
      }
    }
  },
  { state: 1, city: 1, _id: 0 }
);
```

Ausgabe

```
[
  { "state": "Rhode Island", "city": "Providence" },
  { "state": "New Hampshire", "city": "Concord" }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$maxDistance` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');
```

```
async function findCapitalsNearBoston() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const capitals = db.collection('capitals');

  const result = await capitals.find({
    location: {
      $nearSphere: {
        $geometry: { type: "Point", coordinates: [-71.0589, 42.3601] },
        $maxDistance: 100000
      }
    }
  }, {
    projection: { state: 1, city: 1, _id: 0 }
  }).toArray();

  console.log(result);
  await client.close();
}

findCapitalsNearBoston();
```

Python

```
from pymongo import MongoClient

def find_capitals_near_boston():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client.test
    capitals = db.capitals

    result = list(capitals.find(
        {
            "location": {
                "$nearSphere": {
                    "$geometry": { "type": "Point", "coordinates": [-71.0589,
 42.3601] },
                    "$maxDistance": 100000
                }
```

```
            }
        },
        {"state": 1, "city": 1, "_id": 0}
    ))

    print(result)
    client.close()

find_capitals_near_boston()
```

$minDistance

`$minDistance`ist ein Suchoperator, der in Verbindung mit `$nearSphere` oder verwendet wird, `$geoNear` um Dokumente zu filtern, die sich mindestens im angegebenen Mindestabstand vom Mittelpunkt befinden. Dieser Operator wird in Amazon DocumentDB unterstützt und funktioniert ähnlich wie sein Gegenstück in MongoDB.

Parameter

- `$minDistance`: Der Mindestabstand (in Metern) vom Mittelpunkt, um Dokumente in die Ergebnisse einzubeziehen.

Beispiel (MongoDB Shell)

In diesem Beispiel finden wir alle Restaurants in einem Umkreis von 2 Kilometern um einen bestimmten Standort in Seattle, Washington.

Erstellen Sie Beispieldokumente

```
db.usarestaurants.insertMany([
  {
    "state": "Washington",
    "city": "Seattle",
    "name": "Noodle House",
    "rating": 4.8,
    "location": {
      "type": "Point",
      "coordinates": [-122.3517, 47.6159]
    }
  },
  {
```

```
    "state": "Washington",
    "city": "Seattle",
    "name": "Pike Place Grill",
    "rating": 4.5,
    "location": {
      "type": "Point",
      "coordinates": [-122.3412, 47.6102]
    }
  },
  {
    "state": "Washington",
    "city": "Bellevue",
    "name": "The Burger Joint",
    "rating": 4.2,
    "location": {
      "type": "Point",
      "coordinates": [-122.2007, 47.6105]
    }
  }
]);
```

Beispiel für eine Abfrage

```
db.usarestaurants.find({
  "location": {
    "$nearSphere": {
      "$geometry": {
        "type": "Point",
        "coordinates": [-122.3516, 47.6156]
      },
      "$minDistance": 1,
      "$maxDistance": 2000
    }
  }
}, {
  "name": 1
});
```

Ausgabe

```
{ "_id" : ObjectId("611f3da985009a81ad38e74b"), "name" : "Noodle House" }
{ "_id" : ObjectId("611f3da985009a81ad38e74c"), "name" : "Pike Place Grill" }
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$minDistance` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function findRestaurantsNearby() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('usarestaurants');

  const result = await collection.find({
    "location": {
      "$nearSphere": {
        "$geometry": {
          "type": "Point",
          "coordinates": [-122.3516, 47.6156]
        },
        "$minDistance": 1,
        "$maxDistance": 2000
      }
    }
  }, {
    "projection": { "name": 1 }
  }).toArray();

  console.log(result);
  client.close();
}

findRestaurantsNearby();
```

Python

```
from pymongo import MongoClient

def find_restaurants_nearby():
```

```
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client.test
    collection = db.usarestaurants

    result = list(collection.find({
        "location": {
            "$nearSphere": {
                "$geometry": {
                    "type": "Point",
                    "coordinates": [-122.3516, 47.6156]
                },
                "$minDistance": 1,
                "$maxDistance": 2000
            }
        }
    }, {
        "projection": {"name": 1}
    }))

    print(result)
    client.close()

find_restaurants_nearby()
```

$near

Der `$near` Operator in Amazon DocumentDB wird verwendet, um Dokumente zu finden, die sich geografisch in der Nähe eines bestimmten Punktes befinden. Er gibt Dokumente zurück, die nach Entfernung sortiert sind, wobei die Dokumente, die sich am nächsten befinden, zuerst angezeigt werden. Dieser Operator erfordert einen 2dSphere-Geodatenindex und ist nützlich für Näherungsabfragen von Standortdaten.

Parameter

- `$geometry`: Ein GeoJSON Point-Objekt, das den Mittelpunkt für die Near-Abfrage definiert.
- `$maxDistance`: (optional) Die maximale Entfernung in Metern vom angegebenen Punkt, die ein Dokument haben darf, um der Abfrage zu entsprechen.

- `$minDistance`: (optional) Die Mindestentfernung in Metern vom angegebenen Punkt, die ein Dokument haben darf, um der Abfrage zu entsprechen.

Anforderungen an den Index

- `2dsphere index`: Erforderlich für Geodatenabfragen zu GeoJSON-Punktdaten.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie Sie den `$near` Operator verwenden können, um die Restaurants zu finden, die einem bestimmten Ort in Seattle, Washington, am nächsten liegen.

Erstellen Sie Beispieldokumente

```
db.usarestaurants.insert([
  {
    "name": "Noodle House",
    "city": "Seattle",
    "state": "Washington",
    "rating": 4.8,
    "location": { "type": "Point", "coordinates": [-122.3517, 47.6159] }
  },
  {
    "name": "Pike Place Grill",
    "city": "Seattle",
    "state": "Washington",
    "rating": 4.2,
    "location": { "type": "Point", "coordinates": [-122.3403, 47.6062] }
  },
  {
    "name": "Lola",
    "city": "Seattle",
    "state": "Washington",
    "rating": 4.5,
    "location": { "type": "Point", "coordinates": [-122.3407, 47.6107] }
  }
]);
```

Erstellen Sie einen 2dSphere-Index

```
db.usarestaurants.createIndex({ "location": "2dsphere" });
```

Abfragebeispiel mit GeoJSON Point

```
db.usarestaurants.find({
  location: {
    $near: {
      $geometry: {
        type: "Point",
        coordinates: [-122.3516, 47.6156]
      },
      $maxDistance: 100,
      $minDistance: 10
    }
  }
});
```

Ausgabe

```
{
  "_id" : ObjectId("69031ec9ea1c2922a1ce5f4a"),
  "name" : "Noodle House",
  "city" : "Seattle",
  "state" : "Washington",
  "rating" : 4.8,
  "location" : {
    "type" : "Point",
    "coordinates" : [ -122.3517, 47.6159 ]
  }
}
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$near` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function findNearbyRestaurants() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
```

```
  const db = client.db('test');
  const restaurants = db.collection('usarestaurants');

  // Create 2dsphere index
  await restaurants.createIndex({ "location": "2dsphere" });

  const result = await restaurants.find({
    location: {
      $near: {
        $geometry: {
          type: "Point",
          coordinates: [-122.3516, 47.6156]
        },
        $maxDistance: 100,
        $minDistance: 10
      }
    }
  }).toArray();

  console.log(result);

  client.close();
}

findNearbyRestaurants();
```

Python

```
from pymongo import MongoClient

def find_nearby_restaurants():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    restaurants = db['usarestaurants']

    # Create 2dsphere index
    restaurants.create_index([("location", "2dsphere")])

    result = list(restaurants.find({
        'location': {
            '$near': {
```

```
                '$geometry': {
                    'type': 'Point',
                    'coordinates': [-122.3516, 47.6156]
                },
                '$maxDistance': 100,
                '$minDistance': 10
            }
        }
    }))

    print(result)

    client.close()

find_nearby_restaurants()
```

$nearSphere

Der `$nearSphere` Operator in Amazon DocumentDB wird verwendet, um Dokumente zu finden, die sich innerhalb einer bestimmten Entfernung von einem Geodatenpunkt befinden. Dieser Operator ist besonders nützlich für geografische Abfragen, z. B. für die Suche nach allen Restaurants in einem bestimmten Umkreis eines bestimmten Standorts.

Parameter

- `$geometry`: Ein GeoJSON-Objekt, das den Referenzpunkt darstellt. Muss ein `Point` Objekt mit `coordinates` Feldern `type` und sein.
- `$minDistance`: (optional) Der Mindestabstand (in Metern) vom Referenzpunkt, den Dokumente haben müssen.
- `$maxDistance`: (optional) Der maximale Abstand (in Metern) vom Referenzpunkt, den Dokumente haben müssen.

Beispiel (MongoDB Shell)

In diesem Beispiel finden wir alle Restaurants im Umkreis von 2 Kilometern (2000 Metern) von einem bestimmten Ort in Seattle, WA.

Erstellen Sie Beispieldokumente

```
db.usarestaurants.insert([
  {
    name: "Noodle House",
    location: { type: "Point", coordinates: [-122.3516, 47.6156] }
  },
  {
    name: "Pike Place Grill",
    location: { type: "Point", coordinates: [-122.3403, 47.6101] }
  },
  {
    name: "Seattle Coffee Co.",
    location: { type: "Point", coordinates: [-122.3339, 47.6062] }
  }
]);
```

Beispiel für eine Abfrage

```
db.usarestaurants.find({
  location: {
    $nearSphere: {
      $geometry: {
        type: "Point",
        coordinates: [-122.3516, 47.6156]
      },
      $minDistance: 1,
      $maxDistance: 2000
    }
  }
}, {
  name: 1
});
```

Ausgabe

```
{ "_id" : ObjectId("611f3da985009a81ad38e74b"), "name" : "Noodle House" }
{ "_id" : ObjectId("611f3da985009a81ad38e74c"), "name" : "Pike Place Grill" }
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$nearSphere` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function findNearbyRestaurants() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const restaurants = db.collection('usarestaurants');

  const result = await restaurants.find({
    location: {
      $nearSphere: {
        $geometry: {
          type: "Point",
          coordinates: [-122.3516, 47.6156]
        },
        $minDistance: 1,
        $maxDistance: 2000
      }
    }
  }, {
    projection: { name: 1 }
  }).toArray();

  console.log(result);
  client.close();
}

findNearbyRestaurants();
```

Python

```
from pymongo import MongoClient

def find_nearby_restaurants():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client.test
    restaurants = db.usarestaurants
```

```
    result = list(restaurants.find({
        'location': {
            '$nearSphere': {
                '$geometry': {
                    'type': 'Point',
                    'coordinates': [-122.3516, 47.6156]
                },
                '$minDistance': 1,
                '$maxDistance': 2000
            }
        }
    }, {
        'name': 1
    }))

    print(result)
    client.close()

find_nearby_restaurants()
```

Abfrage- und Projektionsoperatoren

Dieser Abschnitt enthält detaillierte Informationen zu Abfrage- und Projektionsoperatoren, die von Amazon DocumentDB unterstützt werden.

Themen

- $
- $all
- $and
- $ Bits AllClear
- $ Bits AllSet
- $ Bits AnyClear
- $ Bits AnySet
- $comment
- $elemMatch
- $eq
- $exists

- $expr
- $gt
- $gte
- $in
- $jsonSchema
- $lt
- $mod
- $lte
- $meta
- $ne
- $nin
- $nor
- $not
- $or
- $regex
- $slice
- $size
- $text
- $type

$

Der $ Projektionsoperator begrenzt den Inhalt eines Array-Felds so, dass nur das erste Element zurückgegeben wird, das der Abfragebedingung entspricht. Er wird verwendet, um ein einzelnes passendes Array-Element zu projizieren.

Parameter

- `field.$`: Das Array-Feld mit dem Positionsoperator zur Projektion des ersten passenden Elements.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der $ Projektionsoperator verwendet wird, um nur das passende Array-Element zurückzugeben.

Erstellen Sie Beispieldokumente

```
db.students.insertMany([
  { _id: 1, name: "Alice", grades: [85, 92, 78, 95] },
  { _id: 2, name: "Bob", grades: [70, 88, 92, 65] },
  { _id: 3, name: "Charlie", grades: [95, 89, 91, 88] }
]);
```

Beispiel für eine Abfrage

```
db.students.find(
  { grades: { $gte: 90 } },
  { name: 1, "grades.$": 1 }
);
```

Ausgabe

```
{ "_id" : 1, "name" : "Alice", "grades" : [ 92 ] }
{ "_id" : 2, "name" : "Bob", "grades" : [ 92 ] }
{ "_id" : 3, "name" : "Charlie", "grades" : [ 95 ] }
```

In diesem Beispiel wird für jeden Schüler nur die erste Note zurückgegeben, die größer oder gleich 90 ist.

Codebeispiele

Um ein Codebeispiel für die Verwendung des $ Projektionsoperators anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
```

```
  const db = client.db('test');
  const collection = db.collection('students');

  const result = await collection.find(
    { grades: { $gte: 90 } },
    { projection: { name: 1, "grades.$": 1 } }
  ).toArray();

  console.log(JSON.stringify(result, null, 2));
  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['students']

    result = list(collection.find(
        {'grades': {'$gte': 90}},
        {'name': 1, 'grades.$': 1}
    ))

    print(result)
    client.close()

example()
```

$all

Der `$all` Operator in Amazon DocumentDB wird verwendet, um Dokumente abzugleichen, bei denen der Wert eines Felds ein Array ist und alle angegebenen Elemente enthält, unabhängig von der Reihenfolge der Elemente im Array.

Parameter

- `field`: Der Name des zu prüfenden Feldes.
- `[value1, value2, ...]`: Die Liste der Werte, die im Array übereinstimmen sollen.

Wird **`$elemMatch`** innerhalb eines **`$all`** Ausdrucks verwendet

Einschränkungen in Bezug auf die Verwendung des `$elemMatch` Operators innerhalb eines `$all` Ausdrucks finden Verwenden von $elemMatch innerhalb eines $all-Ausdrucks Sie unter.

Dollar ($) in Feldnamen

Einschränkungen Dollar ($) und Punkt (.) in Feldnamen bei der Abfrage von Feldern mit $ Präfix `$all` in verschachtelten Objekten finden Sie unter.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt die Verwendung des `$all` Operators zum Abrufen von Dokumenten, bei denen das Feld „Farben“ ein Array ist, das sowohl „Rot“ als auch „Blau“ enthält.

Erstellen Sie Beispieldokumente

```
db.example.insertMany([
  { "Item": "Pen", "Colors": ["Red", "Blue", "Green"] },
  { "Item": "Notebook", "Colors": ["Blue", "White"] },
  { "Item": "Poster Paint", "Colors": ["Red", "Yellow", "White"] }
])
```

Beispiel für eine Abfrage

```
db.example.find({ "Colors": { $all: ["Red", "Blue"] } }).pretty()
```

Ausgabe

```
{
  "_id" : ObjectId("6137d6c5b3a1d35e0b6ee6ad"),
  "Item" : "Pen",
  "Colors" : [
```

```
          "Red",
          "Blue",
          "Green"
  ]
}
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$all` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('example');

  const result = await collection.find({ "Colors": { $all: ["Red",
 "Blue"] } }).toArray();
  console.log(result);

  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['example']

    result = list(collection.find({ "Colors": { "$all": ["Red", "Blue"] } }))
```

```
    print(result)

    client.close()

example()
```

$and

Der `$and` Operator in Amazon DocumentDB wird verwendet, um mehrere Ausdrücke zu kombinieren und sie als eine einzige Bedingung auszuwerten. Er gibt zurück`true`, ob alle angegebenen Ausdrücke als 0 ausgewertet werden`true`, und `false` andernfalls. Dieser Operator ist nützlich, um mehrere Kriterien auf eine Abfrage anzuwenden.

Parameter

- `expression1`: Ein erforderlicher Ausdruck, der einen booleschen Wert ergibt.
- `expression2`: Ein erforderlicher Ausdruck, der einen booleschen Wert ergibt.
- `...`: Zusätzliche erforderliche Ausdrücke, die zu booleschen Werten ausgewertet werden.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$and` Operator verwendet wird, um alle Dokumente in der Sammlung „Benutzer“ zu finden, bei denen das Feld „Alter“ größer als 18 und das Feld „Status“ „aktiv“ ist.

Erstellen Sie Beispieldokumente

```
db.users.insertMany([
  { name: "John", age: 25, status: "active" },
  { name: "Jane", age: 17, status: "active" },
  { name: "Bob", age: 30, status: "inactive" },
  { name: "Alice", age: 22, status: "active" }
]);
```

Beispiel für eine Abfrage

```
db.users.find({
  $and: [
    { age: { $gt: 18 } },
```

```
    { status: "active" }
  ]
});
```

Ausgabe

```
[
  { "_id" : ObjectId("614e3c4b63f5892e7c4e2345"), "name" : "John", "age" : 25,
 "status" : "active" },
  { "_id" : ObjectId("614e3c4b63f5892e7c4e2347"), "name" : "Alice", "age" : 22,
 "status" : "active" }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des $and Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function findActiveUsersOlderThan18() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const users = db.collection('users');

  const activeUsersOlderThan18 = await users.find({
    $and: [
      { age: { $gt: 18 } },
      { status: 'active' }
    ]
  }).toArray();

  console.log(activeUsersOlderThan18);
  await client.close();
}

findActiveUsersOlderThan18();
```

Python

```
from pymongo import MongoClient

def find_active_users_older_than_18():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    users = db['users']

    active_users_older_than_18 = list(users.find({
        '$and': [
            {'age': {'$gt': 18}},
            {'status': 'active'}
        ]
    }))

    print(active_users_older_than_18)
    client.close()

find_active_users_older_than_18()
```

$ Bits AllClear

Der `$bitsAllClear` Operator in Amazon DocumentDB wird verwendet, um die Dokumente abzugleichen, bei denen alle angegebenen Bits in einem Feld gelöscht (auf 0 gesetzt) wurden. Dieser Operator kann nützlich sein, um bitweise Operationen mit gespeicherten Daten durchzuführen.

Parameter

- `field`: Das Feld, in dem geprüft werden soll, ob die angegebenen Bits gelöscht wurden.
- `value`: Die numerische Bitmaske, die angibt, welche Bits geprüft werden sollen, oder eine Liste von Bitpositionen, die überprüft werden sollen. Eine numerische Bitmaske kann binär (0b...), dezimal, hexadezimal (0x...), oktal (0o...) oder binär () sein. BinData In einer Liste von Bitpositionen ist die Position des niedrigstwertigen Bits 0.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt die Verwendung des `$bitsAllClear` Operators in Amazon DocumentDB.

Erstellen Sie Beispieldokumente

```
db.collection.insertMany([
  { _id: 1, bits: 0b1010 },
  { _id: 2, bits: 0b1100 },
  { _id: 3, bits: 0b0101 }
]);
```

Beispiel für eine Abfrage

```
db.collection.find({
  bits: { $bitsAllClear: 0b0011 }
})
```

Ausgabe

```
{ "_id" : 2, "bits" : 12 }
```

Die Abfrage prüft, ob alle durch die Bitmaske angegebenen Bits `0b0011` (die zwei niedrigstwertigen Bits) im `bits` Feld gelöscht wurden. Das Dokument mit `_id` 2 erfüllt diese Bedingung, da in seinem `bits` Feld diese Bits gelöscht wurden.

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$bitsAllClear` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
```

```
  const db = client.db('test');
  const collection = db.collection('collection');

  const result = await collection.find({
    bits: { $bitsAllClear: 0b0011 }
  }).toArray();

  console.log(result);

  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['collection']

    result = list(collection.find({
        'bits': { '$bitsAllClear': 0b0011 }
    }))

    print(result)

    client.close()

example()
```

$ Bits AllSet

Der `$bitsAllSet` Operator in Amazon DocumentDB wird verwendet, um Dokumente abzufragen, bei denen ein bestimmter Satz von Bits in einem Feld alle auf 1 gesetzt ist. Dieser Operator ermöglicht es Ihnen, bitweise Operationen an Feldwerten durchzuführen. Er kann nützlich sein, wenn Sie den Status einzelner Bits innerhalb eines numerischen Werts überprüfen müssen.

Parameter

- `field`: Der Name des numerischen Felds, für das die bitweise Operation ausgeführt werden soll.
- `value`: Die numerische Bitmaske, die angibt, welche Bits geprüft werden sollen, oder eine Liste von Bitpositionen, die überprüft werden sollen. Eine numerische Bitmaske kann binär (0b...), dezimal, hexadezimal (0x...), oktal (0o...) oder binär () sein. BinData In einer Liste von Bitpositionen ist die Position des niedrigstwertigen Bits 0.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$bitsAllSet` Operator verwendet wird, um Dokumente zu finden, in denen in dem `flags` Feld alle Bits gesetzt sind, die durch die Bitmaske angegeben sind.

Erstellen Sie Beispieldokumente

```
db.collection.insert([
  { _id: 1, flags: 0b1010 },
  { _id: 2, flags: 0b1100 },
  { _id: 3, flags: 0b1110 }
])
```

Beispiel für eine Abfrage

```
db.collection.find({ flags: { $bitsAllSet: 0b1100 } })
```

Ausgabe

```
{ "_id": 2, "flags": 12 },
{ "_id": 3, "flags": 14 }
```

In diesem Beispiel sucht die Abfrage nach Dokumenten, in denen für das `flags` Feld alle Bits gesetzt sind, die durch die Bitmaske `0b1100` (die den Dezimalwert 12 darstellt) angegeben sind. Die Dokumente mit `_id` 2 und 3 entsprechen diesen Kriterien, da für ihre `flags` Feldwerte alle erforderlichen Bits gesetzt sind (das dritte und das viertniedrigste Bit).

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$bitsAllSet` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function findWithBitsAllSet() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('collection');

  const result = await collection.find({ flags: { $bitsAllSet:
 0b1100 } }).toArray();
  console.log(result);

  await client.close();
}

findWithBitsAllSet();
```

Python

```
from pymongo import MongoClient

def find_with_bits_all_set():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client.test
    collection = db.collection

    result = list(collection.find({ 'flags': { '$bitsAllSet': 0b1100 } }))
    print(result)

    client.close()

find_with_bits_all_set()
```

$ Bits AnyClear

Der `$bitsAnyClear` Operator in Amazon DocumentDB wird verwendet, um die Dokumente abzugleichen, bei denen eines der angegebenen Bits in einem Feld gelöscht (auf 0 gesetzt) wurde. Dies kann nützlich sein, um bitweise Operationen an Feldwerten durchzuführen, die in Dokumenten gespeichert sind.

Parameter

- `field`: Das zu prüfende Feld.
- `value`: Die numerische Bitmaske, die angibt, welche Bits geprüft werden sollen, oder eine Liste von Bitpositionen, die überprüft werden sollen. Eine numerische Bitmaske kann binär (0b...), dezimal, hexadezimal (0x...), oktal (0o...) oder binär () sein. BinData In einer Liste von Bitpositionen ist die Position des niedrigstwertigen Bits 0.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$bitsAnyClear` Operator verwendet wird, um zu überprüfen, ob ein Bit im `status` Feld der `items` Sammlung leer ist.

Erstellen Sie Beispieldokumente

```
db.items.insertMany([
  { "_id": 1, "status": 7 },
  { "_id": 2, "status": 15 },
  { "_id": 3, "status": 31 }
]);
```

Beispiel für eine Abfrage

```
db.items.find({ "status": { $bitsAnyClear: 8 } })
```

Ausgabe

```
{ "_id" : 1, "status" : 7 }
```

In diesem Beispiel sucht die Abfrage nach Dokumenten, in denen das `status` Feld Leerzeichen (0) in der Bitmaske 8 (binär`1000`) enthält. Das Dokument mit den `status` Werten 7 (binär`111`)

entspricht der Abfrage, da die angegebene Bitmaske mindestens ein Bit Clear enthält. Das passende Clear-Bit ist das viertniedrigstwertige Bit.

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$bitsAnyClear` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('items');

  const result = await collection.find({ "status": { $bitsAnyClear:
 8 } }).toArray();
  console.log(result);

  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client.test
    collection = db.items

    result = list(collection.find({ "status": { "$bitsAnyClear": 8 } }))
    print(result)
```

```
    client.close()

example()
```

$ Bits AnySet

Der `$bitsAnySet` Operator in Amazon DocumentDB wird verwendet, um Dokumente abzufragen, bei denen mindestens ein Bit in den angegebenen Bits in einem Feld auf 1 gesetzt ist. Dieser Operator ermöglicht es Ihnen, bitweise Operationen an den in Feldern gespeicherten Werten durchzuführen, was eine effiziente Abfrage und Analyse von Daten mit bitweisen Eigenschaften ermöglicht.

Parameter

- `field`: Der Feldname, auf den die bitweise Operation angewendet werden soll.
- `value`: Die numerische Bitmaske, die angibt, welche Bits geprüft werden sollen, oder eine Liste von Bitpositionen, die überprüft werden sollen. Eine numerische Bitmaske kann binär (0b...), dezimal, hexadezimal (0x...), oktal (0o...) oder binär () sein. BinData In einer Liste von Bitpositionen ist die Position des niedrigstwertigen Bits 0.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$bitsAnySet` Operator verwendet wird, um Dokumente zu finden, bei denen mindestens ein Bit im `flags` Feld gesetzt ist.

Erstellen Sie Beispieldokumente

```
db.collection.insertMany([
  { _id: 1, flags: 0b1010 },
  { _id: 2, flags: 0b1100 },
  { _id: 3, flags: 0b0011 },
  { _id: 4, flags: 0b0100 }
]);
```

Beispiel für eine Abfrage

```
db.collection.find({
  flags: { $bitsAnySet: 0b1010 }
```

```
})
```

Ausgabe

```
{ "_id" : 1, "flags" : 10 }
{ "_id" : 2, "flags" : 12 }
{ "_id" : 3, "flags" : 3 }
```

Die Abfrage gibt die Dokumente zurück, in denen mindestens eines der in der Bitmaske angegebenen Bits im `flags` Feld gesetzt `0b1010` ist.

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$bitsAnySet` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function main() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('collection');

  const result = await collection.find({
    flags: { $bitsAnySet: 0b1010 }
  }).toArray();

  console.log(result);

  await client.close();
}

main();
```

Python

```
from pymongo import MongoClient
```

```
client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
db = client['test']
collection = db['collection']

result = list(collection.find({
    'flags': { '$bitsAnySet': 0b1010 }
}))

print(result)

client.close()
```

$comment

Der `$comment` Operator in Amazon DocumentDB wird verwendet, um einen Kommentar an eine Abfrage anzuhängen. Dies kann nützlich sein, um zusätzlichen Kontext oder zusätzliche Informationen zur Abfrage bereitzustellen, was für Debugging- oder Dokumentationszwecke hilfreich sein kann. Der angehängte Kommentar wird als Teil der Ausgabe von Operationen wie db.currentOp () erscheinen.

Parameter

- `string`: Der Kommentar, der der Abfrage angehängt ist.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$comment` Operator in Amazon DocumentDB verwendet wird.

Erstellen Sie Beispieldokumente

```
db.users.insertMany([
  { name: "John Doe", age: 30, email: "john.doe@example.com" },
  { name: "Jane Smith", age: 25, email: "jane.smith@example.com" },
  { name: "Bob Johnson", age: 35, email: "bob.johnson@example.com" }
]);
```

Beispiel für eine Abfrage

```
db.users.find({ age: { $gt: 25 } }, { _id: 0, name: 1, age: 1 }).comment("Retrieve
 users older than 25");
```

Ausgabe

```
{ "name" : "John Doe", "age" : 30 }
{ "name" : "Bob Johnson", "age" : 35 }
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$comment` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function main() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const users = db.collection('users');

  const result = await users.find({ age: { $gt: 25 } }, { projection: { _id: 0,
 name: 1, age: 1 } })
                            .comment('Retrieve users older than 25')
                            .toArray();

  console.log(result);

  await client.close();
}

main();
```

Python

```
from pymongo import MongoClient

def main():
```

```
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client.test
    users = db.users

    result = list(users.find({ 'age': { '$gt': 25 }}, { '_id': 0, 'name': 1, 'age':
 1 })
                .comment('Retrieve users older than 25'))

    print(result)

    client.close()

if __name__ == '__main__':
    main()
```

$elemMatch

Der `$elemMatch` Operator in Amazon DocumentDB wird verwendet, um ein Array-Feld abzufragen und Dokumente zurückzugeben, bei denen mindestens ein Element im Array den angegebenen Kriterien entspricht. Dieser Operator ist besonders nützlich, wenn Sie komplexe Datenstrukturen mit verschachtelten Arrays oder eingebetteten Dokumenten haben.

Planner Version 2.0 fügte Indexunterstützung für hinzu. `$elemMatch`

Parameter

- `field`: Das abzufragende Array-Feld.
- `query`: Die Kriterien, die mit den Array-Elementen verglichen werden sollen.

Verwendung **`$elemMatch`** innerhalb eines **`$all`** Ausdrucks

Einschränkungen in Bezug auf die Verwendung des `$elemMatch` Operators innerhalb eines `$all` Ausdrucks finden `Verwenden von $elemMatch innerhalb eines $all-Ausdrucks` Sie unter.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$elemMatch` Operator verwendet wird, um Dokumente zu finden, bei denen das `parts` Array mindestens ein Element enthält, das den angegebenen Kriterien entspricht.

Erstellen Sie Beispieldokumente

```
db.col.insertMany([
  { _id: 1, parts: [{ part: "xyz", qty: 10 }, { part: "abc", qty: 20 }] },
  { _id: 2, parts: [{ part: "xyz", qty: 5 }, { part: "abc", qty: 10 }] },
  { _id: 3, parts: [{ part: "xyz", qty: 15 }, { part: "abc", qty: 100 }] },
  { _id: 4, parts: [{ part: "abc", qty: 150 }] }
]);
```

Beispiel für eine Abfrage

```
db.col.find({
  parts: { "$elemMatch": { part: "xyz", qty: { $lt: 11 } } }
})
```

Ausgabe

```
{ "_id" : 1, "parts" : [ { "part" : "xyz", "qty" : 10 }, { "part" : "abc", "qty" :
 20 } ] }
{ "_id" : 2, "parts" : [ { "part" : "xyz", "qty" : 5 }, { "part" : "abc", "qty" :
 10 } ] }
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$elemMatch` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
```

```
  const col = db.collection('col');

  const result = await col.find({
    parts: {
      "$elemMatch": { part: "xyz", qty: { $lt: 11 } }
    }
  }).toArray();

  console.log(JSON.stringify(result, null, 2));
  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    col = db['col']

    result = list(col.find({
      'parts': {
        '$elemMatch': {'part': 'xyz', 'qty': {'$lt': 11}}
      }
    }))

    print(result)
    client.close()

example()
```

$eq

Der `$eq` Operator in Amazon DocumentDB wird verwendet, um Dokumente abzugleichen, bei denen der Wert eines Felds dem angegebenen Wert entspricht. Dieser Operator wird häufig in der `find()` Methode zum Abrufen von Dokumenten verwendet, die die angegebenen Kriterien erfüllen.

Parameter

- `field`: Das Feld, das auf die Gleichheitsbedingung überprüft werden soll.
- `value`: Der Wert, der mit dem Feld verglichen werden soll.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der $eq Operator verwendet wird, um alle Dokumente zu finden, bei denen das name Feld gleich ist. `"Thai Curry Palace"`

Erstellen Sie Beispieldokumente

```
db.restaurants.insertMany([
  { name: "Thai Curry Palace", cuisine: "Thai", features: ["Private Dining"] },
  { name: "Italian Bistro", cuisine: "Italian", features: ["Outdoor Seating"] },
  { name: "Mexican Grill", cuisine: "Mexican", features: ["Takeout"] }
]);
```

Beispiel für eine Abfrage

```
db.restaurants.find({ name: { $eq: "Thai Curry Palace" } });
```

Ausgabe

```
{ "_id" : ObjectId("68ee586f916df9d39f3d9414"), "name" : "Thai Curry Palace",
 "cuisine" : "Thai", "features" : [ "Private Dining" ] }
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des $eq Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function findByName(name) {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
```

```
  const collection = db.collection('restaurants');

  const results = await collection.find({ name: { $eq: name } }).toArray();
  console.log(results);

  await client.close();
}

findByName("Thai Curry Palace");
```

Python

```
from pymongo import MongoClient

def find_by_name(name):
    client = MongoClient("mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false")
    db = client["test"]
    collection = db["restaurants"]

    results = list(collection.find({ "name": { "$eq": name } }))
    print(results)

    client.close()

find_by_name("Thai Curry Palace")
```

$exists

Der `$exists` Operator wird verwendet, um zu überprüfen, ob ein Feld in einem Dokument existiert oder nicht. `$exists`besonders nützlich bei der Arbeit mit Sparse-Indizes in Amazon DocumentDB, bei denen das indizierte Feld möglicherweise nicht in allen Dokumenten vorhanden ist.

Um einen Sparse-Index zu verwenden, den Sie in einer Abfrage erstellt haben, müssen Sie die `$exists`-Bedingungen für die Felder verwenden, die der Index abdecken. Wenn Sie es weglassen`$exists`, verwendet Amazon DocumentDB den Sparse-Index nicht für die Abfrage.

Parameter

- `field`: Der Feldname, dessen Existenz überprüft werden soll.

- `value`: Ein boolescher Wert (`true`oder`false`), der angibt, ob das Feld in den entsprechenden Dokumenten existieren (`true`) oder nicht existieren (`false`) soll.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt die Verwendung des `$exists` Operators mit einem spärlichen Index für das `special_diets` Feld in der `food` Sammlung.

Erstellen Sie Beispieldokumente

```
db.food.insertMany([
  { _id: 1, name: "Apple", special_diets: ["vegetarian", "gluten-free"] },
  { _id: 2, name: "Broccoli" },
  { _id: 3, name: "Chicken", special_diets: ["dairy-free"] }
]);
```

Erstellen Sie einen spärlichen Index für das Feld `special_diets`

```
db.food.createIndex({ "special_diets": 1 }, { sparse: true, name:
 "special_diets_sparse_asc" });
```

Beispiel für eine Abfrage

```
db.food.find({ "special_diets": { $exists: true } });
```

Ausgabe

```
[
  { "_id" : 1, "name" : "Apple", "special_diets" : [ "vegetarian", "gluten-free" ] },
  { "_id" : 3, "name" : "Chicken", "special_diets" : [ "dairy-free" ] }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$exists` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');
```

```
async function main() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('food');

  const result = await collection.find({ "special_diets": { $exists:
 true } }).toArray();
  console.log(result);

  await client.close();
}

main();
```

Python

```
import pymongo

client = pymongo.MongoClient('mongodb://<username>:<password>@<cluster-
endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
db = client['test']
collection = db['food']

result = list(collection.find({"special_diets": {"$exists": True}}))
print(result)

client.close()
```

$expr

Neu ab Version 4.0.

Wird von Elastic Cluster nicht unterstützt.

Der `$expr` Operator in Amazon DocumentDB ermöglicht es Ihnen, Aggregationsausdrücke innerhalb der Abfragesprache zu verwenden. Er ermöglicht es Ihnen, komplexe Vergleiche und Berechnungen für Felder innerhalb eines Dokuments durchzuführen, ähnlich wie Sie Aggregationspipeline-Phasen verwenden würden.

Parameter

- `expression`: Ein Ausdruck, der einen booleschen Wert zurückgibt, sodass Sie Vergleiche und Berechnungen für Dokumentfelder durchführen können.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$expr` Operator verwendet wird, um alle Dokumente zu finden, bei denen das `manufacturingCost` Feld größer als das `price` Feld ist.

Erstellen Sie Beispieldokumente

```
db.inventory.insertMany([
  { item: "abc", manufacturingCost: 500, price: 100 },
  { item: "def", manufacturingCost: 300, price: 450 },
  { item: "ghi", manufacturingCost: 400, price: 120 }
]);
```

Beispiel für eine Abfrage

```
db.inventory.find({
  $expr: {
    $gt: ["$manufacturingCost", "$price"]
  }
})
```

Ausgabe

```
{ "_id" : ObjectId("60b9d4d68d2cac581bc5a89a"), "item" : "abc", "manufacturingCost" :
 500, "price" : 100 },
{ "_id" : ObjectId("60b9d4d68d2cac581bc5a89c"), "item" : "ghi", "manufacturingCost" :
 400, "price" : 120 }
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$expr` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');
```

```
async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('inventory');

  const result = await collection.find({
    $expr: {
      $gt: ['$manufacturingCost', '$price']
    }
  }).toArray();

  console.log(result);
  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['inventory']

    result = list(collection.find({
        '$expr': {
            '$gt': ['$manufacturingCost', '$price']
        }
    }))

    print(result)
    client.close()

example()
```

$gt

Der `$gt` Operator in Amazon DocumentDB wird verwendet, um Dokumente auszuwählen, bei denen der Wert des angegebenen Felds größer als der angegebene Wert ist. Dieser Operator ist nützlich, um Daten auf der Grundlage numerischer Vergleiche zu filtern und abzufragen.

Parameter

- `field`: Das zu vergleichende Feld.
- `value`: Der Wert, mit dem verglichen werden soll.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$gt` Operator verwendet wird, um alle Dokumente zu finden, bei denen das `age` Feld größer als 30 ist.

Erstellen Sie Beispieldokumente

```
db.users.insertMany([
  { name: "John", age: 25 },
  { name: "Jane", age: 32 },
  { name: "Bob", age: 45 },
  { name: "Alice", age: 28 }
]);
```

Beispiel für eine Abfrage

```
db.users.find({ age: { $gt: 30 } });
```

Ausgabe

```
{ "_id" : ObjectId("6249e5c22a5d39884a0a0001"), "name" : "Jane", "age" : 32 },
{ "_id" : ObjectId("6249e5c22a5d39884a0a0002"), "name" : "Bob", "age" : 45 }
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$gt` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function findUsersOlderThan30() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const users = await db.collection('users').find({ age: { $gt: 30 } }).toArray();
  console.log(users);
  await client.close();
}

findUsersOlderThan30();
```

Python

```
from pymongo import MongoClient

def find_users_older_than_30():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client.test
    users = list(db.users.find({ 'age': { '$gt': 30 } }))
    print(users)
    client.close()

find_users_older_than_30()
```

$gte

Der `$gte` Operator in Amazon DocumentDB wird verwendet, um Werte abzugleichen, die größer oder gleich einem bestimmten Wert sind. Dieser Operator ist nützlich, um Daten auf der Grundlage numerischer Vergleiche zu filtern und abzufragen.

Parameter

- `field`: Das Feld, das mit dem angegebenen Wert verglichen werden soll.
- `value`: Der Wert, der mit dem Feld verglichen werden soll.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt die Verwendung des `$gte` Operators in Amazon DocumentDB, um alle Dokumente zu finden, bei denen das Feld „Alter“ größer oder gleich 25 ist.

Erstellen Sie Beispieldokumente

```
db.users.insertMany([
  { _id: 1, name: "John", age: 20 },
  { _id: 2, name: "Jane", age: 25 },
  { _id: 3, name: "Bob", age: 30 },
  { _id: 4, name: "Alice", age: 35 }
]);
```

Beispiel für eine Abfrage

```
db.users.find({ age: { $gte: 25 } }, { _id: 0, name: 1, age: 1 });
```

Ausgabe

```
{ "name" : "Jane", "age" : 25 }
{ "name" : "Bob", "age" : 30 }
{ "name" : "Alice", "age" : 35 }
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$gte` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function findUsersAboveAge(age) {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const users = db.collection('users');

  const result = await users.find({ age: { $gte: age } }, { projection: { _id: 0,
 name: 1, age: 1 } }).toArray();
```

```
  console.log(result);

  await client.close();
}

findUsersAboveAge(25);
```

Python

```
from pymongo import MongoClient

def find_users_above_age(age):
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client.test
    users = db.users

    result = list(users.find({ 'age': { '$gte': age } }, { '_id': 0, 'name': 1,
 'age': 1 }))
    print(result)

    client.close()

find_users_above_age(25)
```

$in

Der `$in` Operator in Amazon DocumentDB ist ein logischer Abfrageoperator, mit dem Sie Dokumente finden können, bei denen der Wert eines Felds einem der in einem Array angegebenen Werte entspricht.

Parameter

- `field`: Das Feld, das mit dem angegebenen Array verglichen werden soll.
- `[value1, value2, ...]`: Ein Array von Werten, die mit dem angegebenen Feld abgeglichen werden sollen.

Dollar (**$**) in Feldnamen

Einschränkungen Dollar ($) und Punkt (.) in Feldnamen bei der Abfrage von Feldern mit $ Präfix `$in` in verschachtelten Objekten finden Sie unter.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$in` Operator verwendet wird, um Dokumente zu finden, bei denen das `color` Feld einer der Werte im bereitgestellten Array ist.

Erstellen Sie Beispieldokumente

```
db.colors.insertMany([
  { "_id": 1, "color": "red" },
  { "_id": 2, "color": "green" },
  { "_id": 3, "color": "blue" },
  { "_id": 4, "color": "yellow" },
  { "_id": 5, "color": "purple" }
])
```

Beispiel für eine Abfrage

```
db.colors.find({ "color": { "$in": ["red", "blue", "purple"] } })
```

Ausgabe

```
{ "_id": 1, "color": "red" },
{ "_id": 3, "color": "blue" },
{ "_id": 5, "color": "purple" }
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$in` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function findByIn() {
```

```
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('colors');

  const result = await collection.find({ "color": { "$in": ["red", "blue",
 "purple"] } }).toArray();
  console.log(result);

  await client.close();
}

findByIn();
```

Python

```
from pymongo import MongoClient

def find_by_in():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client.test
    collection = db.colors

    result = list(collection.find({ "color": { "$in": ["red", "blue",
 "purple"] } }))
    print(result)

    client.close()

find_by_in()
```

$jsonSchema

Neu ab Version 4.0.

Wird von Elastic Cluster nicht unterstützt.

Der `$jsonSchema` Operator in Amazon DocumentDB wird verwendet, um Dokumente auf der Grundlage eines bestimmten JSON-Schemas zu filtern. Mit diesem Operator können Sie Dokumente

abfragen, die einem bestimmten JSON-Schema entsprechen, und so sicherstellen, dass die abgerufenen Dokumente bestimmten Struktur- und Datentypanforderungen entsprechen.

Wenn Sie den `$jsonSchema` Bewertungsabfrageoperator als Teil einer Sammlungserstellung verwenden, können Sie das Schema der Dokumente überprüfen, die in die Sammlung eingefügt werden. Verwenden der JSON-SchemavalidierungWeitere Informationen finden Sie unter.

Parameter

- `required`(Array): Gibt die erforderlichen Felder im Dokument an.
- `properties`(Objekt): Definiert den Datentyp und andere Einschränkungen für jedes Feld im Dokument.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$jsonSchema` Operator verwendet wird, um die `employees` Sammlung so zu filtern, dass nur Dokumente abgerufen werden`name`, die die `age` Felder `employeeId` und enthalten und das `employeeId` Feld vom Typ `string` ist.

Erstellen Sie Beispieldokumente

```
db.employees.insertMany([
  { "name": { "firstName": "Carol", "lastName": "Smith" }, "employeeId": "1" },
  { "name": { "firstName": "Emily", "lastName": "Brown" }, "employeeId": "2", "age":
 25 },
  { "name": { "firstName": "William", "lastName": "Taylor" }, "employeeId": 3, "age":
 24 },
  { "name": { "firstName": "Jane", "lastName": "Doe" }, "employeeId": "4" }
]);
```

Beispiel für eine Abfrage

```
db.employees.aggregate([
  { $match: {
    $jsonSchema: {
      required: ["name", "employeeId", "age"],
      properties: { "employeeId": { "bsonType": "string" } }
    }
  }}
]);
```

Ausgabe

```
{ "_id" : ObjectId("6908e8b61f77fc26b2ecd26f"), "name" : { "firstName" : "Emily",
 "lastName" : "Brown" }, "employeeId" : "2", "age" : 25 }
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$jsonSchema` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function filterByJsonSchema() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('employees');

  const result = await collection.aggregate([
    {
      $match: {
        $jsonSchema: {
          required: ['name', 'employeeId', 'age'],
          properties: { 'employeeId': { 'bsonType': 'string' } }
        }
      }
    }
  ]).toArray();

  console.log(result);
  await client.close();
}

filterByJsonSchema();
```

Python

```
from pymongo import MongoClient
```

```
def filter_by_json_schema():
  client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
  db = client['test']
  collection = db['employees']

  result = list(collection.aggregate([
    {
      '$match': {
        '$jsonSchema': {
          'required': ['name', 'employeeId', 'age'],
          'properties': {'employeeId': {'bsonType': 'string'}}
        }
      }
    }
  ]))

  print(result)
  client.close()

filter_by_json_schema()
```

$lt

Der `$lt` Operator in Amazon DocumentDB wird verwendet, um Werte abzugleichen, die unter dem angegebenen Wert liegen. Dieser Operator ist nützlich, um Daten auf der Grundlage numerischer Vergleiche zu filtern und abzufragen.

Parameter

- `field`: Der zu prüfende Feldname.
- `value`: Der Wert, mit dem verglichen werden soll.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$lt` Operator verwendet wird, um Dokumente abzurufen, deren `Inventory.0nHand` Wert kleiner als 50 ist.

Erstellen Sie Beispieldokumente

```
db.example.insertMany([
  { "_id": 1, "Inventory": { "OnHand": 25, "Sold": 60 }, "Colors": ["Red", "Blue"] },
  { "_id": 2, "Inventory": { "OnHand": 75, "Sold": 40 }, "Colors": ["Red", "White"] },
  { "_id": 3, "Inventory": { "OnHand": 10, "Sold": 85 }, "Colors": ["Red", "Green"] }
]);
```

Beispiel für eine Abfrage

```
db.example.find({ "Inventory.OnHand": { $lt: 50 } })
```

Ausgabe

```
{ "_id" : 1, "Inventory" : { "OnHand" : 25, "Sold" : 60 }, "Colors" : [ "Red",
 "Blue" ] }
{ "_id" : 3, "Inventory" : { "OnHand" : 10, "Sold" : 85 }, "Colors" : [ "Red",
 "Green" ] }
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$lt` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('example');

  const result = await collection.find({ "Inventory.OnHand": { $lt:
 50 } }).toArray();
  console.log(result);

  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['example']

    result = list(collection.find({ "Inventory.OnHand": { "$lt": 50 } }))
    print(result)

    client.close()

example()
```

$mod

Der $mod Abfrageoperator wählt Dokumente aus, in denen ein durch einen Divisor geteilter Feldwert einen angegebenen Rest hat. Dies ist nützlich, um Dokumente auf der Grundlage modularer arithmetischer Bedingungen zu filtern.

Parameter

- `divisor`: Die Zahl, durch die dividiert werden soll.
- `remainder`: Der erwartete Restwert.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der $mod Operator verwendet wird, um alle Bestellungen zu finden, bei denen die Menge eine ungerade Zahl ist.

Erstellen Sie Beispieldokumente

```
db.orders.insertMany([
  { _id: 1, item: "Widget", quantity: 15 },
  { _id: 2, item: "Gadget", quantity: 20 },
  { _id: 3, item: "Tool", quantity: 7 },
```

```
  { _id: 4, item: "Device", quantity: 12 },
  { _id: 5, item: "Part", quantity: 9 }
]);
```

Beispiel für eine Abfrage

```
db.orders.find({ quantity: { $mod: [2, 1] } });
```

Ausgabe

```
{ "_id" : 1, "item" : "Widget", "quantity" : 15 }
{ "_id" : 3, "item" : "Tool", "quantity" : 7 }
{ "_id" : 5, "item" : "Part", "quantity" : 9 }
```

Diese Abfrage gibt Dokumente zurück, bei denen die Menge geteilt durch 2 einen Rest von 1 hat, wodurch praktisch alle ungeraden Mengen ausgewählt werden.

Codebeispiele

Um ein Codebeispiel für die Verwendung des $mod Abfrageoperators anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('orders');

  const result = await collection.find({ quantity: { $mod: [2, 1] } }).toArray();

  console.log(JSON.stringify(result, null, 2));
  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['orders']

    result = list(collection.find({'quantity': {'$mod': [2, 1]}}))

    print(result)
    client.close()

example()
```

$lte

Der `$lte` Operator in Amazon DocumentDB wird verwendet, um Dokumente abzugleichen, bei denen der Wert eines angegebenen Felds kleiner oder gleich dem angegebenen Wert ist. Dieser Operator ist nützlich, um Daten auf der Grundlage numerischer Vergleiche zu filtern und abzufragen.

Parameter

- `field`: Das zu vergleichende Feld.
- `value`: Der Wert, mit dem verglichen werden soll.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt die Verwendung des `$lte` Operators zum Abrufen von Dokumenten, bei denen das `quantity` Feld kleiner oder gleich 10 ist.

Erstellen Sie Beispieldokumente

```
db.inventory.insertMany([
  { item: "canvas", qty: 100 },
  { item: "paint", qty: 50 },
```

```
  { item: "brush", qty: 10 },
  { item: "paper", qty: 5 }
]);
```

Beispiel für eine Abfrage

```
db.inventory.find({ qty: { $lte: 10 } });
```

Ausgabe

```
{ "_id" : ObjectId("..."), "item" : "brush", "qty" : 10 },
{ "_id" : ObjectId("..."), "item" : "paper", "qty" : 5 }
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$lte` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require("mongodb");

async function main() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db("test");
  const collection = db.collection("inventory");

  const result = await collection.find({ qty: { $lte: 10 } }).toArray();
  console.log(result);

  await client.close();
}

main();
```

Python

```
from pymongo import MongoClient
```

```
def main():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client["test"]
    collection = db["inventory"]

    result = list(collection.find({ "qty": { "$lte": 10 } }))
    print(result)

    client.close()

if __name__ == "__main__":
    main()
```

$meta

Der `$meta` Operator wird verwendet, um auf Metadaten zuzugreifen, die mit der aktuellen Abfrageausführung verknüpft sind. Dieser Operator wird hauptsächlich für Textsuchoperationen verwendet, bei denen die Metadaten Informationen über die Relevanz der übereinstimmenden Dokumente liefern können.

Parameter

- `textScore`: Ruft das Ergebnis der Textsuche für das Dokument ab. Diese Bewertung gibt die Relevanz des Dokuments für die Textsuchabfrage an.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$meta` Operator verwendet wird, um das Ergebnis der Textsuche für Dokumente abzurufen, die einer Textsuchabfrage entsprechen.

Erstellen Sie Beispieldokumente

```
db.documents.insertMany([
  { _id: 1, title: "Coffee Basics", content: "Coffee is a popular beverage made from
 roasted coffee beans." },
  { _id: 2, title: "Coffee Culture", content: "Coffee coffee coffee - the ultimate
 guide to coffee brewing and coffee preparation." },
```

```
  { _id: 3, title: "Tea vs Coffee", content: "Many people prefer tea over coffee for
 its health benefits." }
]);
```

Textindex erstellen

```
db.documents.createIndex({ content: "text" });
```

Beispiel für eine Abfrage

```
db.documents.find(
  { $text: { $search: "coffee" } },
  { _id: 0, title: 1, content: 1, score: { $meta: "textScore" } }
).sort({ score: { $meta: "textScore" } });
```

Ausgabe

```
[
  {
    title: 'Coffee Culture',
    content: 'Coffee coffee coffee - the ultimate guide to coffee brewing and coffee
 preparation.',
    score: 0.8897688388824463
  },
  {
    title: 'Coffee Basics',
    content: 'Coffee is a popular beverage made from roasted coffee beans.',
    score: 0.75990891456604
  },
  {
    title: 'Tea vs Coffee',
    content: 'Many people prefer tea over coffee for its health benefits.',
    score: 0.6079270839691162
  }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$meta` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function findWithTextScore() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('documents');

  const result = await collection.find(
    { $text: { $search: "coffee" } },
    { projection: { _id: 0, title: 1, content: 1, score: { $meta: "textScore" } } }
  ).sort({ score: { $meta: "textScore" } }).toArray();

  console.log(result);
  client.close();
}

findWithTextScore();
```

Python

```
from pymongo import MongoClient

client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
db = client['test']
collection = db['documents']

for doc in collection.find(
    {'$text': {'$search': 'coffee'}},
    {'_id': 0, 'title': 1, 'content': 1, 'score': {'$meta': 'textScore'}}
).sort([('score', {'$meta': 'textScore'})]):
    print(doc)

client.close()
```

$ne

Der `$ne` Operator wird verwendet, um Dokumente abzugleichen, bei denen der Wert eines Felds nicht dem angegebenen Wert entspricht. Es ist ein Vergleichsoperator, der in Abfrageprädikaten zum Filtern von Dokumenten verwendet werden kann.

Planner Version 2.0 hat Indexunterstützung für hinzugefügt. `$ne`

Parameter

- `field`: Das zu überprüfende Feld.
- `value`: Der Wert, gegen den geprüft werden soll.

Beispiel (MongoDB Shell)

In diesem Beispiel finden wir alle Dokumente in der `users` Sammlung, bei denen das `status` Feld ungleich ist. `"active"`

Erstellen Sie Beispieldokumente

```
db.users.insertMany([
  { name: "John", status: "active" },
  { name: "Jane", status: "inactive" },
  { name: "Bob", status: "suspended" },
  { name: "Alice", status: "active" }
]);
```

Beispiel für eine Abfrage

```
db.users.find({ status: { $ne: "active" } });
```

Ausgabe

```
[
  {
    _id: ObjectId('...'),
    name: 'Jane',
    status: 'inactive'
  },
```

```
  {
    _id: ObjectId('...'),
    name: 'Bob',
    status: 'suspended'
  }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des $ne Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function main() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const users = db.collection('users');

  const result = await users.find({ status: { $ne: 'active' } }).toArray();
  console.log(result);

  await client.close();
}

main();
```

Python

```
from pymongo import MongoClient

client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
db = client['test']
users = db['users']

result = list(users.find({ 'status': { '$ne': 'active' } }))
```

```
print(result)

client.close()
```

$nin

Der `$nin` Operator wird verwendet, um Werte abzugleichen, die sich nicht im angegebenen Array befinden. Es ist die Umkehrung des `$in` Operators, der mit Werten übereinstimmt, die sich im angegebenen Array befinden.

Planner Version 2.0 fügte Indexunterstützung für `$nin` hinzu.

Parameter

- `field`: Das zu überprüfende Feld.
- `array`: Das Array von Werten, anhand dessen geprüft werden soll.

Dollar (**$**) in Feldnamen

Einschränkungen Dollar ($) und Punkt (.) in Feldnamen bei der Abfrage von Feldern mit $ Präfix `$nin` in verschachtelten Objekten finden Sie unter.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$nin` Operator verwendet wird, um Dokumente zu finden, bei denen das `category` Feld nicht „Fiction“ oder „Mystery“ entspricht.

Erstellen Sie Beispieldokumente

```
db.books.insertMany([
  { title: "The Great Gatsby", author: "F. Scott Fitzgerald", category: "Fiction" },
  { title: "To Kill a Mockingbird", author: "Harper Lee", category: "Fiction" },
  { title: "The Girl on the Train", author: "Paula Hawkins", category: "Mystery" },
  { title: "The Martian", author: "Andy Weir", category: "Science Fiction" },
  { title: "The Alchemist", author: "Paulo Coelho", category: "Philosophy" }
])
```

Beispiel für eine Abfrage

```
db.books.find({
  category: {
    $nin: ["Fiction", "Mystery"]
  }
})
```

Ausgabe

```
[
  {
    _id: ObjectId('...'),
    title: 'The Martian',
    author: 'Andy Weir',
    category: 'Science Fiction'
  },
  {
    _id: ObjectId('...'),
    title: 'The Alchemist',
    author: 'Paulo Coelho',
    category: 'Philosophy'
  }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$nin` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function findBooksNotInCategories(categories) {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const books = await db.collection('books').find({
    category: {
      $nin: categories
```

```
    }
  }).toArray();
  console.log(books);
  client.close();
}

findBooksNotInCategories(['Fiction', 'Mystery']);
```

Python

```
from pymongo import MongoClient

def find_books_not_in_categories(categories):
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    books = list(db.books.find({
        'category': {
            '$nin': categories
        }
    }))
    print(books)
    client.close()

find_books_not_in_categories(['Fiction', 'Mystery'])
```

$nor

Der `$nor` Operator wird verwendet, um Dokumente abzugleichen, bei denen keine der angegebenen Abfragebedingungen zutrifft. Er ähnelt der logischen Operation „NOR“, bei der das Ergebnis wahr ist, wenn keiner der Operanden wahr ist.

Parameter

- `expression1`: Der erste Ausdruck, der ausgewertet werden soll.
- `expression2`: Der zweite auszuwertende Ausdruck.
- `expressionN`: Zusätzliche auszuwertende Ausdrücke.

Beispiel (MongoDB Shell)

Das folgende Beispiel demonstriert die Verwendung des `$nor` Operators, indem Dokumente abgerufen werden, bei denen das `qty` Feld nicht weniger als 20 ist und das `size` Feld nicht „XL“ entspricht.

Erstellen Sie Beispieldokumente

```
db.items.insertMany([
  { qty: 10, size: "M" },
  { qty: 15, size: "XL" },
  { qty: 25, size: "L" },
  { qty: 30, size: "XL" }
])
```

Beispiel für eine Abfrage

```
db.items.find({
  $nor: [
    { qty: { $lt: 20 } },
    { size: "XL" }
  ]
})
```

Ausgabe

```
[
  { "_id" : ObjectId("..."), "qty" : 25, "size" : "L" }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$nor` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
```

```
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('items');

  const result = await collection.find({
    $nor: [
      { qty: { $lt: 20 } },
      { size: "XL" }
    ]
  }).toArray();

  console.log(result);

  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['items']

    result = list(collection.find({
        '$nor': [
            { 'qty': { '$lt': 20 } },
            { 'size': 'XL' }
        ]
    }))

    print(result)

    client.close()

example()
```

$not

Der `$not` Operator wird verwendet, um das Ergebnis eines bestimmten Ausdrucks zu negieren. Damit können Sie Dokumente auswählen, bei denen die angegebene Bedingung nicht erfüllt ist.

Planner Version 2.0 hat Indexunterstützung für `$not {eq}` und hinzugefügt`$not {in}`.

Parameter

- `expression`: Der Ausdruck, der negiert werden soll.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$not` Operator verwendet wird, um Dokumente zu finden, bei denen das `status` Feld nicht „aktiv“ entspricht.

Erstellen Sie Beispieldokumente

```
db.users.insertMany([
  { name: "John", status: "active" },
  { name: "Jane", status: "inactive" },
  { name: "Bob", status: "pending" },
  { name: "Alice", status: "active" }
]);
```

Beispiel für eine Abfrage

```
db.users.find({ status: { $not: { $eq: "active" } } });
```

Ausgabe

```
[
  {
    _id: ObjectId('...'),
    name: 'Jane',
    status: 'inactive'
  },
  {
    _id: ObjectId('...'),
    name: 'Bob',
    status: 'pending'
```

```
  }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des $not Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient, Filters } = require('mongodb');

async function main() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('users');

  const result = await collection.find({
    status: { $not: { $eq: "active" } }
  }).toArray();

  console.log(result);

  await client.close();
}

main();
```

Python

```
from pymongo import MongoClient
from bson.son import SON

client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
db = client['test']
collection = db['users']

result = collection.find({
    "status": {"$not": {"$eq": "active"}}
```

```
})

for doc in result:
    print(doc)

client.close()
```

$or

Der `$or` Operator wird verwendet, um eine logische ODER-Operation für ein Array von zwei oder mehr Ausdrücken auszuführen. Er gibt Dokumente zurück, die mindestens einem der Ausdrücke entsprechen. Dieser Operator ist nützlich, wenn Sie nach Dokumenten abfragen müssen, die eine von mehreren Bedingungen erfüllen.

Parameter

- `expression1`: Der erste Ausdruck, der ausgewertet werden soll.
- `expression2`: Der zweite auszuwertende Ausdruck.
- `...`: Zusätzliche auszuwertende Ausdrücke (optional).

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$or` Operator verwendet `make` wird, um Dokumente zu finden, bei denen der entweder "TruckForYou" beim Modell „Heavy H1" oder" SportForYou "beim Modell „Bolid 1" ist.

Erstellen Sie Beispieldokumente

```
db.cars.insertMany([
  { make: "TruckForYou", model: "Heavy H1", year: 2020 },
  { make: "SportForYou", model: "Bolid 1", year: 2021 },
  { make: "TruckForYou", model: "Cargo 5", year: 2019 },
  { make: "SportForYou", model: "Racer 2", year: 2022 }
]);
```

Beispiel für eine Abfrage

```
db.cars.find({
  $or: [
```

```
    { make: "TruckForYou", model: "Heavy H1" },
    { make: "SportForYou", model: "Bolid 1" }
  ]
});
```

Ausgabe

```
[
  {
    _id: ObjectId('...'),
    make: 'TruckForYou',
    model: 'Heavy H1',
    year: 2020
  },
  {
    _id: ObjectId('...'),
    make: 'SportForYou',
    model: 'Bolid 1',
    year: 2021
  }
]
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$or` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function findCarsByMakeModel() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const cars = db.collection('cars');

  const result = await cars.find({
    $or: [
      { make: "TruckForYou", model: "Heavy H1" },
      { make: "SportForYou", model: "Bolid 1" }
    ]
```

```
  }).toArray();

  console.log(result);
  client.close();
}

findCarsByMakeModel();
```

Python

```
from pymongo import MongoClient

def find_cars_by_make_model():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    cars = db.cars

    result = list(cars.find({
        '$or': [
            {'make': 'TruckForYou', 'model': 'Heavy H1'},
            {'make': 'SportForYou', 'model': 'Bolid 1'}
        ]
    }))

    print(result)
    client.close()

find_cars_by_make_model()
```

$regex

Mit dem `$regex` Operator können Sie einen Abgleich mit regulären Ausdrücken für Zeichenkettenfelder durchführen. Es ist ein leistungsstarkes Tool zum Suchen und Filtern von Dokumenten, die auf komplexen Mustern basieren.

Parameter

- `regular expression`: Das reguläre Ausdrucksmuster, das mit dem Feld abgeglichen werden soll.

- `$options`: (optional) Stellt Optionen zur Änderung des Suchverhaltens bereit, z. B. Berücksichtigung von Groß- und Kleinschreibung, globaler Abgleich usw.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$regex` Operator verwendet wird, um nach Dokumenten zu suchen, bei denen das Feld „Name“ einem bestimmten Muster entspricht.

Erstellen Sie Beispieldokumente

```
db.users.insertMany([
  { name: "John Doe" },
  { name: "Jane Smith" },
  { name: "Alice Johnson" },
  { name: "Bob Williams" },
  { name: "Charlie Davis" }
]);
```

Beispiel für eine Abfrage

```
db.users.find({ name: { $regex: /^A/ } })
```

Ausgabe

```
[
  { "_id" : ObjectId("..."), "name" : "Alice Johnson" }
]
```

Diese Abfrage gibt alle Dokumente zurück, bei denen das Feld „Name“ mit dem Buchstaben „A“ beginnt.

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$regex` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');
```

```
async function main() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('users');

  const results = await collection.find({ name: { $regex: /^A/ } }).toArray();
  console.log(results);

  await client.close();
}

main();
```

Python

```
from pymongo import MongoClient

def main():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['users']

    results = list(collection.find({ 'name': { '$regex': '^A' } }))
    print(results)

    client.close()

if __name__ == "__main__":
    main()
```

$slice

Der `$slice` Projektionsoperator begrenzt die Anzahl der Array-Elemente, die in einem Abfrageergebnis zurückgegeben werden. Er ermöglicht es Ihnen, eine bestimmte Anzahl von Elementen vom Anfang oder Ende eines Array-Felds abzurufen, ohne das gesamte Array zu laden.

Parameter

- `field`: Das zu projizierende Array-Feld.
- `count`: Anzahl der zurückzugebenden Elemente. Positive Werte geben Elemente vom Anfang zurück, negative Werte vom Ende.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$slice` Projektionsoperator verwendet wird, um nur die ersten beiden Elemente aus einem Array-Feld zurückzugeben.

Erstellen Sie Beispieldokumente

```
db.inventory.insertMany([
  { _id: 1, item: "notebook", tags: ["office", "school", "supplies", "writing"] },
  { _id: 2, item: "pen", tags: ["office", "writing"] },
  { _id: 3, item: "folder", tags: ["office", "supplies", "storage", "organization"] }
]);
```

Beispiel für eine Abfrage

```
db.inventory.find(
  {},
  { item: 1, tags: { $slice: 2 } }
)
```

Ausgabe

```
{ "_id" : 1, "item" : "notebook", "tags" : [ "office", "school" ] }
{ "_id" : 2, "item" : "pen", "tags" : [ "office", "writing" ] }
{ "_id" : 3, "item" : "folder", "tags" : [ "office", "supplies" ] }
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$slice` Projektionsoperators anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
```

```
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('inventory');

  const result = await collection.find(
    {},
    { projection: { item: 1, tags: { $slice: 2 } } }
  ).toArray();

  console.log(JSON.stringify(result, null, 2));
  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['inventory']

    result = list(collection.find(
        {},
        {'item': 1, 'tags': {'$slice': 2}}
    ))

    print(result)
    client.close()

example()
```

$size

Der `$size` Abfrageoperator sucht nach Dokumenten, in denen ein Array-Feld genau die angegebene Anzahl von Elementen hat. Dies ist nützlich, um Dokumente anhand der Array-Länge zu filtern.

Parameter

- `field`: Das zu prüfende Array-Feld.
- `count`: Die genaue Anzahl der Elemente, die das Array enthalten muss.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$size` Operator verwendet wird, um alle Produkte zu finden, die genau drei Tags haben.

Erstellen Sie Beispieldokumente

```
db.products.insertMany([
  { _id: 1, name: "Laptop", tags: ["electronics", "computers", "portable"] },
  { _id: 2, name: "Mouse", tags: ["electronics", "accessories"] },
  { _id: 3, name: "Desk", tags: ["furniture", "office", "workspace"] },
  { _id: 4, name: "Monitor", tags: ["electronics"] }
]);
```

Beispiel für eine Abfrage

```
db.products.find({ tags: { $size: 3 } });
```

Ausgabe

```
{ "_id" : 1, "name" : "Laptop", "tags" : [ "electronics", "computers", "portable" ] }
{ "_id" : 3, "name" : "Desk", "tags" : [ "furniture", "office", "workspace" ] }
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$size` Abfrageoperators anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
```

```
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('products');

  const result = await collection.find({ tags: { $size: 3 } }).toArray();

  console.log(JSON.stringify(result, null, 2));
  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['products']

    result = list(collection.find({'tags': {'$size': 3}}))

    print(result)
    client.close()

example()
```

$text

Der `$text` Operator wird verwendet, um eine Volltextsuche in textindizierten Feldern innerhalb einer Dokumentensammlung durchzuführen. Mit diesem Operator können Sie nach Dokumenten suchen, die bestimmte Wörter oder Ausdrücke enthalten. Er kann mit anderen Abfrageoperatoren kombiniert werden, um Ergebnisse anhand zusätzlicher Kriterien zu filtern.

Parameter

- `$search`: Die Textzeichenfolge, nach der gesucht werden soll.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$text` Operator verwendet wird, um nach Dokumenten zu suchen, die das Wort „Interesse“ enthalten, und die Ergebnisse anhand eines Felds „star_rating“ zu filtern.

Erstellen Sie Beispieldokumente

```
db.test.insertMany([
  { "_id": 1, "star_rating": 4, "comments": "apple is red" },
  { "_id": 2, "star_rating": 5, "comments": "pie is delicious" },
  { "_id": 3, "star_rating": 3, "comments": "apples, oranges - healthy fruit" },
  { "_id": 4, "star_rating": 2, "comments": "bake the apple pie in the oven" },
  { "_id": 5, "star_rating": 5, "comments": "interesting couch" },
  { "_id": 6, "star_rating": 5, "comments": "interested in couch for sale, year 2022" }
]);
```

Textindex erstellen

```
db.test.createIndex({ comments: "text" });
```

Beispiel für eine Abfrage

```
db.test.find({$and: [{star_rating: 5}, {$text: {$search: "interest"}}]})
```

Ausgabe

```
{ "_id" : 5, "star_rating" : 5, "comments" : "interesting couch" }
{ "_id" : 6, "star_rating" : 5, "comments" : "interested in couch for sale, year
 2022" }
```

Der obige Befehl gibt Dokumente mit einem textindizierten Feld zurück, das eine beliebige Form von „Interesse“ und ein „Star_Rating“ gleich 5 enthält.

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$text` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function searchDocuments() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('test');

  const result = await collection.find({
    $and: [
      { star_rating: 5 },
      { $text: { $search: 'interest' } }
    ]
  }).toArray();

  console.log(result);
  client.close();
}

searchDocuments();
```

Python

```
from pymongo import MongoClient

def search_documents():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db.test

    result = list(collection.find({
        '$and': [
            {'star_rating': 5},
            {'$text': {'$search': 'interest'}}
        ]
    }))

    print(result)
```

```
    client.close()

search_documents()
```

$type

Der `$type` Operator wird verwendet, um den Datentyp eines Felds in einem Dokument zu überprüfen. Er kann verwendet werden, wenn typspezifische Operationen oder Validierungen erforderlich sind. Der `$type` Operator gibt den BSON-Typ des ausgewerteten Ausdrucks zurück. Der zurückgegebene Typ ist eine Zeichenfolge, die dem Typ des Felds oder Ausdrucks entspricht.

Planner Version 2.0 fügte Indexunterstützung für hinzu`$type`.

Parameter

- `expression`: Der auszuwertende Ausdruck.

Beispiel (MongoDB Shell)

Erstellen Sie Beispieldokumente

```
db.documents.insertMany([
  { _id: 1, name: "John", age: 30, email: "john@example.com" },
  { _id: 2, name: "Jane", age: "25", email: 123456 },
  { _id: 3, name: 123, age: true, email: null }
]);
```

Beispiel für eine Abfrage

```
db.documents.find({
  $or: [
    { age: { $type: "number" } },
    { email: { $type: "string" } },
    { name: { $type: "string" } }
  ]
})
```

Ausgabe

```
[
```

```
  { "_id": 1, "name": "John", "age": 30, "email": "john@example.com" },
  { "_id": 2, "name": "Jane", "age": "25", "email": 123456 }
]
```

Diese Abfrage gibt die Dokumente zurück, in denen das `age` Feld vom Typ „Zahl“, das `email` Feld vom Typ „Zeichenfolge“ und das `name` Feld vom Typ „Zeichenfolge“ ist.

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$type` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function findByType() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('documents');

  const results = await collection.find({
    $or: [
      { age: { $type: 'number' } },
      { email: { $type: 'string' } },
      { name: { $type: 'string' } }
    ]
  }).toArray();

  console.log(results);
  client.close();
}

findByType();
```

Python

```
from pymongo import MongoClient

def find_by_type():
```

```
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['documents']

    results = list(collection.find({
        '$or': [
            {'age': {'$type': 'number'}},
            {'email': {'$type': 'string'}},
            {'name': {'$type': 'string'}}
        ]
    }))

    print(results)
    client.close()

find_by_type()
```

Operatoren aktualisieren

Dieser Abschnitt enthält detaillierte Informationen zu Aktualisierungsoperatoren, die von Amazon DocumentDB unterstützt werden.

Themen

- $
- $[]
- $ [<Kennung>]
- $ hinzufügen ToSet
- $bit
- $currentDate
- $each
- $inc
- $max
- $min
- $mul

- $pop
- $position
- $pull
- $pullAll
- $push
- $rename
- $set
- $ gesetzt OnInsert
- $slice
- $sort
- $unset

$

Der $ Positionsoperator aktualisiert das erste Array-Element, das der Abfragebedingung entspricht. Er dient als Platzhalter für die Position des übereinstimmenden Array-Elements.

Parameter

- `field.$`: Das Array-Feld mit dem Positionsoperator zur Aktualisierung des ersten passenden Elements.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der $ Positionsoperator verwendet wird, um ein bestimmtes Array-Element zu aktualisieren.

Erstellen Sie Beispieldokumente

```
db.inventory.insertMany([
  { _id: 1, item: "Widget", quantities: [10, 20, 30] },
  { _id: 2, item: "Gadget", quantities: [5, 15, 25] }
]);
```

Beispiel für eine Abfrage

```
db.inventory.updateOne(
  { _id: 1, quantities: 20 },
  { $set: { "quantities.$": 22 } }
);
```

Ausgabe

```
{
  "_id" : 1,
  "item" : "Widget",
  "quantities" : [ 10, 22, 30 ]
}
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des $ Positionsoperators anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function updateDocument() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('inventory');

  await collection.updateOne(
    { _id: 1, quantities: 20 },
    { $set: { "quantities.$": 22 } }
  );

  const updatedDocument = await collection.findOne({ _id: 1 });
  console.log(updatedDocument);

  await client.close();
}

updateDocument();
```

Python

```
from pymongo import MongoClient

def update_document():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client.test
    collection = db.inventory

    collection.update_one(
        {'_id': 1, 'quantities': 20},
        {'$set': {'quantities.$': 22}}
    )

    updated_document = collection.find_one({'_id': 1})
    print(updated_document)

    client.close()

update_document()
```

$[]

Der `$[]` All-Position-Operator aktualisiert alle Elemente in einem Array. Er wird verwendet, wenn Sie jedes Element in einem Array-Feld ändern müssen.

Parameter

- `field.$[]`: Das Array-Feld mit dem All-Position-Operator zur Aktualisierung aller Elemente.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$[]` Operator verwendet wird, um alle Array-Elemente zu aktualisieren.

Erstellen Sie Beispieldokumente

```
db.products.insertOne({
```

```
  _id: 1,
  name: "Laptop",
  prices: [1000, 1100, 1200]
});
```

Beispiel für eine Abfrage

```
db.products.updateOne(
  { _id: 1 },
  { $inc: { "prices.$[]": 50 } }
);
```

Ausgabe

```
{
  "_id" : 1,
  "name" : "Laptop",
  "prices" : [ 1050, 1150, 1250 ]
}
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$[]` Operators anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function updateDocument() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('products');

  await collection.updateOne(
    { _id: 1 },
    { $inc: { "prices.$[]": 50 } }
  );

  const updatedDocument = await collection.findOne({ _id: 1 });
```

```
  console.log(updatedDocument);

  await client.close();
}

updateDocument();
```

Python

```
from pymongo import MongoClient

def update_document():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client.test
    collection = db.products

    collection.update_one(
        {'_id': 1},
        {'$inc': {'prices.$[]': 50}}
    )

    updated_document = collection.find_one({'_id': 1})
    print(updated_document)

    client.close()

update_document()
```

$ [<Kennung>]

Der `$[<identifier>]` gefilterte Positionsoperator aktualisiert alle Array-Elemente, die den angegebenen Filterbedingungen entsprechen. Er wird mit der `arrayFilters` Option verwendet, Array-Elemente selektiv zu aktualisieren.

Parameter

- `field.$[identifier]`: Das Array-Feld mit dem gefilterten Positionsoperator.
- `arrayFilters`: Eine Reihe von Filterbedingungen, die bestimmen, welche Elemente aktualisiert werden sollen.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$[<identifier>]` Operator verwendet wird, um bestimmte Array-Elemente auf der Grundlage einer Bedingung zu aktualisieren.

Erstellen Sie Beispieldokumente

```
db.students.insertOne({
  _id: 1,
  name: "Alice",
  grades: [
    { subject: "Math", score: 85 },
    { subject: "Science", score: 92 },
    { subject: "History", score: 78 }
  ]
});
```

Beispiel für eine Abfrage

```
db.students.updateOne(
  { _id: 1 },
  { $inc: { "grades.$[elem].score": 5 } },
  { arrayFilters: [{ "elem.score": { $gte: 80 } }] }
);
```

Ausgabe

```
{
  "_id" : 1,
  "name" : "Alice",
  "grades" : [
    { "subject" : "Math", "score" : 90 },
    { "subject" : "Science", "score" : 97 },
    { "subject" : "History", "score" : 78 }
  ]
}
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$[<identifier>]` Operators anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function updateDocument() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('students');

  await collection.updateOne(
    { _id: 1 },
    { $inc: { "grades.$[elem].score": 5 } },
    { arrayFilters: [{ "elem.score": { $gte: 80 } }] }
  );

  const updatedDocument = await collection.findOne({ _id: 1 });
  console.log(updatedDocument);

  await client.close();
}

updateDocument();
```

Python

```
from pymongo import MongoClient

def update_document():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client.test
    collection = db.students

    collection.update_one(
        {'_id': 1},
        {'$inc': {'grades.$[elem].score': 5}},
        array_filters=[{'elem.score': {'$gte': 80}}]
    )

    updated_document = collection.find_one({'_id': 1})
```

```
    print(updated_document)

    client.close()

update_document()
```

$ hinzufügen ToSet

Der `$addToSet` Operator in Amazon DocumentDB wird nur verwendet, um einem Array einen Wert hinzuzufügen, wenn der Wert nicht bereits im Array vorhanden ist. Dies ist nützlich, um sicherzustellen, dass ein Array eindeutige Elemente enthält.

Parameter

- `field`: Das zu aktualisierende Feld.
- `value`: Der Wert, der dem Array-Feld hinzugefügt werden soll. Dies kann ein einzelner Wert oder ein Ausdruck sein.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$addToSet` Operator verwendet wird, um einem Array eindeutige Elemente hinzuzufügen.

Erstellen Sie Beispieldokumente

```
db.products.insertMany([
  { "_id": 1, "item": "apple", "tags": ["fruit", "red", "round"] },
  { "_id": 2, "item": "banana", "tags": ["fruit", "yellow"] },
  { "_id": 3, "item": "cherry", "tags": ["fruit", "red"] }
])
```

Beispiel für eine Abfrage

```
db.products.update(
  { "item": "apple" },
  { $addToSet: { "tags": "green" } }
)
```

Ausgabe

```
{ "_id": 1, "item": "apple", "tags": ["fruit", "red", "round", "green"] }
```

In diesem Beispiel fügt der `$addToSet` Operator das Tag „green“ zum Array „tags“ des Dokuments hinzu, wobei das Feld „item“ den Wert „apple“ hat. Da „grün“ noch nicht im Array enthalten war, wurde es hinzugefügt.

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$addToSet` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('products');

  await collection.updateOne(
    { "item": "apple" },
    { $addToSet: { "tags": "green" } }
  );

  const updatedDoc = await collection.findOne({ "item": "apple" });
  console.log(updatedDoc);

  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
```

```
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client.test
    collection = db.products

    collection.update_one(
        {"item": "apple"},
        {"$addToSet": {"tags": "green"}}
    )

    updated_doc = collection.find_one({"item": "apple"})
    print(updated_doc)

    client.close()

example()
```

$bit

Der `$bit` Operator in Amazon DocumentDB ermöglicht es Ihnen, bitweise Operationen an den Bits eines bestimmten Feldes durchzuführen. Dies kann für Aufgaben wie das Setzen, Löschen oder Überprüfen des Zustands einzelner Bits innerhalb einer Zahl nützlich sein.

Parameter

- `field`: Das Feld, in dem bitweise Operationen ausgeführt werden sollen.
- `and`: Ein ganzzahliger Wert, der verwendet wird, um eine bitweise UND-Operation für das Feld durchzuführen.
- `or`: Ein ganzzahliger Wert, der verwendet wird, um eine bitweise OR-Operation für das Feld durchzuführen.
- `xor`: Ein ganzzahliger Wert, der verwendet wird, um eine bitweise XOR-Operation für das Feld durchzuführen.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$bit` Operator verwendet wird, um bitweise Operationen an einem numerischen Feld durchzuführen.

Erstellen Sie Beispieldokumente

```
db.numbers.insert([
  { "_id": 1, "number": 5 },
  { "_id": 2, "number": 12 }
])
```

Beispiel für eine Abfrage

```
db.numbers.update(
  { "_id": 1 },
  { "$bit": { "number": { "and": 3 } } }
)
```

Ausgabe

```
{
  "_id": 1,
  "number": 1
}
```

In diesem Beispiel wird der `$bit` Operator verwendet, um eine bitweise UND-Operation für das Feld „Zahl“ des Dokuments mit dem `_id` Wert 1 durchzuführen. Das Ergebnis ist, dass der Wert des Felds „Zahl“ auf 1 gesetzt wird, was das Ergebnis der bitweisen UND-Operation zwischen dem ursprünglichen Wert 5 und dem Wert 3 ist.

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$bit` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function main() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
```

```
  const collection = db.collection('numbers');

  await collection.updateOne(
    { "_id": 1 },
    { "$bit": { "number": { "and": 3 } } }
  );

  const result = await collection.findOne({ "_id": 1 });
  console.log(result);

  await client.close();
}

main();
```

Python

```
from pymongo import MongoClient

client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
db = client['test']
collection = db['numbers']

collection.update_one(
    {"_id": 1},
    {"$bit": {"number": {"and": 3}}}
)

result = collection.find_one({"_id": 1})
print(result)

client.close()
```

$currentDate

Der `$currentDate` Operator wird verwendet, um den Wert eines Felds auf das aktuelle Datum und die aktuelle Uhrzeit festzulegen. Dieser Operator ist nützlich, um ein Feld automatisch mit dem aktuellen Zeitstempel zu aktualisieren, wenn ein Dokument eingefügt oder aktualisiert wird.

Parameter

- `field`: Das Feld, das mit dem aktuellen Datum und der aktuellen Uhrzeit aktualisiert werden soll.
- `type`: (optional) Gibt den BSON-Typ an, der für das aktuelle Datum verwendet werden soll. Kann `date` oder `timestamp` sein.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$currentDate` Operator verwendet wird, um das `lastModified` Feld auf das aktuelle Datum und die aktuelle Uhrzeit einzustellen, wenn ein neues Dokument eingefügt wird.

Erstellen Sie Beispieldokumente

```
db.users.insert({
  name: "John Doe",
  email: "john.doe@example.com"
})
```

Beispiel für eine Abfrage

```
db.users.updateOne(
  { name: "John Doe" },
  { $currentDate: { lastModified: true } }
)
```

Aktualisiertes Dokument anzeigen

```
db.users.findOne({ name: "John Doe" })
```

Ausgabe

```
{
  _id: ObjectId('...'),
  name: 'John Doe',
  email: 'john.doe@example.com',
  lastModified: ISODate('2025-10-25T22:50:29.963Z')
}
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$currentDate` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function updateUserWithCurrentDate() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const users = db.collection('users');

  await users.updateOne(
    { name: 'John Doe' },
    { $currentDate: { lastModified: true } }
  );

  console.log('User updated with current date');
  client.close();
}

updateUserWithCurrentDate();
```

Python

```
from pymongo import MongoClient

def update_user_with_current_date():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    users = db.users

    result = users.update_one(
        {'name': 'John Doe'},
        {'$currentDate': {'lastModified': True}}
    )
```

```
    print('User updated with current date')
    client.close()

update_user_with_current_date()
```

$each

Der `$each` Operator wird in Verbindung mit anderen Aktualisierungsoperatoren wie `$push` und verwendet`$addToSet`, um einem Array-Feld mehrere Werte hinzuzufügen. Es ermöglicht das Hinzufügen mehrerer Elemente zu einem Array in einem einzigen Vorgang, anstatt mehrere Aktualisierungsvorgänge ausführen zu müssen.

Parameter

- `value`: Das Array von Werten, die dem Array-Feld hinzugefügt werden sollen.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$each` Operator zusammen mit dem `$push` Operator verwendet wird, um einem Array-Feld mehrere Elemente hinzuzufügen.

Erstellen Sie Beispieldokumente

```
db.fruits.insertOne({
  _id: 1,
  fruits: ["apple", "banana"]
})
```

Beispiel für eine Abfrage

```
db.fruits.updateOne(
  { _id: 1 },
  { $push: { fruits: { $each: ["cherry", "durian", "elderberry"] } } }
)
```

Aktualisiertes Dokument anzeigen

```
db.fruits.findOne({ _id: 1 })
```

Ausgabe

```
{
  _id: 1,
  fruits: [ 'apple', 'banana', 'cherry', 'durian', 'elderberry' ]
}
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$each` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('fruits');

  await collection.updateOne(
    { _id: 1 },
    { $push: { fruits: { $each: ["cherry", "durian", "elderberry"] } } }
  );

  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
```

```
    collection = db['fruits']

    collection.update_one(
        {'_id': 1},
        {'$push': {'fruits': {'$each': ['cherry', 'durian', 'elderberry']}}}
    )

    client.close()

example()
```

$inc

Der `$inc` Operator wird verwendet, um den Wert eines Felds um einen bestimmten Betrag zu erhöhen. Er wird verwendet, um ein numerisches Feld, z. B. einen Zähler oder eine Bewertung, zu aktualisieren, ohne dass der aktuelle Wert abgerufen, der neue Wert berechnet und das Feld anschließend aktualisiert werden muss.

Parameter

- `field`: Der Name des Feldes, das erhöht werden soll.
- `amount`: Der Betrag, um den das Feld erhöht werden soll. Dies kann ein positiver oder negativer Wert sein.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$inc` Operator verwendet wird, um das `age` Feld eines Dokuments zu erhöhen.

Erstellen Sie Beispieldokumente

```
db.users.insertOne({_id: 123, name: "John Doe", age: 30})
```

Beispiel für eine Abfrage

```
db.users.updateOne({_id: 123}, {$inc: {age: 1}})
```

Aktualisiertes Dokument anzeigen

```
db.users.findOne({_id: 123})
```

Ausgabe

```
{ "_id" : 123, "name" : "John Doe", "age" : 31 }
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$inc` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function updateWithInc() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('users');

  const result = await collection.updateOne(
    { _id: 123 },
    { $inc: { age: 1 } }
  );

  console.log(result);

  await client.close();
}

updateWithInc();
```

Python

```
from pymongo import MongoClient

def update_with_inc():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
```

```
    db = client['test']
    collection = db['users']

    result = collection.update_one(
        {'_id': 123},
        {'$inc': {'age': 1}}
    )

    print(result.modified_count)

    client.close()

update_with_inc()
```

$max

Der `$max` Aktualisierungsoperator aktualisiert den Wert eines Felds nur, wenn der angegebene Wert größer als der aktuelle Feldwert ist. Dieser Operator ist nützlich, um Maximalwerte bei Aktualisierungen beizubehalten.

Parameter

- `field`: Das zu aktualisierende Feld.
- `value`: Der Wert, der mit dem aktuellen Feldwert verglichen werden soll.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$max` Operator verwendet wird, um die höchste aufgezeichnete Punktzahl für einen Spieler zu aktualisieren.

Erstellen Sie Beispieldokumente

```
db.scores.insertMany([
  { _id: 1, player: "Alice", highScore: 85 },
  { _id: 2, player: "Bob", highScore: 92 },
  { _id: 3, player: "Charlie", highScore: 78 }
])
```

Beispiel aktualisieren

```
db.scores.updateOne(
  { _id: 1 },
  { $max: { highScore: 95 } }
)
```

Ergebnis

Das `highScore` Feld für Alice wird auf 95 aktualisiert, weil 95 größer als der aktuelle Wert von 85 ist.

```
{ "_id": 1, "player": "Alice", "highScore": 95 }
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$max` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('scores');

  const result = await collection.updateOne(
    { _id: 1 },
    { $max: { highScore: 95 } }
  );

  console.log(result);
  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient
```

```
def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['scores']

    result = collection.update_one(
        { '_id': 1 },
        { '$max': { 'highScore': 95 } }
    )

    print(result)
    client.close()

example()
```

$min

Der `$min` Aktualisierungsoperator aktualisiert den Wert eines Felds nur, wenn der angegebene Wert kleiner als der aktuelle Feldwert ist. Dieser Operator ist nützlich, um Mindestwerte bei Aktualisierungen beizubehalten.

Parameter

- `field`: Das zu aktualisierende Feld.
- `value`: Der Wert, der mit dem aktuellen Feldwert verglichen werden soll.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$min` Operator verwendet wird, um die niedrigste gemessene Temperatur für eine Wetterstation zu aktualisieren.

Erstellen Sie Beispieldokumente

```
db.weather.insertMany([
  { _id: 1, station: "Station A", lowestTemp: 15 },
  { _id: 2, station: "Station B", lowestTemp: 20 },
  { _id: 3, station: "Station C", lowestTemp: 18 }
```

```
])
```

Beispiel aktualisieren

```
db.weather.updateOne(
  { _id: 1 },
  { $min: { lowestTemp: 12 } }
)
```

Ergebnis

Das `lowestTemp` Feld für Station A wird auf 12 aktualisiert, weil 12 kleiner als der aktuelle Wert von 15 ist.

```
{ "_id": 1, "station": "Station A", "lowestTemp": 12 }
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$min` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('weather');

  const result = await collection.updateOne(
    { _id: 1 },
    { $min: { lowestTemp: 12 } }
  );

  console.log(result);
  await client.close();
}
```

```
example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['weather']

    result = collection.update_one(
        { '_id': 1 },
        { '$min': { 'lowestTemp': 12 } }
    )

    print(result)
    client.close()

example()
```

$mul

Der `$mul` Operator in Amazon DocumentDB wird verwendet, um den Wert eines Felds mit einer bestimmten Zahl zu multiplizieren. Dies kann nützlich sein, um mehrere Dokumente automatisch und konsistent zu aktualisieren, z. B. um Flugmeilen auf der Grundlage eines Kreditkartenstatus zu aktualisieren.

Parameter

- `field`: Das Feld, das multipliziert werden soll.
- `multiplier`: Die Zahl, mit der der Feldwert multipliziert werden soll.

Beispiel (MongoDB Shell)

Dieses Beispiel zeigt, wie der `$mul` Operator verwendet wird, um den `flight_miles` Wert für alle Dokumente zu verdoppeln, in denen sich das `credit_card` Feld befindet`true`.

Erstellen Sie Beispieldokumente

```
db.miles.insertMany([
  { "_id": 1, "member_since": new Date("1987-01-01"), "credit_card": false,
 "flight_miles": [1205, 2560, 880] },
  { "_id": 2, "member_since": new Date("1982-01-01"), "credit_card": true,
 "flight_miles": [2410, 5120, 1780, 5560] },
  { "_id": 3, "member_since": new Date("1999-01-01"), "credit_card": true,
 "flight_miles": [2410, 1760] }
]);
```

Beispiel für eine Abfrage

```
db.miles.update(
  { "credit_card": { "$eq": true } },
  { "$mul": { "flight_miles.$[]": NumberInt(2) } },
  { "multi": true }
);
```

Ausgabe

```
{ "_id" : 1, "member_since" : ISODate("1987-01-01T00:00:00Z"), "credit_card" : false,
 "flight_miles" : [ 1205, 2560, 880 ] }
{ "_id" : 2, "member_since" : ISODate("1982-01-01T00:00:00Z"), "credit_card" : true,
 "flight_miles" : [ 4820, 10240, 3560, 11120 ] }
{ "_id" : 3, "member_since" : ISODate("1999-01-01T00:00:00Z"), "credit_card" : true,
 "flight_miles" : [ 4820, 3520 ] }
```

Für Kunden, die eine Kreditkarte besitzen, wurden ihre Flugmeilen verdoppelt.

Der `$[]` Positions-Array-Operator wird verwendet, um die `$mul` Operation auf jedes Element im `flight_miles` Array anzuwenden.

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$mul` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');
```

```
async function updateFlightMiles() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('miles');

  await collection.updateMany(
    { credit_card: true },
    { $mul: { 'flight_miles.$[]': 2 } }
  );

  const documents = await collection.find().toArray();
  console.log(documents);

  await client.close();
}

updateFlightMiles();
```

Python

```
from pymongo import MongoClient

def update_flight_miles():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client.test
    collection = db.miles

    collection.update_many(
        {'credit_card': True},
        {'$mul': {'flight_miles.$[]': 2}}
    )

    documents = list(collection.find())
    print(documents)

    client.close()

update_flight_miles()
```

$pop

Der $pop Operator in Amazon DocumentDB wird verwendet, um das erste oder letzte Element aus einem Array-Feld zu entfernen. Dies ist besonders nützlich, wenn Sie ein Array mit fester Größe verwalten oder eine warteschlangenartige Datenstruktur innerhalb eines Dokuments implementieren müssen.

Parameter

- `field`: Der Name des Array-Felds, aus dem ein Element entfernt werden soll.
- `value`: Ein ganzzahliger Wert, der die Position des zu entfernenden Elements bestimmt. Ein Wert von 1 entfernt das letzte Element, während ein Wert von das erste Element `-1` entfernt.

Beispiel (MongoDB Shell)

Dieses Beispiel zeigt, wie der $pop Operator verwendet wird, um das erste und das letzte Element aus einem Array-Feld zu entfernen.

Erstellen Sie Beispieldokumente

```
db.users.insertMany([
  { "_id": 1, "name": "John Doe", "hobbies": ["reading", "swimming", "hiking"] },
  { "_id": 2, "name": "Jane Smith", "hobbies": ["cooking", "gardening", "painting"] }
])
```

Beispiel für eine Abfrage

```
// Remove the first element from the "hobbies" array
db.users.update({ "_id": 1 }, { $pop: { "hobbies": -1 } })

// Remove the last element from the "hobbies" array
db.users.update({ "_id": 2 }, { $pop: { "hobbies": 1 } })
```

Ausgabe

```
{ "_id" : 1, "name" : "John Doe", "hobbies" : [ "swimming", "hiking" ] }
{ "_id" : 2, "name" : "Jane Smith", "hobbies" : [ "cooking", "gardening" ] }
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des $pop Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('users');

  // Remove the first element from the "hobbies" array
  await collection.updateOne({ "_id": 1 }, { $pop: { "hobbies": -1 } });

  // Remove the last element from the "hobbies" array
  await collection.updateOne({ "_id": 2 }, { $pop: { "hobbies": 1 } });

  const users = await collection.find().toArray();
  console.log(users);

  await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['users']

    # Remove the first element from the "hobbies" array
    collection.update_one({"_id": 1}, {"$pop": {"hobbies": -1}})
```

```
    # Remove the last element from the "hobbies" array
    collection.update_one({"_id": 2}, {"$pop": {"hobbies": 1}})

    users = list(collection.find())
    print(users)

    client.close()

example()
```

$position

Der `$position` Modifikator in Amazon DocumentDB gibt die Position im Array an, an der der `$push` Operator Elemente einfügt. Ohne den `$position` Modifikator fügt der `$push` Operator Elemente am Ende des Arrays ein.

Parameter

- `field`: Das zu aktualisierende Array-Feld.
- `num`: Die Position im Array, an der Elemente eingefügt werden sollen, basierend auf einer Nullindizierung.

Hinweis: Um den `$position` Modifikator verwenden zu können, muss er zusammen mit dem Modifikator erscheinen. `$each`

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$position` Operator verwendet wird, um Aufgaben an bestimmten Positionen in einem Projektmanagementsystem einzufügen.

Erstellen Sie Beispieldokumente

```
db.projects.insertOne({ "_id": 1, "name": "Website Redesign", "tasks": ["Design
 mockups"] })
```

Abfragebeispiel 1 — Fügen Sie am Anfang dringende Aufgaben hinzu

```
db.projects.updateOne(
   { _id: 1 },
```

```
   {
     $push: {
        tasks: {
           $each: ["Security audit", "Performance review"],
           $position: 0
        }
     }
   }
)
```

Ausgang 1

```
{ "_id": 1, "name": "Website Redesign", "tasks": ["Security audit", "Performance
 review", "Design mockups"] }
```

Abfragebeispiel 2 — Aufgaben an einer bestimmten Position hinzufügen

```
db.projects.insertOne({ "_id": 2, "name": "Mobile App", "tasks": ["Setup project",
 "Create wireframes", "Deploy to store"] })

db.projects.updateOne(
   { _id: 2 },
   {
     $push: {
        tasks: {
           $each: ["Code review", "Testing phase"],
           $position: 2
        }
     }
   }
)
```

Ausgabe 2

```
{ "_id": 2, "name": "Mobile App", "tasks": ["Setup project", "Create wireframes", "Code
 review", "Testing phase", "Deploy to store"] }
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$position` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function insertTasksAtPosition() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('projects');

  await collection.updateOne(
    { _id: 1 },
    {
      $push: {
        tasks: {
          $each: ["Security audit", "Performance review"],
          $position: 0
        }
      }
    }
  );

  const updatedProject = await collection.findOne({ _id: 1 });
  console.log(updatedProject);

  await client.close();
}

insertTasksAtPosition();
```

Python

```
from pymongo import MongoClient

def insert_tasks_at_position():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['projects']

    result = collection.update_one(
```

```
        {'_id': 1},
        {
            '$push': {
                'tasks': {
                    '$each': ['Security audit', 'Performance review'],
                    '$position': 0
                }
            }
        }
    )

    updated_project = collection.find_one({'_id': 1})
    print(updated_project)

    client.close()

insert_tasks_at_position()
```

$pull

Der `$pull` Operator wird verwendet, um alle Instanzen eines Werts oder von Werten, die einer bestimmten Bedingung entsprechen, aus einem Array zu entfernen. Dieser Operator ist nützlich, wenn Sie bestimmte Elemente aus einem Array-Feld innerhalb eines Dokuments entfernen müssen.

Parameter

- `field`: Der Name des Array-Feldes, aus dem die Werte entfernt werden sollen.
- `value`: Der Wert oder die Bedingung, die bestimmt, welche Elemente aus dem Array entfernt werden sollen.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$pull` Operator verwendet wird, um Elemente aus einem Array-Feld zu entfernen.

Erstellen Sie Beispieldokumente

```
db.restaurants.insertMany([
  {
    name: "Pizza Hut",
```

```
    cuisine: "Italian",
    features: ["Delivery", "Takeout", "Dine-in"]
  },
  {
    name: "Sushi Saito",
    cuisine: "Japanese",
    features: ["Dine-in", "Private Dining"]
  },
  {
    name: "Taco Bell",
    cuisine: "Mexican",
    features: ["Delivery", "Takeout", "Drive-thru"]
  }
])
```

Beispiel für eine Abfrage

```
db.restaurants.updateMany(
  { cuisine: "Italian" },
  { $pull: { features: "Takeout" } }
)
```

Ausgabe

```
{
  "acknowledged" : true,
  "matchedCount" : 1,
  "modifiedCount" : 1
}
```

Die obige Abfrage entfernt die Funktion „Mitnehmen“ aus allen Dokumenten, in denen das `cuisine` Feld „Italienisch“ ist.

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$pull` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');
```

```
async function updateRestaurants() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const restaurants = db.collection('restaurants');

  await restaurants.updateMany(
    { cuisine: 'Italian' },
    { $pull: { features: 'Takeout' } }
  );

  const updatedRestaurants = await restaurants.find({}).toArray();
  console.log(updatedRestaurants);

  await client.close();
}

updateRestaurants();
```

Python

```
from pymongo import MongoClient

def update_restaurants():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client.test
    restaurants = db.restaurants

    result = restaurants.update_many(
        { 'cuisine': 'Italian' },
        { '$pull': { 'features': 'Takeout' } }
    )

    updated_restaurants = list(restaurants.find({}))
    print(updated_restaurants)

    client.close()

update_restaurants()
```

$pullAll

Der `$pullAll` Operator in Amazon DocumentDB wird verwendet, um alle Instanzen der angegebenen Werte aus einem Array-Feld zu entfernen. Dies ist besonders nützlich, wenn Sie in einem einzigen Vorgang mehrere Elemente aus einem Array entfernen müssen.

Parameter

- `field`: Der Name des Array-Feldes, aus dem die Elemente entfernt werden sollen.
- `value`: Eine Reihe von Werten, die aus dem Array-Feld entfernt werden sollen.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$pullAll` Operator verwendet wird, um mehrere Elemente aus einem Array-Feld zu entfernen.

Erstellen Sie Beispieldokumente

```
db.restaurants.insert([
  {
    "name": "Taj Mahal",
    "cuisine": "Indian",
    "features": ["Private Dining", "Live Music"]
  },
  {
    "name": "Golden Palace",
    "cuisine": "Chinese",
    "features": ["Private Dining", "Takeout"]
  },
  {
    "name": "Olive Garden",
    "cuisine": "Italian",
    "features": ["Private Dining", "Outdoor Seating"]
  }
])
```

Beispiel für eine Abfrage

```
db.restaurants.update(
  { "name": "Taj Mahal" },
  { $pullAll: { "features": ["Private Dining", "Live Music"] } }
```

```
)
```

Ausgabe

```
{
  "name": "Taj Mahal",
  "cuisine": "Indian",
  "features": []
}
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$pullAll` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function main() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('restaurants');

  await collection.updateMany(
    { "name": "Taj Mahal" },
    { $pullAll: { "features": ["Private Dining", "Live Music"] } }
  );

  const updatedDocument = await collection.findOne({ "name": "Taj Mahal" });
  console.log(updatedDocument);

  await client.close();
}

main();
```

Python

```
from pymongo import MongoClient
```

```
def main():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['restaurants']

    collection.update_many(
        {"name": "Taj Mahal"},
        {"$pullAll": {"features": ["Private Dining", "Live Music"]}}
    )

    updated_document = collection.find_one({"name": "Taj Mahal"})
    print(updated_document)

    client.close()

if __name__ == '__main__':
    main()
```

$push

Der `$push` Operator in Amazon DocumentDB wird verwendet, um ein Element zu einem Array-Feld in einem Dokument hinzuzufügen. Dieser Operator ist besonders nützlich, wenn Sie neue Daten an ein vorhandenes Array anhängen müssen, ohne das gesamte Array zu überschreiben.

Parameter

- `field`: Der Name des Array-Feldes, zu dem das neue Element hinzugefügt werden soll.
- `value`: Der Wert, der dem Array hinzugefügt werden soll.
- `position`: (optional) Ein Modifikator, der die Position im Array angibt, an der das neue Element hinzugefügt werden soll. Zu den unterstützten Modifikatoren gehören $ (am Ende des Arrays hinzufügen) und `$[]` (am Ende des Arrays hinzufügen, dabei alle Array-Filter ignorieren).

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$push` Operator verwendet wird, um einem Array-Feld in einem Dokument neue Elemente hinzuzufügen.

Erstellen Sie Beispieldokumente

```
db.users.insert([
  { _id: 1, name: "John Doe", hobbies: ["reading", "swimming"] },
  { _id: 2, name: "Jane Smith", hobbies: ["gardening", "cooking"] }
])
```

Beispiel für eine Abfrage

```
db.users.updateOne(
  { _id: 1 },
  { $push: { hobbies: "hiking" } }
)
```

Ausgabe

```
{
  "acknowledged" : true,
  "matchedCount" : 1,
  "modifiedCount" : 1
}
```

Nach dem Ausführen des Updates `_id: 1` wird das `hobbies` Array für das Dokument mit aktualisiert`["reading", "swimming", "hiking"]`.

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$push` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function updateDocument() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('users');
```

```
  const result = await collection.updateOne(
    { _id: 1 },
    { $push: { hobbies: "hiking" } }
  );

  console.log(result);
  client.close();
}

updateDocument();
```

Python

```
from pymongo import MongoClient

def update_document():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['users']

    result = collection.update_one(
        {'_id': 1},
        {'$push': {'hobbies': 'hiking'}}
    )

    print(result.raw_result)
    client.close()

update_document()
```

$rename

Der `$rename` Operator in Amazon DocumentDB wird verwendet, um ein Feld in einem Dokument umzubenennen. Dieser Operator kann besonders nützlich sein, wenn Sie die Struktur Ihrer Dokumente aktualisieren oder sie an neue Datenmodelle anpassen müssen.

Parameter

- `field`: Das Feld, das umbenannt werden soll.

- `newName`: Der neue Name für das Feld.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie Sie den `$rename` Operator verwenden, um das `"Date.DoW"` Feld `"Date.DayOfWeek"` in einem Dokument umzubenennen, in dem das `"DocName"` Feld auf `"Document 1"` gesetzt ist.

Erstellen Sie Beispieldokumente

```
db.example.insertOne({
    "DocName": "Document 1",
    "Date": {
        "Month": 4,
        "Day": 18,
        "Year": 1987,
        "DoW": "Saturday"
    },
    "Words": 2482
})
```

Beispiel für eine Abfrage

```
db.example.update(
    { "DocName": "Document 1" },
    { $rename: { "Date.DoW": "Date.DayOfWeek" } }
)
```

Ausgabe

```
{
    "DocName": "Document 1",
    "Date": {
        "Month": 4,
        "Day": 18,
        "Year": 1987,
        "DayOfWeek": "Saturday"
    },
    "Words": 2482
}
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$rename` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function example() {
    const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
    const db = client.db('test');
    const collection = db.collection('example');

    await collection.updateOne(
        { "DocName": "Document 1" },
        { $rename: { "Date.DoW": "Date.DayOfWeek" } }
    );

    const updatedDoc = await collection.findOne({ "DocName": "Document 1" });
    console.log(updatedDoc);

    await client.close();
}

example();
```

Python

```
from pymongo import MongoClient

def example():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['example']

    collection.update_one(
        {"DocName": "Document 1"},
        {"$rename": {"Date.DoW": "Date.DayOfWeek"}}
```

```
    )

    updated_doc = collection.find_one({"DocName": "Document 1"})
    print(updated_doc)

    client.close()

example()
```

$set

Der `$set` Operator in Amazon DocumentDB wird verwendet, um den Wert eines bestimmten Felds in einem Dokument zu aktualisieren. Mit diesem Operator können Sie neue Felder hinzufügen oder bestehende Felder innerhalb eines Dokuments ändern. Es ist ein grundlegender Aktualisierungsoperator im MongoDB-Java-Treiber, der mit Amazon DocumentDB kompatibel ist.

Parameter

- `field`: Das zu aktualisierende Feld.
- `value`: Der neue Wert für das Feld.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$set` Operator verwendet wird, um das `Item` Feld in einem Dokument zu aktualisieren.

Erstellen Sie Beispieldokumente

```
db.example.insert([
  {
    "Item": "Pen",
    "Colors": ["Red", "Green", "Blue", "Black"],
    "Inventory": {
      "OnHand": 244,
      "MinOnHand": 72
    }
  },
  {
    "Item": "Poster Paint",
    "Colors": ["Red", "Green", "Blue", "White"],
```

```
    "Inventory": {
      "OnHand": 120,
      "MinOnHand": 36
    }
  }
])
```

Beispiel für eine Abfrage

```
db.example.update(
  { "Item": "Pen" },
  { $set: { "Item": "Gel Pen" } }
)
```

Ausgabe

```
{
  "Item": "Gel Pen",
  "Colors": ["Red", "Green", "Blue", "Black"],
  "Inventory": {
    "OnHand": 244,
    "MinOnHand": 72
  }
}
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$set` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function updateDocument() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('example');

  await collection.updateOne(
```

```
    { "Item": "Pen" },
    { $set: { "Item": "Gel Pen" } }
  );

  const updatedDocument = await collection.findOne({ "Item": "Gel Pen" });
  console.log(updatedDocument);

  await client.close();
}

updateDocument();
```

Python

```
from pymongo import MongoClient

def update_document():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client.test
    collection = db.example

    collection.update_one(
        {"Item": "Pen"},
        {"$set": {"Item": "Gel Pen"}}
    )

    updated_document = collection.find_one({"Item": "Gel Pen"})
    print(updated_document)

    client.close()

update_document()
```

$ gesetzt OnInsert

Der `$setOnInsert` Operator in Amazon DocumentDB wird verwendet, um den Wert eines Felds festzulegen, wenn ein Dokument eingefügt wird. Er hat jedoch keine Auswirkung, wenn das Dokument aktualisiert wird.

Parameter

- `field`: Das Feld, das festgelegt werden soll.
- `value`: Der Wert, der dem Feld zugewiesen werden soll.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt die Verwendung des `$setOnInsert` Operators in Amazon DocumentDB. Es erstellt ein neues Dokument, wenn das Dokument noch nicht existiert, hat aber keine Auswirkung, wenn das Dokument aktualisiert wird.

Erstellen Sie Beispieldokumente

```
db.users.insertOne({
  _id: 1,
  name: "John Doe",
  age: 30
})
```

Abfragebeispiel 1 — Bestehendes Dokument aktualisieren

```
db.users.update(
  { _id: 1 },
  {
    $set: { age: 31 },
    $setOnInsert: { createdAt: new Date() }
  },
  { upsert: true }
)
```

Ausgabe 1

```
{
  _id: 1,
  name: "John Doe",
  age: 31
}
```

Die Ausgabe zeigt, dass das Dokument aktualisiert wurde, das `createdAt` Feld jedoch NICHT hinzugefügt wurde, da das Dokument bereits vorhanden war. Der `$setOnInsert` Operator gilt nur beim Einfügen neuer Dokumente.

Abfragebeispiel 2 — Neues Dokument einfügen (upsert)

```
db.users.update(
  { _id: 2 },
  {
    $set: { name: "Jane Smith", age: 25 },
    $setOnInsert: { createdAt: new Date() }
  },
  { upsert: true }
)
```

Ausgabe 2

```
{
  _id: 2,
  name: "Jane Smith",
  age: 25,
  createdAt: ISODate("2025-10-31T09:57:52.459Z")
}
}
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$setOnInsert` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function updateWithSetOnInsert() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const users = db.collection('users');

  await users.updateOne(
    { _id: 1 },
    {
      $set: { age: 31 },
      $setOnInsert: { createdAt: new Date() }
```

```
    },
    { upsert: true }
  );

  const updatedUser = await users.findOne({ _id: 1 });
  console.log(updatedUser);

  await client.close();
}

updateWithSetOnInsert();
```

Python

```
from pymongo import MongoClient

def update_with_set_on_insert():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    users = db['users']

    result = users.update_one(
        {'_id': 1},
        {
            '$set': {'age': 31},
            '$setOnInsert': {'createdAt': datetime.datetime.now()}
        },
        upsert=True
    )

    updated_user = users.find_one({'_id': 1})
    print(updated_user)

    client.close()

update_with_set_on_insert()
```

$slice

Der `$slice` Aktualisierungsoperator ändert ein Array, indem er seine Größe begrenzt. Wenn er zusammen mit dem `$push` Operator verwendet wird, schränkt er die Anzahl der Elemente in einem Array ein und behält nur die angegebene Anzahl der neuesten oder ältesten Elemente bei.

Parameter

- `field`: Das zu ändernde Array-Feld.
- `count`: Maximale Anzahl von Elementen, die beibehalten werden sollen. Positive Werte behalten die ersten N Elemente, negative Werte behalten die letzten N Elemente.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$slice` Aktualisierungsoperator with verwendet wird`$push`, um ein Array mit fester Größe mit aktuellen Ergebnissen zu verwalten.

Erstellen Sie Beispieldokumente

```
db.students.insertOne({
  _id: 1,
  name: "Alice",
  scores: [85, 90, 78]
});
```

Beispiel für eine Abfrage

```
db.students.updateOne(
  { _id: 1 },
  {
    $push: {
      scores: {
        $each: [92, 88],
        $slice: -3
      }
    }
  }
)
```

Ausgabe

```
{
  "_id" : 1,
  "name" : "Alice",
  "scores" : [ 78, 92, 88 ]
}
```

In diesem Beispiel behält der `$slice: -3` Modifikator nur die letzten drei Elemente bei, nachdem er neue Werte in das Array übertragen hat.

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$slice` Aktualisierungsoperators anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function updateDocument() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('students');

  await collection.updateOne(
    { _id: 1 },
    {
      $push: {
        scores: {
          $each: [92, 88],
          $slice: -3
        }
      }
    }
  );

  const updatedDocument = await collection.findOne({ _id: 1 });
  console.log(updatedDocument);

  await client.close();
}
```

```
updateDocument();
```

Python

```
from pymongo import MongoClient

def update_document():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client.test
    collection = db.students

    collection.update_one(
        {'_id': 1},
        {
            '$push': {
                'scores': {
                    '$each': [92, 88],
                    '$slice': -3
                }
            }
        }
    )

    updated_document = collection.find_one({'_id': 1})
    print(updated_document)

    client.close()

update_document()
```

$sort

Der `$sort` Aktualisierungsmodifikator ordnet Array-Elemente an, wenn er zusammen mit dem `$push` Operator verwendet wird. Er ordnet Array-Elemente auf der Grundlage der angegebenen Feldwerte oder der Elemente selbst in aufsteigender oder absteigender Reihenfolge an.

Parameter

- `field`: Das zu ändernde Array-Feld.

- `order`: Wird 1 für aufsteigende oder `-1` absteigende Reihenfolge verwendet.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$sort` Modifikator mit verwendet wird`$push`, um neue Quizergebnisse hinzuzufügen und sie in absteigender Reihenfolge zu sortieren.

Erstellen Sie Beispieldokumente

```
db.students.insertOne({
  _id: 1,
  name: "Bob",
  quizzes: [
    { score: 85, date: "2024-01-15" },
    { score: 92, date: "2024-02-10" }
  ]
});
```

Beispiel für eine Abfrage

```
db.students.updateOne(
  { _id: 1 },
  {
    $push: {
      quizzes: {
        $each: [{ score: 78, date: "2024-03-05" }],
        $sort: { score: -1 }
      }
    }
  }
)
```

Ausgabe

```
{
  "_id" : 1,
  "name" : "Bob",
  "quizzes" : [
    { "score" : 92, "date" : "2024-02-10" },
    { "score" : 85, "date" : "2024-01-15" },
    { "score" : 78, "date" : "2024-03-05" }
  ]
```

```
}
```

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$sort` Aktualisierungsmodifikators anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function updateDocument() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('students');

  await collection.updateOne(
    { _id: 1 },
    {
      $push: {
        quizzes: {
          $each: [{ score: 78, date: "2024-03-05" }],
          $sort: { score: -1 }
        }
      }
    }
  );

  const updatedDocument = await collection.findOne({ _id: 1 });
  console.log(updatedDocument);

  await client.close();
}

updateDocument();
```

Python

```
from pymongo import MongoClient

def update_document():
```

```
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client.test
    collection = db.students

    collection.update_one(
        {'_id': 1},
        {
            '$push': {
                'quizzes': {
                    '$each': [{'score': 78, 'date': '2024-03-05'}],
                    '$sort': {'score': -1}
                }
            }
        }
    )

    updated_document = collection.find_one({'_id': 1})
    print(updated_document)

    client.close()

update_document()
```

$unset

Der `$unset` Operator in Amazon DocumentDB wird verwendet, um ein bestimmtes Feld aus einem Dokument zu entfernen. Wenn ein Feld mit entfernt wird`$unset`, wird das Feld aus dem Dokument gelöscht, und die Dokumentgröße wird entsprechend reduziert. Dies kann nützlich sein, wenn Sie unnötige Daten aus Ihren Dokumenten entfernen möchten.

Parameter

- `field`: Das Feld, das aus dem Dokument entfernt werden soll. Dies kann ein einzelnes Feld oder ein gepunkteter Pfad zu einem verschachtelten Feld sein.

Beispiel (MongoDB Shell)

Das folgende Beispiel zeigt, wie der `$unset` Operator verwendet wird, um das `Words` Feld aus einem Dokument in der `example` Sammlung zu entfernen.

Erstellen Sie Beispieldokumente

```
db.example.insert({
    "DocName": "Document 1",
    "Date": {
        "Month": 4,
        "Day": 18,
        "Year": 1987,
        "DoW": "Saturday"
    },
    "Words": 2482
})
```

Beispiel für eine Abfrage

```
db.example.update(
    { "DocName" : "Document 1" },
    { $unset: { Words:1 } }
)
```

Ausgabe

```
{
    "DocName": "Document 1",
    "Date": {
        "Month": 4,
        "Day": 18,
        "Year": 1987,
        "DoW": "Saturday"
    }
}
```

In diesem Beispiel wird der `$unset` Operator verwendet, um das `Words` Feld aus dem Dokument zu entfernen, das „Dokument 1" `DocName` entspricht. Das resultierende Dokument enthält das `Words` Feld nicht mehr.

Codebeispiele

Um ein Codebeispiel für die Verwendung des `$unset` Befehls anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten:

Node.js

```
const { MongoClient } = require('mongodb');

async function removeField() {
  const client = await MongoClient.connect('mongodb://
<username>:<password>@<cluster-endpoint>:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false');
  const db = client.db('test');
  const collection = db.collection('example');

  const result = await collection.updateOne(
    { "DocName": "Document 1" },
    { $unset: { "Words": 1 } }
  );

  console.log(`Modified ${result.modifiedCount} document(s)`);
  client.close();
}

removeField();
```

Python

```
from pymongo import MongoClient

def remove_field():
    client = MongoClient('mongodb://<username>:<password>@<cluster-endpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')
    db = client['test']
    collection = db['example']

    result = collection.update_one(
        {"DocName": "Document 1"},
        {"$unset": {"Words": 1}}
    )

    print(f"Modified {result.modified_count} document(s)")
    client.close()

remove_field()
```

Generative künstliche Intelligenz von Amazon DocumentDB

Amazon DocumentDB bietet Funktionen, mit denen Modelle für maschinelles Lernen (ML) und generative künstliche Intelligenz (KI) in Echtzeit mit in Amazon DocumentDB gespeicherten Daten arbeiten können. Kunden müssen keine Zeit mehr damit verbringen, separate Infrastrukturen zu verwalten, Code für die Verbindung mit einem anderen Service zu schreiben und Daten aus ihrer Primärdatenbank zu duplizieren.

Weitere Informationen zu künstlicher Intelligenz und dazu, wie Sie Ihre KI-Anforderungen unterstützen AWS können, finden Sie in diesem "What-is" Artikel.

Topics

- No-code maschinelles Lernen mit Amazon SageMaker AI Canvas
- Vektorsuche für Amazon DocumentDB

No-code maschinelles Lernen mit Amazon SageMaker AI Canvas

Mit Amazon SageMaker AI Canvas können Sie Ihre eigenen AI/ML Modelle erstellen, ohne eine einzige Codezeile schreiben zu müssen. Sie können ML-Modelle für gängige Anwendungsfälle wie Regression und Prognose erstellen und auf Foundation Models (FMs) von Amazon Bedrock zugreifen und diese auswerten. Sie können auch von Amazon SageMaker AI aus auf öffentliche FMs zugreifen, JumpStart um Inhalte zu generieren, Text zu extrahieren und Text zusammenzufassen, um generative KI-Lösungen zu unterstützen.

Wie erstellt man ML-Modelle ohne Code mit AI Canvas SageMaker

Amazon DocumentDB ist jetzt in Amazon SageMaker AI Canvas integriert, um maschinelles Lernen (ML) ohne Code mit in Amazon DocumentDB gespeicherten Daten zu ermöglichen. Sie können jetzt ML-Modelle für Regressions- und Prognoseanforderungen erstellen und Basismodelle für die Zusammenfassung und Generierung von Inhalten verwenden, indem Sie in Amazon DocumentDB gespeicherte Daten verwenden, ohne eine einzige Codezeile schreiben zu müssen.

SageMaker AI Canvas bietet eine visuelle Oberfläche, über die Amazon DocumentDB-Kunden Prognosen erstellen können, ohne dass AI/ML Fachwissen erforderlich ist oder eine einzige Codezeile geschrieben werden muss. Kunden können jetzt den SageMaker AI Canvas-Workspace aus den AWS-Managementkonsole Amazon DocumentDB DocumentDB-Daten für die

Datenvorbereitung und das Modelltraining starten, importieren und verknüpfen. Daten in Amazon DocumentDB können jetzt in SageMaker AI Canvas verwendet werden, um Modelle zur Vorhersage der Kundenabwanderung, zur Aufdeckung von Betrug, zur Vorhersage von Wartungsausfällen, zur Prognose von Geschäftskennzahlen und zur Generierung von Inhalten zu erstellen und zu erweitern. Kunden können jetzt mithilfe der systemeigenen Integration von SageMaker AI Canvas mit Quick ML-driven Erkenntnisse veröffentlichen und teamübergreifend teilen. Datenerfassungspipelines in SageMaker AI Canvas werden standardmäßig auf sekundären Amazon DocumentDB DocumentDB-Instances ausgeführt, wodurch sichergestellt wird, dass die Leistung von Anwendungs- und SageMaker AI Canvas-Erfassungs-Workloads nicht beeinträchtigt wird.

Amazon DocumentDB-Kunden können mit SageMaker AI Canvas beginnen, indem sie zur neuen Amazon DocumentDB No-Code ML-Konsolenseite navigieren und sich mit neuen oder verfügbaren SageMaker AI Canvas-Arbeitsbereichen verbinden.

Konfiguration der SageMaker AI-Domäne und des Benutzerprofils

Sie können von SageMaker AI-Domänen aus, die im Modus Nur VPC ausgeführt werden, eine Verbindung zu Amazon DocumentDB-Clustern herstellen. Durch den Start einer SageMaker KI-Domain in Ihrer VPC können Sie den Datenfluss von Ihren SageMaker AI Studio- und Canvas-Umgebungen aus steuern. Auf diese Weise können Sie den Internetzugang einschränken, den Datenverkehr mithilfe standardmäßiger AWS Netzwerk- und Sicherheitsfunktionen überwachen und überprüfen und über VPC-Endpunkte eine Verbindung zu anderen AWS Ressourcen herstellen. Informationen zum Erstellen Ihrer SageMaker KI-Domain für die Verbindung mit Ihrem Amazon DocumentDB-Cluster finden Sie unter Amazon SageMaker AI Canvas Getting started und Configure Amazon SageMaker AI Canvas in a VPC without internet access im Amazon SageMaker AI Developer Guide.

Konfiguration von IAM-Zugriffsberechtigungen für Amazon DocumentDB und AI Canvas SageMaker

Ein Amazon DocumentDB DocumentDB-Benutzer, `AmazonDocDBConsoleFullAccess` der seiner zugehörigen Rolle und Identität zugeordnet ist, kann auf die AWS-Managementkonsole zugreifen. Fügen Sie der oben genannten Rolle oder Identität die folgenden Aktionen hinzu, um Zugriff auf maschinelles Lernen ohne Code mit Amazon SageMaker AI Canvas zu gewähren.

```
"sagemaker:CreatePresignedDomainUrl",
"sagemaker:DescribeDomain",
"sagemaker:ListDomains",
```

```
"sagemaker:ListUserProfiles"
```

Datenbankbenutzer und Rollen für SageMaker AI Canvas erstellen

Mithilfe der rollenbasierten Zugriffskontrolle (RBAC) in Amazon DocumentDB können Sie den Zugriff auf die Aktionen einschränken, die Benutzer an Datenbanken ausführen können. Bei RBAC werden einem Benutzer eine oder mehrere Rollen gewährt. Diese Rollen bestimmen die Operationen, die ein Benutzer mit Datenbankressourcen ausführen kann.

Als Canvas-Benutzer stellen Sie mit Benutzernamen und Passwort eine Verbindung zu einer Amazon DocumentDB DocumentDB-Datenbank her. Mithilfe der Amazon DocumentDB RBAC-Funktionalität können Sie eine Datenbank user/role für einen Canvas-Benutzer erstellen, der Lesezugriff auf die jeweiligen Datenbanken hat.

Verwenden Sie zum Beispiel den Vorgang: `createUser`

```
db.createUser({
user: "canvas_user",
pwd: "<insert-password>",
roles: [{role: "read", db: "sample-database-1"}]
})
```

Dadurch wird eine erstellt`canvas_user`, die über Leseberechtigungen für die `sample-database-1` Datenbank verfügt. Ihre Canvas-Analysten können diese Anmeldeinformationen verwenden, um auf Daten in Ihrem Amazon DocumentDB-Cluster zuzugreifen. Weitere Informationen finden Datenbankzugriff mit Role-Based Access Control Sie unter.

Verfügbare Regionen

Die No-Code-Integration ist in Regionen verfügbar, in denen sowohl Amazon DocumentDB als auch Amazon SageMaker AI Canvas unterstützt werden. Zu den Regionen gehören:

- us-east-1 (N. Virginia)
- us-east-2 (Ohio)
- us-west-2 (Oregon)
- ap-northeast-1 (Tokyo)
- ap-northeast-2 (Seoul)

- ap-south-1 (Mumbai)
- ap-southeast-1 (Singapur)
- ap-southeast-2 (Sydney)
- eu-central-1 (Frankfurt)
- eu-west-1 (Ireland)

Informationen zur aktuellen regionalen Verfügbarkeit finden Sie unter Amazon SageMaker SageMaker AI Canvas im Amazon AI Developer Guide.

Vektorsuche für Amazon DocumentDB

Die Vektorsuche ist eine Methode, die beim maschinellen Lernen verwendet wird, um Datenpunkte zu finden, die einem bestimmten Datenpunkt ähneln, indem ihre Vektordarstellungen anhand von Entfernungs- oder Ähnlichkeitsmetriken verglichen werden. Je näher sich die beiden Vektoren im Vektorraum befinden, desto ähnlicher wird davon ausgegangen, dass sich die zugrunde liegenden Elemente ähneln. Diese Technik hilft dabei, die semantische Bedeutung der Daten zu erfassen. Dieser Ansatz ist in verschiedenen Anwendungen nützlich, z. B. in Empfehlungssystemen, Verarbeitung natürlicher Sprache und Bilderkennung.

Die Vektorsuche für Amazon DocumentDB kombiniert die Flexibilität und die umfangreichen Abfragefunktionen einer JSON-based Dokumentendatenbank mit der Leistungsfähigkeit der Vektorsuche. Wenn Sie Ihre vorhandenen Amazon DocumentDB-Daten oder eine flexible Dokumentendatenstruktur verwenden möchten, um Anwendungsfälle für maschinelles Lernen und generative KI wie semantische Suche, Produktempfehlungen, Personalisierung, Chatbots, Betrugserkennung und Anomalieerkennung zu erstellen, dann ist die Vektorsuche für Amazon DocumentDB die ideale Wahl für Sie. Die Vektorsuche ist auf instanzbasierten Amazon DocumentDB 5.0-Clustern verfügbar.

Topics

- Vektoren einfügen
- Einen Vektorindex erstellen
- Eine Indexdefinition abrufen
- Abfragen von Vektoren
- Funktionen und Einschränkungen

- Best Practices

Vektoren einfügen

Um Vektoren in Ihre Amazon DocumentDB DocumentDB-Datenbank einzufügen, können Sie bestehende Einfügemethoden verwenden:

Beispiel

Im folgenden Beispiel wird eine Sammlung von fünf Dokumenten in einer Testdatenbank erstellt. Jedes Dokument enthält zwei Felder: den Produktnamen und die entsprechende Vektoreinbettung.

```
db.collection.insertMany([
  {"product_name": "Product A", "vectorEmbedding": [0.2, 0.5, 0.8]},
  {"product_name": "Product B", "vectorEmbedding": [0.7, 0.3, 0.9]},
  {"product_name": "Product C", "vectorEmbedding": [0.1, 0.2, 0.5]},
  {"product_name": "Product D", "vectorEmbedding": [0.9, 0.6, 0.4]},
  {"product_name": "Product E", "vectorEmbedding": [0.4, 0.7, 0.2]}
]);
```

Einen Vektorindex erstellen

Amazon DocumentDB unterstützt sowohl die Indexierung mit Hierarchical Navigable Small World (HNSW) als auch die Indexierungsmethoden Inverted File with Flat Compression (IVFFlat). Ein IVFFlat-Index unterteilt Vektoren in Listen und durchsucht anschließend eine ausgewählte Teilmenge der Listen, die dem Abfragevektor am nächsten sind. Andererseits organisiert ein HNSW-Index die Vektordaten in einem vielschichtigen Diagramm. HNSW hat zwar im Vergleich zu IVFflat langsamere Erstellungszeiten, bietet aber eine bessere Abfrageleistung und einen besseren Abruf. Im Gegensatz zu IVFFlat ist bei HNSW kein Trainingsschritt erforderlich, sodass der Index ohne anfängliches Laden der Daten generiert werden kann. Für die meisten Anwendungsfälle empfehlen wir die Verwendung des HNSW-Indextyps für die Vektorsuche.

Wenn Sie keinen Vektorindex erstellen, führt Amazon DocumentDB eine exakte Suche nach dem nächsten Nachbarn durch und gewährleistet so einen perfekten Wiedererkennungswert. In Produktionsszenarien ist Geschwindigkeit jedoch entscheidend. Wir empfehlen die Verwendung von Vektorindizes, bei denen ein gewisser Rückruf gegen eine höhere Geschwindigkeit eingetauscht werden kann. Es ist wichtig zu beachten, dass das Hinzufügen eines Vektorindexes zu unterschiedlichen Abfrageergebnissen führen kann.

Vorlagen

Sie können die folgenden `createIndex` oder `runCommand` Vorlagen verwenden, um einen Vektorindex für ein Vektorfeld zu erstellen:

Using createIndex

In bestimmten Treibern, wie z. B. Mongosh und Java, `createIndex` kann die Verwendung der `vectorOptions` Parameter in zu einem Fehler führen. In solchen Fällen empfehlen wir die Verwendung von`runCommand`:

```
db.collection.createIndex(
  { "<vectorField>": "vector" },
  { "name": "<indexName>",
    "vectorOptions": {
      "type": " <hnsw> | <ivfflat> ",
      "dimensions": <number_of_dimensions>,
      "similarity": " <euclidean> | <cosine> | <dotProduct> ",
      "lists": <number_of_lists> [applicable for IVFFlat],
      "m": <max number of connections> [applicable for HNSW],
      "efConstruction": <size of the dynamic list for index build> [applicable for
 HNSW]
    }
  }
);
```

Using runCommand

In bestimmten Treibern wie Mongosh und Java `createIndex` kann die Verwendung der `vectorOptions` Parameter in zu einem Fehler führen. In solchen Fällen empfehlen wir die Verwendung von`runCommand`:

```
db.runCommand(
  { "createIndexes": "<collection>",
  "indexes": [{
      key: { "<vectorField>": "vector" },
      vectorOptions: {
          type: " <hnsw> | <ivfflat> ",
          dimensions: <number of dimensions>,
          similarity: " <euclidean> | <cosine> | <dotProduct> ",
          lists: <number_of_lists> [applicable for IVFFlat],
          m: <max number of connections> [applicable for HNSW],
          efConstruction: <size of the dynamic list for index build> [applicable for
 HNSW]
```

```
            },
        name: "myIndex"
        }]
    }
);
```

Parameter	Anforderung	Datentyp	Description	Wert (e)
name	optional	Zeichenfolge	Gibt den Namen des Indexes an.	Alphanumerisch
type	optional		Gibt den Indextyp an.	Unterstützt: hnsw oder ivfflat Standard: HNSW (Engine-Patch 3.0.4574 und höher)
dimensions	Erforderlich	Ganzzahl	Gibt die Anzahl der Dimensionen in den Vektordaten an.	Maximal 2.000 Dimensionen.
similarity	Erforderlich	Zeichenfolge	Gibt die Entfernungsmetrik an, die für die Ähnlichkeitsberechnung verwendet wird.	• **euclidean** • **cosine** • **dotProduct**
lists	erforderlich für IVFflat	Ganzzahl	Gibt die Anzahl der Cluster an, die der IVFFlat-Index verwendet, um die Vektordaten zu gruppieren. Die empfohlen	Minimum: 1 Maximum: Weitere Informationen finden Sie in der Funktionen und Einschrän

Parameter	Anforderung	Datentyp	Description	Wert (e)
			e Einstellung ist die Anzahl von documents /1000 für bis zu 1 Mio. Dokumente und `sqrt(# of documents)` für über 1 Mio. Dokumente.	kungen folgenden Tabelle mit den Listen pro Instanztyp.
`m`	optional	Ganzzahl	Gibt die maximale Anzahl von Verbindun gen für einen HNSW-Index an	Standard: 16 Bereich [2, 100]
`efConstru ction`	optional	Ganzzahl	Gibt die Größe der dynamischen Kandidatenliste für die Erstellung des Graphen für den HNSW-Inde x an. `efConstru ction` muss größer oder gleich (2 * m) sein	Standard: 64 Bereich [4, 1000]

Es ist wichtig, dass Sie den Wert von Unterparametern wie `lists` für IVFFlat `m` und `efConstruction` für HNSW entsprechend festlegen accuracy/recall, da sich dies auf die Erstellungszeit und die Leistung Ihrer Suche auswirkt. Ein höherer Listenwert erhöht die Geschwindigkeit der Abfrage, da er die Anzahl der Vektoren in jeder Liste reduziert, was zu kleineren Regionen führt. Eine kleinere Regionsgröße kann jedoch zu mehr Erinnerungsfehlern führen, was

wiederum zu einer geringeren Genauigkeit führt. Bei HNSW `efConstruction` erhöht sich durch die Erhöhung des Werts von `m` und die Genauigkeit, aber auch die Zeit und Größe der Indexerstellung. Im Folgenden sind einige Beispiele aufgeführt:

Beispiele

HNSW

```
db.collection.createIndex(
  { "vectorEmbedding": "vector" },
  { "name": "myIndex",
    "vectorOptions": {
      "type": "hnsw",
      "dimensions": 3,
      "similarity": "euclidean",
      "m": 16,
      "efConstruction": 64
    }
  }
);
```

IVFFlat

```
db.collection.createIndex(
  { "vectorEmbedding": "vector" },
  { "name": "myIndex",
    "vectorOptions": {
      "type": "ivfflat",
      "dimensions": 3,
      "similarity": "euclidean",
      "lists":1
    }
  }
)
```

Eine Indexdefinition abrufen

Sie können die Details Ihrer Indizes, einschließlich Vektorindizes, mit dem `getIndexes` folgenden Befehl anzeigen:

Beispiel

```
db.collection.getIndexes()
```

Beispielausgabe

```
[
 {
  "v" : 4,
  "key" : {
   "_id" : 1
  },
  "name" : "_id_",
  "ns" : "test.collection"
 },
 {
  "v" : 4,
  "key" : {
   "vectorEmbedding" : "vector"
  },
  "name" : "myIndex",
  "vectorOptions" : {
   "type" : "ivfflat",
   "dimensions" : 3,
   "similarity" : "euclidean",
   "lists" : 1
  },
  "ns" : "test.collection"
 }
]
```

Abfragen von Vektoren

Amazon DocumentDB unterstützt zwei Vektorsuchoperatoren für die Abfrage von Vektoren:

Klassischer Vektor-Suchoperator

Verwenden Sie die folgende Vorlage, um einen Vektor abzufragen:

```
db.collection.aggregate([
  {
    $search: {
      "vectorSearch": {
        "vector": <query vector>,
```

```
        "path": "<vectorField>",
        "similarity": "<distance metric>",
        "k": <number of results>,
        "probes":<number of probes> [applicable for IVFFlat],
        "efSearch":<size of the dynamic list during search> [applicable for HNSW]
      }
    }
  }
]);
```

Parameter	Anforderung	Typ	Description	Wert (e)
vectorSearch	Erforderlich	operator	Wird im Befehl $search verwendet, um die Vektoren abzufragen.	
vector	Erforderlich	Array	Gibt den Abfragevektor an, der verwendet wird, um ähnliche Vektoren zu finden.	
path	Erforderlich	Zeichenfolge	Definiert den Namen des Vektorfeldes.	
k	Erforderlich	Ganzzahl	Gibt die Anzahl der Ergebnisse an, die die Suche zurückgibt.	
similarity	Erforderlich	Zeichenfolge	Gibt die Entfernungsmetrik an, die	• **euclidean** • **cosine**

Parameter	Anforderung	Typ	Description	Wert (e)
			für die Ähnlichkeitsberechnung verwendet wird.	• **`dotProduct`**
`probes`	optional	Ganzzahl	Die Anzahl der Cluster, die bei der Vektorsuche untersucht werden sollen. Ein höherer Wert sorgt für einen besseren Abruf auf Kosten der Geschwindigkeit. Er kann auf die Anzahl der Listen für die exakte Suche nach dem nächsten Nachbarn gesetzt werden (ab diesem Zeitpunkt verwendet der Planer den Index nicht mehr). Die empfohlene Einstellung, um mit der Feinabstimmung zu beginnen, ist`sqrt(# of lists)`.	Standard: 1

Parameter	Anforderung	Typ	Description	Wert (e)
`efSearch`	optional	Ganzzahl	Gibt die Größe der dynamischen Kandidatenliste an, die der HNSW-Index bei der Suche verwendet. Ein höherer Wert von `efSearch` ermöglicht einen besseren Abruf auf Kosten der Geschwindigkeit.	Standard: 40 Bereich [1, 1000]

Es ist wichtig, den Wert von `efSearch` (HNSW) oder `probes` (IVFFlat) fein abzustimmen, um die gewünschte Leistung und Genauigkeit zu erreichen. Sehen Sie sich die folgenden Beispieloperationen an:

HNSW

```
db.collection.aggregate([
  {
    $search: {
      "vectorSearch": {
        "vector": [0.2, 0.5, 0.8],
        "path": "vectorEmbedding",
        "similarity": "euclidean",
        "k": 2,
        "efSearch": 40
      }
    }
  }
]);
```

IVFFlat

```
db.collection.aggregate([
```

```
  {
    $search: {
      "vectorSearch": {
        "vector": [0.2, 0.5, 0.8],
        "path": "vectorEmbedding",
        "similarity": "euclidean",
        "k": 2,
        "probes": 1
      }
    }
  }
]);
```

Beispielausgabe

Die Ausgabe dieser Operation sieht in etwa wie folgt aus:

```
{ "_id" : ObjectId("653d835ff96bee02cad7323c"), "product_name" : "Product A",
 "vectorEmbedding" : [ 0.2, 0.5, 0.8 ] }
{ "_id" : ObjectId("653d835ff96bee02cad7323e"), "product_name" : "Product C",
 "vectorEmbedding" : [ 0.1, 0.2, 0.5 ] }
```

`$vectorSearch-Operator` (ab Amazon DocumentDB 8.0 verfügbar)

Verwenden Sie die folgende Vorlage, um einen Vektor abzufragen:

```
db.collection.aggregate([
{
  "$vectorSearch": {
    "exact": true | false,
    "index": "<index-name>" [supports only HNSW index],
    "limit": <number-of-results> [same as k],
    "path": "<vector field-to-search>",
    "queryVector": <array-of-numbers>,
    "numCandidates": <number-of-candidates> [same as efSearch],
  }
}])
```

Funktionen und Einschränkungen

Versionskompatibilität

- Die Vektorsuche für Amazon DocumentDB ist nur auf Amazon DocumentDB 5.0+ instanzbasierten Clustern verfügbar.

Vektoren

- Amazon DocumentDB kann Vektoren mit bis zu 2.000 Dimensionen indizieren. Es können jedoch bis zu 16.000 Dimensionen ohne Index gespeichert werden.

Indizes

- Für die Erstellung eines IVFFlat-Indexes ist die empfohlene Einstellung für den Parameter Listen die Anzahl von documents/1000 für bis zu 1 Million Dokumente und `sqrt(# of documents)` für mehr als 1 Million Dokumente. Aufgrund eines Arbeitsspeicherlimits unterstützt Amazon DocumentDB einen bestimmten Höchstwert des Lists-Parameters, der von der Anzahl der Dimensionen abhängt. Zu Ihrer Information enthält die folgende Tabelle die Höchstwerte des Listenparameters für Vektoren mit 500, 1000 und 2.000 Dimensionen:

Instance-Typ	Listen mit 500 Dimensionen	Listen mit 1000 Dimensionen	Listen mit 2000 Dimensionen
t3.med	372	257	150
r5l	915	741	511
r5.xl	1.393	1.196	901
r5,2 xl	5.460	5.230	4.788
r5,4 xl	7.842	7.599	7.138
r5,8 xl	11.220	10.974	10.498
r5,12 xl	13.774	13.526	13.044
r5,16xl	15.943	15.694	15.208
r5,24 xl	19.585	19.335	18.845

- Keine anderen Indexoptionen wie `compound` Vektorindizes `sparse` oder `partial` werden von Vektorindizes unterstützt.
- Die parallele Indexerstellung wird für den HNSW-Index in Amazon DocumentDB 5.0 nicht unterstützt.

Vektor-Abfrage

- Bei der Vektor-Suchanfrage ist es wichtig, die Parameter wie `probes` oder `efSearch` für optimale Ergebnisse zu optimieren. Je höher der Wert des `efSearch` Parameters `probes` oder, desto höher der Abruf und desto niedriger die Geschwindigkeit. Die empfohlene Einstellung, um mit der Feinabstimmung des Sondenparameters zu beginnen, ist`sqrt(# of lists)`.

Best Practices

Lernen Sie bewährte Methoden für die Arbeit mit der Vektorsuche in Amazon DocumentDB kennen. Dieser Abschnitt wird fortlaufend aktualisiert, wenn neue bewährte Methoden identifiziert werden.

- Bei der Indexerstellung von Inverted File with Flat Compression (IVFFlat) werden die Datenpunkte auf der Grundlage von Ähnlichkeiten gruppiert und organisiert. Damit ein Index effektiver ist, empfehlen wir Ihnen daher, vor der Indexerstellung zumindest einige Daten zu laden.
- Bei Vektor-Suchanfragen ist es wichtig, die Parameter genau einzustellen, um `efSearch` optimale Ergebnisse zu erzielen. `probes` Je höher der Wert des `efSearch` Parameters `probes` oder ist, desto höher ist der Recall und desto niedriger ist die Geschwindigkeit. Die empfohlene Einstellung, um mit der Feinabstimmung des `probes` Parameters zu beginnen, ist`sqrt(lists)`.

Ressourcen

- Vektorsuche: Was ist ein neuer Blogbeitrag
- Beispiel für einen semantischen Suchcode
- Codebeispiele für die Vektorsuche in Amazon DocumentDB

Migration zu Amazon DocumentDB

Amazon DocumentDB ist ein vollständig verwalteter Datenbankservice, der mit der MongoDB-API kompatibel ist. Sie können Ihre Daten von MongoDB-Datenbanken, die lokal oder auf Amazon Elastic Compute Cloud (Amazon EC2) laufen, nach Amazon DocumentDB migrieren, indem Sie den in diesem Abschnitt beschriebenen Prozess verwenden.

Themen

- Migrieren Sie zu Amazon DocumentDB mit AWS Database Migration Service (DMS): Schnellstartanleitung
- Runbook zur Amazon DocumentDB-Migration
- Migration von Couchbase Server

Migrieren Sie zu Amazon DocumentDB mit AWS Database Migration Service (DMS): Schnellstartanleitung

Topics

- Bereiten Sie die DMS-Quelle vor
- DMS einrichten
- DocumentDB-Komprimierung aktivieren
- Erstellen Sie eine Replikationsaufgabe
- Überwachen des Fortschritts
- Zusätzliche Informationen

Bereiten Sie die DMS-Quelle vor

Informationen Change-Streams aktivieren zum Aktivieren von DocumentDB-Change-Streams oder zum Aktivieren des MongoDB-Oplogs zur Unterstützung von DMS Change Data Capture (CDC) finden Sie unter.

- Die DMS-Quelle muss alle laufenden Änderungen beibehalten, bis der DMS-Vollladevorgang für alle enthaltenen Sammlungen abgeschlossen ist.

- DocumentDB-Change-Streams sind zeitbasiert. Stellen Sie sicher, dass Ihre `change_stream_log_retention_duration` Einstellung groß genug ist, um die Zeit bis zum vollständigen Laden abzudecken.
- Der MongoDB-Oplog hat eine feste Größe. Stellen Sie sicher, dass es so dimensioniert ist, dass es alle Operationen unter Volllast aufnehmen kann.

DMS einrichten

Erstellen Sie DMS-Instanz-, Quell- und Zielendpunkte und testen Sie jeden Endpunkt.

DocumentDB-Komprimierung aktivieren

Aktivieren Sie die Komprimierung, indem Sie eine benutzerdefinierte Parametergruppe an Ihren DocumentDB-Cluster anhängen und den Parameter default_collection_compression auf aktiviert aktualisieren. Weitere Informationen finden Sie unter Verwaltung der Dokumentenkomprimierung auf Sammlungsebene.

Erstellen Sie eine Replikationsaufgabe

1. Wählen Sie in der DMS-Konsole im Navigationsbereich Migrieren oder replizieren und dann Aufgaben aus.
2. Wählen Sie Create task aus.
3. Gehen Sie auf der Seite Aufgabe erstellen im Abschnitt Aufgabenkonfiguration wie folgt vor:
   - Geben Sie eine eindeutige und aussagekräftige Task-ID ein (z. B. „mongodb-docdb-replication“).
   - Wählen Sie den Quellendpunkt, den Sie zuvor erstellt haben, im Dropdownmenü Quelldatenbank-Endpunkt aus.
   - Wählen Sie den Zielendpunkt, den Sie zuvor erstellt haben, im Dropdownmenü Zieldatenbank-Endpunkt aus.
   - Wählen Sie als Aufgabentyp die Option Migrieren und replizieren aus.
4. Gehen Sie im Abschnitt Einstellungen wie folgt vor:
   - Aktivieren Sie für Task-Protokolle das Kästchen CloudWatch Protokolle aktivieren.
   - Wählen Sie für den Bearbeitungsmodus (oben im Abschnitt) die Option JSON-Editor und legen Sie die folgenden Attribute fest:

- Stellen Sie `ParallelApplyThreads` den Wert auf 5 (unter`TargetMetadata`) ein. Dies ermöglicht ~1000 insert/update /delete-Operationen pro Sekunde in CDC.
- Auf 16 (`MaxFullLoadSubTasks`unter) gesetzt. `FullLoadSettings` Erwägen Sie, diesen Wert je nach Größe Ihrer Instanz zu erhöhen.
- Für große Sammlungen (über 100 GB) aktivieren Sie die automatische Partition (unter Table Mapping und unter dem `parallel-load` Attribut):
  - „Typ“: „auto Partitionen“
  - „Anzahl der Partitionen“: 16

Überwachen des Fortschritts

Verwenden Sie die AWS DMS Konsole oder erstellen Sie ein benutzerdefiniertes Dashboard (Dashboarder-Tool), um die Migration zu verfolgen. Konzentrieren Sie sich auf die folgenden Kennzahlen:

- FullLoadThroughputBandwidthTarget— Misst die Netzwerkbandbreite (in KB/second), die von DMS bei der Übertragung von Daten an die Zieldatenbank während der Volllastphase der Migration verwendet wird.
- CDCLatencyTarget— Misst die Zeitverzögerung (in Sekunden) zwischen dem Zeitpunkt, an dem eine Änderung in der Quelldatenbank erfolgt, und dem Zeitpunkt, an dem diese Änderung auf die Zieldatenbank angewendet wird.
- CDCThroughputRowsTarget— Misst die Anzahl der Zeilen pro Sekunde, die DMS während der laufenden Replikationsphase der Migration auf die Zieldatenbank anwendet.

Zusätzliche Informationen

Weitere Informationen zu Amazon DocumentDB und AWS DMS finden Sie unter: Weitere Informationen finden Sie unter.

- Runbook zur Amazon DocumentDB-Migration
- Migration von MongoDB zu Amazon DocumentDB

Runbook zur Amazon DocumentDB-Migration

Dieses Runbook bietet einen umfassenden Leitfaden für die Migration einer MongoDB-Datenbank zu Amazon DocumentDB mithilfe von AWS Database Migration Service (DMS). Es wurde entwickelt, um Datenbankadministratoren, Cloud-Techniker und Entwickler während der gesamten Migration zu unterstützen — von der ersten Entdeckung bis zur Validierung nach der Migration.

Angesichts der Unterschiede in der Implementierung und den unterstützten Funktionen zwischen MongoDB und Amazon DocumentDB betont dieses Runbook einen strukturierten und systematischen Ansatz. Es beschreibt wichtige Bewertungen vor der Migration, hebt Kompatibilitätsaspekte hervor und beschreibt detailliert die wichtigsten Aufgaben, die erforderlich sind, um eine erfolgreiche Migration mit minimalen Unterbrechungen sicherzustellen.

Das Runbook ist in die folgenden Themen gegliedert:

- Kompatibilität— Machen Sie sich mit den unterstützten MongoDB-Funktionen und Datentypen in Amazon DocumentDB vertraut und identifizieren Sie potenzielle Inkompatibilitäten.
- Workload-Erkennung— Analysieren Sie bestehende MongoDB-Workloads, einschließlich read/write Muster, Datenvolumen und Leistungsbasislinien.
- Indexmigration— Analysieren Sie Strategien zum Extrahieren und Transformieren von MongoDB-Indizes für eine optimale Leistung in Amazon DocumentDB.
- Benutzermigration— Erläutern Sie den Ansatz für die Migration von Datenbankbenutzern, Rollen und Zugriffskontrollen zu Amazon DocumentDB.
- Datenmigrationen— Erläutern Sie verschiedene Methoden zur Datenmigration AWS DMS, einschließlich Volllast und Erfassung von Änderungsdaten (CDC).
- Überwachen— Erläutern Sie die verschiedenen Überwachungsansätze bei der Migration mithilfe von DMS oder systemeigenen Tools.
- Validierung— Bereitstellung von Verfahren für Datenintegritätsprüfungen, Funktionsvalidierung und Leistungsvergleiche nach der Migration.

Wenn Teams die Anleitungen in diesem Runbook befolgen, können sie einen reibungslosen, sicheren und effizienten Übergang zu Amazon DocumentDB sicherstellen und gleichzeitig die Anwendungsfunktionalität beibehalten und Risiken minimieren.

Kompatibilität

Topics

- Kompatibilität der Kernfunktionen
- Amazon DocumentDB DocumentDB-Kompatibilitätsbewertungstool

Bei der Migration von MongoDB zu Amazon DocumentDB sind eine gründliche Erstbeurteilung und Funktionskompatibilitätsprüfung für eine erfolgreiche Migration unerlässlich. Dieser Prozess beginnt mit einer umfassenden Bestandsaufnahme Ihrer MongoDB-Funktionen, einschließlich Aggregationspipeline-Operatoren, Abfragemustern, Indizes und Datenmodellen.

Da Amazon DocumentDB mit den APIs MongoDB 3.6, 4.0, 5.0 und 8.0 kompatibel ist, müssen Anwendungen, die neuere MongoDB-specific Funktionen verwenden, möglicherweise umgestaltet werden. Zu den kritischen Bereichen, die bewertet werden müssen, gehören Sharding-Mechanismen (Amazon DocumentDB verwendet einen anderen Ansatz), Transaktionsimplementierungen, Change-Stream-Funktionen und Indextypen (insbesondere Sparse-Indizes und partielle Indizes).

Auch die Leistungsmerkmale unterscheiden sich, da Amazon DocumentDB für Unternehmens-Workloads mit vorhersehbarer Leistung optimiert ist. Beim Testen sollten repräsentative Workloads auf beiden Systemen ausgeführt werden, um Abfragemuster zu identifizieren, die möglicherweise optimiert werden müssen.

Während der Bewertungsphase ist es wichtig, die Ausführungspläne zu überwachen, um potenzielle Leistungslücken zu erkennen. Dies hilft bei der Erstellung eines klaren Migrationsplans, in dem notwendige Anwendungsänderungen identifiziert und realistische Zeitpläne für einen reibungslosen Übergang festgelegt werden.

Kompatibilität der Kernfunktionen

Umfassende Funktionsunterstützung

- CRUD-Operationen — Genießen Sie volle Unterstützung für alle grundlegenden Erstellungs-, Lese-, Aktualisierungs- und Löschvorgänge, einschließlich Bulk- und Abfrageoperatoren, wodurch eine nahtlose Anwendungskompatibilität gewährleistet wird.
- Umfangreiche Indizierungsfunktionen — Nutzen Sie die umfassende Unterstützung für Einzelfeld-, Verbund-, TTL-, Teil-, Sparse- und 2dsphären-Indizes, um Ihre Abfrageleistung und Textindizes (Version 5) für textbasierte Suchvorgänge zu optimieren.
- Enterprise-grade Replikation — Profitieren Sie von einem robusten automatischen Failover-Mechanismus mit Read Replicas für hervorragende Hochverfügbarkeit ohne Betriebsaufwand.

- Fortschrittliche Backup-Lösungen — Mit dem automatisierten Backup-System mit Point-in-Time Recovery (PITR) und manuellen Snapshots auf Abruf zum Schutz Ihrer Daten können Sie sich darauf verlassen.

Verbessert AWS-integrierte Funktionen

- Optimierte Aggregation — Nutzen Sie die am häufigsten verwendeten Aggregationsstufen (`$match`,, `$group` `$sort``$project`, usw.) mit optimierter Leistung für Unternehmens-Workloads.
- Transaktionsunterstützung — Implementieren Sie Transaktionen mit mehreren Dokumenten und mehreren Sammlungen, perfekt für die meisten Anforderungen von Geschäftsanwendungen.
- Real-time Datenverfolgung — Aktivieren Sie Change-Streams mit einem einfachen Befehl und verlängern Sie die Aufbewahrungsdauer von Change-Streams durch eine einfache Parametergruppeneinstellung für die Überwachung von Datenänderungen in Echtzeit.
- Location-based Dienste — Implementieren Sie Geodatenanwendungen mit Unterstützung für `$geoNear` Operator- und 2dSphere-Indizes.
- Textsuchfunktionen — Nutzen Sie die integrierte Textsuchfunktion für die Suche nach Inhalten.

Vorteile moderner Architektur

- Cloud-native Design — Genießen Sie eine AWS optimierte Architektur, die ältere Funktionen durch effizientere Aggregations-Pipeline-Operationen ersetzt. MapReduce
- Verbesserte Sicherheit — Profitieren Sie von AWS Identity and Access Management (IAM),, SCRAM-SHA-1 SCRAM-SHA-256, X.509 Zertifikatsauthentifizierung und passwortbasierter Authentifizierung.
- Vorhersehbare Leistung — Erleben Sie eine konsistente Leistung, die speziell für Unternehmens-Workloads optimiert wurde.

Einen umfassenden Überblick über die Funktionen von Amazon DocumentDB finden Sie unter Unterstützte MongoDB-APIs, Operationen und Datentypen in Amazon DocumentDB und Funktionale Unterschiede: Amazon DocumentDB und MongoDB zur Maximierung des Potenzials Ihrer Datenbank.

Amazon DocumentDB unterstützt nicht alle von MongoDB angebotenen Indizes. Wir bieten ein kostenloses Index-Tool zur Überprüfung der Kompatibilität. Wir empfehlen, das Indextool

auszuführen, um die Inkompatibilität zu beurteilen und die Problemumgehungen entsprechend zu planen.

Amazon DocumentDB DocumentDB-Kompatibilitätsbewertungstool

Das Kompatibilitätstool von MongoDB zu Amazon DocumentDB ist ein Open-Source-Hilfsprogramm, GitHub das dabei hilft, die Kompatibilität von MongoDB-Workloads mit Amazon DocumentDB zu bewerten, indem MongoDB-Protokolle oder Anwendungsquellcode analysiert werden.

Schlüssel-Features

- Identifiziert MongoDB-API-Nutzungsmuster in Ihrem Workload
- Weist vor der Migration auf mögliche Kompatibilitätsprobleme hin
- Generiert detaillierte Kompatibilitätsberichte mit Empfehlungen
- Als eigenständiges Hilfsprogramm verfügbar, das lokal ausgeführt werden kann

Bewertungsmethoden

Log-based Bewertung

- Vorteile:
  - Erfasst das tatsächliche Laufzeitverhalten und Abfragemuster
  - Identifiziert reale Nutzungshäufigkeiten und Leistungsmerkmale
  - Erkennt dynamische Abfragen, die im Quellcode möglicherweise nicht sichtbar sind
  - Kein Zugriff auf den Quellcode der Anwendung erforderlich
- Nachteile:
  - Erfordert Zugriff auf MongoDB-Protokolle mit aktivierter Profilerstellung
  - Erfasst nur Vorgänge, die während des Protokollierungszeitraums stattgefunden haben
  - Möglicherweise fehlen selten genutzte Funktionen oder saisonale Workloads

Analyse des Quellcodes

- Vorteile:
  - Umfassende Abdeckung aller potenziellen MongoDB-Operationen in der Codebasis
  - Kann Probleme in selten ausgeführten Codepfaden identifizieren

  - Erkennt clientseitige Logik, die von Amazon DocumentDB DocumentDB-Unterschieden betroffen sein könnte
  - Sie müssen die Anwendung nicht ausführen, um die Bewertung durchzuführen
- Nachteile:
  - Kann Code kennzeichnen, der zwar existiert, aber nie in der Produktion ausgeführt wird
  - Erfordert Zugriff auf den vollständigen Quellcode der Anwendung
  - Eingeschränkte Fähigkeit, dynamisch erstellte Abfragen zu analysieren

Um optimale Ergebnisse zu erzielen, empfehlen wir, wenn möglich beide Bewertungsmethoden zu verwenden, um sich vor der Migration ein vollständiges Bild der Kompatibilitätsprobleme zu machen.

Workload-Erkennung

Die Migration von MongoDB zu Amazon DocumentDB erfordert ein gründliches Verständnis der bestehenden Datenbank-Arbeitslast. Bei der Workload-Erkennung werden Ihre Datenbanknutzungsmuster, Datenstrukturen, Abfrageleistung und Betriebsabhängigkeiten analysiert, um einen reibungslosen Übergang mit minimalen Unterbrechungen sicherzustellen. In diesem Abschnitt werden die wichtigsten Schritte beschrieben, die bei der Workload-Erkennung erforderlich sind, um eine effektive Migration von MongoDB zu Amazon DocumentDB zu ermöglichen.

Topics

- Bewertung der bestehenden MongoDB-Bereitstellung
- Identifizieren von Unterschieden im Datenmodell
- Abfrage- und Leistungsanalyse
- Überprüfung der Sicherheit und Zugriffskontrolle
- Überlegungen zum Betrieb und zur Überwachung

Bewertung der bestehenden MongoDB-Bereitstellung

Vor der Migration ist es wichtig, die aktuelle MongoDB-Umgebung zu evaluieren, einschließlich:

- Cluster-Architektur — Identifizieren Sie die Anzahl der Knoten, Replikatgruppen und Sharding-Konfigurationen. Bei der Migration von MongoDB zu Amazon DocumentDB ist es wichtig, Ihre MongoDB-Sharding-Konfiguration zu verstehen, da Amazon DocumentDB kein benutzergesteuertes Sharding unterstützt. Für Anwendungen, die für eine Shard-

MongoDB-Umgebung entwickelt wurden, müssen architektonische Änderungen vorgenommen werden, da Amazon DocumentDB mit seiner speicherbasierten Architektur einen anderen Skalierungsansatz verwendet. Bei der Umstellung auf Amazon DocumentDB müssen Sie Ihre Datenverteilungsstrategie anpassen und möglicherweise gemeinsam genutzte Sammlungen konsolidieren.

- Speicher und Datenvolumen — Messen Sie die Gesamtdatengröße und Indexgröße Ihres Clusters. Ergänzen Sie dies mit dem Oplog-Überprüfungstool, um Schreibmuster und die Geschwindigkeit des Datenwachstums zu verstehen. Weitere Informationen zur Dimensionierung Ihres Clusters finden Sie unterDimensionierung der Instanzen.
- Workload-Muster — Analysieren Sie den Lese- und Schreibdurchsatz, die Häufigkeit der Abfrageausführung und die Indexierungseffizienz.
- Betriebliche Abhängigkeiten — Dokumentieren Sie alle Anwendungen, Dienste und Integrationen, die auf MongoDB basieren.

Identifizieren von Unterschieden im Datenmodell

Amazon DocumentDB ist es zwar MongoDB-compatible, es gibt jedoch Unterschiede bei den unterstützten Funktionen, wie z. B.:

- Transaktionen — Amazon DocumentDB unterstützt ACID-Transaktionen, jedoch mit einigenEinschränkungen.
- Schemadesign — Stellen Sie sicher, dass Dokumentstrukturen, eingebettete Dokumente und Verweise den Best Practices von Amazon DocumentDB entsprechen.

Abfrage- und Leistungsanalyse

Das Verständnis des Abfrageverhaltens hilft bei der Optimierung der Leistung bei der Migration und nach der Migration. Zu den wichtigsten zu analysierenden Bereichen gehören:

- Langsame Abfragen — Identifizieren Sie Abfragen mit hoher Ausführungszeit mithilfe der Profiling-Tools von MongoDB.
- Abfragemuster — Kategorisieren Sie gängige Abfragetypen, einschließlich CRUD-Operationen und -Aggregationen.
- Indexnutzung — Beurteilen Sie, ob Indizes in Amazon DocumentDB effektiv genutzt werden oder optimiert werden müssen. Verwenden Sie die `$indexStats` Aggregationspipeline-Phase in Kombination mit der `explain()` Methode für Ihre kritischen Abfragen, um die Indexnutzung

zu bewerten und die Leistung in Amazon DocumentDB zu optimieren. Beginnen Sie mit der Ausführung`db.collection.aggregate([{$indexStats{}}])`, um zu ermitteln, welche Indizes verwendet werden. Sie können detailliertere Analysen durchführen, indem Sie Ihre häufigsten Abfragen mit `explainPlan` ausführen.

- Parallelität und Verteilung der Arbeitslast — Bewerten Sie Lese- und Schreibverhältnisse, Verbindungspooling und Leistungsengpässe.

Überprüfung der Sicherheit und Zugriffskontrolle

Authentifizierung und Autorisierung

- MongoDB RBAC zu Amazon DocumentDB IAM und RBAC — Ordnen Sie die rollenbasierten Zugriffskontrollbenutzer und Rollen von MongoDB AWS Identity and Access Management (IAM) - Richtlinien und Amazon DocumentDB SCRAM-Authentifizierungsbenutzern zu.
- Strategie zur Benutzermigration — Planen Sie die Migration von Datenbankbenutzern, benutzerdefinierten Rollen und Rechten zu den von Amazon DocumentDB unterstützten Authentifizierungsmechanismen.
- Rechteunterschiede — Identifizieren Sie MongoDB-Rechte ohne direkte Amazon DocumentDB DocumentDB-Entsprechungen (z. B. Clusterverwaltungsrollen).
- Anwendungsauthentifizierung — Aktualisieren Sie die Verbindungszeichenfolgen und die Verwaltung der Anmeldeinformationen für die Passwortrichtlinien von Amazon DocumentDB. Sie können den Secrets Manager verwenden, um Ihre Anmeldeinformationen zu speichern und Passwörter zu wechseln.
- Verwaltung von Dienstkonten — Richten Sie Prozesse für die Verwaltung der Anmeldeinformationen für Dienstkonten in ein AWS Secrets Manager.
- Implementierung der geringsten Rechte — Überprüfen und verfeinern Sie die Zugriffskontrollen, um die Prinzipien der geringsten Rechte in der neuen Umgebung zu implementieren.

Verschlüsselung

Stellen Sie sicher, dass die Verschlüsselung im Ruhezustand und bei der Übertragung den Compliance-Anforderungen entspricht.

Netzwerkkonfiguration

Planen Sie die Einrichtung von Virtual Private Cloud (VPC) und die Regeln für Sicherheitsgruppen.

Überlegungen zum Betrieb und zur Überwachung

Um die Zuverlässigkeit des Systems zu gewährleisten, sollte die Workload-Erkennung auch Folgendes beinhalten:

- Backup- und Wiederherstellungsstrategie — Evaluieren Sie bestehende Backup-Methoden und die Backup-Funktionen von Amazon DocumentDB.
- AWS Backup Integration — Nutzen Sie das zentralisierte Backup-Management AWS Backup für alle AWS Dienste, einschließlich Amazon DocumentDB.
- CloudWatch Metriken — Ordnen MongoDB MongoDB-Überwachungsmetriken Amazon CloudWatch DocumentDB-Metriken für CPU, Arbeitsspeicher, Verbindungen und Speicher zu.
- Performance Insights — Implementieren Sie Amazon DocumentDB Performance Insights, um die Datenbanklast zu visualisieren und Leistungsprobleme mit detaillierten Abfrageanalysen zu analysieren.
- Profiler — Konfigurieren Sie den Amazon DocumentDB DocumentDB-Profiler für die Erfassung langsam laufender Vorgänge (ähnlich dem Profiler von MongoDB, jedoch mit Amazon-Einstellungen). DocumentDB-specific
  - Die Aktivierung erfolgt über Parametergruppen mit entsprechenden Schwellenwerten.
  - Analysieren Sie Profiler-Daten, um Optimierungsmöglichkeiten zu identifizieren
- CloudWatch Ereignisse — Richten Sie eine ereignisgesteuerte Überwachung für Amazon DocumentDB-Clusterereignisse ein.
  - Konfigurieren Sie Benachrichtigungen für Backup-Ereignisse, Wartungsfenster und Failover.
  - Integrieren Sie Amazon SNS für Benachrichtigungen und automatische AWS Lambda Antworten.
- Audit-Protokollierung — Planen Sie die Konfiguration der Audit-Protokollierung ein, um Benutzeraktivitäten und sicherheitsrelevante Ereignisse nachzuverfolgen.
- Verbesserte Überwachung — Ermöglicht eine erweiterte Überwachung detaillierter OS-level Messwerte in Intervallen von 1 Sekunde.

Indexmigration

Bei der Migration von MongoDB zu Amazon DocumentDB werden nicht nur Daten, sondern auch Indizes übertragen, um die Abfrageleistung aufrechtzuerhalten und den Datenbankbetrieb zu optimieren. In diesem Abschnitt wird detailliert beschrieben, wie Sie Indizes Schritt für Schritt von MongoDB zu Amazon DocumentDB migrieren und dabei Kompatibilität und Effizienz sicherstellen.

Verwenden des Amazon DocumentDB DocumentDB-Indextools

Klonen Sie das Index-Tool

```
git clone https://github.com/aws-samples/amazon-documentdb-tools.git
cd amazon-documentdb-tools/index-tool
```

```
pip install -r requirements.txt
```

Indizes aus MongoDB exportieren (wenn Sie von MongoDB migrieren)

```
python3 migrationtools/documentdb_index_tool.py --dump-indexes --dir
 mongodb_index_export --uri
'mongodb://localhost:27017'
```

Indizes aus Amazon DocumentDB exportieren (wenn Sie von Amazon DocumentDB migrieren)

```
python3 migrationtools/documentdb_index_tool.py --dump-indexes --dir docdb_index_export
 --uri
'mongodb://user:password@mydocdb.cluster-cdtjj00yfi95.eu-west-
2.docdb.amazonaws.com:27017/?tls=true&tlsCAFile=rds-combined-ca-
bundle.pem&replicaSet=rs0&retryWrites=false'
```

Indizes importieren

```
python3 migrationtools/documentdb_index_tool.py --restore-indexes --skip-incompatible
 --dir
mongodb_index_export --uri 'mongodb://user:password@mydocdb.cluster-cdtjj00yfi95.eu-
west-
2.docdb.amazonaws.com:27017/?tls=true&tlsCAFile=rds-combined-ca-
bundle.pem&replicaSet=rs0&retryWrites=false'
```

Überprüfen Sie die Indizes

```
python3 migrationtools/documentdb_index_tool.py --show-issues --dir
 mongodb_index_export
```

Benutzermigration

Die Migration von Benutzern von MongoDB zu Amazon DocumentDB ist für die Aufrechterhaltung der Zugriffskontrolle, Authentifizierung und Datenbanksicherheit unerlässlich. In diesem Abschnitt werden detaillierte Schritte zur erfolgreichen Migration von MongoDB-Benutzern unter Beibehaltung ihrer Rollen und Berechtigungen mithilfe des Amazon DocumentDB DocumentDB-Export-Benutzertools beschrieben.

Verwenden des Amazon DocumentDB DocumentDB-Tools zum Exportieren von Benutzern

Der Export Users toolexportiert Benutzer und Rollen aus MongoDB oder Amazon DocumentDB in JavaScript Dateien, die dann verwendet werden können, um sie in einem anderen Cluster neu zu erstellen.

Voraussetzungen

```
# Clone the repository
git clone https://github.com/awslabs/amazon-documentdb-tools.git
cd amazon-documentdb-tools/migration/export-users
```

```
# Install required dependencies
pip install pymongo
```

Schritt 1: Benutzer und Rollen exportieren

```
# Export users and roles to JavaScript files
python3 docdbExportUsers.py \
--users-file mongodb-users.js \
--roles-file mongodb-roles.js \
--uri "mongodb://admin:password@source-host:27017/"
```

Schritt 2: Bearbeiten Sie die Benutzerdatei

```
// Example of how to update the users.js file
// Find each user creation statement and add the password
db.getSiblingDB("admin").createUser({
user: "appuser",
// Add password here
pwd: "newpassword",
```

```
roles: [
{ role: "readWrite", db: "mydb" }
]
})
```

Schritt 3: Benutzerdefinierte Rollen in Amazon DocumentDB wiederherstellen

```
# Import roles first
mongo --ssl \
--host target-host:27017 \
--sslCAFile rds-combined-ca-bundle.pem \
--username admin \
--password password \
mongodb-roles.js
```

Schritt 4: Benutzer in Amazon DocumentDB wiederherstellen

```
# Import users after roles are created
mongo --ssl \
--host target-host:27017 \
--sslCAFile rds-combined-ca-bundle.pem \
--username admin \
--password password \
mongodb-users.js
```

Wichtige Hinweise

- Passwörter werden aus Sicherheitsgründen nicht exportiert und müssen manuell zur Datei users.js hinzugefügt werden.
- Rollen müssen vor den Benutzern importiert werden, um eine korrekte Rollenzuweisung sicherzustellen.
- Das Tool generiert JavaScript Dateien, die direkt mit der Mongo-Shell ausgeführt werden können.
- Benutzerdefinierte Rollen und ihre Rechte bleiben während der Migration erhalten.
- Dieser Ansatz ermöglicht die Überprüfung und Änderung der Benutzerberechtigungen vor dem Import.

Diese Methode bietet einen sicheren und flexiblen Ansatz für die Migration von Benutzern und Rollen von MongoDB zu Amazon DocumentDB und ermöglicht gleichzeitig das Zurücksetzen von Kennwörtern während des Migrationsprozesses.

Datenmigrationen

Topics

- Online-Migration
- Offline-Migration
- Voraussetzungen
- Bereiten Sie einen Amazon DocumentDB-Cluster vor
- Führen Sie den Datendump durch (Mongodump)
- Übertragen Sie Dumpdateien in die Wiederherstellungsumgebung
- Daten in Amazon DocumentDB wiederherstellen (mongorestore)

Online-Migration

Dieser Abschnitt enthält detaillierte Schritte zur Durchführung einer Online-Migration von MongoDB zu Amazon DocumentDB, um minimale Ausfallzeiten und kontinuierliche Replikation AWS DMS zu ermöglichen. Zunächst richten Sie einen Amazon DocumentDB-Cluster als Ziel ein und stellen sicher, dass Ihre MongoDB-Instance ordnungsgemäß als Quelle konfiguriert ist. In der Regel ist für die Erfassung von Change Data Capture ein Replikat-Set-Modus erforderlich. Als Nächstes erstellen Sie eine DMS-Replikationsinstanz und definieren Quell- und Zielendpunkte mit den erforderlichen Verbindungsdetails. Nach der Validierung der Endpunkte konfigurieren und starten Sie eine Migrationsaufgabe, die das vollständige Laden von Daten, die laufende Replikation oder beides umfassen kann.

Ziel konfigurieren (Amazon DocumentDB)

> **Note**
>
> Wenn Sie bereits einen Amazon DocumentDB-Cluster für die Migration bereitgestellt haben, können Sie diesen Schritt überspringen.

Erstellen Sie eine benutzerdefinierte Parametergruppe

Informationen zu den AWS-Managementkonsole AWS CLI Oder-Verfahren finden Sie unterAmazon DocumentDB-Cluster-Parametergruppen erstellen.

Erstellen Sie einen Amazon DocumentDB-Cluster

> **Note**
>
> In diesem Handbuch werden zwar weitere Verfahren zum Erstellen eines Amazon DocumentDB-Clusters beschrieben, die Schritte in diesem Abschnitt beziehen sich jedoch speziell auf die Aufgabe, große Datenmengen auf einen neuen Cluster zu migrieren.

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Klicken Sie im Navigationsbereich auf Cluster.

   > **Tip**
   >
   > Wenn der Navigationsbereich auf der linken Seite des Bildschirms nicht angezeigt wird, wählen Sie links oben auf der Seite das Menüsymbol (≡) aus.

3. Wählen Sie in der Amazon DocumentDB-Managementkonsole unter Clusters die Option Create aus.
4. Wählen Sie auf der Seite Amazon DocumentDB-Cluster erstellen im Abschnitt Clustertyp die Option Instance-based Cluster aus (dies ist die Standardoption).
5. Gehen Sie im Abschnitt Cluster-Konfiguration wie folgt vor:

   - Geben Sie als Cluster-ID einen eindeutigen Namen ein, z. **`mydocdbcluster`** B. Beachten Sie, dass die Konsole alle Clusternamen unabhängig von der Art der Eingabe in Kleinbuchstaben ändert.
   - Wählen Sie für Engine-Version 5.0.0 aus.
6. Lassen Sie im Abschnitt Cluster-Speicherkonfiguration die Standardeinstellung von Amazon DocumentDB unverändert (dies ist die Standardoption).
7. Gehen Sie im Abschnitt Instanzkonfiguration wie folgt vor:

   - Wählen Sie für DB-Instance-Klasse die Option Speicheroptimierte Klassen (einschließlich R-Klassen) aus (dies ist die Standardeinstellung).
   - Wählen Sie für Instance-Klasse eine Instance-Klasse aus, die auf der Arbeitslast basiert. Beispiel:

- db.r6g.large: für kleinere Workloads
- db.r6g.4xlarge: für größere Workloads

Als bewährte Methode empfehlen wir, eine möglichst große Instance zu wählen, um einen optimalen Durchsatz bei Volllast zu erzielen, und sie nach Abschluss der Migration herunterzuskalieren.

- Wählen Sie für Anzahl der Instanzen die Option 1 Instanz aus. Die Auswahl einer Instanz trägt zur Kostenminimierung bei. Wir empfehlen, dass Sie nach Abschluss der Volllastmigration auf drei Instanzen skalieren, um eine hohe Verfügbarkeit zu gewährleisten.

8. Geben Sie im Abschnitt Authentifizierung einen Benutzernamen für den Hauptbenutzer ein und wählen Sie dann Selbstverwaltet aus. Geben Sie ein Passwort ein und bestätigen Sie es.
9. Wählen Sie im Abschnitt Netzwerkeinstellungen eine VPC- und Subnetzgruppe aus und konfigurieren Sie dann die VPC-Sicherheitsgruppe. Stellen Sie sicher, dass Ihre Amazon DocumentDB-Sicherheitsgruppe eingehende Verbindungen von der Sicherheitsgruppe der DMS-Instance zulässt, indem Sie die Regeln für eingehenden Datenverkehr aktualisieren.
10. Aktivieren Sie in Encryption-at-restdiesem Abschnitt die Verschlüsselung (empfohlen) und wählen Sie einen KMS-Schlüssel aus oder geben Sie ihn ein.
11. Stellen Sie im Abschnitt Backup den Aufbewahrungszeitraum für Backups ein (1—35 Tage).
12. Überprüfen Sie Ihre Konfiguration und wählen Sie Create cluster aus.

    Die Bereitstellungszeit beträgt in der Regel zwischen 10 und 15 Minuten.

Quelle konfigurieren

MongoDB und Amazon DocumentDB können je nach Szenario beide als Migrationsquellen dienen:

- MongoDB als Quelle — Häufig bei der Migration von einer lokalen oder selbstverwalteten MongoDB zu einer Amazon DocumentDB oder anderen Datenbankdiensten. AWS Erfordert die Ausführung im Replikatgruppenmodus mit einem ausreichend dimensionierten Oplog (stellen Sie sicher, dass es so dimensioniert ist, dass es alle Operationen bei Volllast aufnehmen kann), um die Erfassung von Änderungsdaten während der Migration zu unterstützen.
- Amazon DocumentDB als Quelle — Wird in der Regel für regionsübergreifende Replikation, Versions-Upgrades oder die Migration zu anderen Datenbankdiensten wie MongoDB Atlas verwendet. ErfordertChange-Streams aktivieren, dass der `change_stream_log_retention_duration` Parameter in der Cluster-Parametergruppe festgelegt wird, um laufende Änderungen während der Migration zu erfassen. Stellen Sie sicher,

dass Ihre `change_stream_log_retention_duration` Einstellung groß genug ist, um die Zeit abzudecken, die bis zum Vollladen benötigt wird.

Bevor Sie mit der Migration beginnen, konfigurieren Sie Ihre Quelle so, dass der AWS DMS Zugriff möglich ist.

Erstellen Sie einen MongoDB-Benutzer mit den richtigen Berechtigungen:

```
db.createUser({
user: "dmsUser",
pwd: "yourSecurePassword",
roles: [{ role: "readAnyDatabase", db: "admin" }]
})
```

Konfigurieren Sie Netzwerk und Authentifizierung.

Gehen Sie bei der Konfiguration der Netzwerkkonnektivität für die Migration von MongoDB zu DMS wie folgt vor:

EC2-hosted MongoDB-Quelle

- Ändern Sie die EC2-Sicherheitsgruppe, um eingehenden Datenverkehr von der Sicherheitsgruppe der DMS-Replikationsinstanz zuzulassen.
- Fügen Sie eine Regel für den TCP-Port 27017 (oder Ihren benutzerdefinierten MongoDB-Port) hinzu.
- Verwenden Sie die Sicherheitsgruppen-ID der DMS-Replikationsinstanz als Quelle für eine präzise Zugriffskontrolle.
- Stellen Sie sicher, dass das Subnetz der EC2-Instanz über eine Route zum Subnetz der DMS-Replikationsinstanz verfügt.

On-premises MongoDB-Quelle

- Konfigurieren Sie Ihre Firewall so, dass eingehende Verbindungen von den öffentlichen IP-Adressen der DMS-Replikationsinstanz zugelassen werden.
- Wenn Sie Direct Connect oder ein VPN verwenden, stellen Sie sicher, dass das Routing zwischen Ihrem Netzwerk und der VPC, die die DMS-Instanz enthält, ordnungsgemäß ist.
- Testen Sie die Konnektivität mit Telnet- oder NC-Befehlen vom DMS-Subnetz zu Ihrem MongoDB-Server.

MongoDB Atlas-Quelle

- Fügen Sie IP-Adressen einer DMS-Replikationsinstanz zur IP-Zulassungsliste von MongoDB Atlas hinzu.
- Konfigurieren Sie VPC-Peering zwischen AWS VPC und MongoDB Atlas VPC, wenn Atlas auf läuft. AWS
- AWS PrivateLink Richten Sie private Konnektivität (Enterprise-Stufe) ein, wenn die Ausführung auf einem anderen Cloud-Anbieter erfolgt.
- Erstellen Sie einen dedizierten Benutzer mit entsprechenden read/write Berechtigungen.
- Verwenden Sie eine MongoDB Atlas-Verbindungszeichenfolge, bei der der SSL-Modus auf „verify-full“ gesetzt ist.
- Stellen Sie sicher, dass die Protokollgröße für die Dauer der Migration ausreichend ist.

Amazon DocumentDB DocumentDB-Quelle

Konfigurieren Sie Ihre Amazon DocumentDB DocumentDB-Quellsicherheitsgruppe so, dass eingehender Datenverkehr von der Sicherheitsgruppe der DMS-Replikationsinstanz zugelassen wird.

Erstellen Sie eine DMS-Replikationsinstanz

Wir empfehlen die Verwendung von DMS Buddy für die Bereitstellung Ihrer DMS-Infrastruktur, da dadurch eine optimale Migrationsinfrastruktur mit optimalen DMS-Einstellungen und Instanzgrößen geschaffen wird.

Wenn Sie es vorziehen, manuell zu konfigurieren, gehen Sie wie folgt vor:

1. Öffnen Sie die AWS DMS-Konsole und wählen Sie Create Replication instance.
2. Geben Sie Details zur Replikationsinstanz ein:
    - Instanzname: Wählen Sie einen eindeutigen Namen.
    - Instanzklasse: Wählen Sie basierend auf der Arbeitslast aus. Beispiel: dms.r5.large (kleine Workloads), dms.r5.4xlarge (große Workloads).
    - Motorversion: 3.5.4
    - Zugewiesener Speicher: Die Standardeinstellung ist 100 GB (bei Bedarf erhöhen). Dies hängt von der Größe des Dokuments updates/second und der Dauer des vollen Ladevorgangs ab.
    - Multi-AZ Bereitstellung: Aktivieren Sie diese Option für hohe Verfügbarkeit, falls erforderlich.

- Wählen Sie dieselbe VPC wie Amazon DocumentDB.
- Stellen Sie sicher, dass Sicherheitsgruppen eingehenden Datenverkehr von der Quelle und Amazon DocumentDB zulassen.

3. Wählen Sie Create Replication Instance und warten Sie, bis der Status verfügbar ist.

DMS-Endpunkte erstellen

Erstellen Sie einen Quellendpunkt

Für eine MongoDB-Quelle

1. Wählen Sie in der DMS-Konsole im Navigationsbereich Migrieren oder Replizieren und dann Endpoints aus.
2. Wählen Sie Endpunkt erstellen aus.
3. Wählen Sie auf der Seite „Endpunkt erstellen“ die Option Quellendpunkt aus.
4. Gehen Sie im Abschnitt Endpunktkonfiguration wie folgt vor:

   - Geben Sie eine eindeutige und aussagekräftige Endpunkt-ID ein (z. B. „mongodb-source“).
   - Wählen Sie MongoDB als Quell-Engine.
   - Wählen Sie für Zugriff auf Endpunktdatenbank die Option Zugriffsinformationen manuell bereitstellen aus.
   - Geben Sie als Servername Ihren *MongoDB server DNS name/IP address* ein.
   - Geben Sie für Port 27017 ein (Standard-MongoDB-Port).
   - Wählen Sie für den Authentifizierungsmodus den entsprechenden Modus für Ihre Anwendung (password/SSL) (Standard ist Secrets Manager).
   - Wenn der Authentifizierungsmodus Passwort ist, geben Sie Folgendes an:
     - Benutzername und Passwort: Geben Sie MongoDB-Anmeldeinformationen ein.
     - Datenbankname: Ihr Quelldatenbankname.
     - Authentifizierungsmechanismus: SCRAM-SHA-1 (Standard) oder geeigneter Mechanismus

5. Behalten Sie für den Metadatenmodus die Standardeinstellung Dokument bei.
6. Zusätzliche Verbindungsattribute:

   - authSource=admin (wenn die Authentifizierungsdatenbank anders ist)
   - <your-replica-set-name>ReplicaSet= (erforderlich für CDC)

Für eine Amazon DocumentDB DocumentDB-Quelle

1. Wählen Sie in der DMS-Konsole im Navigationsbereich Migrieren oder Replizieren und dann Endpoints aus.
2. Wählen Sie Endpunkt erstellen aus.
3. Wählen Sie auf der Seite Endpunkt erstellen die Option Quellendpunkt aus.
4. Gehen Sie im Abschnitt Endpunktkonfiguration wie folgt vor:

   - Geben Sie eine eindeutige und aussagekräftige Endpunkt-ID ein (z. B. „docdb-source“).
   - Wählen Sie Amazon DocumentDB als Quell-Engine.
   - Wählen Sie für Zugriff auf Endpunktdatenbank die Option Zugriffsinformationen manuell bereitstellen aus.
   - Geben Sie als Servername Ihren *source Amazon DocumentDB cluster endpoint* ein.
   - Geben Sie für Port 27017 ein (Standardport von Amazon DocumentDB).
   - Wählen Sie für den SSL-Modus verify-full (empfohlen für Amazon DocumentDB).
   - Wählen Sie für CA Certificate das Amazon RDS-Root-CA-Zertifikat aus.
   - Wählen Sie für den Authentifizierungsmodus den entsprechenden Modus für Ihre Anwendung (password/SSL) (Standard ist Secrets Manager).
   - Wenn der Authentifizierungsmodus Passwort ist, geben Sie Folgendes an:
     - Benutzername und Passwort: Geben Sie Ihre Amazon DocumentDB DocumentDB-Anmeldeinformationen ein.
     - Datenbankname: Ihr Quelldatenbankname.
     - Authentifizierungsmechanismus: SCRAM-SHA-1 (Standard) oder geeigneter Mechanismus
5. Behalten Sie für den Metadatenmodus die Standardeinstellung Dokument bei.

Einen Zielendpunkt erstellen (Amazon DocumentDB)

1. Wählen Sie in der DMS-Konsole im Navigationsbereich Migrieren oder Replizieren und anschließend Endpoints aus.
2. Wählen Sie Endpunkt erstellen aus.
3. Wählen Sie auf der Seite Endpunkt erstellen die Option Zielendpunkt aus.
4. Gehen Sie im Abschnitt Endpunktkonfiguration wie folgt vor:

   - Geben Sie eine eindeutige und aussagekräftige Endpunkt-ID ein (z. B. „docdb-target“).

- Wählen Sie Amazon DocumentDB als Ziel-Engine.
- Wählen Sie für Access to Endpoint Database die Methode aus, mit der Sie den Zugriff auf die Datenbank authentifizieren möchten:
  - Wenn Sie AWS Secrets Manager wählen, wählen Sie im Feld Secret das Geheimnis aus, in dem Sie Ihre Amazon DocumentDB DocumentDB-Anmeldeinformationen speichern.
  - Wenn Sie Zugangsinformationen manuell bereitstellen wählen:
    - Geben Sie als Servername Ihren ein*target Amazon DocumentDB cluster endpoint*.
    - Geben Sie für Port 27017 ein (Standardport von Amazon DocumentDB).
    - Wählen Sie für den SSL-Modus verify-full (empfohlen für Amazon DocumentDB).
    - Laden Sie für CA Certificate das CA-Zertifikatspaket für die SSL-Verifizierung herunter und geben Sie es an.
    - Wählen Sie für den Authentifizierungsmodus den entsprechenden Modus für Ihre Anwendung (password/SSL) (Standard ist Secrets Manager).
    - Wenn der Authentifizierungsmodus Passwort ist, geben Sie Folgendes an:
      - Benutzername und Passwort: Geben Sie Ihre Amazon DocumentDB DocumentDB-Anmeldeinformationen ein.
      - Datenbankname: Ihr Quelldatenbankname.
      - Authentifizierungsmechanismus: SCRAM-SHA-1 (Standard) oder geeigneter Mechanismus

5. Behalten Sie für den Metadatenmodus die Standardeinstellung Dokument bei.

Replikationsaufgabe erstellen

1. Wählen Sie in der DMS-Konsole im Navigationsbereich Migrieren oder replizieren und dann Aufgaben aus.
2. Wählen Sie Create task aus.
3. Gehen Sie auf der Seite Aufgabe erstellen im Abschnitt Aufgabenkonfiguration wie folgt vor:

   - Geben Sie eine eindeutige und aussagekräftige Task-ID ein (z. B. „mongodb-docdb-replication“).
   - Wählen Sie den Quellendpunkt, den Sie zuvor erstellt haben, im Dropdownmenü Quelldatenbank-Endpunkt aus.

- Wählen Sie den Zielendpunkt, den Sie zuvor erstellt haben, im Dropdownmenü Zieldatenbank-Endpunkt aus.
- Wählen Sie als Aufgabentyp die Option Migrieren und replizieren aus.

4. Gehen Sie im Abschnitt Einstellungen wie folgt vor:

   - Behalten Sie für den Target-Tabellenvorbereitungsmodus die Standardeinstellung bei.
   - Behalten Sie für Aufgabe nach Abschluss des vollständigen Ladevorgangs die Standardeinstellung bei.
   - Lassen Sie für LOB-Spalteneinstellungen die Einstellung Eingeschränkter LOB-Modus unverändert.
   - Behalten Sie für die Datenvalidierung die Standardeinstellung Ausschalten bei.
   - Aktivieren Sie für Aufgabenprotokolle das Kontrollkästchen CloudWatch Protokolle aktivieren.
   - Lassen Batch-optimized Sie für Anwenden die Standardeinstellung deaktiviert (aus).

5. Wählen Sie ganz oben im Bereich Aufgabeneinstellungen im Bearbeitungsmodus die Option JSON-Editor aus und legen Sie die folgenden Attribute fest:

```
{
  "TargetMetadata": {
    "ParallelApplyThreads": 5
  },
  "FullLoadSettings": {
    "MaxFullLoadSubTasks": 16
  }
}
```

6. Fügen Sie im Abschnitt Tabellenzuordnungen eine neue Auswahlregel hinzu:

   - Fügen Sie als Schemaname die zu migrierende Quelldatenbank hinzu. Verwenden Sie%, um mehrere Datenbanken anzugeben.
   - Fügen Sie als Name der Schematabelle die Quellsammlung hinzu, die migriert werden soll. Verwenden Sie%, um mehrere Sammlungen anzugeben.
   - Behalten Sie für Aktion die Standardeinstellung Include bei

7. Fügen Sie für große Sammlungen (über 100 GB) die Regel für Tabelleneinstellungen hinzu:

   - Fügen Sie als Schemaname die zu migrierende Quelldatenbank hinzu. Verwenden Sie%, um mehrere Datenbanken anzugeben.

- Fügen Sie als Name der Schematabelle die Quellsammlung hinzu, die migriert werden soll. Verwenden Sie%, um mehrere Sammlungen anzugeben.
- Geben Sie für Anzahl der Partitionen den Wert 16 ein (sollte kleiner sein als`MaxFullLoadSubTask`).

8. Vergewissern Sie sich, dass die Option im Abschnitt „Bewertung vor der Migration“ ausgeschaltet ist.

Offline-Migration

In diesem Abschnitt wird der Prozess zur Durchführung einer Offline-Migration von einer selbstverwalteten MongoDB-Instance zu Amazon DocumentDB mithilfe nativer MongoDB-Tools beschrieben: und. `mongodump` `mongorestore`

Voraussetzungen

Anforderungen an Source MongoDB

- Zugriff auf die MongoDB-Quellinstanz mit entsprechenden Berechtigungen.
- Installieren Sie`mongodump`. falls erforderlich (es wird während einer MongoDB-Installation installiert).
- Stellen Sie sicher, dass genügend Speicherplatz für die Dump-Dateien vorhanden ist.

Amazon DocumentDB DocumentDB-Anforderungen von Target

- Stellen Sie sicher, dass Sie einen Amazon DocumentDB-Cluster bereitgestellt haben.
- Stellen Sie sicher, dass sich in derselben VPC wie Amazon DocumentDB eine EC2-Instance befindet, um die Migration zu erleichtern.
- Netzwerkkonnektivität muss zwischen Ihrer Quellumgebung und Amazon DocumentDB verfügbar sein.
- mongorestore muss auf der EC2-Migrationsinstanz installiert sein.
- Für den Zugriff auf Amazon DocumentDB müssen entsprechende IAM-Berechtigungen konfiguriert werden.

Allgemeine Anforderungen

- AWS CLI muss konfiguriert sein (wenn AWS Dienste für die Zwischenspeicherung verwendet werden)
- Für die Datenübertragung muss ausreichend Bandbreite verfügbar sein.
- Das Ausfallzeitfenster sollte genehmigt werden (wenn Sie eine Live-Migration durchführen, sollten Sie andere Methoden in Betracht ziehen)

Bereiten Sie einen Amazon DocumentDB-Cluster vor

Erstellen Sie einen Amazon DocumentDB-Cluster in AWS:

- Passen Sie eine Instance-Größe an, die auf Ihrer Arbeitslast basiert.
- Konfigurieren Sie eine VPC, Subnetze und Sicherheitsgruppen.
- Aktivieren Sie die erforderlichen Parameter über Parametergruppen.

Führen Sie den Datendump durch (Mongodump)

Wählen Sie eine der folgenden Optionen, um eine Dump-Datei zu erstellen:

- Option 1: Einfach

```
mongodump --
uri="mongodb://<source_user>:<source_password>@<source_host>:<source_port>/
<database>" --
out=/path/to/dump
```

- Option 2: Bessere Steuerung und Leistung

```
mongodump \
--uri="mongodb://<source_user>:<source_password>@<sourcehost>:<source_port>" \
--out=/path/to/dump \
--gzip \# Compress output
--numParallelCollections=4 \# Parallel collections dump
--ssl \# If using SSL
--authenticationDatabase=admin \ # If auth is required
--readPreference=secondaryPreferred # If replica set
```

- Option 3: Große Datenbanken

```
mongodump \
```

```
--host=<source_host> \
--port=<source_port> \
--username=<source_user> \
--password=<source_password> \
--db=<specific_db> \# Only dump specific DB
--collection=<specific_collection> \ # Only dump specific collection
--query='{ "date": { "$gt": "2020-01-01" } }' \ # Filter documents
--archive=/path/to/archive.gz \# Single archive output
--gzip \
--ssl
```

Übertragen Sie Dumpdateien in die Wiederherstellungsumgebung

Wählen Sie eine geeignete Methode, die auf Ihrer Dump-Größe basiert:

- Klein — Direkt auf Ihre Migrationsmaschine kopieren (EC2-Instanz, die Sie zuvor erstellt haben):

```
scp -r /path/to/dump user@migration-machine:/path/to/restore
```

- Medium — Amazon S3 als Zwischenspeicher verwenden:

```
aws s3 cp --recursive /path/to/dump s3://your-bucket/mongodb-dump/
```

- Groß — Bei sehr großen Datenbanken sollten Sie eine physische Übertragung in Betracht ziehen AWS DataSync .

Daten in Amazon DocumentDB wiederherstellen (mongorestore)

Bevor Sie mit dem Wiederherstellungsprozess beginnen, erstellen Sie die Indizes in Amazon DocumentDB. Sie können das Amazon DocumentDB Index-Tool verwenden, um Indizes zu exportieren und zu importieren.

Wählen Sie eine der folgenden Optionen, um Daten wiederherzustellen:

- Option 1: Grundlegende Wiederherstellung

```
mongorestore --uri="mongodb://<docdb_user>:<docdb_password>@<docdb_endpoint>:27017"
/path/to/dump
```

- Option 2: Bessere Steuerung und Leistung

```
mongorestore \
--uri="mongodb://<docdb_user>:<docdb_password>@<docdb_endpoint>:27017" \
--ssl \
--sslCAFile=/path/to/rds-combined-ca-bundle.pem \ # DocumentDB CA cert
--gzip \# If dumped with gzip
--numParallelCollections=4 \# Parallel restoration
--numInsertionWorkersPerCollection=4 \# Parallel documents insertion
--noIndexRestore \# skip indexes as they are pre-created
/path/to/dump
```

- Option 3: Große Datenbanken oder spezifische Kontrollen

```
mongorestore \
--host=<docdb_endpoint> \
--port=27017 \
--username=<docdb_user> \
--password=<docdb_password> \
--ssl \
--sslCAFile=/path/to/rds-combined-ca-bundle.pem \
--archive=/path/to/archive.gz \# If using archive format
--gzip \
--nsInclude="db1.*" \# Only restore specific namespaces
--nsExclude="db1.sensitive_data" \ # Exclude specific collections if needed
--noIndexRestore \# skip indexes as they are pre-created
--writeConcern="{w: 'majority'}" # Ensure write durability
```

Überwachen

Dieser Abschnitt bietet einen detaillierten Überwachungsprozess, mit dem Sie den Fortschritt, die Leistung und den Zustand einer laufenden Migration aus folgenden Quellen verfolgen können:

MongoDB nach Amazon DocumentDB

oder

Amazon DocumentDB zu Amazon DocumentDB

Die Schritte zur Überwachung gelten unabhängig von der Migrationsmethode (AWS DMS, mongodump/mongorestore, oder anderen Tools).

AWS DMS Überwachung der Migration (falls zutreffend)

Überwachen Sie die folgenden wichtigen CloudWatch Kennzahlen:

Metriken zur Volllastphase

- FullLoadThroughputBandwidthTarget— Netzwerkbandbreite (KB/second) bei Volllast
- FullLoadThroughputRowsTarget— Anzahl der pro Sekunde rows/documents geladenen
- FullLoadThroughputTablesTarget— Anzahl der tables/collections Abgeschlossenen pro Minute
- FullLoadProgressPercent— Prozentsatz der abgeschlossenen Volllast
- TablesLoaded— Anzahl der tables/collections erfolgreich geladenen
- TablesLoading— Anzahl der tables/collections aktuell geladenen
- TablesQueued— Anzahl der Personen, die tables/collections darauf warten, geladen zu werden
- TablesErrored— Nummer tables/collections , die nicht geladen werden konnte

Metriken der CDC-Phase

- CDCLatencyTarget— Zeitverzögerung (Sekunden) zwischen Quellenänderung und Zielanwendung
- CDCLatencySource— Zeitverzögerung (Sekunden) zwischen der Änderung der Quelle und dem Lesen durch das DMS
- CDCThroughputRowsTarget— Zeilen pro Sekunde, die während der laufenden Replikation angewendet werden
- CDCThroughputBandwidthTarget— Netzwerkbandbreite (KB/second) während CDC
- CDCIncomingChanges— Anzahl der von der Quelle empfangenen Änderungsereignisse
- CDCChangesMemoryTarget— Verwendeter Speicher (MB) zum Speichern von Änderungen auf der Zielseite

Metriken für Ressourcen

- CPUUtilization — CPU-Auslastung der Replikationsinstanz
- FreeableMemory— Verfügbarer Speicher auf der Replikationsinstanz
- FreeStorageSpace— Verfügbarer Speicher auf der Replikationsinstanz
- NetworkTransmitThroughput— Netzwerkdurchsatz für die Replikationsinstanz

- NetworkReceiveThroughput— Netzwerkdurchsatz für die Replikationsinstanz

Metriken für Fehler

- ErrorsCount— Gesamtzahl der Fehler während der Migration
- TableErrorsCount— Anzahl der tabellenspezifischen Fehler
- RecordsErrorsCount— Anzahl der datensatzspezifischen Fehler

Erstellen Sie CloudWatch Alarme für kritische Messwerte, z. B. `CDCLatencyTarget` um Benachrichtigungen `CPUUtilization` zu erhalten, wenn sich die Migrationsleistung verschlechtert.

DMS-Protokolle (Protokolle) CloudWatch

1. Gehen Sie zur Amazon CloudWatch Logs-Konsole.
2. Suchen Sie nach Ihrer Protokollgruppe und wählen Sie sie aus. Es wird ähnlich aussehen wie „dms-tasks —“.
3. Suchen Sie nach Protokollstreams, die möglicherweise Fehlerinformationen enthalten:
   - Streams mit „Fehler“ im Namen
   - Streams mit Task-IDs oder Endpunktnamen
   - Die neuesten Log-Streams zum Zeitpunkt Ihrer Migration
4. Suchen Sie in diesen Streams nach Schlüsselwörtern wie:
   - „Fehler“
   - „Ausnahme“
   - „gescheitert“
   - „Warnung“

Status der DMS-Aufgabe (mit AWS CLI)

```
aws dms describe-replication-tasks --filters Name=replication-task id,Values=<task_id>
 --query
"ReplicationTasks[0].Status"
```

Erwarteter Statusfluss:

erstellen → bereit → läuft → stoppt → gestoppt (oder fehlgeschlagen)

Überwachen Sie mit dem **`docdb-Dashboarder`**

Das `docdb-dashboarder` Tool bietet eine umfassende Überwachung für Amazon DocumentDB-Cluster, indem es automatisch CloudWatch Dashboards mit wichtigen Leistungskennzahlen generiert. Diese Dashboards zeigen wichtige Metriken auf Cluster-Ebene (Replikatverzögerung, Betriebszähler), Metriken auf Instance-Ebene (CPU, Arbeitsspeicher, Verbindungen) und Speichermetriken (Volumennutzung, Backup-Speicher). Für Migrationsszenarien bietet das Tool spezielle Dashboards, die den Migrationsfortschritt anhand von Kennzahlen wie CDC-Replikationsverzögerung und Betriebsraten verfolgen. Die Dashboards können mehrere Cluster gleichzeitig überwachen und bieten Unterstützung für Instanzen. NVMe-backed Durch die Visualisierung dieser Kennzahlen können Teams proaktiv Leistungsengpässe erkennen, die Ressourcenzuweisung optimieren und den reibungslosen Betrieb ihrer Amazon DocumentDB DocumentDB-Bereitstellungen sicherstellen. Das Tool macht die manuelle Erstellung von Dashboards überflüssig und bietet gleichzeitig eine konsistente Überwachung in allen Umgebungen. Anweisungen zur Einrichtung und erweiterte Konfigurationsoptionen finden Sie im Amazon DocumentDB Dashboarder Tool-Repository. GitHub

Validierung

Topics

- Checkliste für die Validierung
- Schema- und Indexvalidierung
- Datenerhebung und Validierung auf Feldebene
- Validierung mit einem DataDiffer Tool

Dieser Abschnitt enthält einen detaillierten Validierungsprozess zur Sicherstellung der Datenkonsistenz, Integrität und Anwendungskompatibilität nach der Migration von:

MongoDB nach Amazon DocumentDB

oder

Amazon DocumentDB zu Amazon DocumentDB

Die Validierungsschritte gelten unabhängig von der Migrationsmethode (AWS DMS, mongodump/mongorestore, oder anderen Tools).

Checkliste für die Validierung

Stellen Sie sicher, dass die Anzahl der Dokumente in jeder Sammlung zwischen Quelle und Ziel übereinstimmt:

MongoDB-Quelle

```
mongo --host <source_host> --port <port> --username <user> -- password <password> --
eval
"db.<collection>.count()"
```

Amazon DocumentDB DocumentDB-Ziel

```
mongo --host <target_host> --port <port> --username <user> -- password <password> --
eval
"db.<collection>.count()"
```

Schema- und Indexvalidierung

Stellen Sie Folgendes sicher:

- Alle Sammlungen sind im Ziel vorhanden.
- Indizes werden korrekt repliziert.
- Schemadefinitionen (sofern erzwungen) sind identisch.

Überprüfen Sie die Sammlungen (Quelle im Vergleich zu Ziel)

```
mongo --host <source_host> --eval "show collections"
mongo --host <target_host> --ssl --eval "show collections"
```

Indizes überprüfen (Quelle im Vergleich zu Ziel)

```
mongo --host <source_host> --eval" db.<collection>.getIndexes()"
mongo --host <target_host> --ssl –eval" db.<collection>.getIndexes()"
```

Vergleichen Sie die Liste der Sammlungen, um sicherzustellen, dass keine Sammlungen fehlen oder zusätzliche Sammlungen vorhanden sind.

Überprüfen Sie Indizes, indem Sie Indexnamen, Schlüsseldefinitionen, eindeutige Einschränkungen und TTL-Indizes (falls vorhanden) überprüfen.

Überprüfen Sie die Schemavalidierungsregeln (wenn Sie die Schemavalidierung in MongoDB verwenden)

```
mongo --host <source_host> --eval" db.getCollectionInfos({name: '<collection>'})
[0].options.validator"
   mongo --host <target_host> --ssl -eval" db.getCollectionInfos({name:
 '<collection>'})[0].options.validator"
```

Datenerhebung und Validierung auf Feldebene

Sie können Dokumente nach dem Zufallsprinzip auswählen und Felder zwischen Quelle und Ziel vergleichen.

Manuelle Probenahme

Ruft fünf zufällige Dokumente ab (Quelle):

```
mongo --host <source_host> --eval "db.<collection>.aggregate([{ \$sample: { size:
 5 } }])"
```

Ruft dieselben Dokument-IDs ab (Ziel):

```
mongo --host <target_host> --ssl -eval "db.<collection>.find({ _id: { \$in:
 [<list_of_ids>] } })"
```

Automatische Probenahme

```
import pymongo
# Connect to source and target
source_client = pymongo.MongoClient("<source_uri>")
target_client = pymongo.MongoClient("<target_uri>", ssl=True)
source_db = source_client["<db_name>"]
target_db = target_client["<db_name>"]
# Compare 100 random documents
for doc in source_db.<collection>.aggregate([{ "$sample":
{ "size": 100 } }]):
target_doc = target_db.<collection>.find_one({ "_id":
doc["_id"] })
```

```
if target_doc != doc:
print(f"# Mismatch in _id: {doc['_id']}")
else:
print(f"# Match: {doc['_id']}")
```

Validierung mit einem DataDiffer Tool

Das DataDiffer Tool bietet eine zuverlässige Möglichkeit, Daten zwischen Quell- und Zieldatenbanken zu vergleichen.

Voraussetzungen

Vor der Installation des DataDiffer Tools müssen die folgenden Voraussetzungen erfüllt sein:

- Python 3.7+
- PyMongo Bibliothek
- Netzwerkkonnektivität sowohl zu Quell- als auch zu Amazon DocumentDB DocumentDB-Zielclustern

Einrichtung und Installation

Klonen Sie das Repository und navigieren Sie zum Verzeichnis DataDiffer

```
git clone https://github.com/awslabs/amazon-documentdb-tools.git
cd amazon-documentdb-tools/migration/data-differ
```

Installieren Sie die erforderlichen Abhängigkeiten

```
pip install -r requirements.txt
```

Datenvalidierung wird ausgeführt

Erstellen Sie eine Konfigurationsdatei (z. B. config.json) mit Verbindungsdetails

```
{
"source": {
"uri": "mongodb://username:password@source-mongodb-
host:27017/?replicaSet=rs0",
"db": "your_database",
```

```
"collection": "your_collection"
},
"target": {
"uri": "mongodb://username:password@target-docdb-
cluster.region.docdb.amazonaws.com:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0",
"db": "your_database",
"collection": "your_collection"
},
"options": {
"batch_size": 1000,
"threads": 4,
"sample_size": 0,
"verbose": true
}
}
```

Führen Sie das Tool aus DataDiffer

```
python differ.py --config config.json
```

Verwenden Sie bei großen Sammlungen Stichproben, um eine Teilmenge von Daten zu validieren

```
python differ.py --config config.json --sample-size 10000
```

Um mehrere Sammlungen zu validieren, erstellen Sie separate Konfigurationsdateien oder verwenden Sie den Batch-Modus

```
python differ.py --batch-config batch_config.json
```

Ergebnisse interpretieren

Das Tool gibt Folgendes aus:

- Gesamtzahl der Dokumente in Quell- und Zieldokument
- Anzahl der übereinstimmenden Dokumente
- Anzahl der fehlenden Dokumente
- Anzahl der Dokumente mit Unterschieden
- Detaillierter Bericht über Unterschiede (falls vorhanden)

Best Practices

Im Folgenden finden Sie bewährte Methoden für die Verwendung des DataDiffer Tools:

- Schrittweise ausführen — Überprüfen Sie zunächst die Anzahl der Dokumente, nehmen Sie dann Stichproben für wichtige Dokumente vor und führen Sie abschließend, falls erforderlich, einen vollständigen Vergleich durch.
- Suchen Sie nach Schemaunterschieden — Amazon DocumentDB hat im Vergleich zu MongoDB einige Einschränkungen. Das Tool hebt inkompatible Datentypen oder Strukturen hervor.
- In Ruhephasen validieren — Führen Sie die Validierung aus, wenn die Schreibvorgänge minimal sind, um die Konsistenz zu gewährleisten.
- Überwachen Sie die Ressourcennutzung — Der Vergleichsprozess kann ressourcenintensiv sein. Passen Sie die Chargengröße und die Fadenzahl entsprechend an.
- Indizes validieren — Stellen Sie nach der Datenvalidierung sicher, dass alle erforderlichen Indizes auf dem Amazon DocumentDB DocumentDB-Zielcluster erstellt wurden.
- Validierungsergebnisse dokumentieren — Führen Sie als Teil Ihrer Migrationsdokumentation eine Aufzeichnung der Validierungsergebnisse für jede Sammlung.

Migration von Couchbase Server

Topics

- Einführung
- Vergleich mit Amazon DocumentDB
- Erkennung
- Planung
- Migration
- Validierung

Einführung

In diesem Handbuch werden die wichtigsten Punkte vorgestellt, die bei der Migration von Couchbase Server zu Amazon DocumentDB zu beachten sind. Es werden Überlegungen zu den Ermittlungs-, Planungs-, Ausführungs- und Validierungsphasen Ihrer Migration erläutert. Außerdem wird erklärt, wie Sie Offline- und Online-Migrationen durchführen.

Vergleich mit Amazon DocumentDB

	Couchbase-Server	Amazon DocumentDB
Organisation der Daten	In den Versionen 7.0 und höher sind Daten in Buckets, Bereichen und Sammlungen organisiert. In früheren Versionen wurden Daten in Buckets organisiert.	Daten sind in Datenbanken und Sammlungen organisiert.
Kompatibilität	Für jeden Dienst (z. B. Daten, Index, Suche usw.) gibt es separate APIs. Sekundäre Suchvorgänge verwenden SQL++ (früher bekannt als N1QL), eine Abfragesprache, die auf ANSI-standard SQL basiert und daher vielen Entwicklern vertraut ist.	Amazon DocumentDB ist mit der MongoDB-API kompatibel.
Architektur	Jeder Cluster-Instance ist Speicher zugeordnet. Sie können die Rechenleistung nicht unabhängig vom Speicher skalieren.	Amazon DocumentDB wurde für die Cloud entwickelt und vermeidet die Einschränkungen herkömmlicher Datenbankarchitekturen. Die Rechen- und Speicherebene sind in Amazon DocumentDB getrennt, und die Rechenschicht kann unabhängig vom Speicher skaliert werden.
Fügen Sie bei Bedarf Lesekapazität hinzu	Cluster können durch Hinzufügen von Instanzen skaliert werden. Da der Speicher an die Instanz angehängt wird, auf der der Dienst ausgeführt wird, hängt die Zeit, die für die Skalierung benötigt wird, von der Datenmenge ab, die auf	Sie können die Leseskalierung für Ihren Amazon DocumentDB-Cluster erreichen, indem Sie bis zu 15 Amazon DocumentDB DocumentDB-Replikate im Cluster erstellen. Es hat keine Auswirkungen auf die Speicherschicht.

	Couchbase-Server	Amazon DocumentDB
	die neue Instanz verschoben oder neu verteilt werden muss.	
Schnelle Wiederherstellung nach einem Knotenausfall	Cluster verfügen über automatische Failover-Funktionen, aber die Zeit, bis der Cluster wieder voll funktionsfähig ist, hängt von der Datenmenge ab, die auf die neue Instanz verschoben werden muss.	Amazon DocumentDB kann in der Regel innerhalb von 30 Sekunden ein Failover auf den Primärserver durchführen und den Cluster innerhalb von 8 bis 10 Minuten wieder auf volle Stärke zurücksetzen, unabhängig von der Datenmenge im Cluster.
Skalieren Sie den Speicher, wenn die Datenmenge wächst	Bei selbstverwalteten Clustern werden Speicher und iOS nicht automatisch skaliert.	Amazon DocumentDB DocumentDB-Speicher und iOS werden automatisch skaliert.
Daten Backup, ohne die Leistung zu beeinträchtigen	Backups werden vom Backup-Dienst durchgeführt und sind standardmäßig nicht aktiviert. Da Speicher und Datenverarbeitung nicht getrennt sind, kann dies Auswirkungen auf die Leistung haben.	Amazon DocumentDB-Backups sind standardmäßig aktiviert und können nicht deaktiviert werden. Backups werden von der Speicherebene verwaltet, sodass sie keine Auswirkungen auf die Rechenebene haben. Amazon DocumentDB unterstützt die Wiederherstellung aus einem Cluster-Snapshot und die Wiederherstellung zu einem bestimmten Zeitpunkt.

	Couchbase-Server	Amazon DocumentDB
Haltbarkeit der Daten	In einem Cluster können maximal 3 Replikatkopien von Daten vorhanden sein, also insgesamt 4 Kopien. Für jede Instanz, in der der Datendienst ausgeführt wird, sind 1, 2 oder 3 Replikatkopien der Daten aktiv.	Amazon DocumentDB verwaltet unabhängig von der Anzahl der Recheninstanzen 6 Kopien von Daten mit einem Schreibqu orum von 4 und persist true. Kunden erhalten eine Bestätigu ng, nachdem die Speicherebene 4 Kopien der Daten gespeichert hat.
Konsistenz	Sofortige Konsistenz der K/ V Abläufe wird unterstützt. Das Couchbase SDK leitet K/ V Anfragen an die spezifische Instanz weiter, die die aktive Kopie der Daten enthält. Sobald ein Update bestätigt wurde, kann der Client dieses Update garantiert lesen. Die Replikation von Updates auf andere Dienste (Index, Suche, Analytik, Eventing) ist letztlich konsistent.	Amazon DocumentDB DocumentDB-Replikate sind letztendlich konsistent. Wenn sofortige Konsistenzlesevorgänge erforderlich sind, kann der Client von der primären Instance aus lesen.
Replikation	Cross-Data Center Replication (XDCR) ermöglicht eine gefilterte, passive/active aktiv-aktive Replikati on von Daten in vielen: vielen Topologien.	Globale Amazon DocumentD B-Cluster bieten Aktiv-Passiv-Replikation in 1:many (bis zu 10) Topologien.

Erkennung

Die Migration zu Amazon DocumentDB erfordert ein gründliches Verständnis der bestehenden Datenbank-Arbeitslast. Bei der Workload-Erkennung werden Ihre Couchbase-Cluster-Konfiguration und die Betriebsmerkmale — Datensatz, Indizes und Arbeitslast — analysiert, um einen reibungslosen Übergang mit minimalen Unterbrechungen zu gewährleisten.

Cluster-Konfiguration

Couchbase verwendet eine serviceorientierte Architektur, bei der jede Funktion einem Dienst entspricht. Führen Sie den folgenden Befehl für Ihren Couchbase-Cluster aus, um festzustellen, welche Dienste verwendet werden (siehe Informationen zu Knoten abrufen):

```
curl -v -u <administrator>:<password> \
  http://<ip-address-or-hostname>:<port>/pools/nodes | \
  jq '[.nodes[].services[]] | unique'
```

Beispielausgabe:

```
[
  "backup",
  "cbas",
  "eventing",
  "fts",
  "index",
  "kv",
  "n1ql"
]
```

Die Couchbase-Dienste umfassen Folgendes:

Datendienst (kv)

Der Datendienst bietet read/write Zugriff auf Daten im Speicher und auf der Festplatte.

Amazon DocumentDB unterstützt K/V Operationen mit JSON-Daten über die MongoDB-API.

Abfragedienst (n1ql)

Der Abfragedienst unterstützt das Abfragen von JSON-Daten über SQL++.

Amazon DocumentDB unterstützt die Abfrage von JSON-Daten über die MongoDB-API.

Indexdienst (Index)

Der Indexdienst erstellt und verwaltet Indizes für Daten und ermöglicht so eine schnellere Abfrage.

Amazon DocumentDB unterstützt einen Standard-Primärindex und die Erstellung von Sekundärindizes für JSON-Daten über die MongoDB-API.

Suchdienst (fts)

Der Suchdienst unterstützt die Erstellung von Indizes für die Volltextsuche.

Mit der nativen Volltextsuchfunktion von Amazon DocumentDB können Sie mithilfe von speziellen Textindizes über die MongoDB-API eine Textsuche in großen Textdatensätzen durchführen. Für erweiterte Suchanwendungsfälle bietet die Amazon DocumentDB Zero-ETL-Integration mit Amazon OpenSearch Service erweiterte Suchfunktionen wie Fuzzy-Suche, sammlungsübergreifende Suche und mehrsprachige Suche in Amazon DocumentDB DocumentDB-Daten.

Analyseservice (CBAS)

Der Analysedienst unterstützt die Analyse von JSON-Daten nahezu in Echtzeit.

Amazon DocumentDB unterstützt Ad-hoc-Abfragen von JSON-Daten über die MongoDB-API. Sie können mit Apache Spark, der auf Amazon EMR läuft, auch komplexe Abfragen für Ihre JSON-Daten in Amazon DocumentDB ausführen.

Veranstaltungsservice (Eventing)

Der Eventing-Dienst führt als Reaktion auf Datenänderungen benutzerdefinierte Geschäftslogik aus.

Amazon DocumentDB automatisiert ereignisgesteuerte Workloads, indem es jedes Mal AWS Lambda Funktionen aufruft, wenn sich Daten mit Ihrem Amazon DocumentDB-Cluster ändern.

Backup-Dienst (Backup)

Der Backup-Service plant vollständige und inkrementelle Datensicherungen und Zusammenführungen früherer Datensicherungen.

Amazon DocumentDB sichert Ihre Daten kontinuierlich auf Amazon S3 mit einer Aufbewahrungsdauer von 1—35 Tagen, sodass Sie innerhalb des Aufbewahrungszeitraums für Backups an jedem beliebigen Punkt schnell wiederherstellen können. Amazon DocumentDB erstellt im Rahmen dieses kontinuierlichen Backup-Prozesses auch automatische Schnappschüsse Ihrer Daten. Sie können auch die Sicherung und Wiederherstellung von Amazon DocumentDB mit AWS Backup verwalten. .

Betriebliche Eigenschaften

Verwenden Sie das Discovery Tool for Couchbase, um die folgenden Informationen zu Ihrem Datensatz, Ihren Indizes und Ihrer Arbeitslast abzurufen. Diese Informationen helfen Ihnen bei der Größe Ihres Amazon DocumentDB-Clusters.

Dataset

Das Tool ruft die folgenden Bucket-, Bereichs- und Sammlungsinformationen ab:

1. Bucket-Name
2. Bucket-Typ
3. Name des Bereichs
4. Name der Sammlung
5. Gesamtgröße (Byte)
6. Gesamtzahl der Artikel
7. Artikelgröße (Byte)

Indizes

Das Tool ruft die folgenden Indexstatistiken und alle Indexdefinitionen für alle Buckets ab. Beachten Sie, dass Primärindizes ausgeschlossen sind, da Amazon DocumentDB automatisch einen Primärindex für jede Sammlung erstellt.

1. Bucket-Name
2. Name des Bereichs
3. Name der Sammlung
4. Indexname
5. Indexgröße (Byte)

Workload

Das Tool ruft Metriken ab K/V und fragt N1QL ab. K/V Metrikwerte werden auf Bucket-Ebene und SQL++-Metriken auf Cluster-Ebene gesammelt.

Die Befehlszeilenoptionen des Tools lauten wie folgt:

```
python3 discovery.py \
  --username <source cluster username> \
  --password <source cluster password> \
  --data_node <data node IP address or DNS name> \
  --admin_port <administration http REST port> \
  --kv_zoom <get bucket statistics for specified interval> \
```

```
  --tools_path <full path to Couchbase tools> \
  --index_metrics <gather index definitions and SQL++ metrics> \
  --indexer_port <indexer service http REST port> \
  --n1ql_start <start time for sampling> \
  --n1ql_step <sample interval over the sample period>
```

Hier sehen Sie ein Beispiel für einen Befehl.

```
python3 discovery.py \
  --username username \
  --password ******** \
  --data_node "http://10.0.0.1" \
  --admin_port 8091 \
  --kv_zoom week \
  --tools_path "/opt/couchbase/bin" \
  --index_metrics true \
  --indexer_port 9102 \
  --n1ql_start -60000 \
  --n1ql_step 1000
```

K/V Die Metrikwerte basieren auf Stichproben der letzten Woche alle 10 Minuten (siehe HTTP-Methode und URI). SQL++-Metrikwerte basieren auf Stichproben der letzten 60 Sekunden alle 1 Sekunde (siehe Allgemeine Bezeichnungen). Die Ausgabe des Befehls wird in den folgenden Dateien gespeichert:

collection-stats.csv — Informationen zu Bucket, Umfang und Sammlung

```
bucket,bucket_type,scope_name,collection_name,total_size,total_items,document_size
beer-sample,membase,_default,_default,2796956,7303,383
gamesim-sample,membase,_default,_default,114275,586,196
pillowfight,membase,_default,_default,1901907769,1000006,1902
travel-sample,membase,inventory,airport,547914,1968,279
travel-sample,membase,inventory,airline,117261,187,628
travel-sample,membase,inventory,route,13402503,24024,558
travel-sample,membase,inventory,landmark,3072746,4495,684
travel-sample,membase,inventory,hotel,4086989,917,4457
...
```

index-stats.csv — Indexnamen und -größen

```
bucket,scope,collection,index-name,index-size
```

```
beer-sample,_default,_default,beer_primary,468144
gamesim-sample,_default,_default,gamesim_primary,87081
travel-sample,inventory,airline,def_inventory_airline_primary,198290
travel-sample,inventory,airport,def_inventory_airport_airportname,513805
travel-sample,inventory,airport,def_inventory_airport_city,487289
travel-sample,inventory,airport,def_inventory_airport_faa,526343
travel-sample,inventory,airport,def_inventory_airport_primary,287475
travel-sample,inventory,hotel,def_inventory_hotel_city,497125
...
```

kv-stats.csv — Metriken für alle Buckets abrufen, festlegen und löschen

```
bucket,gets,sets,deletes
beer-sample,0,0,0
gamesim-sample,0,0,0
pillowfight,369,521,194
travel-sample,0,0,0
```

n1ql-stats.csv — SQL++ wählt Metriken für den Cluster aus, löscht sie und fügt sie ein

```
selects,deletes,inserts
0,132,87
```

indexes- .txt <bucket-name>— Indexdefinitionen aller Indizes im Bucket. Beachten Sie, dass Primärindizes ausgeschlossen sind, da Amazon DocumentDB automatisch einen Primärindex für jede Sammlung erstellt.

```
CREATE INDEX `def_airportname` ON `travel-sample`(`airportname`)
CREATE INDEX `def_city` ON `travel-sample`(`city`)
CREATE INDEX `def_faa` ON `travel-sample`(`faa`)
CREATE INDEX `def_icao` ON `travel-sample`(`icao`)
CREATE INDEX `def_inventory_airport_city` ON `travel-
sample`.`inventory`.`airport`(`city`)
CREATE INDEX `def_inventory_airport_faa` ON `travel-
sample`.`inventory`.`airport`(`faa`)
CREATE INDEX `def_inventory_hotel_city` ON `travel-sample`.`inventory`.`hotel`(`city`)
CREATE INDEX `def_inventory_landmark_city` ON `travel-
sample`.`inventory`.`landmark`(`city`)
CREATE INDEX `def_sourceairport` ON `travel-sample`(`sourceairport`)
...
```

Planung

In der Planungsphase legen Sie die Anforderungen an den Amazon DocumentDB-Cluster und die Zuordnung der Couchbase-Buckets, -Bereiche und -Sammlungen zu Amazon DocumentDB DocumentDB-Datenbanken und -Sammlungen fest.

Anforderungen für Amazon DocumentDB-Cluster

Verwenden Sie die in der Ermittlungsphase gesammelten Daten, um die Größe Ihres Amazon DocumentDB-Clusters zu bestimmen. Weitere Informationen zur Dimensionierung Ihres Amazon DocumentDB-Clusters finden Sie unter Instance-Größe.

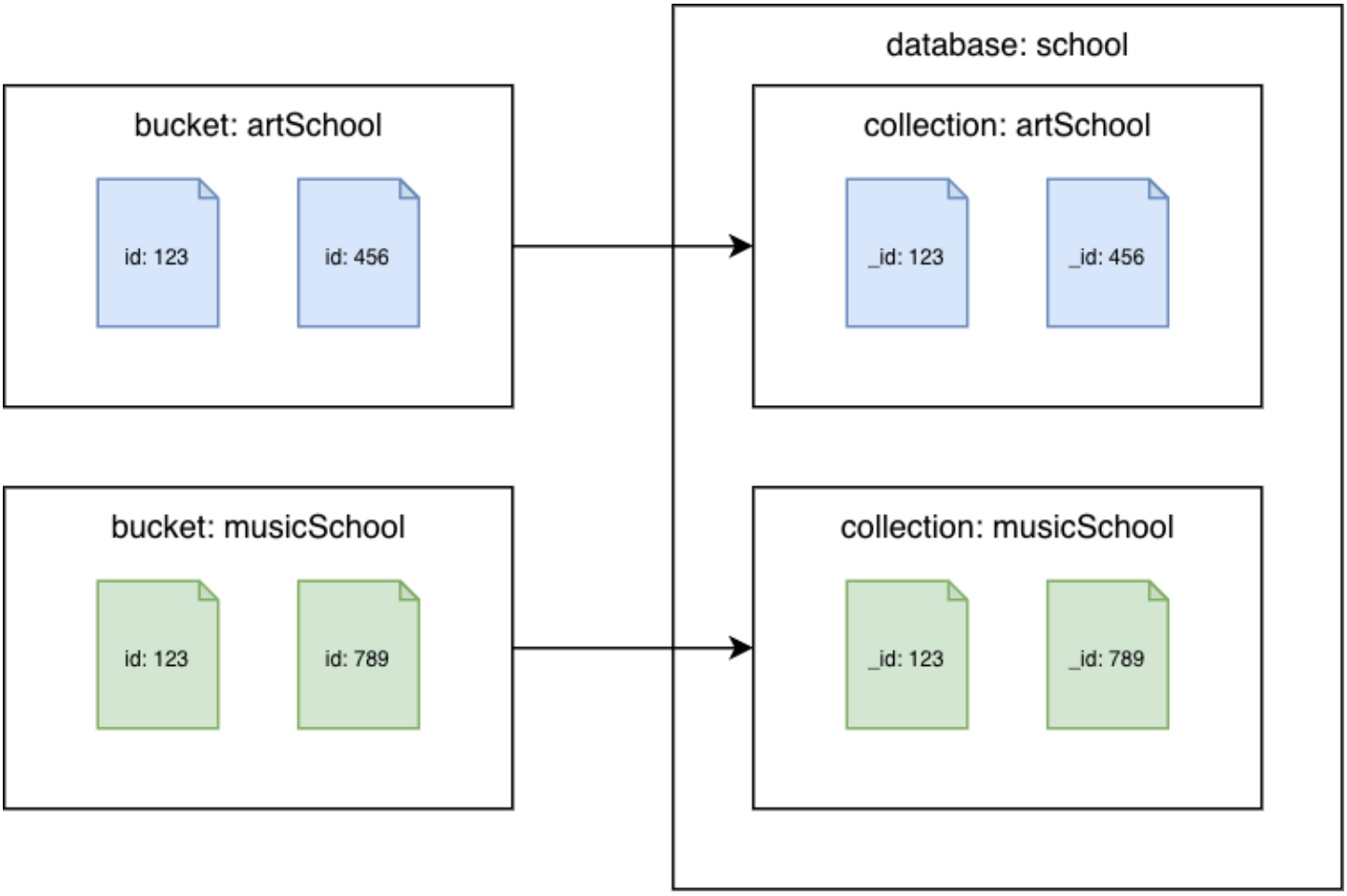
Zuordnung von Buckets, Bereichen und Sammlungen zu Datenbanken und Sammlungen

Ermitteln Sie die Datenbanken und Sammlungen, die in Ihren Amazon DocumentDB-Clustern vorhanden sein werden. Ziehen Sie die folgenden Optionen in Betracht, je nachdem, wie die Daten in Ihrem Couchbase-Cluster organisiert sind. Dies sind nicht die einzigen Optionen, aber sie bieten Ausgangspunkte, die Sie in Betracht ziehen sollten.

Couchbase Server 6.x oder früher

Couchbase-Buckets zu Amazon DocumentDB-Sammlungen

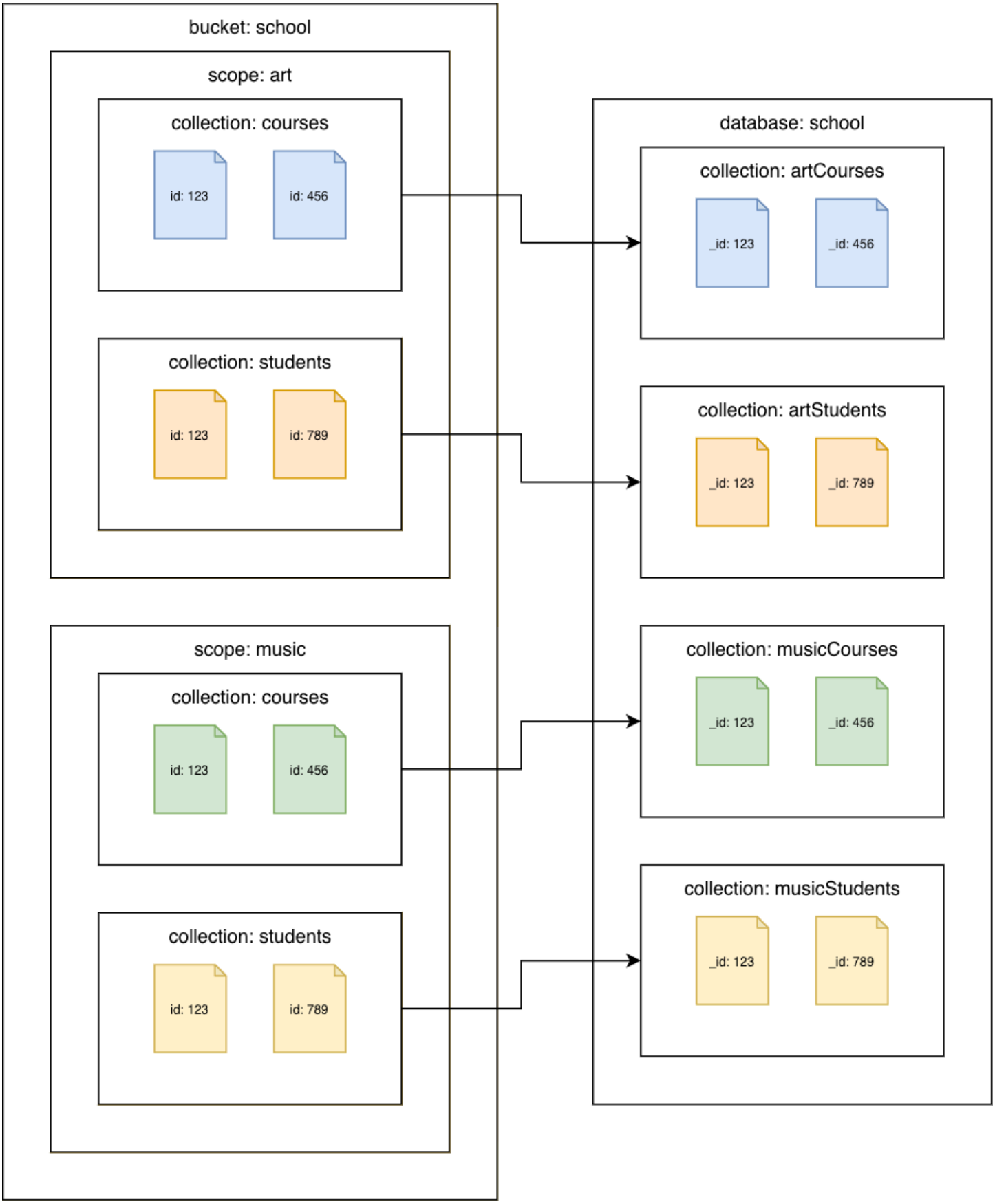
Migrieren Sie jeden Bucket in eine andere Amazon DocumentDB-Sammlung. In diesem Szenario wird der `id` Couchbase-Dokumentwert als Amazon DocumentDB `_id` DocumentDB-Wert verwendet.



Couchbase Server 7.0 oder höher

Couchbase-Sammlungen zu Amazon DocumentDB-Sammlungen

Migrieren Sie jede Sammlung zu einer anderen Amazon DocumentDB-Sammlung. In diesem Szenario wird der `id` Couchbase-Dokumentwert als Amazon DocumentDB `_id` DocumentDB-Wert verwendet.


bucket: school
scope: art
collection: courses
id: 123
id: 456
collection: students
id: 123
id: 789
scope: music
collection: courses
id: 123
id: 456
collection: students
id: 123
id: 789
database: school
collection: artCourses
_id: 123
_id: 456
collection: artStudents
_id: 123
_id: 789
collection: musicCourses
_id: 123
_id: 456
collection: musicStudents
_id: 123
_id: 789

Migration

Indexmigration

Bei der Migration zu Amazon DocumentDB werden nicht nur Daten, sondern auch Indizes übertragen, um die Abfrageleistung aufrechtzuerhalten und den Datenbankbetrieb zu optimieren. In diesem Abschnitt wird detailliert beschrieben, wie Sie Indizes Schritt für Schritt zu Amazon DocumentDB migrieren und dabei Kompatibilität und Effizienz sicherstellen.

Verwenden Sie Amazon Q, um `CREATE INDEX` SQL++-Anweisungen in Amazon DocumentDB DocumentDB-Befehle `createIndex()` zu konvertieren.

1. Laden Sie die Index-.txt-Datei <bucket name>(en) hoch, die mit dem Discovery Tool for Couchbase erstellt wurden.
2. Geben Sie die folgende Aufforderung ein:

   ```
   Convert the Couchbase CREATE INDEX statements to Amazon DocumentDB
   createIndex commands
   ```

Amazon Q generiert entsprechende Amazon DocumentDB `createIndex()` DocumentDB-Befehle. Beachten Sie, dass Sie möglicherweise die Sammlungsnamen aktualisieren müssen, je nachdem, wie Sie die Couchbase-Buckets, -Bereiche und -Sammlungen den Amazon DocumentDB-Sammlungen zugeordnet haben.

Beispiel:

indexes-beer-sample.txt

```
CREATE INDEX `beerType` ON `beer-sample`(`type`)
CREATE INDEX `code` ON `beer-sample`(`code`) WHERE (`type` = "brewery")
```

Beispiel für eine Amazon Q-Ausgabe (Auszug):

```
db.beerSample.createIndex(
  { "type": 1 },
  {
    "name": "beerType",
    "background": true
  }
)
```

```
db.beerSample.createIndex(
  { "code": 1 },
  {
    "name": "code",
    "background": true,
    "partialFilterExpression": { "type": "brewery" }
  }
)
```

Weitere Informationen zu Indizes, die Amazon Q nicht konvertieren kann, finden Sie unter Amazon DocumentDB DocumentDB-Indizes verwalten und Indizes und Indexeigenschaften.

Code umgestalten, um die MongoDB-APIs zu verwenden

Clients verwenden die Couchbase-SDKs, um eine Verbindung zum Couchbase-Server herzustellen. Amazon DocumentDB-Clients verwenden MongoDB-Treiber, um eine Verbindung zu Amazon DocumentDB herzustellen. Alle von den Couchbase SDKs unterstützten Sprachen werden auch von MongoDB-Treibern unterstützt. Weitere Informationen zum Treiber für Ihre Sprache finden Sie unter MongoDB-Treiber.

Da sich die APIs zwischen Couchbase Server und Amazon DocumentDB unterscheiden, müssen Sie Ihren Code umgestalten, um die entsprechenden MongoDB-APIs zu verwenden. Sie können Amazon Q verwenden, um die K/V API-Aufrufe und SQL++-Abfragen in die entsprechenden MongoDB-APIs zu konvertieren:

1. Laden Sie die Quellcodedatei (en) hoch.
2. Geben Sie die folgende Eingabeaufforderung ein:

```
Convert the Couchbase API code to Amazon DocumentDB API code
```

Mithilfe des Python-Codebeispiels Hello Couchbase generiert Amazon Q Folgendes (Auszug):

```
from datetime import timedelta
from pymongo import MongoClient

# Connection parameters
database_name = "travel-sample"

# Connect to Amazon DocumentDB cluster
client = MongoClient('<Amazon DocumentDB connection string>')
```

```
# Get reference to database and collection
db = client['travel-sample']
airline_collection = db['airline']

# upsert document function
def upsert_document(doc):
    print("\nUpsert Result: ")
    try:
        # key will equal: "airline_8091"
        key = doc["type"] + "_" + str(doc["id"])
        doc['_id'] = key # Amazon DocumentDB uses _id as primary key
        result = airline_collection.update_one(
            {'_id': key},
            {'$set': doc},
            upsert=True
        )
        print(f"Modified count: {result.modified_count}")
    except Exception as e:
        print(e)

# get document function
def get_airline_by_key(key):
    print("\nGet Result: ")
    try:
        result = airline_collection.find_one({'_id': key})
        print(result)
    except Exception as e:
        print(e)

# query for document by callsign
def lookup_by_callsign(cs):
    print("\nLookup Result: ")
    try:
        result = airline_collection.find(
            {'callsign': cs},
            {'name': 1, '_id': 0}
        )
        for doc in result:
            print(doc['name'])
    except Exception as e:
        print(e)

# Test document
```

```
airline = {
    "type": "airline",
    "id": 8091,
    "callsign": "CBS",
    "iata": None,
    "icao": None,
    "name": "Couchbase Airways",
}

upsert_document(airline)
get_airline_by_key("airline_8091")
lookup_by_callsign("CBS")
```

Beispiele für das Herstellen einer Verbindung zu Amazon DocumentDB in Python, PHP, Go, Java, C#/.NET Node.js, R und Ruby finden Sie unter Programmgesteuert mit Amazon DocumentDB verbinden.

Wählen Sie den Migrationsansatz

Bei der Migration von Daten zu Amazon DocumentDB gibt es zwei Optionen:

1. Offline-Migration
2. Online-Migration

Offline-Migration

Ziehen Sie eine Offline-Migration in Betracht, wenn:

- Ausfallzeiten sind akzeptabel: Bei der Offline-Migration werden Schreibvorgänge in die Quelldatenbank gestoppt, die Daten exportiert und anschließend in Amazon DocumentDB importiert. Dieser Vorgang führt zu Ausfallzeiten für Ihre Anwendung. Wenn Ihre Anwendung oder Ihr Workload diesen Zeitraum der Nichtverfügbarkeit verträgt, ist eine Offline-Migration eine praktikable Option.
- Migration kleinerer Datensätze oder Durchführung von Machbarkeitsnachweisen: Bei kleineren Datensätzen ist der Zeitaufwand für den Export- und Importvorgang relativ kurz, sodass die Offline-Migration eine schnelle und einfache Methode darstellt. Es eignet sich auch gut für Entwicklungs-, Test- und Machbarkeitsnachweisumgebungen, in denen Ausfallzeiten weniger kritisch sind.

- Einfachheit hat Priorität: Die Offline-Methode mit cbexport und mongoimport ist im Allgemeinen der einfachste Ansatz zur Datenmigration. Sie vermeidet die Komplexität der Erfassung von Änderungsdaten (CDC), die mit Online-Migrationsmethoden verbunden ist.
- Es müssen keine laufenden Änderungen repliziert werden: Wenn die Quelldatenbank während der Migration nicht aktiv Änderungen empfängt oder wenn diese Änderungen nicht unbedingt erfasst und während des Migrationsprozesses auf das Ziel angewendet werden müssen, ist ein Offline-Ansatz angemessen.

Topics

- Couchbase Server 6.x oder früher
- Couchbase Server 7.0 oder höher

Couchbase Server 6.x oder früher

Couchbase-Bucket zur Amazon DocumentDB-Sammlung

Exportieren Sie Daten mit cbexport json, um einen JSON-Dump aller Daten im Bucket zu erstellen. Für die `--format` Option können Sie oder verwenden. `lines` `list`

```
cbexport json \
  --cluster <source cluster endpoint> \
  --bucket <bucket name> \
  --format <lines | list> \
  --username <username> \
  --password <password> \
  --output export.json \
  --include-key _id
```

Importieren Sie die Daten mithilfe von mongoimport in eine Amazon DocumentDB-Sammlung mit der entsprechenden Option zum Importieren der Zeilen oder Listen:

Zeilen:

```
mongoimport \
  --db <database> \
  --collection <collection> \
  --uri "<Amazon DocumentDB cluster connection string>" \
  --file export.json
```

Liste:

```
mongoimport \
  --db <database> \
  --collection <collection> \
  --uri "<Amazon DocumentDB cluster connection string>" \
  --jsonArray \
  --file export.json
```

Couchbase Server 7.0 oder höher

Verwenden Sie die Tools cbexport und mongoimport, um eine Offline-Migration durchzuführen:

Couchbase-Bucket mit Standardbereich und Standardsammlung

Exportieren Sie Daten mit cbexport json, um einen JSON-Dump aller Sammlungen im Bucket zu erstellen. Für die `--format` Option können Sie oder verwenden. `lines` `list`

```
cbexport json \
  --cluster <source cluster endpoint> \
  --bucket <bucket name> \
  --format <lines | list> \
  --username <username> \
  --password <password> \
  --output export.json \
  --include-key _id
```

Importieren Sie die Daten mithilfe von mongoimport in eine Amazon DocumentDB-Sammlung mit der entsprechenden Option zum Importieren der Zeilen oder Listen:

Zeilen:

```
mongoimport \
  --db <database> \
  --collection <collection> \
  --uri "<Amazon DocumentDB cluster connection string>" \
  --file export.json
```

Liste:

```
mongoimport \
```

```
  --db <database> \
  --collection <collection> \
  --uri "<Amazon DocumentDB cluster connection string>" \
  --jsonArray \
  --file export.json
```

Couchbase-Sammlungen zu Amazon DocumentDB-Sammlungen

Exportieren Sie Daten mit cbexport json, um für jede Sammlung einen JSON-Dump zu erstellen. Verwenden Sie die `--include-data` Option, um jede Sammlung zu exportieren. Für die `--format` Option können Sie `lines` oder verwendenlist. Verwenden Sie die `--collection-field` Optionen `--scope-field` und, um den Namen des Bereichs und der Sammlung in den angegebenen Feldern in jedem JSON-Dokument zu speichern.

```
cbexport json \
  --cluster <source cluster endpoint> \
  --bucket <bucket name> \
  --include-data <scope name>.<collection name> \
  --format <lines | list> \
  --username <username> \
  --password <password> \
  --output export.json \
  --include-key _id \
  --scope-field "_scope" \
  --collection-field "_collection"
```

Da cbexport die `_collection` Felder `_scope` und zu jedem exportierten Dokument hinzugefügt hat, können Sie sie mit Suchen und Ersetzen oder einer beliebigen Methode aus jedem Dokument in der Exportdatei entfernen. `sed`

Importieren Sie die Daten für jede Sammlung mithilfe von mongoimport in eine Amazon DocumentDB-Sammlung mit der entsprechenden Option zum Importieren der Zeilen oder Listen:

Zeilen:

```
mongoimport \
--db <database> \
--collection <collection> \
--uri "<Amazon DocumentDB cluster connection string>" \
--file export.json
```

Liste:

```
mongoimport \
--db <database> \
--collection <collection> \
--uri "<Amazon DocumentDB cluster connection string>" \
--jsonArray \
--file export.json
```

Online-Migration

Ziehen Sie eine Online-Migration in Betracht, wenn Sie Ausfallzeiten minimieren möchten und laufende Änderungen nahezu in Echtzeit auf Amazon DocumentDB repliziert werden müssen.

Unter So führen Sie eine Live-Migration von Couchbase zu Amazon DocumentDB durch, um zu erfahren, wie Sie eine Live-Migration zu Amazon DocumentDB durchführen. Die Dokumentation führt Sie durch die Bereitstellung der Lösung und die Durchführung einer Live-Migration eines Buckets zu einem Amazon DocumentDB-Cluster.

Topics

- Couchbase Server 6.x oder früher
- Couchbase Server 7.0 oder höher

Couchbase Server 6.x oder früher

Couchbase-Bucket zur Amazon DocumentDB-Sammlung

Das Migrationsprogramm für Couchbase ist vorkonfiguriert, um eine Online-Migration eines Couchbase-Buckets zu einer Amazon DocumentDB-Sammlung durchzuführen. Wenn man sich die Konfiguration des Sink-Connectors ansieht, ist der `document.id.strategy` Parameter so konfiguriert, dass er den Nachrichtenschlüsselwert als `_id` Feldwert verwendet (siehe Eigenschaften der Sink-Connector-ID-Strategie):

```
ConnectorConfiguration:
  document.id.strategy:
 'com.mongodb.kafka.connect.sink.processor.id.strategy.ProvidedInKeyStrategy'
```

Couchbase Server 7.0 oder höher

Couchbase-Bucket mit Standardbereich und Standardsammlung

Das Migrationsprogramm für Couchbase ist vorkonfiguriert, um eine Online-Migration eines Couchbase-Buckets zu einer Amazon DocumentDB-Sammlung durchzuführen. Wenn man sich die Konfiguration des Sink-Connectors ansieht, ist der `document.id.strategy` Parameter so konfiguriert, dass er den Nachrichtenschlüsselwert als `_id` Feldwert verwendet (siehe Eigenschaften der Sink-Connector-ID-Strategie):

```
ConnectorConfiguration:
  document.id.strategy:
 'com.mongodb.kafka.connect.sink.processor.id.strategy.ProvidedInKeyStrategy'
```

Couchbase-Sammlungen zu Amazon DocumentDB-Sammlungen

Konfigurieren Sie den Quell-Connector so, dass jede Couchbase-Sammlung in jedem Bereich zu einem separaten Thema gestreamt wird (siehe Quellkonfigurationsoptionen). Beispiel:

```
ConnectorConfiguration:
  # add couchbase.collections configuration
  couchbase.collections: '<scope 1>.<collection 1>, <scope 1>.<collection 2>, ...'
```

Konfigurieren Sie den Sink Connector so, dass er von jedem Thema in eine separate Amazon DocumentDB-Sammlung streamt (siehe Eigenschaften der Sink Connector-Konfiguration). Beispiel:

```
ConnectorConfiguration:
  # remove collection configuration
  #collection: 'test'

  # modify topics configuration
  topics: '<bucket>.<scope 1>.<collection 1>, <bucket>.<scope 1>.<collection 2>, ...'

  # add topic.override.%s.%s configurations for each topic
  topic.override.<bucket>.<scope 1>.<collection 1>.collection: '<collection>'
  topic.override.<bucket>.<scope 1>.<collection 2>.collection: '<collection>'
```

Validierung

Dieser Abschnitt enthält einen detaillierten Validierungsprozess zur Überprüfung der Datenkonsistenz und Integrität nach der Migration zu Amazon DocumentDB. Die Validierungsschritte gelten unabhängig von der Migrationsmethode.

Topics

- Stellen Sie sicher, dass alle Sammlungen im Ziel vorhanden sind
- Überprüfen Sie die Anzahl der Dokumente zwischen Quell- und Zielclustern
- Dokumente zwischen Quell- und Zielclustern vergleichen

Stellen Sie sicher, dass alle Sammlungen im Ziel vorhanden sind

Couchbase-Quelle

Option 1: Abfrage-Workbench

```
SELECT RAW `path`
  FROM system:keyspaces
  WHERE `bucket` = '<bucket>'
```

Option 2: CBQ-Tool

```
cbq \
  -e <source cluster endpoint> \
  -u <username> \
  -p <password> \
  -q "SELECT RAW `path`
       FROM system:keyspaces
       WHERE `bucket` = '<bucket>'"
```

Amazon DocumentDB DocumentDB-Ziel

mongosh (siehe Connect zu Ihrem Amazon DocumentDB-Cluster herstellen):

```
db.getSiblingDB('<database>')
```

```
db.getCollectionNames()
```

Überprüfen Sie die Anzahl der Dokumente zwischen Quell- und Zielclustern

Couchbase-Quelle

Couchbase Server 6.x oder früher

Option 1: Query Workbench

```
SELECT COUNT(*)
FROM `<bucket>`
```

Option 2: cbq

```
cbq \
  -e <source cluster endpoint> \
  -u <username> \
  -p <password> \
  -q "SELECT COUNT(*)
       FROM `<bucket:>`"
```

Couchbase Server 7.0 oder höher

Option 1: Query Workbench

```
SELECT COUNT(*)
FROM `<bucket>`.`<scope>`.`<collection>`
```

Option 2: cbq

```
cbq \
  -e <source cluster endpoint> \
  -u <username> \
  -p <password> \
  -q "SELECT COUNT(*)
       FROM `<bucket:>`.`<scope>`.`<collection>`"
```

Amazon DocumentDB DocumentDB-Ziel

mongosh (siehe Connect zu Ihrem Amazon DocumentDB-Cluster herstellen):

```
db = db.getSiblingDB('<database>')
db.getCollection('<collection>').countDocuments()
```

Dokumente zwischen Quell- und Zielclustern vergleichen

Couchbase-Quelle

Couchbase Server 6.x oder früher

Option 1: Query Workbench

```
SELECT META().id as _id, *
FROM `<bucket>`
LIMIT 5
```

Option 2: cbq

```
cbq \
  -e <source cluster endpoint>
  -u <username> \
  -p <password> \
  -q "SELECT META().id as _id, *
       FROM `<bucket>` \
       LIMIT 5"
```

Couchbase Server 7.0 oder höher

Option 1: Query Workbench

```
SELECT COUNT(*)
FROM `<bucket>`.`<scope>`.`<collection>`
```

Option 2: cbq

```
cbq \
  -e <source cluster endpoint> \
  -u <username> \
  -p <password> \
  -q "SELECT COUNT(*)
       FROM `<bucket:>`.`<scope>`.`<collection>`"
```

Amazon DocumentDB DocumentDB-Ziel

mongosh (siehe Connect zu Ihrem Amazon DocumentDB-Cluster herstellen):

```
db = db.getSiblingDB('<database>')
db.getCollection('<collection>').find({
  _id: {
    $in: [
      <_id 1>, <_id 2>, <_id 3>, <_id 4>, <_id 5>
    ]
  }
})
```

Amazon DocumentDB aktualisieren

Topics

- Unterstützungstermine der Amazon DocumentDB DocumentDB-Engine-Version
- Direktes Upgrade der Hauptversion von Amazon DocumentDB
- Upgrade der Nebenversion von Amazon DocumentDB
- Aktualisieren Ihres Amazon DocumentDB-Clusters mit AWS Database Migration Service
- Long-Term Support- (LTS, Langzeit-Support) Versionen nutzen

Unterstützungstermine der Amazon DocumentDB DocumentDB-Engine-Version

Sie können die folgenden Daten verwenden, um Ihre Test- und Upgrade-Zyklen zu planen.

Veröffentlichungskalender für Amazon DocumentDB DocumentDB-Hauptversionen

Amazon DocumentDB unterstützt derzeit die folgenden Hauptversionen. Informationen zum Upgrade Ihrer Engine-Version finden Sie unter Aktualisierung einer Hauptversion der Engine oderEin Upgrade durchführen mit AWS DMS.

Engine-Version	Datum der Veröffentlichung	Ende des Standard-Supports	Beginn des erweiterten Support (Preis für das erste Jahr)	Beginn des erweiterten Support (Preis für 3. Jahr)	Ende des erweiterten Support
Version 3.6	9. Januar 2019	30. März 2026	31. März 2026	31. März 2028	30. März 2029
Ausführung 4.0	9. November 2020	N/A	N/A	N/A	N/A
Ausführung 5.0	1. März 2023	N/A	N/A	N/A	N/A

Engine-Version	Datum der Veröffentlichung	Ende des Standard-Supports	Beginn des erweiterten Support (Preis für das erste Jahr)	Beginn des erweiterten Support (Preis für 3. Jahr)	Ende des erweiterten Support
Ausführung 8.0	14. November 2025	N/A	N/A	N/A	N/A

Amazon DocumentDB unterstützt mehrere Engine-Versionen im Rahmen der Standardunterstützung. Gegen eine Gebühr für erweiterten Support können Sie eine Version auch nach Ablauf des Standard-Supportdatums weiter ausführen. Weitere Informationen finden Sie unter Erweiterter Support für Amazon DocumentDB Amazon DocumentDB DocumentDB-Preise.

Veröffentlichungskalender für Amazon DocumentDB-Nebenversionen

Amazon DocumentDB unterstützt derzeit die folgenden Nebenversionen. Der Zeitplan für die Veröffentlichung hängt von zusätzlichen Funktionen oder Korrekturen ab. Bei Nebenversionen kann es sein, dass der Standardsupport vor den entsprechenden Hauptversionen ausläuft. Informationen zum Upgrade Ihrer Engine-Version finden Sie unterAktualisierung einer kleineren Engine-Version.

> **Note**
>
> Nebenversionen sind ab der Hauptversion 5.0 verfügbar.

Engine-Version	Datum der Veröffentlichung
Version 5.0.0 (LTS)	16. Februar 2026
Version 5.0.1	8. Juni 2026

Amazon DocumentDB bezeichnet bestimmte Versionen als Long-Term Support (LTS) -Versionen. Weitere Informationen finden Sie unter Long-Term Support- (LTS, Langzeit-Support) Versionen nutzen.

Direktes Upgrade der Hauptversion von Amazon DocumentDB

Sie können ein direktes Major Version Upgrade (MVU) Ihres Amazon DocumentDB-Clusters durchführen und dabei dieselben Endpunkte, Speicher und Tags beibehalten. Ihre Anwendungen funktionieren weiterhin ohne Änderungen. Diese Funktion ist in allen Regionen, in denen Amazon DocumentDB verfügbar ist, ohne zusätzliche Kosten verfügbar.

> **Important**
>
> Ihr Cluster ist während des Upgrades nicht verfügbar und wird mehrfach neu gestartet. Stellen Sie nach dem Start des Upgrades keine Verbindung zum Cluster her, lesen Sie nicht aus dem Cluster und schreiben Sie nicht in ihn. Die Ausfallzeit hängt von der Anzahl der Sammlungen, Indizes, Datenbanken und Instanzen ab. Wir empfehlen, das Upgrade während Ihres Wartungsfensters oder zu Zeiten mit geringer Auslastung durchzuführen.
> Nach dem Upgrade können Sie kein Downgrade auf eine frühere Version durchführen.
> Sie können Ihren Snapshot vor dem Upgrade bei Bedarf auf einem neuen Cluster wiederherstellen.

Topics

- Unterstützte Upgrade-Pfade
- Voraussetzungen
- Best Practices
- Was ändert sich nach dem Upgrade von Amazon DocumentDB 5.0 auf 8.0
- Post-upgrade Überlegungen zu Clustern, die von 3.6 oder 4.0 aktualisiert wurden
- Das Upgrade wird durchgeführt
- Fehlerbehebung

Unterstützte Upgrade-Pfade

Quellversion	Zielversion
Amazon DocumentDB 3.6	Amazon DocumentDB 5.0
Amazon DocumentDB 4.0	Amazon DocumentDB 5.0

Quellversion	Zielversion
Amazon DocumentDB 5.0	Amazon DocumentDB 8.0

> **Note**
>
> In-place MVU wird für globale Cluster oder elastische Cluster nicht unterstützt. Um einen globalen Cluster zu aktualisieren, entfernen Sie die sekundären Cluster, konvertieren Sie den primären in einen regionalen Cluster, führen Sie die MVU durch und erstellen Sie dann den globalen Cluster neu, indem Sie sekundäre Cluster mit denselben Namen hinzufügen, um Ihre Endpunkte beizubehalten. Es fallen I/O Gebühren an, während der aktualisierte Primärserver Daten auf die neuen Sekundärsysteme repliziert. Die detaillierten Schritte finden Sie unter Einen Cluster aus einem globalen Amazon DocumentDB-Cluster entfernen.

Voraussetzungen

- Instance-Typ — Amazon DocumentDB 4.0+ unterstützt keine db.r4-Instances. Ändern Sie vor dem Upgrade alle `db.r4.*` Instances in Instances oder eine neuere `db.r5.*` Version. Siehe Ändern einer Amazon DocumentDB DocumentDB-Instance und Unterstützte Instance-Klassen nach Region.
- Betriebssystem-Patches — Wenden Sie vor dem Upgrade alle ausstehenden Betriebssystem-Wartungsaktionen auf alle Instanzen an. Siehe Betriebssystem-Updates für Amazon DocumentDB.

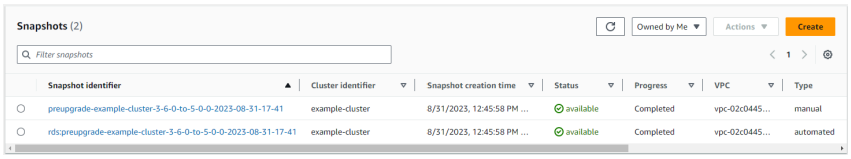
  > **Note**
  >
  > Ausstehende Engine-Patches auf Clusterebene können Instanz-Betriebssystem-Patches verbergen. Wenden Sie bei Bedarf zuerst Engine-Patches an. Siehe Durchführen eines Patch-Updates für die Engine-Version eines Clusters.

- Indexgrenzwerte für Burstable-Instances (Instances der T-Familie) — Wenn Sie über mehr als 3.000 Indizes für Burstable-Instances verfügen, skalieren Sie vor dem Upgrade die Primär-Instances auf mindestens db.r5.large. Sie können nach Abschluss des Upgrades wieder herunterskalieren.

Instance	Maximale Anzahl an Indizes für MVU
db.t4g.medium	3.000
db.t3.medium	10 K

- Parametergruppe — Wir empfehlen, vor dem Upgrade eine benutzerdefinierte Cluster-Parametergruppe für die Zielversion bereit zu haben. Wenn keine angegeben ist, wird die Standardparametergruppe für die Zielversion verwendet (z. B. `default.docdb5.0` oder`default.docdb8.0`).
- Manueller Snapshot — Erstellen Sie vor dem Upgrade einen manuellen Snapshot. Der Upgrade-Prozess erstellt einen automatischen Snapshot mit dem Namen`preupgrade-<name>-<version>-<timestamp>`, aber wir empfehlen dringend, ein eigenes Backup zu erstellen. Siehe Einen manuellen Cluster-Snapshot erstellen.

> **Note**
>
> Der durch den Upgrade-Prozess erstellte auto Snapshot wird nicht automatisch gelöscht, nachdem das direkte Upgrade der Hauptversion abgeschlossen ist. Für diesen Snapshot fallen keine Gebühren an, solange er sich innerhalb der Aufbewahrungsfrist befindet. Sie können sich dafür entscheiden, diesen Snapshot zu löschen, sobald Sie bestätigt haben, dass Ihr Cluster erfolgreich aktualisiert wurde.



Best Practices

Vor dem Upgrade — Testen mit einem Klon

1. Wird verwendetKlonen eines Volumes für einen Amazon DocumentDB-Cluster, um einen Klon Ihres Clusters zu erstellen. Es fallen keine Speicherkosten an, es sei denn, Sie ändern die Daten auf dem Klon.

2. Ordnen Sie die Anzahl der Instanzen des Klons dem Zielcluster zu, um eine realistische Zeitschätzung zu erhalten.
3. Führen Sie die MVU auf dem Klon durch und testen Sie ihn vollständig auf funktionale Unterschiede.
4. Prüfen Sie anhand von running `describe-db-clusters`and looking for`PendingModifiedValues.EngineVersion`, ob bereits ein Upgrade geplant ist. Wenn Sie den Cluster geändert und ausgewählt haben, ihn im nächsten Wartungsfenster anzuwenden, ist der Zeitplan nicht in der Konsole sichtbar, Sie können ihn jedoch in der folgenden Datei einsehen AWS CLI:

```
aws docdb describe-db-clusters \
  --region us-east-1 \
  --db-cluster-identifier mydocdbcluster
```

```
"PendingModifiedValues": {
    "EngineVersion": "5.0.0"
},
```

5. Wenn der Test erfolgreich ist, fahren Sie mit dem Upgrade auf Ihrem Produktionscluster fort.

Während des Upgrades

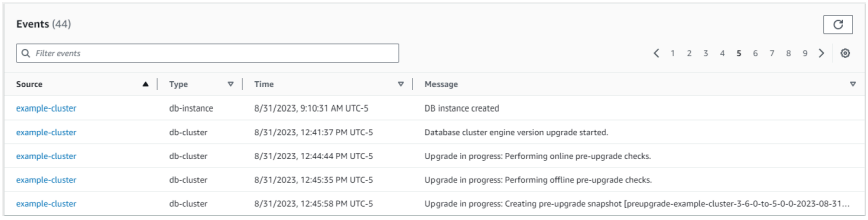
Sie können den Fortschritt Ihres direkten Hauptversions-Upgrades überwachen, indem Sie Cluster-Wartungsereignisse abonnieren. Wenn das Upgrade abgeschlossen ist, erhalten Sie die Meldung „Die Datenbankcluster-Hauptversion wurde aktualisiert“. Dieses und andere Ereignisse, die während des Upgrades auftreten, werden im Abschnitt Ereignisse und Tags der Cluster-Detailseite in der Amazon DocumentDB DocumentDB-Konsole angezeigt. Der Cluster-Status ändert sich dann von `upgrading` zu`available`.

Die folgenden Ereignisse werden während des Upgrades generiert:

1. Das Upgrade der Hauptversion der Datenbank-Cluster-Engine wurde gestartet. Der Cluster bleibt online.
2. Upgrade-Vorbereitung im Gange: Die Online-Upgrade-Vorabprüfungen werden gestartet.
3. Upgrade-Vorbereitung im Gange: Die Online-Upgrade-Vorabprüfungen wurden abgeschlossen.
4. Der Datenbankcluster wird offline geschaltet, während die primäre Instanz den patch/upgrade Vorgang abschließt.

5. Upgrade-Vorbereitung läuft: Die Offline-Upgrade-Vorabprüfungen werden gestartet.
6. Upgrade-Vorbereitung läuft: Die Offline-Upgrade-Vorprüfungen wurden abgeschlossen.
7. <version-to><timestamp>Aktualisierung läuft: Der Snapshot vor dem Upgrade wird erstellt [preupgrade- <cluster-name>- <version-from>-to- -].
8. Aktualisierung läuft: Volume wird geklont.
9. Aktualisierung läuft: Writer wird aktualisiert.
10. Aktualisierung läuft: Lesegeräte werden aktualisiert.
11. Die Hauptversion der Datenbank-Cluster-Engine wurde aktualisiert.

Ereignisse werden in der Konsole auf der Seite Ereignisse angezeigt:



Von der aus können Sie ausführen AWS CLI, `aws docdb describe-events`um den Upgrade-Fortschritt zu überwachen. Um Benachrichtigungen automatisch zu erhalten, abonnieren Sie Ereignisse und leiten Sie sie für E-Mails, Push-Nachrichten oder andere Versandmethoden an Amazon SNS weiter. `aws docdb create-event-subscription` Weitere Informationen finden Sie unter Amazon DocumentDB DocumentDB-Veranstaltungen abonnieren.

```
aws docdb describe-events
  --source-identifier mydocdbcluster
  --source-type db-cluster
```

Daraufhin erhalten Sie ein Ergebnis, das dem hier dargestellten entspricht:

```
{
    "Events": [
        {
            "SourceIdentifier": "mydocdbcluster",
            "SourceType": "db-cluster",
            "Message": "Database cluster engine version upgrade started.",
            "EventCategories": [
                "maintenance"
            ],
```

```
            "Date": "2023-07-11T23:20:32.444000+00:00",
            "SourceArn": "arn:aws:rds:us-east-1:xxxx:cluster:mycluster"
        }
    ]
}
```

Nach dem Upgrade

> **Warning**
>
> Unmittelbar nach dem direkten Upgrade der Hauptversion füllt Ihr Amazon DocumentDB-Cluster die Index-Metadaten erneut auf, die die Datenbank-Engine zur Optimierung von Abfrageausführungsplänen verwendet. Sobald dieser Vorgang abgeschlossen ist, kehrt die Abfrageleistung auf das erwartete Niveau zurück. Der Vorgang ist in der Regel in wenigen Minuten abgeschlossen, kann jedoch je nach Anzahl der Indizes in Ihrem Cluster bis zu zwei Stunden dauern.
> Starten Sie up/down Ihre Writer-Instanz während dieser Zeit nicht neu, führen Sie kein Failover durch oder skalieren Sie sie nicht, da dies die Neuberechnung der Index-Metadaten stören kann. Wir empfehlen, zu warten, bis Sie die erwartete Abfrageleistung erreicht haben, bevor Sie solche Änderungen vornehmen.
> Verfolgen Sie den Fortschritt anhand der folgenden Cluster-Ereignisse:
>
> - Post-upgrade Clusterstatus: Die Aktualisierung der Index-Metadaten wurde gestartet
> - Post-upgrade Clusterstatus: Die Aktualisierung der Index-Metadaten wurde in X Sekunden abgeschlossen
>
> Wenden Sie sich an den AWS Support, wenn die Aktualisierung der Index-Metadaten nicht innerhalb von drei Stunden abgeschlossen wurde oder wenn nach Abschluss des Vorgangs weiterhin Leistungsprobleme auftreten.

1. Erstellen Sie manuell einen Snapshot des aktualisierten Clusters für den Fall, dass Sie den Status nach dem Upgrade wiederherstellen müssen. Der automatische Snapshot-Vorgang wird fortgesetzt, sobald das direkte Upgrade der Hauptversion abgeschlossen ist.
2. Tag-Cluster wurden von 3.6 aktualisiert. Fügen Sie ein Tag hinzu, um Cluster zu unterscheiden, für die Version 3.6 aktualisiert wurde. (siehethe section called “Post-upgrade Überlegungen zu Clustern, die von 3.6 oder 4.0 aktualisiert wurden”).

3. Aktualisiere deinen Treiber. Um neue Funktionen zu verwenden (z. B. Sortierung, Ansichten oder Zstd-Komprimierung in 8.0), führen Sie ein Upgrade auf die entsprechende MongoDB-API-Version durch. Weitere Informationen finden Sie unter Was ist neu in Amazon DocumentDB 8.0.
4. Testen Sie gründlich. Überprüfen Sie Ihre Anwendung anhand des aktualisierten Clusters.

Was ändert sich nach dem Upgrade von Amazon DocumentDB 5.0 auf 8.0

Nach einem Upgrade der Hauptversion von Amazon DocumentDB 5.0 auf 8.0 werden die folgenden Funktionen aktiviert oder geändert:

- Sortierung. Amazon DocumentDB 8.0 unterstützt die Sortierung. Nach dem Upgrade ist die Sortierung für neue Sammlungen und deren Indizes sowie für neue Indizes vorhandener Sammlungen standardmäßig aktiviert.
- Textindex. Neue Textindizes werden mit Text Index V2 erstellt, der einen aktualisierten Textsuchparser für eine verbesserte MongoDB-Kompatibilität verwendet. Bestehende Textindizes sind nicht betroffen.
- Version des Abfrageplaners. Wenn Sie keine benutzerdefinierte Parametergruppe hatten, wird eine neue Standardparametergruppe für Amazon DocumentDB 8.0 erstellt, wobei Planner Version 3 automatisch ausgewählt ist. Mit Query Planner Version 3 sind auch Ansichten verfügbar.
- Komprimierung. Amazon DocumentDB 8.0 unterstützt die wörterbuchbasierte Dokumentenkomprimierung mithilfe des Zstd-Algorithmus. Nach dem Upgrade werden neue Sammlungen mit standardmäßig aktivierter Zstd-Komprimierung erstellt. Bestehende Sammlungen aus Version 5.0 behalten ihre Komprimierungseinstellungen bei. Um die Vorteile der Zstd-Komprimierung für bestehende Sammlungen zu nutzen, können Sie deren Komprimierungseinstellungen ändern. Weitere Informationen finden Sie unter Dictionary-based Komprimierung.
- Neuerstellung des Index. Wenn Sie ein Upgrade von Amazon DocumentDB 5.0 auf Amazon DocumentDB 8.0 durchführen, ist keine Indexneuerstellung erforderlich.

> **Important**
>
> Amazon DocumentDB 8.0 erfordert TLS 1.2 oder höher. TLS 1.0 und TLS 1.1 werden nicht mehr unterstützt.

> **Note**
>
> Eine vollständige Liste der funktionalen Unterschiede finden Sie unterAmazon DocumentDB DocumentDB-Kompatibilität mit MongoDB.

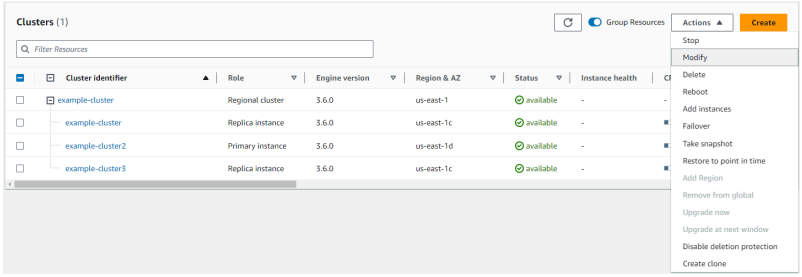
Post-upgrade Überlegungen zu Clustern, die von 3.6 oder 4.0 aktualisiert wurden

- Neuerstellung des Index. Eine MVU behält die ursprünglichen Indizes bei. Amazon DocumentDB 5.0 hat die Indexverwaltung und die Garbage-Collection verbessert, insbesondere für Indizes mit niedriger Kardinalität. Nach dem Upgrade von 3.6 oder 4.0 empfehlen wir, Ihre Indizes neu zu erstellen, um eine optimale Abfrageleistung zu gewährleisten (optional, erfordert zusätzliche Gebühren). I/O Siehe Indexverwaltung mit `ReIndex`.
- Numerischer Vergleich von Unterdokumenten (nur 3.6). Cluster, die von 3.6 aktualisiert wurden, übernehmen das Verhalten von 3.6, bei dem numerische Typen in Unterdokumenten nicht typübergreifend verglichen werden. `{a: {b: NumberLong(1)}}`Entspricht beispielsweise `{a: {b: 1}}` in 3.6 nicht, aber sie sind in 4.0 und höher gleich. Dieses Verhalten wirkt sich auf alle Cluster aus, die von 3.6 aktualisiert wurden.

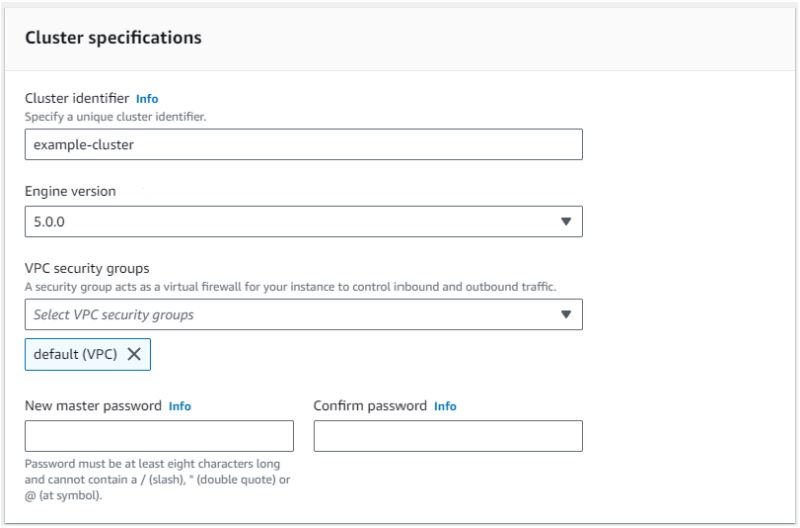
Das Upgrade wird durchgeführt

Using the AWS-Managementkonsole

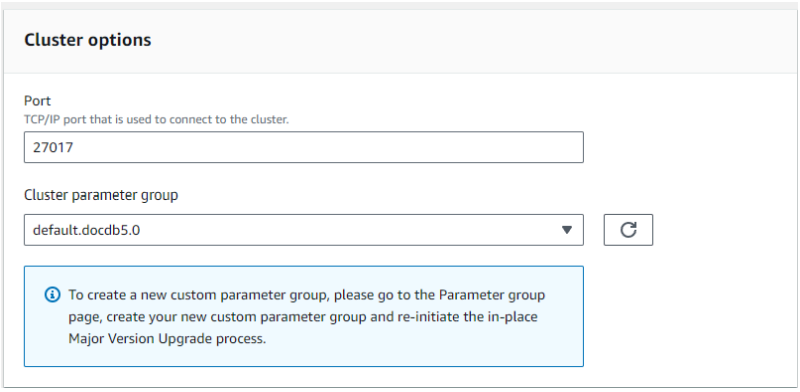
1. Melden Sie sich bei der Amazon DocumentDB DocumentDB-Konsole an AWS-Managementkonsoleund öffnen Sie sie.
2. Wählen Sie in der Cluster-Tabelle den Quell-Cluster aus, klicken Sie auf Aktionen und dann auf Ändern.



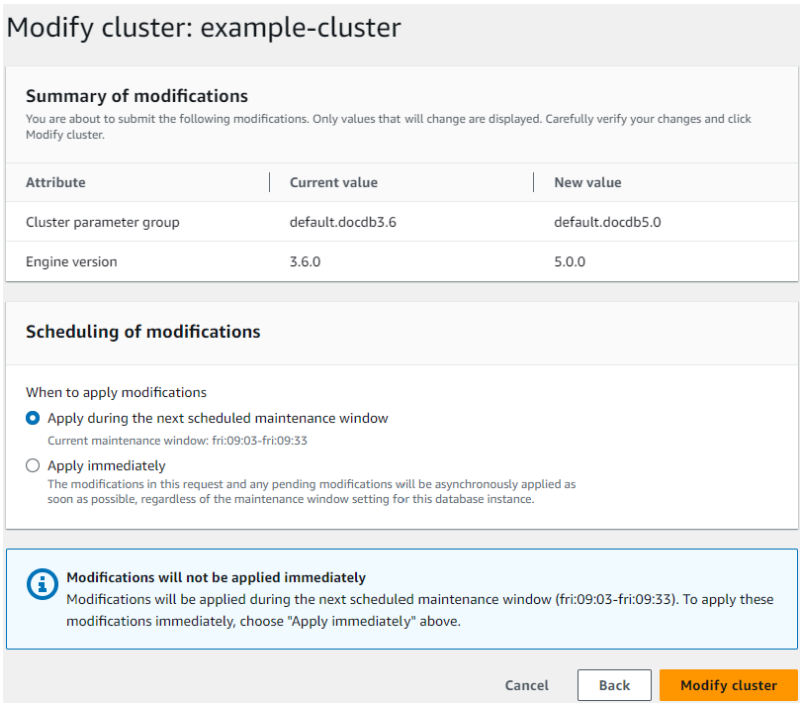
3. Wählen Sie in den Clusterspezifikationen die Zielversion (z. B. 5.0.0 oder 8.0.0) aus der Dropdownliste Engine-Version aus.



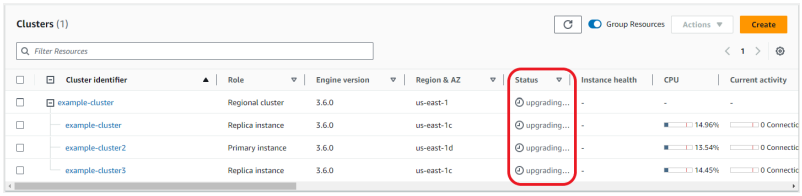
4. Wählen Sie unter Clusteroptionen Ihre Cluster-Parametergruppe für die Ziel-Engine-Version aus. Sie können den Standard (z. B. default.docdb5.0 oder default.docdb8.0) oder eine von Ihnen erstellte benutzerdefinierte Parametergruppe verwenden.



5. Wählen Sie Weiter, wählen Sie Ihre bevorzugte Zeitplanung (sofort anwenden oder nächstes Wartungsfenster) und wählen Sie dann Cluster modifizieren.



6. Überwachen Sie den Clusterstatus in der Cluster-Tabelle, wenn er sich beim Upgrade ändert:



Using the AWS CLI

[modify-db-cluster](#)Mit der `--allow-major-version-upgrade` Flagge verwenden:

```
aws docdb modify-db-cluster \
  --db-cluster-identifier mydocdbcluster \
  --allow-major-version-upgrade \
  --engine-version 8.0.0 \
  --apply-immediately \
  --cluster-parameter-group mydocdbparametergroup \
  --region us-east-1
```

Ersetzen Sie jedes *placeholder* durch die Informationen Ihres Clusters.

Fehlerbehebung

- Upgrade-Fehler und Rollback. Wenn das Upgrade fehlschlägt, wird automatisch versucht, ein Rollback durchzuführen. Ein erfolgreicher Rollback generiert das Ereignis: „Der Datenbank-Cluster befindet sich in einem Zustand, der nicht aktualisiert werden kann.“ Ihr Cluster kehrt in den Zustand vor dem Upgrade zurück und Sie können ihn weiter verwenden. Wenden Sie sich zur Problembehebung an den AWS Support, bevor Sie es erneut versuchen.
- Post-upgrade Leistung. Während der Aktualisierung der Index-Metadaten können vorübergehende Leistungseinbußen und eine hohe CPU-Auslastung auftreten. Wenn die Leistungsminderung länger als 3 Stunden anhält, wenden Sie sich an den AWS Support.

Wenn Sie weitere Unterstützung benötigen, wenden Sie sich an den AWS Support.

Upgrade der Nebenversion von Amazon DocumentDB

> **Note**
>
> In diesem Thema werden kleinere Versionsupgrades innerhalb derselben Hauptversion behandelt (z. B. das Upgrade von 5.0.0 auf 5.0.1). Informationen zum Upgrade auf eine andere Hauptversion finden Sie unter. Direktes Upgrade der Hauptversion von Amazon DocumentDB

Sie können die Minor-Engine-Version Ihres Amazon DocumentDB-Clusters aktualisieren (z. B. von 5.0.0 auf 5.0.1), indem Sie den Cluster ändern. Upgrades für kleinere Versionen können sofort oder während des nächsten Wartungsfensters angewendet werden.

Vor dem Durchführen eines Nebenversions-Upgrades

Bevor Sie ein Upgrade auf eine kleinere Version durchführen, können die folgenden Aktionen hilfreich sein:

- Führen Sie das Upgrade in Zeiten geringer Auslastung durch, um die Auswirkungen kurzzeitiger Ausfallzeiten zu verringern.
- Stellen Sie mithilfe des `describe-db-engine-versions` Befehls sicher, dass es sich bei der Ziel-Nebenversion um ein gültiges Upgrade-Ziel für Ihre aktuelle Version handelt.

- Bei globalen Clustern müssen die sekundären Cluster vor dem primären Cluster aktualisiert werden. Weitere Informationen finden Sie unter Patchen globaler Cluster.

> **Important**
>
> - Upgrades sind unidirektionale Operationen — Sie können nach dem Upgrade kein Downgrade mehr durchführen.
> - Bei Ihrem Cluster kommt es während des Upgrade-Vorgangs zu kurzen Ausfallzeiten.

Durchführen eines Nebenversions-Upgrades

Using the AWS-Managementkonsole

Um ein Upgrade einer Nebenversion durchzuführen, verwenden Sie AWS-Managementkonsole:

1. Melden Sie sich bei der Amazon DocumentDB DocumentDB-Konsole an AWS-Managementkonsoleund öffnen Sie sie.
2. Wählen Sie in der Cluster-Tabelle den Cluster aus, für den Sie ein Upgrade durchführen möchten, klicken Sie auf Aktionen und dann auf Ändern.
3. Wählen Sie im Dialogfeld Cluster ändern im Abschnitt Clusterspezifikationen die Ziel-Nebenversion aus dem Dropdownmenü Engine-Version aus.
4. Scrollen Sie nach unten und wählen Sie Weiter.
5. Wählen Sie im Abschnitt Planung von Änderungen aus, ob die Änderung sofort oder während des nächsten Wartungsfensters übernommen werden soll.

   Wählen Sie Cluster ändern aus.

Using the AWS CLI

Verwenden Sie den `modify-db-cluster`Befehl mit dem `--engine-version` Parameter:

```
aws docdb modify-db-cluster \
    --db-cluster-identifier mydocdbcluster \
    --engine-version 5.0.1 \
    --apply-immediately \
```

```
    --region us-east-1
```

Ersetzen Sie im obigen Beispiel jeden *user input placeholder* durch die Informationen Ihres Clusters.

> **Note**
>
> Wenn Sie das Upgrade nicht sofort, sondern im nächsten Wartungsfenster anwenden möchten, verwenden Sie `--no-apply-immediately` anstelle von`--apply-immediately`.

Das Upgrade der Nebenversion wird überprüft

Überprüfen Sie nach Abschluss des Upgrades die Engine-Version mit dem AWS CLI:

```
aws docdb describe-db-clusters \
    --db-cluster-identifier mydocdbcluster \
    --query 'DBClusters[0].EngineVersion'
```

Die Ausgabe dieser Operation sieht in etwa wie folgt aus:

```
"5.0.1"
```

Aktualisieren Ihres Amazon DocumentDB-Clusters mit AWS Database Migration Service

> **Important**
>
> Amazon DocumentDB folgt nicht denselben Support-Lebenszyklen wie MongoDB, und der Zeitplan für das Ende der Nutzungsdauer von MongoDB gilt nicht für Amazon DocumentDB.

Sie können Ihren Amazon DocumentDB-Cluster mit minimaler Ausfallzeit auf eine höhere Version aktualisieren, indem Sie AWS DMS. AWS DMS ist ein vollständig verwalteter Service, der die Migration von älteren Amazon DocumentDB DocumentDB-Versionen, relationalen Datenbanken und nicht-relationalen Datenbanken zu Ihrem Amazon DocumentDB DocumentDB-Zielcluster erleichtert.

Topics

- Schritt 1: Change Streams aktivieren
- Schritt 2: Ändern Sie die Aufbewahrungsdauer für Change-Streams
- Schritt 3: Migrieren Sie Ihre Indizes
- Schritt 4: Erstellen Sie ein AWS DMS replication instance
- Schritt 5: Erstellen Sie eine AWS DMS Quell-Endpunkt
- Schritt 6: Erstellen Sie eine AWS DMS Zielendpunkt
- Schritt 7: Erstellen Sie eine Migrationsaufgabe und führen Sie sie aus
- Schritt 8: Ändern des Anwendungsendpunkts auf den Amazon DocumentDB DocumentDB-Zielcluster

Schritt 1: Change Streams aktivieren

Um eine Migration mit minimalen Ausfallzeiten durchzuführen, ist Zugriff auf die Change-Streams des Clusters AWS DMS erforderlich. Amazon DocumentDB DocumentDB-Change-Streams bieten eine zeitlich geordnete Abfolge von Aktualisierungsereignissen, die in den Sammlungen und Datenbanken Ihres Clusters auftreten. Das Lesen aus dem Change-Stream ermöglicht es AWS DMS , Change Data Capture (CDC) durchzuführen und inkrementelle Aktualisierungen auf den Amazon DocumentDB DocumentDB-Zielcluster anzuwenden.

Um Change-Streams für alle Sammlungen in einer bestimmten Datenbank zu aktivieren, authentifizieren Sie sich mit der Mongo-Shell bei Ihrem Amazon DocumentDB-Cluster und führen Sie die folgenden Befehle aus:

```
db.adminCommand({modifyChangeStreams: 1,
    database: "db_name",
    collection: "",
    enable: true});
```

Schritt 2: Ändern Sie die Aufbewahrungsdauer für Change-Streams

Ändern Sie als Nächstes den Aufbewahrungszeitraum für den Change-Stream je nachdem, wie lange Sie Änderungsereignisse im Change-Stream behalten möchten. Wenn Sie beispielsweise davon ausgehen, dass Ihre Amazon AWS DMS DocumentDB-Cluster-Migration 12 Stunden dauern wird, sollten Sie die Aufbewahrung des Change-Streams auf einen Wert von mehr als 12 Stunden festlegen. Die Standardaufbewahrungsdauer für Ihren Amazon DocumentDB-Cluster beträgt drei

Stunden. Sie können die Aufbewahrungsdauer des Change-Stream-Protokolls für Ihren Amazon DocumentDB-Cluster zwischen einer Stunde und sieben Tagen ändern, indem Sie die AWS-Managementkonsole oder die AWS CLI verwenden. Weitere Informationen finden Sie unter Ändern der Aufbewahrungsdauer für das Change-Stream-Protokoll.

Schritt 3: Migrieren Sie Ihre Indizes

Erstellen Sie dieselben Indizes auf Ihrem Amazon DocumentDB DocumentDB-Zielcluster wie auf Ihrem Amazon DocumentDB DocumentDB-Quellcluster. Es AWS DMS wickelt zwar die Migration von Daten ab, migriert aber keine Indizes. Um die Indizes zu migrieren, verwenden Sie das Amazon DocumentDB Index Tool, um Indizes aus dem Amazon DocumentDB DocumentDB-Quellcluster zu exportieren. Sie können das Tool herunterladen, indem Sie einen Klon des Amazon DocumentDB GitHub DocumentDB-Tools-Repos erstellen und den Anweisungen unter folgen. `README.md` Sie können das Tool von einer Amazon EC2 EC2-Instance oder einer AWS Cloud9 Umgebung aus ausführen, die in derselben Amazon VPC wie Ihr Amazon DocumentDB-Cluster läuft.

Ersetzen Sie im folgenden Beispiel jede Information durch Ihre *`user input placeholder`* eigenen Informationen.

Der folgende Code gibt Indizes aus Ihrem Amazon DocumentDB DocumentDB-Quellcluster aus:

```
python migrationtools/documentdb_index_tool.py --dump-indexes
--uri mongodb://sample-user:user-password@sample-source-cluster.node.us-
east 1.docdb.amazonaws.com:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false'
--dir ~/index.js/

2020-02-11 21:51:23,245: Successfully authenticated to database: admin2020-02-11
 21:46:50,432: Successfully connected to instance docdb-40-xx.cluster-xxxxxxxx.us-
east-1.docdb.amazonaws.com:27017
2020-02-11 21:46:50,432: Retrieving indexes from server...2020-02-11 21:46:50,440:
 Completed writing index metadata to local folder: /home/ec2-user/index.js/
```

Sobald Ihre Indizes erfolgreich exportiert wurden, stellen Sie diese Indizes in Ihrem Amazon DocumentDB DocumentDB-Zielcluster wieder her. Verwenden Sie das Amazon DocumentDB Index Tool, um die Indizes wiederherzustellen, die Sie im vorherigen Schritt exportiert haben. Der folgende Befehl stellt die Indizes in Ihrem Amazon DocumentDB DocumentDB-Zielcluster aus dem angegebenen Verzeichnis wieder her.

```
python migrationtools/documentdb_index_tool.py --restore-indexes
```

```
--uri mongodb://sample-user:user-password@sample-destination-
cluster.node.us-east 1.docdb.amazonaws.com:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false'
--dir ~/index.js/

2020-02-11 21:51:23,245: Successfully authenticated to database: admin2020-02-11
 21:51:23,245: Successfully connected to instance docdb-50-xx.cluster-xxxxxxxx.us-
east-1.docdb.amazonaws.com:27017
2020-02-11 21:51:23,264: testdb.coll: added index: _id
```

Um zu überprüfen, ob Sie die Indizes korrekt wiederhergestellt haben, stellen Sie mit der Mongo-Shell eine Verbindung zu Ihrem Amazon DocumentDB DocumentDB-Zielcluster her und listen Sie die Indizes für eine bestimmte Sammlung auf. Sehen Sie sich den folgenden Code an:

```
mongo --ssl
--host docdb-xx-xx.cluster-xxxxxxxx.us-east-1.docdb.amazonaws.com:27017
--sslCAFile rds-ca-2019-root.pem --username documentdb --password documentdb

db.coll.getIndexes()
```

Schritt 4: Erstellen Sie ein AWS DMS replication instance

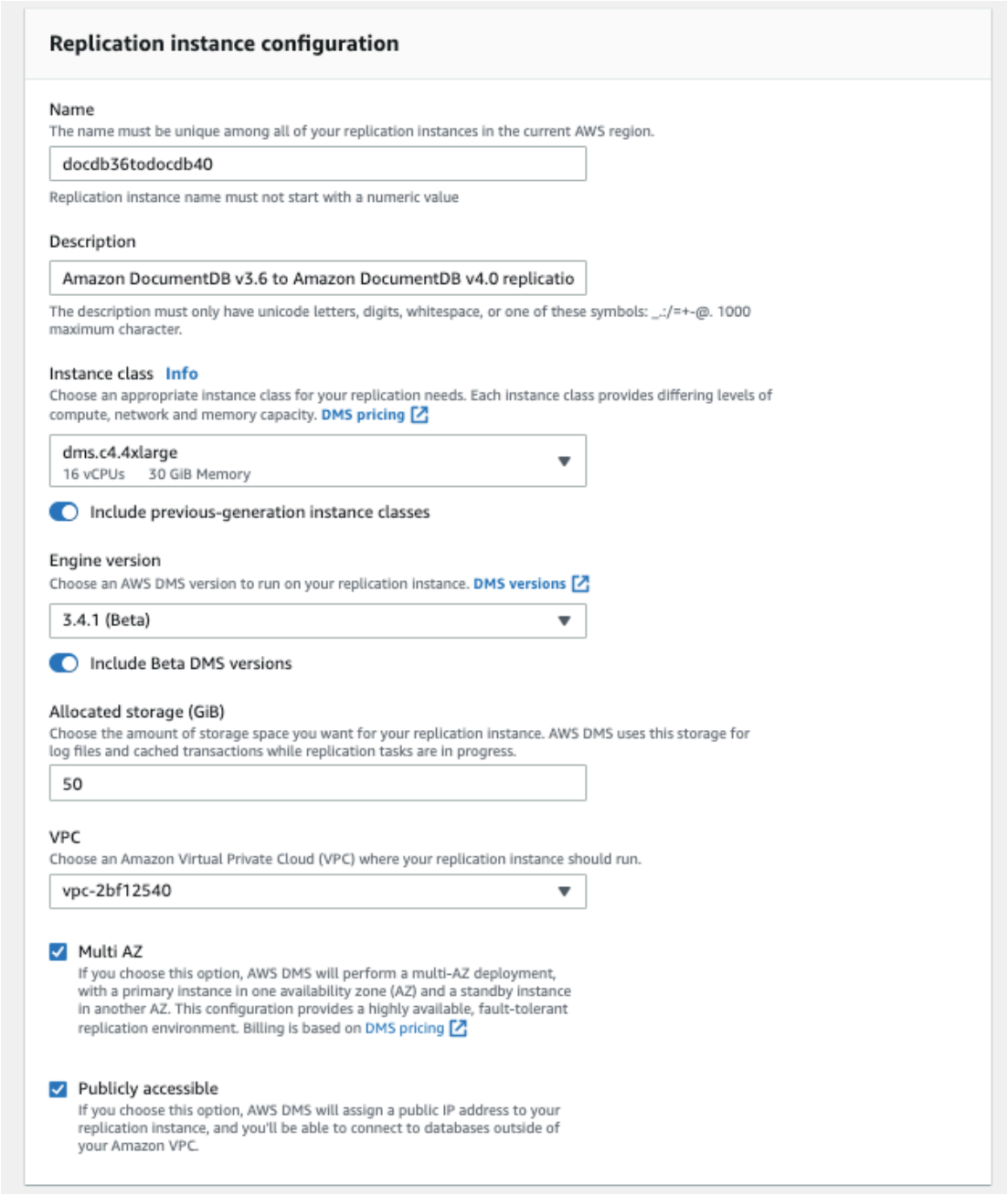
Eine AWS DMS Replikationsinstanz stellt eine Verbindung her und liest Daten aus Ihrem Amazon DocumentDB DocumentDB-Quellcluster und schreibt sie in Ihren Amazon DocumentDB DocumentDB-Zielcluster. Die AWS DMS Replikationsinstanz kann sowohl Massenlade- als auch CDC-Operationen ausführen. Der Großteil dieser Verarbeitung findet im Speicher statt. Bei großen Vorgängen kann jedoch eine gewisse Pufferung auf der Festplatte erforderlich sein. Zwischengespeicherte Transaktionen und Protokolldateien werden ebenfalls auf Festplatte geschrieben. Sobald die Daten migriert sind, streamt die Replikationsinstanz auch alle Änderungsereignisse, um sicherzustellen, dass Quelle und Ziel synchron sind.

So erstellen Sie eine AWS DMS Replikationsinstanz:

1. Öffnen Sie die AWS DMS Konsole.
2. Wählen Sie im Navigationsbereich Replication instances (Replikations-Instances) aus.
3. Wählen Sie Create replication instance (Replikations-Instance erstellen) aus und geben Sie die folgenden Informationen ein:

   - Geben Sie unter Name einen Namen Ihrer Wahl ein. Beispiel, `docdb36todocdb40`.

- Geben Sie unter Beschreibung eine Beschreibung Ihrer Wahl ein. Für lititem eine Replikationsinstanz von Amazon DocumentDB 3.6 auf Amazon DocumentDB 4.0.
- Wählen Sie für Instance-Klasse die Größe entsprechend Ihren Anforderungen aus.
- Wählen Sie für Engine-Version `3.4.1.`
- Wählen Sie für Amazon VPC die Amazon VPC aus, die Ihre Amazon DocumentDB DocumentDB-Quell- und Zielcluster beherbergt.
- Verwenden Sie für Allocation Storage (GiB) den Standardwert von 50 GiB. Wenn Sie einen Workload mit hohem Schreibdurchsatz haben, erhöhen Sie diesen Wert entsprechend Ihrer Arbeitslast.
- Wählen Sie für Ja Multi-AZ, wenn Sie Hochverfügbarkeits- und Failover-Unterstützung benötigen.
- Für Publicly accessible (Öffentlich zugänglich) aktivieren Sie diese Option.



4. Wählen Sie Create replication instance (Replikations-Instance erstellen) aus.

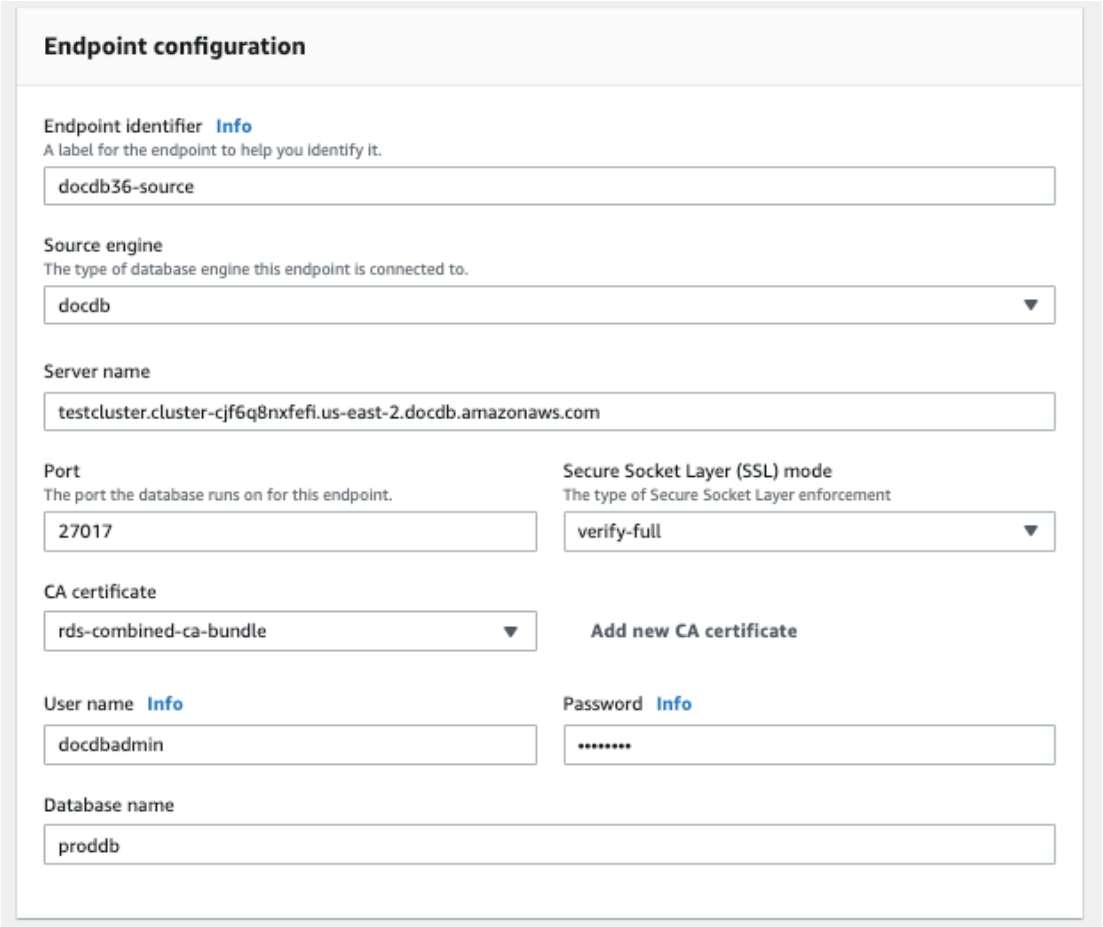
Schritt 5: Erstellen Sie eine AWS DMS Quell-Endpunkt

Der Quellendpunkt wird für den Amazon DocumentDB DocumentDB-Quellcluster verwendet.

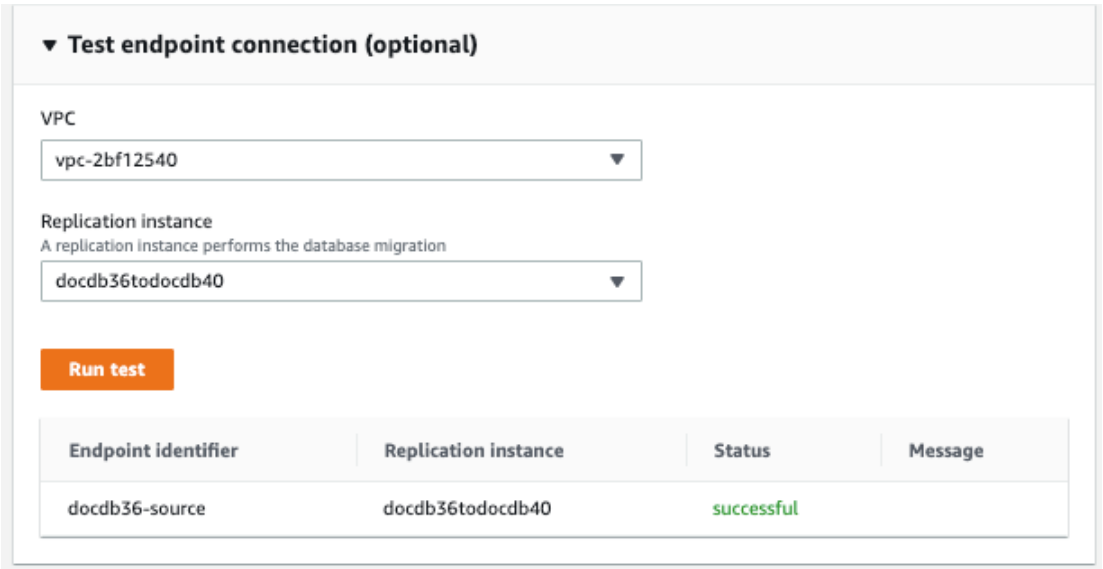
Um einen Quellendpunkt zu erstellen

1. Öffnen Sie die AWS DMS Konsole.
2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Wählen Sie die folgenden Informationen aus `Create endpoint` und geben Sie sie ein:

   - Für Endpoint type (Endpunkttyp) wählen Sie Source (Quelle) aus.
   - >Geben Sie für Endpoint Identifier beispielsweise `docdb-source` einen Namen ein, den Sie sich leicht merken können.
   - Wählen Sie `docdb` für Source Engine.
   - Geben Sie als Servername den DNS-Namen Ihres Amazon DocumentDB DocumentDB-Quell-Clusters ein.
   - Geben Sie für Port die Portnummer Ihres Amazon DocumentDB DocumentDB-Quell-Clusters ein.
   - Wählen Sie `verify-full` für den SSL-Modus.
   - Wählen Sie für CA-Zertifikat die Option Neues CA-Zertifikat hinzufügen aus. Laden Sie das neue CA-Zertifikat (neues CA-Zertifikat herunter, um ein TLS-Verbindungspaket zu erstellen. Geben Sie als Certificate Identifier ein `rds-combined-ca-bundle`. Wählen Sie unter Import certificate file (Zertifikatsdatei importieren) die Option Choose file (Datei auswählen) und navigieren Sie zu der `.pem`-Datei, die Sie zuvor heruntergeladen haben. Wählen Sie die Datei aus und öffnen Sie sie. Wählen Sie Zertifikat importieren und wählen Sie dann `rds-combined-ca-bundle` aus der Dropdownliste Zertifikat auswählen
   - Geben Sie unter Benutzername den primären Benutzernamen Ihres Amazon DocumentDB DocumentDB-Quell-Clusters ein.
   - Geben Sie unter Passwort das primäre Passwort Ihres Amazon DocumentDB DocumentDB-Quell-Clusters ein.
   - Geben Sie unter Datenbankname den Datenbanknamen ein, für den Sie ein Upgrade durchführen möchten.



4. Testen Sie Ihre Verbindung, um sicherzustellen, dass sie erfolgreich eingerichtet wurde.



5. Klicken Sie auf Endpunkt erstellen.

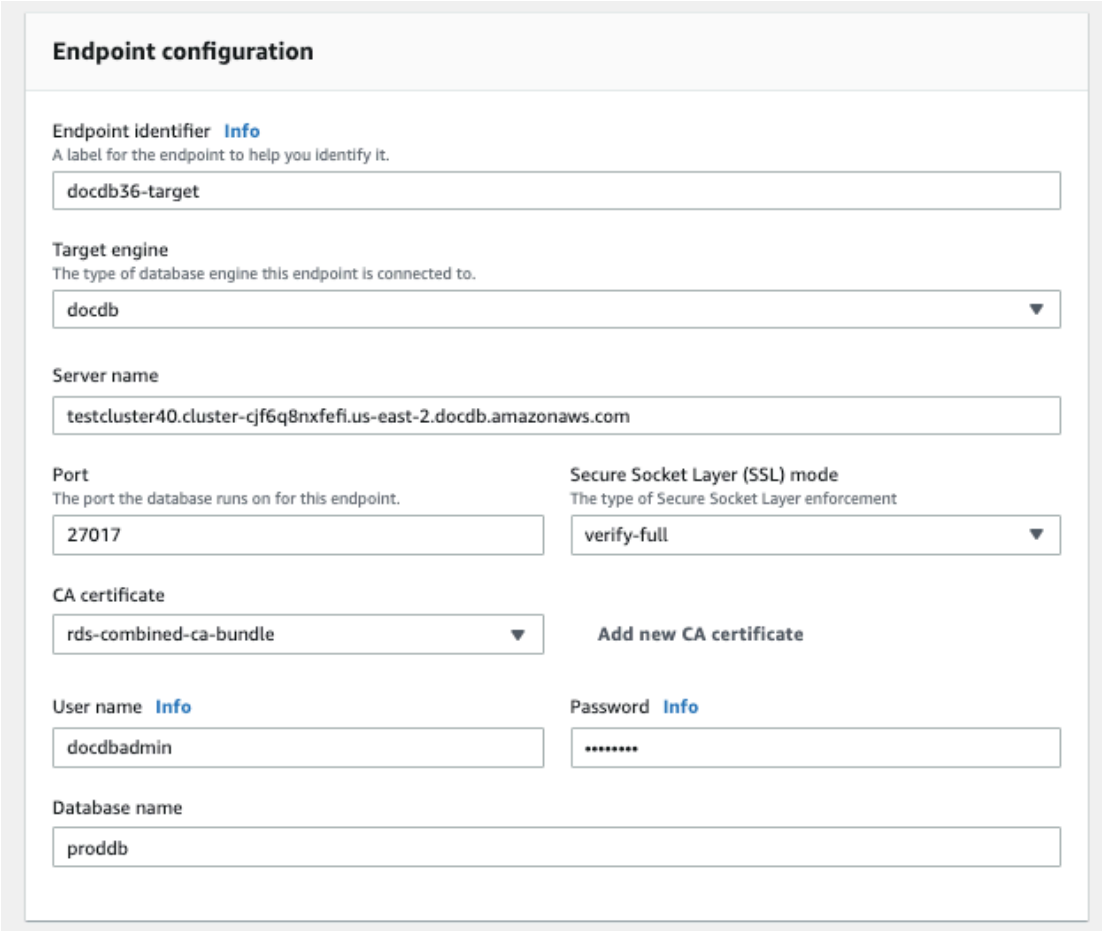
> **Note**
>
> AWS DMS kann jeweils nur eine Datenbank migrieren.

Schritt 6: Erstellen Sie eine AWS DMS Zielendpunkt

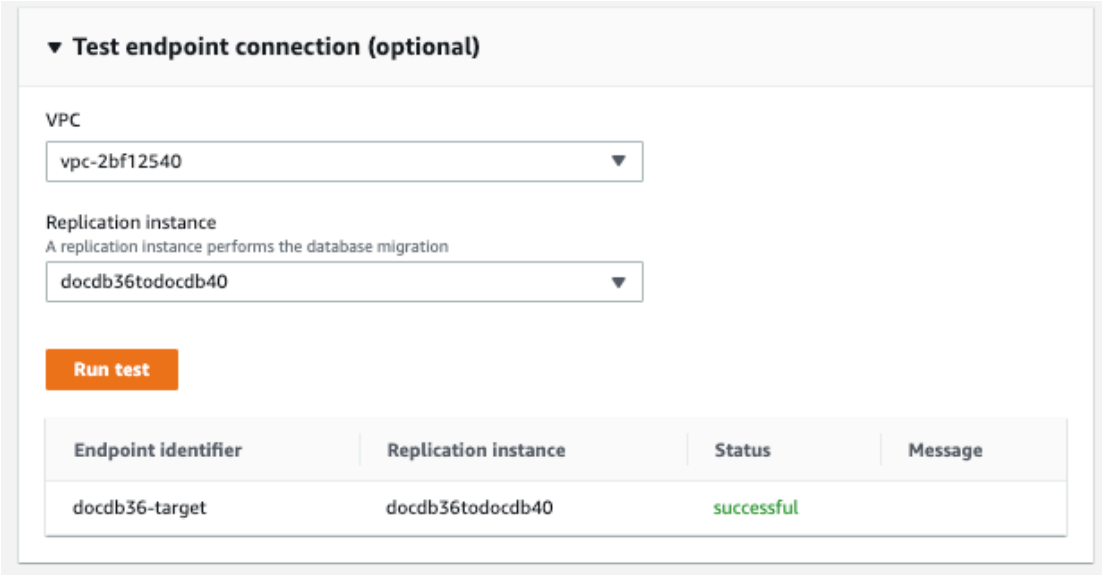
Der Zielendpunkt ist für Ihren Amazon DocumentDB DocumentDB-Zielcluster.

Um einen Zielendpunkt zu erstellen:

1. Öffnen Sie die AWS DMS -Konsole.
2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Wählen Sie Create endpoint (Endpunkt erstellen) und geben Sie die folgenden Informationen ein:
   - Für Endpoint type (Endpunkttyp) wählen Sie Target (Ziel) aus.
   - Für Endpoint Identifier (Endpunkt-ID) geben Sie einen Namen ein, der leicht zu merken ist, zum Beispiel `docdb-target`.
   - Wählen Sie für Source Engine`docdb`.
   - Geben Sie als Servername den DNS-Namen Ihres Amazon DocumentDB DocumentDB-Ziel-Clusters ein.
   - Geben Sie für Port die Portnummer Ihres Amazon DocumentDB DocumentDB-Ziel-Clusters ein.
   - Wählen Sie `verify-full` für den SSL-Modus.
   - Wählen Sie für CA-Zertifikat das vorhandene `rds-combined-ca-bundle` Zertifikat aus der Drop-down-Liste Zertifikat auswählen aus.
   - Geben Sie unter Benutzername den primären Benutzernamen Ihres Amazon DocumentDB DocumentDB-Ziel-Clusters ein.
   - Geben Sie unter Passwort das primäre Passwort Ihres Amazon DocumentDB DocumentDB-Ziel-Clusters ein.
   - Geben Sie als Datenbankname denselben Datenbanknamen ein, den Sie zur Einrichtung Ihres Quellendpunkts verwendet haben.



4. Testen Sie Ihre Verbindung, um sicherzustellen, dass sie erfolgreich eingerichtet wurde.



5. Klicken Sie auf Endpunkt erstellen.

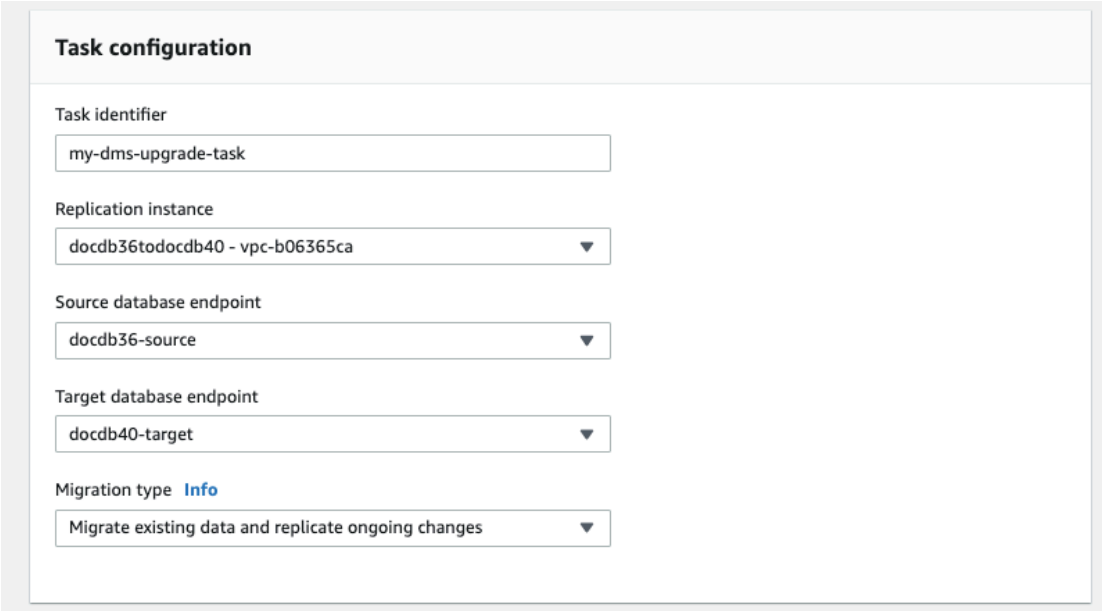
Schritt 7: Erstellen Sie eine Migrationsaufgabe und führen Sie sie aus

Eine AWS DMS Aufgabe verbindet die Replikationsinstanz mit Ihrer Quell- und Zielinstanz. Wenn Sie eine Migrationsaufgabe erstellen, geben Sie den Quellendpunkt, den Zielendpunkt, die Replikationsinstanz und alle gewünschten Migrationseinstellungen an. Eine AWS DMS Aufgabe kann mit drei verschiedenen Migrationstypen erstellt werden: Migration vorhandener Daten, Migration vorhandener Daten und Replikation laufender Änderungen oder nur Datenänderungen. Da der Zweck dieser Anleitung darin besteht, einen Amazon DocumentDB-Cluster mit minimaler Ausfallzeit zu aktualisieren, nutzen die Schritte die Option, vorhandene Daten zu migrieren und laufende Änderungen zu replizieren. Mit dieser Option werden Änderungen bei der Migration Ihrer vorhandenen Daten AWS DMS erfasst. AWS DMS erfasst weiterhin Änderungen und wendet sie an, auch nachdem die Massendaten geladen wurden. Schließlich sind die Quell- und Zieldatenbanken synchronisiert, unter Berücksichtigung einer minimalen Ausfallzeit während der Migration.

Im Folgenden finden Sie die Schritte zum Erstellen einer Migrationsaufgabe für eine Migration mit minimalen Ausfallzeiten:

1. Öffnen Sie die AWS DMS Konsole.
2. Wählen Sie im Navigationsbereich die Option Datenbankmigrationsaufgaben aus.
3. Wählen Sie Aufgabe zur Datenbankmigration erstellen und geben Sie die folgenden Informationen in den Abschnitt Aufgabenkonfiguration ein:

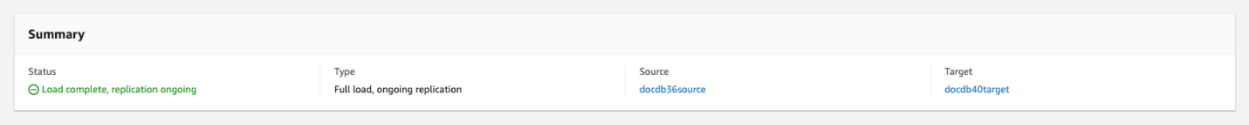
   - Geben Sie unter Task-ID beispielsweise einen Namen ein, den Sie sich leicht merken können`my-dms-upgrade-task`.
   - Geben Sie für Descriptive Amazon Resource Name (ARN) einen benutzerfreundlichen Namen ein, um den standardmäßigen DMS-ARN zu überschreiben.
   - Für Replication instance (Replikations-Instance) wählen Sie die Replikations-Instance aus, die Sie in Schritt 4: Erstellen Sie ein AWS DMS replication instance erstellt haben.
   - Wählen Sie für Quelldatenbank-Endpunkt den Quellendpunkt aus, in dem Sie ihn erstellt haben. Schritt 5: Erstellen Sie eine AWS DMS Quell-Endpunkt
   - Wählen Sie für Zieldatenbank-Endpunkt den Zielendpunkt aus, in dem Sie ihn erstellt habenSchritt 6: Erstellen Sie eine AWS DMS Zielendpunkt.
   - Wählen Sie als Migrationstyp die Option Migrieren und replizieren aus.



4. Geben Sie im Abschnitt Aufgabeneinstellungen die folgenden Informationen ein:

   - Wählen Sie für den Abschnitt Zieltabellenvorbereitungsmodus die Option Nichts tun aus. Dadurch wird sichergestellt, dass die in Schritt 3 erstellten Indizes nicht gelöscht werden.
   - Wählen Sie im Unterabschnitt Task-Protokolle die Option Protokolle aktivieren aus. CloudWatch
   - Wählen Sie für die Startkonfiguration der Migrationsaufgabe die Option Automatisch bei Erstellung aus. Dadurch wird die Migrationsaufgabe automatisch gestartet, sobald Sie sie erstellt haben.
   - Wählen Sie Datenbankmigrationsaufgabe erstellen aus.

AWS DMS beginnt jetzt mit der Migration von Daten aus Ihrem Amazon DocumentDB DocumentDB-Quellcluster zu Ihrem Amazon DocumentDB DocumentDB-Zielcluster. Der Aufgabenstatus sollte sich von „Wird gestartet“ auf „Wird ausgeführt“ ändern. Sie können den Fortschritt überwachen, indem Sie in der AWS DMS Konsole Aufgaben auswählen. Nach mehreren minutes/hours Schritten (abhängig von der Größe Ihrer Migration) sollte sich der Status von „Laden abgeschlossen“ ändern, wobei die Replikation läuft. Das bedeutet, dass AWS DMS Sie eine vollständige Lastmigration Ihres Amazon DocumentDB-Quell-Clusters zu einem Amazon DocumentDB DocumentDB-Zielcluster abgeschlossen haben und jetzt Änderungsereignisse repliziert haben.



Irgendwann werden Ihre Quelle und Ihr Ziel synchron sein. Sie können überprüfen, ob sie synchron sind, indem Sie einen `count()` Vorgang für Ihre Sammlungen ausführen, um zu überprüfen, ob alle Änderungsereignisse migriert wurden.

Schritt 8: Ändern des Anwendungsendpunkts auf den Amazon DocumentDB DocumentDB-Zielcluster

Nachdem der vollständige Ladevorgang abgeschlossen ist und der CDC-Prozess kontinuierlich repliziert wird, können Sie den Datenbankverbindungsendpunkt Ihrer Anwendung von Ihrem Amazon DocumentDB DocumentDB-Quellcluster auf Ihren Amazon DocumentDB DocumentDB-Zielcluster ändern.

Long-Term Support- (LTS, Langzeit-Support) Versionen nutzen

Amazon DocumentDB bezeichnet bestimmte Versionen als Long-Term Support (LTS) -Versionen. Datenbank-Cluster, die LTS verwenden, können länger auf derselben Version bleiben und weniger Upgrade-Zyklen durchlaufen als Cluster, die Nicht-LTS-Versionen verwenden. LTS-Versionen werden nur bei kritischen Stabilitäts- und Sicherheitspatches gepatcht, ohne dass neue Funktionen eingeführt werden. Zusätzliche optionale Patches können veröffentlicht werden, z. B. Metriken zum Debuggen kritischer Fehler. Diese werden zusammen mit den erforderlichen Patches angewendet.

Aktuelle LTS-Version

Die aktuelle LTS-Version für Amazon DocumentDB ist:

- Nebenversion 5.0.0

Informationen zur Bestimmung der Version, auf der sich Ihr Cluster befindet, finden Sie unterthe section called “Wie überprüfe ich, ob mein vorhandener Engine-Cluster mit Version 5.0.0 auf LTS läuft”.

Einzelheiten zu Supportzeitplänen und Veröffentlichungszyklen für die LTS-Versionen finden Sie unter Support-Daten für Amazon DocumentDB DocumentDB-Engine-Versionen. Amazon DocumentDB wird die nächste LTS-Version über Standardkommunikationskanäle ankündigen.

> **Note**
>
> Eine LTS-Version für Amazon DocumentDB 8.0 wurde noch nicht festgelegt. Wenn Sie LTS benötigen, verwenden Sie Engine-Version 5.0.0 mit Patch-Version 3.0.17983 oder höher.

Wer sollte LTS verwenden

Amazon DocumentDB LTS-Versionen sind für Cluster mit begrenzten Upgrade-Fenstern konzipiert. LTS ist ideal für Produktionsumgebungen, in denen sich die Datenbankverfügbarkeit direkt auf den Geschäftsbetrieb auswirkt.

Ziehen Sie LTS-Versionen in Betracht, wenn:

- Ihre Anwendung hat strenge Verfügbarkeitsanforderungen, die die Upgrade-Möglichkeiten einschränken
- Sie verfügen über alle erforderlichen Funktionen und Erweiterungen der Datenbank-Engine, die Ihre Anwendung benötigt

Ziehen Sie stattdessen Standardversionen in Betracht, wenn:

- Ihre Anwendung kann minimale Unterbrechungen verkraften
- Sie möchten die neuesten Funktionen und Verbesserungen, sobald sie veröffentlicht werden

> **Important**
>
> - Upgrades sind einseitig — Sie können nach dem Upgrade kein Downgrade mehr durchführen
> - Bei Ihrem Cluster kommt es während des Upgrade-Vorgangs zu kurzen Ausfallzeiten

Wie erstelle ich einen neuen LTS-Cluster

Gehen Sie folgendermaßen vor, um einen LTS-Cluster zu erstellen:

1. Erstellen Sie in der Management Console einen neuen Engine-Cluster der Version 5.0.0

2. Stellen Sie nach der Clustererstellung sicher, dass Sie die Engine-Version 5.0.0 verwenden, indem Sie: AWS CLI

```
aws docdb describe-db-clusters \
    --db-cluster-identifier mydocdbcluster \
    --query 'DBClusters[0].EngineVersion'
```

Die Ausgabe dieser Operation sieht in etwa wie folgt aus:

```
"5.0.0"
```

Wie führe ich ein Upgrade von Engine-Version 3.6.0 oder 4.0.0 auf einen 5.0.0 LTS-Cluster durch

Gehen Sie folgendermaßen vor, um ein Upgrade auf einen LTS-Cluster durchzuführen:

1. Führen Sie in der Management Console ein Upgrade (MVU) Ihres Engine-Clusters der Version 3.6.0 oder 4.0.0 auf 5.0.0 durch, nachdem Sie die Amazon DocumentDB DocumentDB-Engine-Version aktualisiert haben
2. Stellen Sie sicher, dass Sie nach dem Upgrade die Engine-Version 5.0.0 verwenden, indem Sie: AWS CLI

```
aws docdb describe-db-clusters \
    --db-cluster-identifier mydocdbcluster \
    --query 'DBClusters[0].EngineVersion'
```

Wie überprüfe ich, ob mein vorhandener Engine-Cluster mit Version 5.0.0 auf LTS läuft

So überprüfen Sie, ob auf Ihrem Engine-Cluster mit Version 5.0.0 eine LTS-Version ausgeführt wird:

1. Stellen Sie sicher, dass Sie die Engine-Version 5.0.0 verwenden, indem Sie: AWS CLI

```
aws docdb describe-db-clusters \
    --db-cluster-identifier mydocdbcluster \
    --query 'DBClusters[0].EngineVersion'
```

2. Führen Sie bei Bedarf ein Upgrade Ihres vorhandenen Engine-Clusters mit Version 5.0.0 durch. Führen Sie anschließend ein Patch-Update auf die Engine-Version eines Clusters durch

Erweiterter Support für Amazon DocumentDB

Mit Amazon DocumentDB Extended Support können Sie gegen Aufpreis eine Engine-Version auch nach Ablauf des Standard-Supportdatums weiter ausführen. Ihre Cluster werden nach Ablauf des Standard-Supportdatums für Extended Support registriert. Wenn Sie die Upgrades bis zum Ende des Standard-Supportdatums der Engine-Version nicht abschließen, werden Ihre Cluster zum Extended Support-Tarif abgerechnet.

Topics

- Überblick über den erweiterten Support
- Gebühren für erweiterten Support
- Verantwortlichkeiten

Amazon DocumentDB Extended Support bietet die folgenden Updates und technischen Support:

- Sicherheitsupdates für kritische und hohe CVEs für Ihre Instance oder Ihren Cluster
- Bugfixes und Patches für kritische Probleme
- Die Möglichkeit, Supportanfragen zu öffnen und Hilfe bei der Fehlerbehebung im Rahmen des standardmäßigen Service Level Agreements von Amazon DocumentDB zu erhalten

Dieses kostenpflichtige Angebot gibt Ihnen mehr Zeit für ein Upgrade auf eine unterstützte Engine-Version. Das Ende des Standard-Supports von Amazon DocumentDB für Version 3.6 ist beispielsweise der 30. März 2026, Sie sind jedoch nicht bereit, vor diesem Datum auf Version 5.0 oder 8.0 zu aktualisieren. In diesem Fall registriert Amazon DocumentDB Ihren Cluster der Version 3.6 am 31. März 2026 beim Extended Support, sodass Sie Amazon DocumentDB Version 3.6 weiterhin verwenden können. Ab dem 1. Juli 2026 wird Ihnen eine erweiterte Support-Prämie für Amazon DocumentDB-Cluster der Version 3.6 AWS berechnet.

Amazon DocumentDB Extended Support ist bis zu 3 Jahre nach dem Standard-Supportdatum der Engine-Version verfügbar. Wenn Sie nach dieser Zeit Ihre Engine-Version nicht auf eine unterstützte Version aktualisiert haben, aktualisiert Amazon DocumentDB Ihre Engine-Version. Wir empfehlen Ihnen, so bald wie möglich ein Upgrade auf eine unterstützte Engine-Version durchzuführen.

Ende des Standard-Supports für Amazon DocumentDB Version 3.6 und Termine für den erweiterten Support:

- Veröffentlichung von Version 3.6 — 9. Januar 2019
- Ende der Standardunterstützung für Version 3.6 — 30. März 2026
- Beginn der Version 3.6 Erweiterter Support, Preis für ein Jahr — 1. Juli 2026
- Beginn der Version 3.6 Extended Support, Preis für Jahr 3 — 31. März 2028
- Ende von Version 3.6 Extended Support — 30. März 2029

Überblick über den erweiterten Support

Amazon DocumentDB aktualisiert Ihren Cluster auf die letzte veröffentlichte Engine-Version (vor dem Ende des Extended Support-Datums), falls Ihr Cluster noch nicht auf dieser Version installiert ist. Der Upgrade-Zeitraum beginnt erst nach dem Standard-Supportdatum für diese Engine-Version.

Sie können neue Cluster mit einer Engine-Version erstellen, die das Ende des Standard-Supportdatums erreicht hat, wenn Sie bereits über einen Cluster auf dieser Engine-Version verfügen. Amazon DocumentDB registriert diese neuen Cluster bei Amazon DocumentDB Extended Support und berechnet Ihnen für dieses Angebot Gebühren. Wenn Sie vor dem Ende des Standard-Supports von Version 3.6 auf eine Engine-Version aktualisieren, für die der Standardsupport von Amazon DocumentDB noch verfügbar ist, wird Ihnen keine erweiterte Support-Prämie berechnet.

Sie können die Registrierung für Amazon DocumentDB Extended Support jederzeit beenden. Um die Registrierung zu beenden, führen Sie für jeden registrierten Cluster ein Upgrade auf eine neuere Engine-Version durch, für die weiterhin Amazon DocumentDB DocumentDB-Standardunterstützung gilt. Das Ende der Registrierung für Amazon DocumentDB Extended Support wird an dem Tag wirksam, an dem Sie ein Upgrade auf eine neuere Engine-Version abschließen, für die der Amazon DocumentDB DocumentDB-Standardsupport noch verfügbar ist.

Weitere Informationen zum Ende des Standard-Supports von Amazon DocumentDB und zum Ende des erweiterten Supports von Amazon DocumentDB finden Sie unter. Unterstützungstermine der Amazon DocumentDB DocumentDB-Engine-Version

Gebühren für erweiterten Support

Ab dem 1. Juli 2026 fallen Gebühren für alle Cluster an, die Extended Support nutzen. Informationen zum Ende des Standard-Supportdatums für Amazon DocumentDB Version 3.6 finden Sie unterUnterstützungstermine der Amazon DocumentDB DocumentDB-Engine-Version.

Die zusätzliche Gebühr für Amazon DocumentDB Extended Support endet, wenn Sie eine der folgenden Maßnahmen ergreifen:

- Führen Sie ein Upgrade auf eine Engine-Version durch, für die der Standardsupport gilt
- Löschen Sie den Cluster, auf dem Version 3.6 ausgeführt wird, nach Ablauf des Standard-Supportdatums

Zum Beispiel wird Amazon DocumentDB Version 3.6 am 31. März 2026 in den erweiterten Support aufgenommen, aber die Gebühren beginnen erst am 1. Juli 2026. Wenn Sie Ihren Amazon DocumentDB-Cluster Version 3.6 am 31. Juli 2026 auf Amazon DocumentDB Version 5.0 aktualisieren, werden Ihnen nur 30 Tage Extended Support für Amazon DocumentDB Version 3.6 in Rechnung gestellt. Weitere Informationen finden Sie unter Amazon DocumentDB DocumentDB-Preise.

Verantwortlichkeiten

Im Folgenden sind die Verantwortlichkeiten von Amazon DocumentDB und Ihre Pflichten beim Amazon DocumentDB Extended Support aufgeführt.

Verantwortlichkeiten von Amazon DocumentDB

Nach Ablauf des Standard-Supportdatums für Amazon DocumentDB Version 3.6 installiert Amazon DocumentDB Patches, Bugfixes und Upgrades für Cluster der Version 3.6, die für Extended Support registriert sind.

Ihre Aufgaben

Sie sind dafür verantwortlich, Ihre Engine vor dem Ende des erweiterten Support von Amazon DocumentDB Version 3.6 auf eine neuere Engine-Version aufzurüsten. Wenn Sie Ihren Cluster nicht aktualisieren, versucht Amazon DocumentDB nach Ablauf des Extended Support-Datums für Amazon DocumentDB Version 3.6, Ihren Cluster auf die neueste Engine-Version zu aktualisieren, die vom Amazon DocumentDB DocumentDB-Standardsupport unterstützt wird.

Sicherheit in Amazon DocumentDB

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von einem Rechenzentrum und einer Netzwerkarchitektur, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame Verantwortung von Ihnen AWS und Ihnen. Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Verwendung von Amazon DocumentDB anwenden können. 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. Third-party Auditoren testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheitsmaßnahmen im Rahmen der AWS Compliance-Programme. Weitere Informationen zu den Compliance-Programmen, die für Amazon DocumentDB (mit MongoDB-Kompatibilität) 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. In Ihre Verantwortung fallen außerdem weitere Faktoren, wie z. B. die Vertraulichkeit der Daten, die Anforderungen Ihrer Organisation sowie geltende Gesetze und Vorschriften.

Amazon DocumentDB ist im Rahmen des Federal Risk and Authorization Management Program (FedRAMP) autorisiert. Es verfügt über eine FedRAMP High-Autorisierung für AWS GovCloud (US-) Regionen und eine FedRAMP Moderate-Autorisierung für US-Regionen. AWS East/West Einzelheiten zu den Compliance-Maßnahmen AWS und den Bemühungen zur Einhaltung der Vorschriften finden Sie unter AWS Services im Umfang nach Compliance-Programmen.

> **Note**
>
> Dieses Kapitel gilt sowohl für instanzbasierte Cluster als auch für Elastic Clusters. Weitere Informationen finden Sie in den folgenden Themen.

Sie erfahren auch, wie Sie andere AWS Dienste nutzen können, mit denen Sie Ihre Amazon DocumentDB DocumentDB-Ressourcen überwachen und sichern können. In den folgenden Themen erfahren Sie, wie Sie Amazon DocumentDB konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen.

Topics

- Passwortverwaltung mit Amazon DocumentDB und AWS Secrets Manager
- Datenschutz in Amazon DocumentDB
- Identity and Access Management für Amazon DocumentDB
- Cross-service verwirrter Stellvertreter, Prävention
- Authentifizierung mit IAM-Identität
- Amazon DocumentDB DocumentDB-Benutzer verwalten
- Datenbankzugriff mit Role-Based Access Control
- Protokollierung und Überwachung in Amazon DocumentDB
- Aktualisierung Ihrer Amazon DocumentDB-TLS-Zertifikate
- Konformitätsprüfung in Amazon DocumentDB
- Resilienz in Amazon DocumentDB
- Infrastruktursicherheit in Amazon DocumentDB
- Amazon DocumentDB DocumentDB-API und VPC-Schnittstellen-Endpunkte (AWS PrivateLink)
- Bewährte Sicherheitsmethoden für Amazon DocumentDB
- Amazon DocumentDB DocumentDB-Ereignisse prüfen
- Amazon VPC und Amazon DocumentDB

Passwortverwaltung mit Amazon DocumentDB und AWS Secrets Manager

Amazon DocumentDB ist in Secrets Manager integriert, um primäre Benutzerkennwörter für Ihre Cluster zu verwalten.

Topics

- Einschränkungen für die Secrets Manager Manager-Integration mit Amazon DocumentDB
- Überblick über die Verwaltung von Primärbenutzerkennwörtern mit AWS Secrets Manager
- Durchsetzung der Amazon DocumentDB DocumentDB-Verwaltung des primären Benutzerkennworts in AWS Secrets Manager
- Verwaltung des primären Benutzerpassworts für einen Cluster mit Secrets Manager

Einschränkungen für die Secrets Manager Manager-Integration mit Amazon DocumentDB

Die Verwaltung von Primärbenutzerkennwörtern mit Secrets Manager wird für die folgenden Funktionen nicht unterstützt:

- Cluster, die Teil einer globalen Amazon DocumentDB DocumentDB-Datenbank sind
- Amazon DocumentDB — Regionsübergreifende Lesereplikate

Überblick über die Verwaltung von Primärbenutzerkennwörtern mit AWS Secrets Manager

Mit AWS Secrets Manager können Sie hartcodierte Anmeldeinformationen in Ihrem Code, einschließlich Datenbankkennwörtern, durch einen API-Aufruf an Secrets Manager ersetzen, um das Geheimnis programmgesteuert abzurufen. Weitere Informationen zu Secrets Manager finden Sie im Benutzerhandbuch für AWS Secrets Manager.

Wenn Sie Datenbankgeheimnisse in Secrets Manager speichern, fallen Gebühren für Ihr AWS Konto an. Informationen zu Preisen finden Sie unter AWS Secrets Manager -Preise.

Sie können angeben, dass Amazon DocumentDB das primäre Benutzerkennwort in Secrets Manager für einen Amazon DocumentDB-Cluster verwaltet, wenn Sie einen der folgenden Vorgänge ausführen:

- Den Cluster erstellen
- Ändern Sie den Cluster

Wenn Sie angeben, dass Amazon DocumentDB das primäre Benutzerkennwort in Secrets Manager verwaltet, generiert Amazon DocumentDB das Passwort und speichert es in Secrets Manager. Sie können direkt mit dem Secret interagieren, um die Anmeldeinformationen für den Hauptbenutzer abzurufen. Sie können auch einen vom Kunden verwalteten Schlüssel angeben, um das Secret zu verschlüsseln, oder den KMS-Schlüssel verwenden, der von Secrets Manager bereitgestellt wird.

Amazon DocumentDB verwaltet die Einstellungen für das Geheimnis und wechselt das Geheimnis standardmäßig alle sieben Tage. Sie können einige Einstellungen ändern, wie zum Beispiel den Rotationsplan. Wenn Sie einen Cluster löschen, der ein Geheimnis in Secrets Manager verwaltet, werden das Geheimnis und die zugehörigen Metadaten ebenfalls gelöscht.

Um eine Verbindung zu einem Cluster mit den Anmeldeinformationen in einem Secret herzustellen, können Sie das Secret von Secrets Manager abrufen. Weitere Informationen finden Sie im AWS Secrets Manager Benutzerhandbuch unter Get Secrets from AWS Secrets Manager and Connect to a SQL database using JDBC with credentials in an AWS Secrets Manager secret.

Durchsetzung der Amazon DocumentDB DocumentDB-Verwaltung des primären Benutzerkennworts in AWS Secrets Manager

Sie können IAM-Bedingungsschlüssel verwenden, um die Amazon DocumentDB DocumentDB-Verwaltung des primären Benutzerkennworts in zu erzwingen. AWS Secrets Manager Die folgende Richtlinie erlaubt es Benutzern nicht, Instances oder Cluster zu erstellen oder wiederherzustellen, es sei denn, das primäre Benutzerkennwort wird von Amazon DocumentDB in Secrets Manager verwaltet.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "rds:CreateDBCluster"
            ],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "rds:ManageMasterUserPassword": false
                }
            }
        }
    ]
}
```

Verwaltung des primären Benutzerpassworts für einen Cluster mit Secrets Manager

Sie können die Amazon DocumentDB DocumentDB-Verwaltung des primären Benutzerkennworts in Secrets Manager konfigurieren, wenn Sie die folgenden Aktionen ausführen:

- Einen Amazon DocumentDB-Cluster erstellen
- Ändern eines Amazon DocumentDB-Clusters

Sie können die Amazon DocumentDB DocumentDB-Konsole oder die verwenden AWS CLI , um diese Aktionen auszuführen.

Datenschutz in Amazon DocumentDB

Das AWS Modell der gilt für den Datenschutz in Amazon DocumentDB. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der AWS Cloud alle Systeme laufen. 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 . Weitere Informationen zum Datenschutz in Europa finden Sie im Zentrum für die Datenschutz-Grundverordnung (DSGVO).

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 Amazon DocumentDB oder anderen Geräten arbeiten und die Konsole AWS CLI, API oder AWS SDKs AWS-Services verwenden. 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.

Themen

- Client-side Verschlüsselung auf Feldebene
- Verschlüsselung von Amazon DocumentDB DocumentDB-Daten im Ruhezustand
- Verschlüsseln von Daten während der Übertragung
- Schlüsselverwaltung

Client-side Verschlüsselung auf Feldebene

Mit der clientseitigen Verschlüsselung auf Feldebene (FLE) von Amazon DocumentDB können Sie sensible Daten in Ihren Client-Anwendungen verschlüsseln, bevor sie in einen Amazon DocumentDB-Cluster übertragen werden. Vertrauliche Daten bleiben verschlüsselt, wenn sie in einem Cluster gespeichert und verarbeitet werden, und werden beim Abrufen in der Client-Anwendung entschlüsselt.

Topics

- Erste Schritte
- Abfragen in der clientseitigen FLE

Erste Schritte

Die Erstkonfiguration der clientseitigen FLE in Amazon DocumentDB ist ein vierstufiger Prozess, der die Erstellung eines Verschlüsselungsschlüssels, die Zuordnung einer Rolle zur Anwendung, die Konfiguration der Anwendung und die Definition des CRUD-Vorgangs mit Verschlüsselungsoptionen umfasst.

Topics

- Schritt 1: Erstellen Sie die Verschlüsselungsschlüssel
- Schritt 2: Ordnen Sie der Anwendung eine Rolle zu
- Schritt 3: Konfigurieren Sie die Anwendung
- Schritt 4: Definieren Sie eine CRUD-Operation
- Beispiel: Konfigurationsdatei für die clientseitige Verschlüsselung auf Feldebene

Schritt 1: Erstellen Sie die Verschlüsselungsschlüssel

Erstellen Sie mithilfe AWS Key Management Service eines symmetrischen Schlüssels, der zum Verschlüsseln und Entschlüsseln des vertraulichen Datenfeldes verwendet wird, und erteilen Sie ihm die erforderlichen IAM-Nutzungsberechtigungen. AWS KMS speichert den Kundenschlüssel (CK), der zur Verschlüsselung von Datenschlüsseln (DKs) verwendet wird. Speichert den Kundenschlüssel in KMS, um Ihre Sicherheitslage zu stärken. Der Datenschlüssel ist der Sekundärschlüssel, der in einer Amazon DocumentDB-Sammlung gespeichert wird und benötigt wird, um sensible Felder zu verschlüsseln, bevor das Dokument in Amazon DocumentDB gespeichert wird. Der Kundenschlüssel verschlüsselt den Datenschlüssel, der wiederum Ihre Daten ver- und entschlüsselt. Wenn Sie einen globalen Cluster verwenden, können Sie einen Schlüssel für mehrere Regionen erstellen, der von verschiedenen Servicerollen in verschiedenen Regionen verwendet werden kann.

Weitere Informationen zum AWS Key Management Service, einschließlich der Erstellung eines Schlüssels, finden Sie im AWS Key Management Service Developer Guide.

Schritt 2: Ordnen Sie der Anwendung eine Rolle zu

Erstellen Sie eine IAM-Richtlinie mit den entsprechenden AWS KMS Berechtigungen. Diese Richtlinie ermöglicht es IAM-Identitäten, an die sie angehängt ist, den im Ressourcenfeld angegebenen KMS-Schlüssel zu verschlüsseln und zu entschlüsseln. Ihre Anwendung nimmt diese IAM-Rolle für die Authentifizierung an. AWS KMS

Die Richtlinie sollte etwa wie folgt aussehen:

```
{ "Effect": "Allow",
"Action": ["kms:Decrypt", "kms:Encrypt"],
"Resource": "Customer Key ARN"
}
```

Schritt 3: Konfigurieren Sie die Anwendung

Inzwischen haben Sie einen Kundenschlüssel definiert AWS KMS und eine IAM-Rolle erstellt und ihr die richtigen IAM-Berechtigungen für den Zugriff auf den Kundenschlüssel erteilt. Importieren Sie die erforderlichen Pakete.

```
import boto3
import json
import base64
from pymongo import MongoClient
from pymongo.encryption import (Algorithm,
                                ClientEncryption)
```

```
# create a session object:
my_session = boto3.session.Session()

# get access_key and secret_key programmatically using get_frozen_credentials() method:
current_credentials = my_session.get_credentials().get_frozen_credentials()
```

1. Geben Sie „aws“ als KMS-Anbietertyp an und geben Sie Ihre Kontoanmeldeinformationen ein, die Sie im vorherigen Schritt abgerufen haben.

   ```
   provider = "aws"
   kms_providers = {
       provider: {
           "accessKeyId": current_credentials.access_key,
           "secretAccessKey": current_credentials.secret_key
       }
   }
   ```

2. Geben Sie den Kundenschlüssel an, der zur Verschlüsselung des Datenschlüssels verwendet wird:

   ```
   customer_key = {
   “region”: “AWS region of the customer_key”,
   ```

```
    “key”: “customer_key ARN”
}

key_vault_namespace = "encryption.dataKeys"

key_alt_name = 'TEST_DATA_KEY'
```

3. Konfigurieren Sie das MongoClient Objekt:

```
client = MongoClient(connection_string)

coll = client.test.coll
coll.drop()

client_encryption = ClientEncryption(
    kms_providers, # pass in the kms_providers variable from the previous step
    key_vault_namespace = key_vault_namespace,
    client,
    coll.codec_options
)
```

4. Generieren Sie Ihren Datenschlüssel:

```
data_key_id = client_encryption.create_data_key(provider,
    customer_key,
    key_alt_name = [key_alt_name])
```

5. Rufen Sie Ihren vorhandenen Datenschlüssel ab:

```
data_key = DataKey("aws",
    master_key = customer_key)
key_id = data_key["_id"]
data_key_id = client[key_vault_namespace].find_one({"_id": key_id})
```

Schritt 4: Definieren Sie eine CRUD-Operation

Definieren Sie den CRUD-Vorgang mit Verschlüsselungsoptionen.

1. Definiert die Sammlung so, dass write/read ein einzelnes Dokument gelöscht wird:

```
coll = client.gameinfo.users
```

2. Explizite Verschlüsselung — Felder verschlüsseln und Folgendes einfügen:

> **Note**
>
> Es muss genau einer der Werte „key_id“ oder „key_alt_name“ angegeben werden.

```
encrypted_first_name = client_encryption.encrypt(
    "Jane",
    Algorithm.AEAD_AES_256_CBC_HMAC_SHA_512_Deterministic,
    key_id=data_key_id
)
encrypted_last_name = client_encryption.encrypt(
    "Doe",
    Algorithm.AEAD_AES_256_CBC_HMAC_SHA_512_Deterministic,
    key_id=data_key_id
)
encrypted_dob = client_encryption.encrypt(
    "1990-01-01",
    Algorithm.AEAD_AES_256_CBC_HMAC_SHA_512_Random,
    key_id=data_key_id
)

coll.insert_one(
    {"gamerTag": "jane_doe90",
    "firstName": encrypted_first_name,
    "lastName": encrypted_last_name,
    "dateOfBirth":encrypted_dob,
    "Favorite_games":["Halo","Age of Empires 2","Medal of Honor"]
})
```

Beispiel: Konfigurationsdatei für die clientseitige Verschlüsselung auf Feldebene

Ersetzen Sie im folgenden Beispiel jede *placeholder* durch Ihre eigenen Informationen.

```
# import python packages:
import boto3
import json
import base64
from pymongo import MongoClient
from pymongo.encryption import (Algorithm,
```

```
                                ClientEncryption)

def main():

    # create a session object:
    my_session = boto3.session.Session()

    # get aws_region from session object:
    aws_region = my_session.region_name

    # get access_key and secret_key programmatically using get_frozen_credentials()
 method:
    current_credentials = my_session.get_credentials().get_frozen_credentials()
    provider = "aws"

    # define the kms_providers which is later used to create the Data Key:
    kms_providers = {
        provider: {
            "accessKeyId": current_credentials.access_key,
            "secretAccessKey": current_credentials.secret_key
        }
    }

    # enter the kms key ARN. Replace the example ARN value.
    kms_arn = "arn:aws:kms:us-east-1:123456789:key/abcd-efgh-ijkl-mnop"
    customer_key = {
        "region": aws_region,
        "key":kms_arn
    }

    # secrets manager is used to store and retrieve user credentials for connecting to
 an Amazon DocumentDB cluster.
    # retrieve the secret using the secret name. Replace the example secret key.
    secret_name = "/dev/secretKey"
    docdb_credentials = json.loads(my_session.client(service_name = 'secretsmanager',
 region_name = "us-east-1").get_secret_value(SecretId = secret_name)['SecretString'])

    connection_params = '/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false'
    conn_str = 'mongodb://' + docdb_credentials["username"] + ':' +
 docdb_credentials["password"] + '@' + docdb_credentials["host"] + ':' +
 str(docdb_credentials["port"]) + connection_params
    client = MongoClient(conn_str)
```

```
    coll = client.test.coll
    coll.drop()

    # store the encryption data keys in a key vault collection (having naming
convention as db.collection):
    key_vault_namespace = "encryption.dataKeys"
    key_vault_db_name, key_vault_coll_name = key_vault_namespace.split(".", 1)

    # set up the key vault (key_vault_namespace) for this example:
    key_vault = client[key_vault_db_name][key_vault_coll_name]
    key_vault.drop()
    key_vault.create_index("keyAltNames", unique=True)

    client_encryption = ClientEncryption(
        kms_providers,
        key_vault_namespace,
        client,
        coll.codec_options)

    # create a new data key for the encrypted field:
    data_key_id = client_encryption.create_data_key(provider, master_key=customer_key,
key_alt_names=["some_key_alt_name"], key_material = None)

    # explicitly encrypt a field:
    encrypted_first_name = client_encryption.encrypt(
    "Jane",
    Algorithm.AEAD_AES_256_CBC_HMAC_SHA_512_Deterministic,
    key_id=data_key_id
    )
    coll.insert_one(
    {"gamerTag": "jane_doe90",
    "firstName": encrypted_first_name
    })
    doc = coll.find_one()
    print('Encrypted document: %s' % (doc,))

    # explicitly decrypt the field:
    doc["firstName"] = client_encryption.decrypt(doc["firstName"])
    print('Decrypted document: %s' % (doc,))

    # cleanup resources:
    client_encryption.close()
    client.close()
```

```
if __name__ == "__main__":
    main()
```

Abfragen in der clientseitigen FLE

Amazon DocumentDB unterstützt nur Gleichheitsabfragen mit clientseitigen FLE-verschlüsselten Werten.

Um beispielsweise Dokumente abzufragen, bei denen der verschlüsselte Gamerscore 500 entspricht, verwendet der Client eine explizite Verschlüsselungsmethode, um den Abfragewert zu verschlüsseln:

```
encrypted_gamerscore_filter = client_encryption.encrypt(
    500,
    Algorithm.AEAD_AES_256_CBC_HMAC_SHA_512_Deterministic,
    key_id=data_key_id
)

coll.find( {
    "gamerscore" : { "$eq" : encrypted_gamerscore_filter }
} )
```

Verschlüsselung von Amazon DocumentDB DocumentDB-Daten im Ruhezustand

> **Note**
>
> AWS KMS ersetzt den Begriff Customer Master Key (CMK) durch AWS KMS keyeinen KMS-Schlüssel. Das Konzept hat sich nicht geändert. Um bahnbrechende Änderungen zu verhindern, AWS KMS werden einige Varianten dieses Begriffs beibehalten.

Sie verschlüsseln ruhende Daten in Ihrem Amazon DocumentDB-Cluster, indem Sie bei der Erstellung Ihres Clusters die Speicherverschlüsselungsoption angeben. Die Speicher-Verschlüsselung ist Cluster-weit aktiviert und wird auf alle Instances angewendet, einschließlich der primären Instance und alle Replikate. Sie wird auch auf das Speichervolumen Ihres Clusters, auf Daten, Indizes, Protokolle, automatisierte Sicherungen und Snapshots angewendet.

Amazon DocumentDB verwendet den 256-Bit-Advanced Encryption Standard (AES-256), um Ihre Daten mit den in () gespeicherten Verschlüsselungsschlüsseln zu verschlüsseln. AWS Key

Management Service AWS KMS Wenn Sie einen Amazon DocumentDB-Cluster mit aktivierter Verschlüsselung im Ruhezustand verwenden, müssen Sie Ihre Anwendungslogik oder Client-Verbindung nicht ändern. Amazon DocumentDB wickelt die Verschlüsselung und Entschlüsselung Ihrer Daten transparent und mit minimalen Auswirkungen auf die Leistung ab.

Amazon DocumentDB ist in eine Methode integriert, die als Umschlagverschlüsselung bekannt ist, AWS KMS und verwendet diese zum Schutz Ihrer Daten. Wenn ein Amazon DocumentDB-Cluster mit einem verschlüsselt ist AWS KMS, bittet Amazon DocumentDB, Ihren KMS-Schlüssel AWS KMS zu verwenden, um einen Chiffretext-Datenschlüssel zur Verschlüsselung des Speichervolumes zu generieren. Der Chiffretext-Datenschlüssel wird mit dem von Ihnen definierten KMS-Schlüssel verschlüsselt und zusammen mit den verschlüsselten Daten und Speichermetadaten gespeichert. Wenn Amazon DocumentDB auf Ihre verschlüsselten Daten zugreifen muss, fordert AWS KMS es die Entschlüsselung des Chiffretext-Datenschlüssels mithilfe Ihres KMS-Schlüssels an und speichert den Klartext-Datenschlüssel im Speicher, um Daten auf dem Speichervolume effizient zu verschlüsseln und zu entschlüsseln.

Die Speicherverschlüsselungsfunktion in Amazon DocumentDB ist für alle unterstützten Instance-Größen und überall dort verfügbar, AWS-Regionen wo Amazon DocumentDB verfügbar ist.

Verschlüsselung im Ruhezustand für einen Amazon DocumentDB-Cluster aktivieren

Sie können die Verschlüsselung im Ruhezustand auf einem Amazon DocumentDB-Cluster aktivieren oder deaktivieren, wenn der Cluster entweder mit dem AWS-Managementkonsole oder dem AWS Command Line Interface ()AWS CLI bereitgestellt wird. Cluster, die Sie mit der Konsole erstellen, haben standardmäßig die Verschlüsselung im Ruhezustand aktiviert. Bei Clustern, die Sie mit dem erstellen, ist AWS CLI die Verschlüsselung im Ruhezustand standardmäßig deaktiviert. Daher müssen Sie die Verschlüsselung im Ruhezustand explizit mit dem `--storage-encrypted`-Parameter aktivieren. In beiden Fällen können Sie nach dem Erstellen des Clusters die Option „Verschlüsselung im Ruhezustand“ nicht ändern.

Amazon DocumentDB verwendet, AWS KMS um Verschlüsselungsschlüssel abzurufen und zu verwalten und die Richtlinien zu definieren, die kontrollieren, wie diese Schlüssel verwendet werden können. Wenn Sie keine AWS KMS Schlüssel-ID angeben, verwendet Amazon DocumentDB den standardmäßigen KMS-Schlüssel für AWS verwaltete Dienste. Amazon DocumentDB erstellt für jeden AWS-Region in Ihrem AWS-Konto einen eigenen KMS-Schlüssel. Weitere Informationen finden Sie unter AWS Key Management Service -Konzepte.

Informationen zu den ersten Schritten beim Erstellen Ihres eigenen KMS-Schlüssels finden Sie unter Erste Schritte im AWS Key Management Service Entwicklerhandbuch.

> **Important**
>
> Sie müssen einen KMS-Schlüssel für die symmetrische Verschlüsselung verwenden, um Ihren Cluster zu verschlüsseln, da Amazon DocumentDB nur KMS-Schlüssel mit symmetrischer Verschlüsselung unterstützt. Verwenden Sie keinen asymmetrischen KMS-Schlüssel, um zu versuchen, die Daten in Ihren Amazon DocumentDB-Clustern zu verschlüsseln. Weitere Informationen finden Sie unter Asymmetrische Schlüssel AWS KMS im Entwicklerhandbuch.AWS Key Management Service

Wenn Amazon DocumentDB nicht mehr auf den KMS-Schlüssel für einen Cluster zugreifen kann — wenn beispielsweise der, dem der Schlüssel gehört AWS-Konto , gesperrt ist, der Schlüssel deaktiviert ist, der Schlüssel zum Löschen geplant ist oder die Schlüsselrichtlinie oder -gewährung, auf die sich Amazon DocumentDB stützt, entfernt wird — geht der Cluster zunächst in den `inaccessible-encryption-credentials-recoverable` Status über. Solange sich der Cluster in diesem Status befindet, stoppt Amazon DocumentDB die Instances des Clusters und Sie können weder aus dem Cluster lesen noch in ihn schreiben, aber der Cluster kann trotzdem wiederhergestellt werden, wenn der Zugriff auf den KMS-Schlüssel innerhalb von 7 Tagen wiederhergestellt wird. Wenn der Zugriff nicht innerhalb von 7 Tagen wiederhergestellt wird, wechselt der Cluster in den `inaccessible-encryption-credentials` Terminalstatus. Ab dem Terminalstatus ist der Cluster nicht mehr verfügbar und der aktuelle Status der Datenbank kann nicht wiederhergestellt werden. Sie können nur mit dem ursprünglichen KMS-Schlüssel Daten aus einer Sicherung wiederherstellen oder eine Point-in-Time-Wiederherstellung durchführen. Für Amazon DocumentDB sind Backups immer für mindestens einen Tag aktiviert.

> **Note**
>
> Cluster, die Teil eines globalen Clusters sind, verhalten sich unterschiedlich. Wenn Amazon DocumentDB feststellt, dass es nicht mehr auf den KMS-Schlüssel zugreifen kann, gehen alle Cluster im globalen Cluster direkt in den `inaccessible-encryption-credentials` Terminalstatus über und überspringen den Status „Wiederherstellbar“. Das liegt daran, dass ein Cluster, der Teil eines globalen Clusters ist, nur gestoppt und gestartet werden kann, wenn er der einzige Cluster im globalen Cluster ist. Für die Wiederherstellung müssen Sie die Wiederherstellung anhand eines Snapshots durchführen oder eine Point-in-Time-Wiederherstellung durchführen. Um die ursprünglichen Cluster zu löschen, müssen Sie zuerst jeden Cluster aus dem globalen Cluster entfernen und ihn dann löschen.

> **Important**
>
> Sie können den KMS-Schlüssel für einen verschlüsselten Cluster nicht ändern, nachdem Sie ihn bereits erstellt haben. Stellen Sie sicher, dass Sie Ihre Anforderungen an den Verschlüsselungsschlüssel bestimmen, bevor Sie Ihren verschlüsselten Cluster erstellen.

Using the AWS-Managementkonsole

Geben Sie beim Erstellen eines Clusters die Option „Verschlüsselung im Ruhezustand“ an. Die Verschlüsselung im Ruhezustand ist standardmäßig aktiviert, wenn Sie einen Cluster mit der AWS-Managementkonsole erstellen. Nachdem der Cluster erstellt wurde, kann er nicht mehr geändert werden.

So legen Sie beim Erstellen eines Clusters die Option „Verschlüsselung im Ruhezustand“ fest

1. Erstellen Sie einen Amazon DocumentDB-Cluster, wie im Abschnitt Erste Schritte beschrieben. Wählen Sie jedoch in Schritt 6 nicht Create Cluster (Cluster erstellen) aus.
2. Wählen Sie unterhalb des Abschnitts Authentication (Authentifizierung) die Option Show advanced settings (Erweiterte Einstellungen anzeigen) aus.
3. Scrollen Sie nach unten zum Encryption-at-restAbschnitt.
4. Wählen Sie die Option aus, die Sie für die Verschlüsselung im Ruhezustand wünschen. Egal, welche Option Sie wählen, nach dem Erstellen des Clusters können Sie sie nicht mehr ändern.
   - Wenn Sie Daten im Ruhezustand in diesem Cluster verschlüsseln möchten, wählen Sie Enable encryption (Verschlüsselung aktivieren) aus.
   - Wenn Sie Daten im Ruhezustand in diesem Cluster nicht verschlüsseln möchten, wählen Sie Disable encryption (Verschlüsselung deaktivieren) aus.
5. Wählen Sie den gewünschten Primärschlüssel aus. Amazon DocumentDB verwendet die AWS Key Management Service (AWS KMS), um Verschlüsselungsschlüssel abzurufen und zu verwalten und um die Richtlinien zu definieren, die steuern, wie diese Schlüssel verwendet werden können. Wenn Sie keine AWS KMS Schlüssel-ID angeben, verwendet Amazon DocumentDB den standardmäßigen KMS-Schlüssel für AWS verwaltete Dienste. Weitere Informationen finden Sie unter AWS Key Management Service -Konzepte.

> **Note**
>
> Nachdem Sie einen verschlüsselten Cluster erstellt haben, können Sie den KMS-Schlüssel für diesen Cluster nicht ändern. Stellen Sie sicher, dass Sie Ihre Anforderungen an den Verschlüsselungsschlüssel bestimmen, bevor Sie Ihren verschlüsselten Cluster erstellen.

6. Füllen Sie die anderen Abschnitte nach Bedarf aus und erstellen Sie Ihren Cluster.

Using the AWS CLI

Um einen Amazon DocumentDB-Cluster mit dem zu verschlüsseln AWS CLI, führen Sie den `create-db-cluster`Befehl aus und geben Sie die `--storage-encrypted` Option an. Amazon DocumentDB-Cluster, die mit dem erstellt wurden, aktivieren standardmäßig AWS CLI keine Speicherverschlüsselung.

Im folgenden Beispiel wird ein Amazon DocumentDB-Cluster mit aktivierter Speicherverschlüsselung erstellt.

Ersetzen Sie in den folgenden Beispielen jedes *`user input placeholder`* durch die Informationen Ihres Clusters.

Example

Für Linux, macOS oder Unix:

```
aws docdb create-db-cluster \
  --db-cluster-identifier mydocdbcluster \
  --port 27017 \
  --engine docdb \
  --master-username SampleUser1 \
  --master-user-password primaryPassword \
  --storage-encrypted
```

Für Windows:

```
aws docdb create-db-cluster ^
  --db-cluster-identifier SampleUser1 ^
```

```
  --port 27017 ^
  --engine docdb ^
  --master-username SampleUser1 ^
  --master-user-password primaryPassword ^
  --storage-encrypted
```

Wenn Sie einen verschlüsselten Amazon DocumentDB-Cluster erstellen, können Sie eine AWS KMS Schlüssel-ID angeben, wie im folgenden Beispiel.

Example

Für Linux, macOS oder Unix:

```
aws docdb create-db-cluster \
  --db-cluster-identifier SampleUser1 \
  --port 27017 \
  --engine docdb \
  --master-username primaryUsername \
  --master-user-password yourPrimaryPassword \
  --storage-encrypted \
  --kms-key-id key-arn-or-alias
```

Für Windows:

```
aws docdb create-db-cluster ^
  --db-cluster-identifier SampleUser1 ^
  --port 27017 ^
  --engine docdb ^
  --master-username SampleUser1 ^
  --master-user-password primaryPassword ^
  --storage-encrypted ^
  --kms-key-id key-arn-or-alias
```

> **Note**
>
> Nachdem Sie einen verschlüsselten Cluster erstellt haben, können Sie den KMS-Schlüssel für diesen Cluster nicht ändern. Stellen Sie sicher, dass Sie Ihre Anforderungen an den Verschlüsselungsschlüssel bestimmen, bevor Sie Ihren verschlüsselten Cluster erstellen.

Auflösen eines Amazon DocumentDB-Clusters in einem Verschlüsselungsstatus, auf den nicht zugegriffen werden kann

Ein Amazon DocumentDB-Cluster wechselt in den Verschlüsselungsstatus „Unzugänglich“, wenn Amazon DocumentDB nicht auf den KMS-Schlüssel zugreifen kann, mit dem der Cluster verschlüsselt wurde. Es gibt zwei solcher Status, und der Wiederherstellungspfad hängt davon ab, in welchem sich der Cluster befindet.

Status „unzugängliche Verschlüsselungsdaten — **`wiederherstellbar`**“

Solange sich der Cluster im `inaccessible-encryption-credentials-recoverable` Status befindet, können Sie den Cluster wieder in den Zustand versetzen, `available` indem Sie den Zugriff von Amazon DocumentDB auf den KMS-Schlüssel wiederherstellen und dann den Cluster starten. Gehen Sie wie folgt vor, um diesen Status zu beheben:

1. Vergewissern Sie sich AWS-Konto , dass der Besitzer des KMS-Schlüssels aktiv ist. Wenn das Konto gesperrt ist, reaktivieren Sie es.
2. Vergewissern Sie sich, dass der KMS-Schlüssel aktiviert ist. Weitere Informationen finden Sie unter Schlüssel aktivieren und deaktivieren im AWS Key Management Service Entwicklerhandbuch.
3. Prüfen Sie, ob der KMS-Schlüssel zum Löschen geplant ist. Ist dies der Fall, brechen Sie das geplante Löschen des Schlüssels ab. Weitere Informationen finden Sie im AWS Key Management Service Entwicklerhandbuch unter Das Löschen von Schlüsseln planen und stornieren.
4. Vergewissern Sie sich, dass die KMS-Schlüsselrichtlinie und alle Zuschüsse, auf die Amazon DocumentDB angewiesen ist, Amazon DocumentDB weiterhin die Verwendung des Schlüssels gestatten.
5. Nachdem der Zugriff auf den KMS-Schlüssel wiederhergestellt ist, starten Sie den Cluster mithilfe von AWS-Managementkonsole oder, indem Sie den Befehl ausführen. `start-db-cluster` AWS CLI

   Example

   Für Linux, macOS oder Unix:

   ```
   aws docdb start-db-cluster \
     --db-cluster-identifier example-cluster
   ```

   Für Windows:

```
aws docdb start-db-cluster ^
  --db-cluster-identifier example-cluster
```

> **Important**
>
> Wenn der Zugriff auf den KMS-Schlüssel nicht innerhalb von 7 Tagen wiederhergestellt wird, wechselt der Cluster in den `inaccessible-encryption-credentials` Terminalstatus, von dem aus er nicht gestartet werden kann.

Status der verschlüsselten **`Anmeldeinformationen nicht zugänglich`**

Der Status ist Terminal. `inaccessible-encryption-credentials` Der Cluster kann nicht gestartet werden, und der Ausführungsstatus der Datenbank kann nicht wiederhergestellt werden. Um Ihre Daten wiederherzustellen, führen Sie eine Wiederherstellung von einem Snapshot aus oder führen Sie eine Point-in-Time-Wiederherstellung auf einem neuen Cluster durch. Sie müssen weiterhin Zugriff auf den ursprünglichen KMS-Schlüssel haben, um die Wiederherstellung durchzuführen. Wenn der KMS-Schlüssel gelöscht wurde, können die Daten nicht wiederhergestellt werden.

Weitere Informationen erhalten Sie unter Wiederherstellung aus einem Cluster-Snapshot und Zu einem bestimmten Zeitpunkt wiederherstellen.

> **Note**
>
> Cluster, die Teil eines globalen Clusters sind, gehen direkt in den `inaccessible-encryption-credentials` Status über, wenn der Zugriff auf den KMS-Schlüssel verloren geht, weil ein Cluster, der Teil eines globalen Clusters ist, nur gestoppt und gestartet werden kann, wenn er der einzige Cluster im globalen Cluster ist. Um einen Cluster zu löschen, der sich in diesem Status befindet, entfernen Sie zuerst jeden Cluster aus dem globalen Cluster und löschen Sie dann die Cluster einzeln.

Wenn Sie einen Cluster, der sich in diesem `inaccessible-encryption-credentials` Status befindet, nicht löschen können, weil der Löschschutz aktiviert ist, deaktivieren Sie den Löschschutz mithilfe von, AWS CLI bevor Sie den Löschvorgang erneut versuchen.

Example

Für Linux, macOS oder Unix:

```
aws docdb modify-db-cluster \
  --db-cluster-identifier example-cluster \
  --no-deletion-protection
```

Für Windows:

```
aws docdb modify-db-cluster ^
  --db-cluster-identifier example-cluster ^
  --no-deletion-protection
```

Anschließend können Sie den Cluster mithilfe des `delete-db-cluster` Befehls löschen.

Example

Für Linux, macOS oder Unix:

```
aws docdb delete-db-cluster \
  --db-cluster-identifier example-cluster \
  --skip-final-snapshot
```

Für Windows:

```
aws docdb delete-db-cluster ^
  --db-cluster-identifier example-cluster ^
  --skip-final-snapshot
```

Wenn der Cluster nicht gelöscht wird, nachdem Sie die vorherigen Befehle ausgeführt haben, wenden Sie sich an den AWS Support.

Einschränkungen für verschlüsselte Amazon DocumentDB-Cluster

Für verschlüsselte Amazon DocumentDB-Cluster gelten die folgenden Einschränkungen.

- Sie können die Verschlüsselung im Ruhezustand für einen Amazon DocumentDB-Cluster nur zum Zeitpunkt der Erstellung aktivieren oder deaktivieren, nicht nachdem der Cluster erstellt wurde. Sie können jedoch eine verschlüsselte Kopie eines unverschlüsselten Clusters erstellen, indem

Sie einen Snapshot des unverschlüsselten Clusters erstellen und dann den unverschlüsselten Snapshot als neuen Cluster wiederherstellen und dabei die Option Verschlüsselung im Ruhezustand angeben.

Weitere Informationen finden Sie unter den folgenden Themen:

- Einen manuellen Cluster-Snapshot erstellen
- Wiederherstellung aus einem Cluster-Snapshot
- Amazon DocumentDB-Cluster-Snapshots kopieren

- Amazon DocumentDB-Cluster mit aktivierter Speicherverschlüsselung können nicht geändert werden, um die Verschlüsselung zu deaktivieren.
- Alle Instances, automatisierten Backups, Snapshots und Indizes in einem Amazon DocumentDB-Cluster werden mit demselben KMS-Schlüssel verschlüsselt.

Verschlüsseln von Daten während der Übertragung

Sie können Transport Layer Security (TLS) verwenden, um die Verbindung zwischen Ihrer Anwendung und einem Amazon DocumentDB-Cluster zu verschlüsseln. Standardmäßig ist die Verschlüsselung bei der Übertragung für neu erstellte Amazon DocumentDB-Cluster aktiviert. Sie kann bei der Erstellung des Clusters oder zu einem späteren Zeitpunkt optional deaktiviert werden. Wenn die Verschlüsselung während der Übertragung aktiviert ist, sind sichere Verbindungen mit TLS erforderlich, um eine Verbindung mit dem Cluster herzustellen. Weitere Informationen zum Herstellen einer Verbindung zu Amazon DocumentDB über TLS finden Sie unter Programmgesteuertes Herstellen einer Verbindung zu Amazon DocumentDB.

TLS-Einstellungen für Amazon DocumentDB-Cluster verwalten

Die Verschlüsselung während der Übertragung für einen Amazon DocumentDB-Cluster wird über den TLS-Parameter in einer Cluster-Parametergruppe verwaltet. Sie können Ihre Amazon DocumentDB-Cluster-TLS-Einstellungen mit dem AWS-Managementkonsole oder dem AWS Command Line Interface (AWS CLI) verwalten. In den folgenden Abschnitten finden Sie weitere Informationen zum Überprüfen und Ändern Ihrer aktuellen TLS-Einstellungen.

Using the AWS-Managementkonsole

Gehen Sie wie folgt vor, um Verwaltungsaufgaben für die TLS-Verschlüsselung mithilfe der Konsole durchzuführen, z. B. Parametergruppen zu identifizieren, den TLS-Wert zu überprüfen und die erforderlichen Änderungen vorzunehmen.

> **Note**
>
> Sofern Sie beim Erstellen eines Clusters keine andere Angabe machen, wird Ihr Cluster mit der standardmäßigen Cluster-Parametergruppe erstellt. Die Parameter in der `default` Cluster-Parametergruppe können nicht geändert werden (z. B.). `tls` enabled/disabled Wenn Ihr Cluster also eine `default`-Cluster-Parametergruppe verwendet, müssen Sie den Cluster so ändern, dass er eine nicht standardmäßige Cluster-Parametergruppe verwendet. Zuerst müssen Sie möglicherweise eine benutzerdefinierte Cluster-Parametergruppe erstellen. Weitere Informationen finden Sie unter Amazon DocumentDB-Cluster-Parametergruppen erstellen.

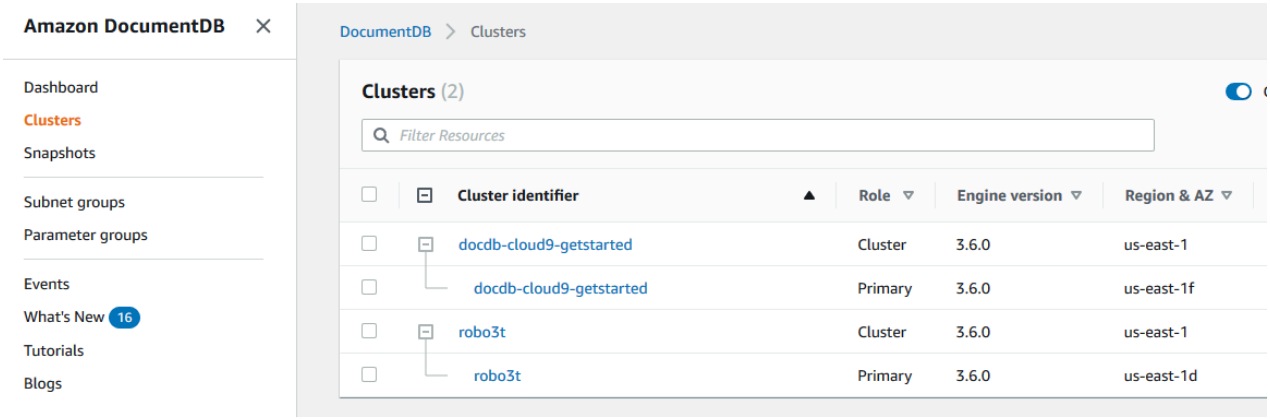
1. Bestimmen Sie, welche Cluster-Parametergruppe Ihr Cluster verwendet.

   a. Öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.

   b. Klicken Sie im Navigationsbereich auf Cluster.

   > **Tip**
   >
   > Wenn der Navigationsbereich auf der linken Seite des Bildschirms nicht angezeigt wird, wählen Sie links oben auf der Seite das Menüsymbol (≡) aus.

   c. Beachten Sie, dass im Navigationsfeld „Cluster“ in der Spalte Cluster Identifier sowohl Cluster als auch Instances angezeigt werden. Instances werden unter Clustern aufgeführt. Der folgende Screenshot dient als Referenz.



   d. Wählen Sie den Cluster aus, an dem Sie interessiert sind.

e. Wählen Sie die Registerkarte Konfiguration und scrollen Sie bis zum Ende der Cluster-Details und suchen Sie die Cluster-Parametergruppe. Der Name der Cluster-Parametergruppe.

   Wenn der Name der Cluster-Parametergruppe `default` lautet (z. B. `default.docdb3.6`), müssen Sie eine benutzerdefinierte Cluster-Parametergruppe erstellen und diese zur Parametergruppe des Clusters machen, bevor Sie fortfahren. Weitere Informationen finden Sie hier:

   1. Amazon DocumentDB-Cluster-Parametergruppen erstellen— Wenn Sie keine benutzerdefinierte Cluster-Parametergruppe haben, die Sie verwenden können, erstellen Sie eine.
   2. Ändern eines Amazon DocumentDB-Clusters— Ändern Sie Ihren Cluster so, dass er die benutzerdefinierte Cluster-Parametergruppe verwendet.

2. Bestimmen Sie den aktuellen Wert des **`tls`**-Cluster-Parameters.

   a. Öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.

   b. Wählen Sie im Navigationsbereich Parameter groups (Parametergruppen) aus.

   c. Wählen Sie aus der Liste der Cluster-Parametergruppen den Namen der von Ihnen gewünschten Cluster-Parametergruppe aus.

   d. Suchen Sie den Abschnitt Cluster-Parameter. Suchen Sie in der Liste der Cluster-Parameter die Zeile des `tls`-Cluster-Parameters. An dieser Stelle sind die folgenden vier Spalten wichtig:

      - Cluster-Parametername — Der Name der Cluster-Parameter. Für die Verwaltung von TLS benötigen Sie den `tls`-Cluster-Parameter.
      - Werte — Der aktuelle Wert jedes Cluster-Parameters.
      - Zulässige Werte — Eine Liste von Werten, die auf einen Cluster-Parameter angewendet werden können.
      - Typ anwenden — Entweder statisch oder dynamisch. Änderungen an statischen Cluster-Parametern können nur übernommen werden, wenn die Instances neu gestartet werden. Änderungen an dynamischen Cluster-Parametern können entweder sofort übernommen werden oder wenn die Instances neu gestartet werden.

3. Ändern Sie den Wert des **`tls`**-Cluster-Parameters.

Wenn der Wert für `tls` nicht der benötigte Wert ist, ändern Sie ihn für diese Cluster-Parametergruppe. Um den Wert des `tls`-Cluster-Parameters zu ändern, fahren Sie nach dem vorherigen Abschnitt mit folgenden Schritten fort.

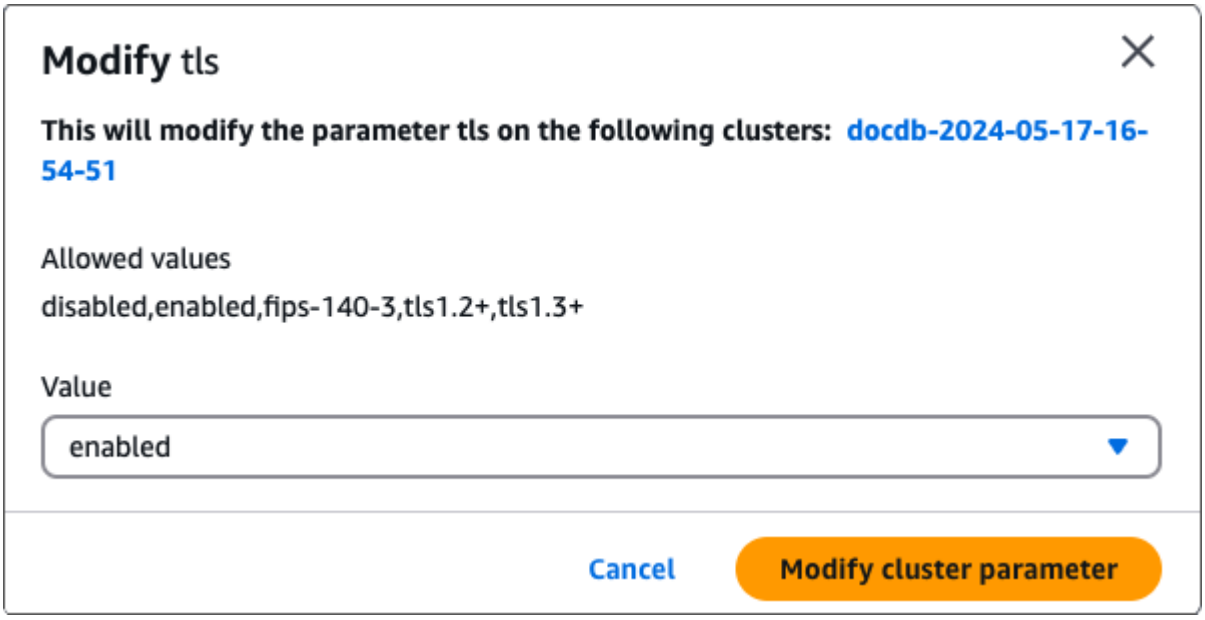
a. Wählen Sie die Schaltfläche links neben dem Namen des Cluster-Parameters (`tls`).

b. Wählen Sie Bearbeiten aus.

c. Um den Wert von zu ändern`tls`, wählen Sie im `tls` Dialogfeld Ändern in der Dropdownliste den gewünschten Wert für den Cluster-Parameter aus.

   Folgende sind gültige Werte:

   - deaktiviert — Deaktiviert TLS
   - aktiviert — Aktiviert TLS. Für Amazon DocumentDB 5.0 und früher ermöglicht dies TLS 1.0 bis 1.3, wir empfehlen jedoch TLS 1.2 oder höher. Ab der Nebenversion 5.0.1, Amazon DocumentDB 8.0 und neuer wird nur TLS 1.2 und höher auf Amazon DocumentDB 5.0 unterstützt.
   - fips-140-3 — Aktiviert TLS mit FIPS. Der Cluster akzeptiert nur sichere Verbindungen gemäß den Anforderungen der Veröffentlichung 140-3 der Federal Information Processing Standards (FIPS). Dies wird erst ab Amazon DocumentDB 5.0-Clustern (Engine-Version 3.0.3727) in diesen Regionen unterstützt: ca-central-1, us-west-2, us-east-1, us-east-2, us-gov-east-1, us-gov-west-1.
   - tls1.2+ — Aktiviert TLS Version 1.2 und höher. Dies wird erst ab Amazon DocumentDB 4.0 (Engine-Version 2.0.10980) und Amazon DocumentDB (Engine-Version 3.0.11051) unterstützt.
   - tls1.3+ — Aktiviert TLS Version 1.3 und höher. Dies wird erst ab Amazon DocumentDB 4.0 (Engine-Version 2.0.10980) und Amazon DocumentDB (Engine-Version 3.0.11051) unterstützt.



d. Wählen Sie Modify Cluster Parameter (Cluster-Parameter ändern). Die Änderung wird beim Neustart auf jede Cluster-Instance angewendet.

4. Starten Sie die Amazon DocumentDB DocumentDB-Instance neu.

   Starten Sie jede Instance des Clusters neu, sodass die Änderung für alle Instances im Cluster übernommen wird.

   a. Öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.

   b. Wählen Sie im Navigationsbereich Instances aus.

   c. Um eine Instance anzugeben, die neu gestartet werden soll, suchen Sie die Instance in der Liste der Instances und wählen Sie die Schaltfläche links neben dem Namen aus.

   d. Wählen Sie Actions (Aktionen) und dann Reboot (Neustart) aus. Bestätigen Sie, dass Sie neu starten möchten, indem Sie auf Reboot (Neustart) klicken.

Using the AWS CLI

Gehen Sie wie folgt vor, um Verwaltungsaufgaben für die TLS-Verschlüsselung mithilfe von durchzuführen AWS CLI, z. B. Parametergruppen zu identifizieren, den TLS-Wert zu überprüfen und die erforderlichen Änderungen vorzunehmen.

> **Note**
>
> Sofern Sie beim Erstellen eines Clusters keine andere Angabe machen, wird Ihr Cluster mit der standardmäßigen Cluster-Parametergruppe erstellt. Die Parameter in der `default` Cluster-Parametergruppe können nicht geändert werden (z. B. `tls` enabled/disabled). Wenn Ihr Cluster also eine `default`-Cluster-Parametergruppe verwendet, müssen Sie den Cluster so ändern, dass er eine nicht standardmäßige Cluster-Parametergruppe verwendet. Möglicherweise müssen Sie zuerst eine benutzerdefinierte Cluster-Parametergruppe erstellen. Weitere Informationen finden Sie unter Amazon DocumentDB-Cluster-Parametergruppen erstellen.

1. Bestimmen Sie, welche Cluster-Parametergruppe Ihr Cluster verwendet.

   Führen Sie den `describe-db-clusters`Befehl mit den folgenden Optionen aus:

   - `--db-cluster-identifier`
   - `--query`

   Ersetzen Sie im folgenden Beispiel jede *`user input placeholder`* durch die Informationen Ihres Clusters.

   ```
   aws docdb describe-db-clusters \
     --db-cluster-identifier mydocdbcluster \
     --query 'DBClusters[*].[DBClusterIdentifier,DBClusterParameterGroup]'
   ```

   Die Ausgabe dieses Vorgangs sieht etwa wie folgt aus (JSON-Format):

   ```
   [
       [
           "mydocdbcluster",
           "myparametergroup"
       ]
   ]
   ```

   Wenn der Name der Cluster-Parametergruppe `default` lautet (z. B. `default.docdb3.6`), benötigen Sie eine benutzerdefinierte Cluster-Parametergruppe und müssen diese zur

Parametergruppe des Clusters machen, bevor Sie fortfahren. Weitere Informationen finden Sie unter den folgenden Themen:

1. Amazon DocumentDB-Cluster-Parametergruppen erstellen— Wenn Sie keine benutzerdefinierte Cluster-Parametergruppe haben, die Sie verwenden können, erstellen Sie eine.
2. Ändern eines Amazon DocumentDB-Clusters— Ändern Sie Ihren Cluster so, dass er die benutzerdefinierte Cluster-Parametergruppe verwendet.

2. Bestimmen Sie den aktuellen Wert des **`tls`**-Cluster-Parameters.

   Um weitere Informationen zu dieser Cluster-Parametergruppe zu erhalten, führen Sie den `describe-db-cluster-parameters`Befehl mit den folgenden Optionen aus:

   - `--db-cluster-parameter-group-name`
   - `--query`

     Beschränkt die Ausgabe nur auf die Interessenfelder: `ParameterNameParameterValue`,`AllowedValues`, und`ApplyType`.

   Ersetzen Sie im folgenden Beispiel jedes *`user input placeholder`* durch die Informationen Ihres Clusters.

```
aws docdb describe-db-cluster-parameters \
  --db-cluster-parameter-group-name myparametergroup \
  --query 'Parameters[*].[ParameterName,ParameterValue,AllowedValues,ApplyType]'
```

   Die Ausgabe dieses Vorgangs sieht etwa wie folgt aus (JSON-Format):

```
[
    [
        "audit_logs",
        "disabled",
        "enabled,disabled",
        "dynamic"
    ],
    [
        "tls",
        "disabled",
        "disabled,enabled,fips-140-3,tls1.2+,tls1.3+",
```

```
        "static"
    ],
    [
        "ttl_monitor",
        "enabled",
        "disabled,enabled",
        "dynamic"
    ]
]
```

3. Ändern Sie den Wert des **`tls`**-Cluster-Parameters.

   Wenn der Wert für `tls` nicht der benötigte Wert ist, ändern Sie ihn für diese Cluster-Parametergruppe. Um den Wert des `tls` Cluster-Parameters zu ändern, führen Sie den `modify-db-cluster-parameter-group`Befehl mit den folgenden Optionen aus:

   - `--db-cluster-parameter-group-name` – Erforderlich. Der Name der zu ändernden Cluster-Parametergruppe. Dabei darf es sich nicht um eine `default.*`-Cluster-Parametergruppe handeln.
   - `--parameters` – Erforderlich. Eine Liste der zu ändernden Parameter der Cluster-Parametergruppe.
     - `ParameterName` – Erforderlich. Der Name des zu ändernden Cluster-Parameters.
     - `ParameterValue` – Erforderlich. Der neue Wert für diesen Cluster-Parameter. Muss einer der `AllowedValues` des Cluster-Parameters sein.
       - `enabled`— Der Cluster akzeptiert sichere Verbindungen mit TLS. Für Amazon DocumentDB 5.0 und früher ermöglicht dies TLS 1.0 bis 1.3, wir empfehlen jedoch TLS 1.2 oder höher. Ab der Nebenversion 5.0.1, Amazon DocumentDB 8.0 und neuer wird nur TLS 1.2 und höher auf Amazon DocumentDB 5.0 unterstützt.
       - `disabled`— Der Cluster akzeptiert keine sicheren Verbindungen mit TLS.
       - `fips-140-3`— Der Cluster akzeptiert nur sichere Verbindungen gemäß den Anforderungen der Veröffentlichung 140-3 der Federal Information Processing Standards (FIPS). Dies wird erst ab Amazon DocumentDB 5.0-Clustern (Engine-Version 3.0.3727) in diesen Regionen unterstützt: ca-central-1, us-west-2, us-east-1, us-east-2, us-gov-east-1, us-gov-west-1.
       - `tls1.2+`— Der Cluster akzeptiert sichere Verbindungen mit TLS Version 1.2 und höher. Dies wird erst ab Amazon DocumentDB 4.0 (Engine-Version 2.0.10980) und Amazon DocumentDB 5.0 (Engine-Version 3.0.11051) unterstützt.

  - `tls1.3+`— Der Cluster akzeptiert sichere Verbindungen mit TLS Version 1.3 und höher. Dies wird erst ab Amazon DocumentDB 4.0 (Engine-Version 2.0.10980) und Amazon DocumentDB 5.0 (Engine-Version 3.0.11051) unterstützt.
- `ApplyMethod`— Wann diese Änderung angewendet werden soll. Für statische Cluster-Parameter wie `tle` muss dieser Wert `pending-reboot` lauten.
  - `pending-reboot`— Die Änderung wird erst auf eine Instanz angewendet, nachdem sie neu gestartet wurde. Sie müssen jede Cluster-Instance einzeln neu starten, damit die Änderung für alle Instances des Clusters übernommen wird.

Ersetzen Sie in den folgenden Beispielen jedes Beispiel durch die *`user input placeholder`* Informationen Ihres Clusters.

Der folgende Code deaktiviert `tls` und wendet die Änderung auf jede Instanz an, wenn sie neu gestartet wird.

```
aws docdb modify-db-cluster-parameter-group \
  --db-cluster-parameter-group-name myparametergroup \
  --parameters "ParameterName=tls,ParameterValue=disabled,ApplyMethod=pending-
reboot"
```

Der folgende Code aktiviert `tls` und wendet die Änderung auf jede Instanz an, wenn sie neu gestartet wird.

```
aws docdb modify-db-cluster-parameter-group \
  --db-cluster-parameter-group-name myparametergroup \
  --parameters "ParameterName=tls,ParameterValue=enabled,ApplyMethod=pending-
reboot"
```

Der folgende Code aktiviert TLS mit `fips-140-3` und wendet die Änderung auf jede Instanz an, wenn sie neu gestartet wird.

```
aws docdb modify-db-cluster-parameter-group \
  --db-cluster-parameter-group-name myparametergroup2 \
  --parameters "ParameterName=tls,ParameterValue=fips-140-3,ApplyMethod=pending-
reboot"
```

Die Ausgabe dieses Vorgangs sieht etwa wie folgt aus (JSON-Format):

```
{
    "DBClusterParameterGroupName": "myparametergroup"
}
```

4. Starten Sie Ihre Amazon DocumentDB DocumentDB-Instance neu.

   Starten Sie jede Instance des Clusters neu, sodass die Änderung für alle Instances im Cluster übernommen wird. Um eine Amazon DocumentDB DocumentDB-Instance neu zu starten, führen Sie den `reboot-db-instance`Befehl mit der folgenden Option aus:

   - `--db-instance-identifier`

   Der folgende Code startet die Instance `mydocdbinstance` neu.

   Ersetzen Sie in den folgenden Beispielen jedes Beispiel *`user input placeholder`* durch die Informationen Ihres Clusters.

   Example

   Für Linux, macOS oder Unix:

   ```
   aws docdb reboot-db-instance \
     --db-instance-identifier mydocdbinstance
   ```

   Für Windows:

   ```
   aws docdb reboot-db-instance ^
     --db-instance-identifier mydocdbinstance
   ```

   Die Ausgabe dieses Vorgangs sieht etwa wie folgt aus (JSON-Format):

   ```
   {
       "DBInstance": {
           "AutoMinorVersionUpgrade": true,
           "PubliclyAccessible": false,
           "PreferredMaintenanceWindow": "fri:09:32-fri:10:02",
           "PendingModifiedValues": {},
           "DBInstanceStatus": "rebooting",
           "DBSubnetGroup": {
   ```

```
            "Subnets": [
                {
                    "SubnetStatus": "Active",
                    "SubnetAvailabilityZone": {
                        "Name": "us-east-1a"
                    },
                    "SubnetIdentifier": "subnet-4e26d263"
                },
                {
                    "SubnetStatus": "Active",
                    "SubnetAvailabilityZone": {
                        "Name": "us-east-1c"
                    },
                    "SubnetIdentifier": "subnet-afc329f4"
                },
                {
                    "SubnetStatus": "Active",
                    "SubnetAvailabilityZone": {
                        "Name": "us-east-1e"
                    },
                    "SubnetIdentifier": "subnet-b3806e8f"
                },
                {
                    "SubnetStatus": "Active",
                    "SubnetAvailabilityZone": {
                        "Name": "us-east-1d"
                    },
                    "SubnetIdentifier": "subnet-53ab3636"
                },
                {
                    "SubnetStatus": "Active",
                    "SubnetAvailabilityZone": {
                        "Name": "us-east-1b"
                    },
                    "SubnetIdentifier": "subnet-991cb8d0"
                },
                {
                    "SubnetStatus": "Active",
                    "SubnetAvailabilityZone": {
                        "Name": "us-east-1f"
                    },
                    "SubnetIdentifier": "subnet-29ab1025"
                }
            ],
```

```
            "SubnetGroupStatus": "Complete",
            "DBSubnetGroupDescription": "default",
            "VpcId": "vpc-91280df6",
            "DBSubnetGroupName": "default"
        },
        "PromotionTier": 2,
        "DBInstanceClass": "db.r5.4xlarge",
        "InstanceCreateTime": "2018-11-05T23:10:49.905Z",
        "PreferredBackupWindow": "00:00-00:30",
        "KmsKeyId": "arn:aws:kms:us-east-1:012345678901:key/0961325d-a50b-44d4-
b6a0-a177d5ff730b",
        "StorageEncrypted": true,
        "VpcSecurityGroups": [
            {
                "Status": "active",
                "VpcSecurityGroupId": "sg-77186e0d"
            }
        ],
        "EngineVersion": "3.6.0",
        "DbiResourceId": "db-SAMPLERESOURCEID",
        "DBInstanceIdentifier": "mydocdbinstance",
        "Engine": "docdb",
        "AvailabilityZone": "us-east-1a",
        "DBInstanceArn": "arn:aws:rds:us-east-1:012345678901:db:sample-cluster-
instance-00",
        "BackupRetentionPeriod": 1,
        "Endpoint": {
            "Address": "mydocdbinstance.corcjozrlsfc.us-
east-1.docdb.amazonaws.com",
            "Port": 27017,
            "HostedZoneId": "Z2R2ITUGPM61AM"
        },
        "DBClusterIdentifier": "mydocdbcluster"
    }
}
```


Es dauert einige Minuten, bis Ihre Instance neu gestartet wird. Sie können die Instance nur verwenden, wenn ihr Status available ist. Sie können mit der Konsole oder der AWS CLI den Status der Instance überwachen. Weitere Informationen finden Sie unter Den Status einer Amazon DocumentDB DocumentDB-Instance überwachen.

Schlüsselverwaltung

Amazon DocumentDB verwendet AWS Key Management Service (AWS KMS), um Verschlüsselungsschlüssel abzurufen und zu verwalten. AWS KMS kombiniert sichere, hochverfügbare Hardware und Software, um ein für die Cloud skaliertes Schlüsselverwaltungssystem bereitzustellen. Mithilfe AWS KMS können Sie Verschlüsselungsschlüssel erstellen und die Richtlinien definieren, die steuern, wie diese Schlüssel verwendet werden können. AWS KMS unterstützt AWS CloudTrail, sodass Sie die Verwendung von Schlüsseln überprüfen können, um sicherzustellen, dass die Schlüssel ordnungsgemäß verwendet werden.

Ihre AWS KMS Schlüssel können in Kombination mit Amazon DocumentDB und unterstützten AWS Diensten wie Amazon Simple Storage Service (Amazon S3), Amazon Relational Database Service (Amazon RDS), Amazon Elastic Block Store (Amazon EBS) und Amazon Redshift verwendet werden. Eine Liste der Dienste, die unterstützt werden AWS KMS, finden Sie unter So verwenden Sie AWS Dienste AWS KMS im Entwicklerhandbuch.AWS Key Management Service Weitere Informationen zu AWS KMS finden Sie unter Was ist AWS Key Management Service?

Identity and Access Management für Amazon DocumentDB

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 Amazon DocumentDB DocumentDB-Ressourcen zu verwenden. IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Themen

- Zielgruppe
- Authentifizierung mit Identitäten
- Verwalten des Zugriffs mit Richtlinien
- So funktioniert Amazon DocumentDB mit IAM
- Identity-based Richtlinienbeispiele für Amazon DocumentDB
- Problembehandlung Amazon DocumentDB DocumentDB-Identität und Zugriff
- Verwaltung der Zugriffsberechtigungen für Ihre Amazon DocumentDB DocumentDB-Ressourcen
- Verwendung identitätsbasierter Richtlinien (IAM-Richtlinien) für Amazon DocumentDB

- AWS verwaltete Richtlinien für Amazon DocumentDB
- Amazon DocumentDB DocumentDB-API-Berechtigungen: Referenz zu Aktionen, Ressourcen und Bedingungen

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von Ihrer Rolle ab:

- Servicebenutzer – Fordern Sie von Ihrem Administrator Berechtigungen an, wenn Sie nicht auf Features zugreifen können (siehe Problembehandlung Amazon DocumentDB DocumentDB-Identität und Zugriff).
- Serviceadministrator – Bestimmen Sie den Benutzerzugriff und stellen Sie Berechtigungsanfragen (siehe So funktioniert Amazon DocumentDB mit IAM).
- IAM-Administrator – Schreiben Sie Richtlinien zur Zugriffsverwaltung (siehe Identity-based Richtlinienbeispiele für Amazon DocumentDB).

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen sich als IAM-Benutzer authentifizieren oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich als föderierte Identität anmelden, indem Sie Anmeldeinformationen aus einer Identitätsquelle wie AWS IAM Identity Center (IAM Identity Center), Single Sign-On-Authentifizierung oder Anmeldeinformationen verwenden. Google/Facebook Weitere Informationen zum Anmelden finden Sie unter So melden Sie sich bei Ihrem AWS-Konto an im Benutzerhandbuch für AWS-Anmeldung .

AWS Bietet für den programmatischen Zugriff ein SDK und eine CLI zum kryptografischen Signieren von Anfragen. Weitere Informationen finden Sie unter AWS Signature Version 4 for API requests im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, dem sogenannten AWS-Konto Root-Benutzer, der vollständigen Zugriff auf alle AWS-Services Ressourcen hat. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Eine Liste der

Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Tasks that require root user credentials im IAM-Benutzerhandbuch.

Verbundidentität

Es hat sich bewährt, dass menschliche Benutzer für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen einen Verbund mit einem Identitätsanbieter verwenden müssen.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensverzeichnis, Ihrem Directory Service Web-Identitätsanbieter oder der AWS-Services mithilfe von Anmeldeinformationen aus einer Identitätsquelle zugreift. Verbundene Identitäten übernehmen Rollen, die temporäre Anmeldeinformationen bereitstellen.

Für die zentrale Zugriffsverwaltung empfehlen wir AWS IAM Identity Center. Weitere Informationen finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center -Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität mit bestimmten Berechtigungen für eine einzelne Person oder Anwendung. Wir empfehlen die Verwendung temporärer Anmeldeinformationen anstelle von IAM-Benutzern mit langfristigen Anmeldeinformationen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Erfordern, dass menschliche Benutzer den Verbund mit einem Identitätsanbieter verwenden müssen, um AWS mithilfe temporärer Anmeldeinformationen darauf zugreifen zu können.

Eine IAM-Gruppe spezifiziert eine Sammlung von IAM-Benutzern und erleichtert die Verwaltung von Berechtigungen für große Gruppen von Benutzern. Weitere Informationen finden Sie unter Anwendungsfälle für IAM-Benutzer im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität mit spezifischen Berechtigungen, die temporäre Anmeldeinformationen bereitstellt. Sie können eine Rolle übernehmen, indem Sie von einer Benutzer- zu einer IAM-Rolle (Konsole) wechseln AWS CLI oder einen AWS API-Vorgang aufrufen. Weitere Informationen finden Sie unter Methoden, um eine Rolle zu übernehmen im IAM-Benutzerhandbuch.

IAM-Rollen sind nützlich für den Verbundbenutzer-Zugriff, temporäre IAM-Benutzerberechtigungen, kontoübergreifenden Zugriff, serviceübergreifenden Zugriff und Anwendungen, die auf Amazon EC2 laufen. Weitere Informationen finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie definiert Berechtigungen, wenn sie mit einer Identität oder Ressource verknüpft sind. AWS bewertet diese Richtlinien, wenn ein Principal eine Anfrage stellt. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Mit Hilfe von Richtlinien legen Administratoren fest, wer Zugriff auf was hat, indem sie definieren, welches Prinzipal welche Aktionen auf welchen Ressourcenund unter welchen Bedingungendurchführen darf.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator erstellt IAM-Richtlinien und fügt sie zu Rollen hinzu, die die Benutzer dann übernehmen können. IAM-Richtlinien definieren Berechtigungen unabhängig von der Methode, die zur Ausführung der Operation verwendet wird.

Identity-based Richtlinien

Identity-based Richtlinien sind Richtliniendokumente für JSON-Berechtigungen, die Sie an eine Identität (Benutzer, Gruppe oder Rolle) anhängen. Diese Richtlinien steuern, welche Aktionen Identitäten 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.

Identity-based Richtlinien können Inline-Richtlinien (direkt in eine einzelne Identität eingebettet) oder verwaltete Richtlinien (eigenständige Richtlinien, die mehreren Identitäten zugeordnet sind) sein. Informationen dazu, wie Sie zwischen verwalteten und Inline-Richtlinien wählen, finden Sie unter Choose between managed policies and inline policies im IAM-Benutzerhandbuch.

Resource-based Richtlinien

Resource-based Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anhängen. Beispiele hierfür sind Vertrauensrichtlinien für IAM-Rollen und Amazon S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben.

Resource-based Richtlinien sind Inline-Richtlinien, die sich in diesem Dienst befinden. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Weitere Richtlinientypen

AWS unterstützt zusätzliche Richtlinientypen, mit denen die maximalen Berechtigungen festgelegt werden können, die durch gängigere Richtlinientypen gewährt werden:

- Berechtigungsgrenzen – Eine Berechtigungsgrenze legt die maximalen Berechtigungen fest, die eine identitätsbasierte Richtlinie einer IAM-Entität erteilen kann. Weitere Informationen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im -IAM-Benutzerhandbuch.
- Service-Kontrollrichtlinien (SCPs) – SCPs legen die maximalen Berechtigungen für eine Organisation oder Organisationseinheit in AWS Organizations fest. Weitere Informationen finden Sie unter Service-Kontrollrichtlinien im AWS Organizations -Benutzerhandbuch.
- Ressourcen-Kontrollrichtlinien (RCPs) – RCPs definieren die maximale Anzahl an Berechtigungen, die Ressourcen in Ihren Konten zur Verfügung stehen. Weitere Informationen finden Sie unter Ressourcen-Kontrollrichtlinien im AWS Organizations -Benutzerhandbuch.
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die als Parameter übergeben werden, wenn Sie eine temporäre Sitzung für eine Rolle oder einen Verbundbenutzer erstellen. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere Arten von Richtlinien für eine Anfrage gelten, sind die sich daraus ergebenden Berechtigungen schwieriger zu verstehen. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie unter Bewertungslogik für Richtlinien im IAM-Benutzerhandbuch.

So funktioniert Amazon DocumentDB mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf Amazon DocumentDB zu verwalten, sollten Sie sich darüber informieren, welche IAM-Funktionen mit Amazon DocumentDB verwendet werden können.

IAM-Funktionen, die Sie mit Amazon DocumentDB verwenden können

IAM-Feature	Instance-based Cluster	Elastische Cluster
Identity-based Richtlinien	Ja	Ja
Resource-based Richtlinien	Nein	Nein

IAM-Feature	Instance-based Cluster	Elastische Cluster
Richtlinienaktionen	Ja	Ja
Richtlinienressourcen	Ja	Ja
Richtlinienbedingungsschlüssel (servicespezifisch)	Ja	Ja
ACLs	Nein	Nein
ABAC (Tags in Richtlinien)	Teilweise	Ja
Temporäre Anmeldeinformationen	Ja	Ja
Prinzipalberechtigungen	Ja	Ja
Servicerollen	Ja	Ja
Service-linked Rollen	Nein	Ja

Einen allgemeinen Überblick darüber, wie Amazon DocumentDB und andere AWS Dienste mit den meisten IAM-Funktionen funktionieren, finden Sie im IAM-Benutzerhandbuch unter AWS Dienste, die mit IAM funktionieren.

Identity-based Richtlinien für Amazon DocumentDB

Unterstützt Richtlinien auf Identitätsbasis: Ja

Identity-based Richtlinien sind Richtliniendokumente für JSON-Berechtigungen, die Sie an eine Identität anhängen können, z. B. an einen IAM-Benutzer, eine Benutzergruppe oder eine Rolle. 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. Informationen zu sämtlichen Elementen, die Sie

in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Identity-based Richtlinienbeispiele für Amazon DocumentDB

Beispiele für identitätsbasierte Amazon DocumentDB DocumentDB-Richtlinien finden Sie unter. Identity-based Richtlinienbeispiele für Amazon DocumentDB

Resource-based Richtlinien innerhalb von Amazon DocumentDB

Unterstützt ressourcenbasierte Richtlinien: Nein

Resource-based Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anhängen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Weitere Informationen finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Richtlinienmaßnahmen für Amazon DocumentDB

Unterstützt Richtlinienaktionen: 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 Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Nehmen Sie Aktionen in eine Richtlinie auf, um Berechtigungen zur Ausführung des zugehörigen Vorgangs zu erteilen.

> **Note**
>
> Für bestimmte Verwaltungsfunktionen verwendet Amazon DocumentDB eine Betriebstechnologie, die mit Amazon Relational Database Service (Amazon RDS) gemeinsam genutzt wird.
> Eine Liste der RDS-Aktionen finden Sie unter Von Amazon Relational Database Service definierte Aktionen in der Service Authorization Reference.
> Informationen zu Richtlinienaktionen für elastische Amazon DocumentDB-Cluster finden Sie unter Von Amazon DocumentDB Elastic Clusters definierte Aktionen in der Service Authorization Reference.

Richtlinienaktionen in Amazon DocumentDB verwenden das folgende Präfix vor der Aktion:

```
aws
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

```
"Action": [
      "aws:action1",
      "aws:action2"
         ]
```

Beispiele für identitätsbasierte Amazon DocumentDB DocumentDB-Richtlinien finden Sie unter. Identity-based Richtlinienbeispiele für Amazon DocumentDB

Richtlinienressourcen für Amazon DocumentDB

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. Als Best Practice geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen

(ARN) an. Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

```
"Resource": "*"
```

> **Note**
>
> Für bestimmte Verwaltungsfunktionen verwendet Amazon DocumentDB eine Betriebstechnologie, die mit Amazon Relational Database Service (Amazon RDS) gemeinsam genutzt wird.
> Eine Liste der RDS-Ressourcentypen und ihrer ARNs finden Sie unter Von Amazon Relational Database Service definierte Ressourcen in der Service Authorization Reference.
> Informationen darüber, mit welchen Aktionen Sie den ARN jeder Ressource angeben können, finden Sie unter Von Amazon Relational Database Service definierte Aktionen.
> Informationen zu Ressourcentypen für Amazon DocumentDB-Eleastic-Cluster finden Sie unter Ressourcentypen, die von Amazon DocumentDB Elastic Clusters definiert wurden in der Service Authorization Reference.

Beispiele für identitätsbasierte Amazon DocumentDB DocumentDB-Richtlinien finden Sie unter. Identity-based Richtlinienbeispiele für Amazon DocumentDB

Schlüssel für Richtlinienbedingungen für Amazon DocumentDB

Unterstützt servicespezifische Richtlinienbedingungsschlüssel: 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 Element `Condition` gibt an, wann Anweisungen auf der Grundlage definierter Kriterien ausgeführt werden. 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. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

> **Note**
>
> Für bestimmte Verwaltungsfunktionen verwendet Amazon DocumentDB eine Betriebstechnologie, die mit Amazon Relational Database Service (Amazon RDS) gemeinsam genutzt wird.
> Eine Liste der RDS-Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für Amazon Relational Database Service in der Service Authorization Reference. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Von Amazon Relational Database Service definierte Aktionen.
> Bedingungsschlüssel für Amazon DocumentDB Eleastic Clusters finden Sie unter Condition Keys for Amazon DocumentDB Elastic Clusters in der Service Authorization Reference.

Beispiele für identitätsbasierte Amazon DocumentDB DocumentDB-Richtlinien finden Sie unter. Identity-based Richtlinienbeispiele für Amazon DocumentDB

ACLs in Amazon DocumentDB

Unterstützt ACLs: Nein

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

ABAC mit Amazon DocumentDB

> **Note**
>
> ABAC wird für instanzbasierte Cluster nur teilweise unterstützt, für elastische Cluster jedoch.

Attribute-based Access Control (ABAC) ist eine Autorisierungsstrategie, die Berechtigungen auf der Grundlage von Attributen definiert, die als Tags bezeichnet werden. Sie können Tags an IAM-Entitäten und AWS -Ressourcen anhängen und dann ABAC-Richtlinien entwerfen, die Operationen zulassen, wenn das Tag des Prinzipals mit dem Tag auf der Ressource übereinstimmt.

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.

Temporäre Anmeldeinformationen mit Amazon DocumentDB verwenden

Unterstützt temporäre Anmeldeinformationen: Ja

Temporäre Anmeldeinformationen ermöglichen kurzfristigen Zugriff auf AWS Ressourcen und werden automatisch erstellt, wenn Sie den Verbund verwenden oder die Rollen wechseln. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Anmeldeinformationen in IAM und AWS-Services , die mit IAM funktionieren im IAM-Benutzerhandbuch.

Cross-service Hauptberechtigungen für Amazon DocumentDB

Unterstützt Forward Access Sessions (FAS): Ja

Forward Access Sessions (FAS) verwenden die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anfrage, Anfragen an nachgelagerte Dienste AWS-Service zu stellen. Einzelheiten zu den Richtlinien für FAS-Anforderungen finden Sie unter Zugriffssitzungen weiterleiten.

Servicerollen für Amazon DocumentDB

Unterstützt Servicerollen: Ja

Eine Servicerolle ist eine IAM-Rolle, die ein Service annimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.

> **Warning**
>
> Das Ändern der Berechtigungen für eine Servicerolle kann die Funktionalität von Amazon DocumentDB beeinträchtigen. Bearbeiten Sie Servicerollen nur, wenn Amazon DocumentDB eine Anleitung dazu bereitstellt.

Service-linked Rollen für Amazon DocumentDB

> **Note**
>
> Service-linked Rollen werden für instanzbasierte Cluster nicht unterstützt, aber für elastische Cluster.

Eine serviceverknüpfte Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Dienst kann die Rolle übernehmen, eine Aktion in Ihrem Namen auszuführen. Service-linked Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Details zum Erstellen oder Verwalten von serviceverknüpften Rollen finden Sie unter AWS -Services, die mit IAM funktionieren. Suchen Sie in der Tabelle nach einem Dienst, der einen `Yes` in der Service-linked Rollenspalte enthält. Wählen Sie den Link Yes (Ja) aus, um die Dokumentation für die serviceverknüpfte Rolle für diesen Service anzuzeigen.

Identity-based Richtlinienbeispiele für Amazon DocumentDB

Standardmäßig sind Benutzer und Rollen nicht berechtigt, Amazon DocumentDB DocumentDB-Ressourcen zu erstellen oder zu ändern. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen.

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 DocumentDB definierten Aktionen und Ressourcentypen, einschließlich des Formats der ARNs für jeden Ressourcentyp, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Relational Database Service in der Service Authorization Reference.

> **Note**
>
> Für bestimmte Verwaltungsfunktionen verwendet Amazon DocumentDB eine Betriebstechnologie, die mit Amazon Relational Database Service (Amazon RDS) gemeinsam genutzt wird.
> Informationen zu Richtlinienaktionen für elastische Amazon DocumentDB-Cluster finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon DocumentDB Elastic Clusters in der Service Authorization Reference.

Themen

- Best Practices für Richtlinien
- Verwenden der Amazon DocumentDB DocumentDB-Konsole
- Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

Best Practices für Richtlinien

Identity-based Richtlinien legen fest, ob jemand Amazon DocumentDB DocumentDB-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder diese löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Wenn Sie identitätsbasierte Richtlinien erstellen oder bearbeiten, befolgen Sie diese Richtlinien 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 Von AWS verwaltete Richtlinien oder Von AWS verwaltete Richtlinien für Auftragsfunktionen 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. 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 Best Practices für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Verwenden der Amazon DocumentDB DocumentDB-Konsole

Um auf die Amazon DocumentDB DocumentDB-Konsole (mit MongoDB-Kompatibilität) zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den Amazon DocumentDB DocumentDB-Ressourcen in Ihrem AWS-Konto aufzulisten und anzuzeigen. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (Benutzer oder 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 die Benutzer ausführen möchten.

Um sicherzustellen, dass Benutzer und Rollen die Amazon DocumentDB-Konsole weiterhin verwenden können, fügen Sie den Entitäten auch die Amazon DocumentDB *ConsoleAccess* - oder *ReadOnly* AWS verwaltete Richtlinie hinzu. Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zu einem Benutzer im IAM-Benutzerhandbuch.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie beinhaltet Berechtigungen, um diese Aktion auf der Konsole oder programmgesteuert mithilfe der API oder durchzuführen. AWS CLI AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
```

```
    ]
}
```

Problembehandlung Amazon DocumentDB DocumentDB-Identität und Zugriff

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit Amazon DocumentDB und IAM auftreten können.

Themen

- Ich bin nicht berechtigt, eine Aktion in Amazon DocumentDB durchzuführen
- Ich bin nicht berechtigt, iam durchzuführen: PassRole
- Ich möchte Personen außerhalb meiner Umgebung zulassen AWS-Konto um auf meine Amazon DocumentDB DocumentDB-Ressourcen zuzugreifen

Ich bin nicht berechtigt, eine Aktion in Amazon DocumentDB durchzuführen

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht zur Durchführung einer Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie die Aktion durchführen können.

Der folgende Beispielfehler tritt auf, wenn der IAM-Benutzer `mateojackson` versucht, über die Konsole Details zu einer fiktiven *`my-example-widget`*-Ressource anzuzeigen, jedoch nicht über `aws:`*`GetWidget`*-Berechtigungen verfügt.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 aws:GetWidget on resource: my-example-widget
```

In diesem Fall muss die Richtlinie für den Benutzer `mateojackson` aktualisiert werden, damit er mit der `aws:`*`GetWidget`*-Aktion auf die *`my-example-widget`*-Ressource zugreifen kann.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich bin nicht berechtigt, iam durchzuführen: PassRole

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht berechtigt sind, die `iam:PassRole` Aktion durchzuführen, müssen Ihre Richtlinien aktualisiert werden, damit Sie eine Rolle an Amazon DocumentDB übergeben können.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Service zu übergeben, anstatt eine neue Servicerolle oder eine dienstbezogene Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in Amazon DocumentDB auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Personen außerhalb meiner Umgebung zulassen AWS-Konto um auf meine Amazon DocumentDB DocumentDB-Ressourcen zuzugreifen

Sie können eine Rolle erstellen, mit der Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation auf Ihre Ressourcen zugreifen können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Im Fall von Diensten, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (Access Control Lists, ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob Amazon DocumentDB diese Funktionen unterstützt, finden Sie unterSo funktioniert Amazon DocumentDB mit IAM.
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM-Benutzerhandbuch unter Gewähren des Zugriffs auf einen IAM-Benutzer in einem anderen AWS-Konto , den Sie besitzen.

- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Verwaltung der Zugriffsberechtigungen für Ihre Amazon DocumentDB DocumentDB-Ressourcen

Jede AWS Ressource gehört einem AWS-Konto, und die Berechtigungen zum Erstellen oder Zugreifen auf die Ressourcen werden durch Berechtigungsrichtlinien geregelt. Ein Kontoadministrator kann IAM-Identitäten (d. h. Benutzern, Gruppen und Rollen) Berechtigungsrichtlinien zuordnen, und einige Dienste (z. B. AWS Lambda) unterstützen auch das Anhängen von Berechtigungsrichtlinien an Ressourcen.

> **Note**
>
> Ein Kontoadministrator (oder Administratorbenutzer) ist ein Benutzer mit Administratorberechtigungen. Weitere Informationen finden Sie unter Bewährte Methoden für IAM im IAM-Benutzerhandbuch.

Themen

- Ressourcen und Abläufe von Amazon DocumentDB
- Grundlegendes zum Eigentum an Ressourcen
- Verwaltung des Zugriffs auf -Ressourcen
- Spezifizierung von Richtlinienelementen: Aktionen, Auswirkungen, Ressourcen und Prinzipien
- Angeben von Bedingungen in einer Richtlinie

Ressourcen und Abläufe von Amazon DocumentDB

In Amazon DocumentDB ist die primäre Ressource ein Cluster. Amazon DocumentDB unterstützt andere Ressourcen, die mit der primären Ressource verwendet werden können, wie Instances, Parametergruppen und Event-Abonnements. Diese Ressourcen werden als Unterressourcen bezeichnet.

Diese Ressourcen und Unterressourcen sind eindeutigen Amazon-Ressourcennamen (ARNs) zugeordnet (siehe Tabelle unten).

Ressourcentyp	ARN-Format
Cluster	`arn:aws:rds:` *`region`*`:`*`account-id`* `:cluster:` *`db-cluster-name`*
Cluster-Parametergruppe	`arn:aws:rds:` *`region`*`:`*`account-id`* `:cluster-pg:` *`cluster-parameter-group-name`*
Cluster-Snapshot	`arn:aws:rds:` *`region`*`:`*`account-id`* `:cluster-snapshot:` *`cluster-snapshot-name`*
Instance	`arn:aws:rds:` *`region`*`:`*`account-id`* `:db:`*`db-instance-name`*
Sicherheitsgruppe	`arn:aws:rds:` *`region`*`:`*`account-id`* `:secgrp:`*`security-group-name`*
Subnetzgruppe	`arn:aws:rds:` *`region`*`:`*`account-id`* `:subgrp:`*`subnet-group-name`*

Amazon DocumentDB bietet eine Reihe von Vorgängen für die Arbeit mit den Amazon DocumentDB DocumentDB-Ressourcen. Eine Liste der verfügbaren Operationen finden Sie unter Aktionen.

Grundlegendes zum Eigentum an Ressourcen

Ein Ressourcenbesitzer ist derjenige AWS-Konto , der eine Ressource erstellt hat. Das heißt, der Ressourcenbesitzer ist derjenige AWS-Konto der Hauptentität (das Root-Konto, ein IAM-Benutzer oder eine IAM-Rolle), die die Anfrage authentifiziert, mit der die Ressource erstellt wird. Die Funktionsweise wird anhand der folgenden Beispiele deutlich:

- Wenn Sie Ihre Root-Kontoanmeldedaten verwenden, AWS-Konto um eine Amazon DocumentDB DocumentDB-Ressource, z. B. eine Instance, zu erstellen, sind Sie AWS-Konto der Eigentümer der Amazon DocumentDB DocumentDB-Ressource.
- Wenn Sie in Ihrem einen IAM-Benutzer erstellen AWS-Konto und diesem Benutzer Berechtigungen zum Erstellen von Amazon DocumentDB DocumentDB-Ressourcen erteilen, kann der Benutzer Amazon DocumentDB DocumentDB-Ressourcen erstellen. Ihr, dem der Benutzer angehört AWS-Konto, besitzt jedoch die Amazon DocumentDB DocumentDB-Ressourcen.
- Wenn Sie in Ihrem Unternehmen eine IAM-Rolle AWS-Konto mit den Berechtigungen zum Erstellen von Amazon DocumentDB DocumentDB-Ressourcen erstellen, kann jeder, der diese Rolle übernehmen kann, Amazon DocumentDB DocumentDB-Ressourcen erstellen. Ihre AWS-Konto, zu der die Rolle gehört, besitzt die Amazon DocumentDB DocumentDB-Ressourcen.

Verwaltung des Zugriffs auf -Ressourcen

Eine Berechtigungsrichtlinie beschreibt, wer Zugriff auf welche Objekte hat. Im folgenden Abschnitt werden die verfügbaren Optionen zum Erstellen von Berechtigungsrichtlinien erläutert.

> **Note**
>
> In diesem Abschnitt wird die Verwendung von IAM im Kontext von Amazon DocumentDB beschrieben. Er enthält keine detaillierten Informationen über den IAM-Service. Eine umfassende IAM-Dokumentation finden Sie unter Was ist IAM? im IAM-Benutzerhandbuch. Für Informationen über die Syntax und Beschreibungen von AWS -IAM-Richtlinien lesen Sie die IAM-Richtlinienreferenz im IAM-Benutzerhandbuch.

An eine IAM-Identität angefügte Richtlinien werden als identitätsbasierte Richtlinien (IAM-Richtlinien) bezeichnet. An Ressourcen angehängte Richtlinien werden als ressourcenbasierte Richtlinien bezeichnet. Amazon DocumentDB unterstützt nur identitätsbasierte Richtlinien (IAM-Richtlinien).

Themen

- Identity-based Richtlinien (IAM-Richtlinien)
- Resource-based Richtlinien

Identity-based Richtlinien (IAM-Richtlinien)

Richtlinien können IAM-Identitäten angefügt werden. Sie können z. B. Folgendes tun:

- Hängen Sie eine Berechtigungsrichtlinie an einen Benutzer oder eine Gruppe in Ihrem Konto an — Ein Kontoadministrator kann eine Berechtigungsrichtlinie verwenden, die einem bestimmten Benutzer zugeordnet ist, um diesem Benutzer Berechtigungen zum Erstellen einer Amazon DocumentDB DocumentDB-Ressource, z. B. einer Instance, zu erteilen.
- Einer Rolle eine Berechtigungsrichtlinie zuweisen (kontoübergreifende Berechtigungen gewähren) – Sie können einer IAM-Rolle eine identitätsbasierte Berechtigungsrichtlinie zuweisen, um kontoübergreifende Berechtigungen zu erteilen. Ein Administrator kann beispielsweise wie folgt eine Rolle erstellen, um einem anderen AWS-Konto oder einem AWS Dienst kontoübergreifende Berechtigungen zu gewähren:
  1. Der Administrator von Konto A erstellt eine IAM-Rolle und fügt ihr eine Berechtigungsrichtlinie an, die Berechtigungen für Ressourcen in Konto A erteilt.
  2. Der Administrator von Konto A weist der Rolle eine Vertrauensrichtlinie zu, die Konto B als den Prinzipal identifiziert, der die Rolle übernehmen kann.
  3. Der Administrator von Konto B kann dann die Berechtigungen zur Übernahme der Rolle an alle Benutzer in Konto B delegieren. Auf diese Weise können die Benutzer in Konto B Ressourcen in Konto A erstellen oder darauf zugreifen. Der Principal in der Vertrauensrichtlinie kann auch ein AWS Dienstprinzipal sein, wenn Sie einem AWS Dienst die Erlaubnis erteilen möchten, diese Rolle zu übernehmen.

  Weitere Informationen zum Delegieren von Berechtigungen mithilfe von IAM finden Sie unter Zugriffsverwaltung im IAM-Benutzerhandbuch.

Im Folgenden finden Sie ein Beispiel für eine Richtlinie, die es dem Benutzer mit der ID ermöglicht, Instanzen für Sie `123456789012` AWS-Konto zu erstellen. Die neue Instance muss eine Optionsgruppe und eine Parametergruppe verwenden, die mit `default` beginnt, und sie muss die Subnetzgruppe `default` verwenden.

JSON

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

```
                "rds:CreateDBInstance"
            ],
            "Resource": [
                "arn:aws:rds:*:123456789012:db:test*",
                "arn:aws:rds:*:123456789012:pg:cluster-pg:default*",
                "arn:aws:rds:*:123456789012:subgrp:default"
            ]
        }
    ]
}
```

Weitere Informationen zur Verwendung identitätsbasierter Richtlinien mit Amazon DocumentDB finden Sie unter. Verwendung identitätsbasierter Richtlinien (IAM-Richtlinien) für Amazon DocumentDB Weitere Informationen zu Benutzern, Gruppen, Rollen und Berechtigungen finden Sie im Thema Identitäten (Benutzer, Gruppen und Rollen) im IAM-Benutzerhandbuch.

Resource-based Richtlinien

Andere Dienste, wie Amazon Simple Storage Service (Amazon S3), unterstützen ebenfalls ressourcenbasierte Berechtigungsrichtlinien. Beispielsweise können Sie einem Amazon S3-Bucket eine Richtlinie zuweisen, um die Zugriffsberechtigungen für diesen Bucket zu verwalten. Amazon DocumentDB unterstützt keine ressourcenbasierten Richtlinien.

Spezifizierung von Richtlinienelementen: Aktionen, Auswirkungen, Ressourcen und Prinzipien

Für jede Amazon DocumentDB DocumentDB-Ressource (siheRessourcen und Abläufe von Amazon DocumentDB) definiert der Service eine Reihe von API-Vorgängen. Weitere Informationen finden Sie unter Aktionen. Um Berechtigungen für diese API-Operationen zu gewähren, definiert Amazon DocumentDB eine Reihe von Aktionen, die Sie in einer Richtlinie angeben können. Für das Durchführen einer API-Operation können Berechtigungen für mehrere Aktionen erforderlich sein.

Grundlegende Richtlinienelemente:

- Ressource – In einer Richtlinie wird der Amazon-Ressourcenname (ARN) zur Identifizierung der Ressource verwendet, für die die Richtlinie gilt.
- Aktion – Mit Aktionsschlüsselwörtern geben Sie die Ressourcenoperationen an, die Sie zulassen oder verweigern möchten. Die `rds:DescribeDBInstances`-Berechtigung erteilt dem Benutzer zum Beispiel Berechtigungen zum Ausführen der `DescribeDBInstances`-Operation.

- Auswirkung – Die von Ihnen festgelegte Auswirkung, wenn der Benutzer die jeweilige Aktion anfordert – entweder „allow“ (Zugriffserlaubnis) oder „deny“ (Zugriffsverweigerung). Wenn Sie den Zugriff auf eine Ressource nicht ausdrücklich gestatten ("Allow"), wird er automatisch verweigert. Sie können den Zugriff auf eine Ressource auch explizit verweigern. So können Sie sicherstellen, dass Benutzer nicht darauf zugreifen können, auch wenn der Zugriff durch eine andere Richtlinie gestattet wird.
- Prinzipal – In identitätsbasierten Richtlinien (IAM-Richtlinien) ist der Benutzer, dem die Richtlinie zugewiesen ist, automatisch der Prinzipal. In ressourcenbasierten Richtlinien müssen Sie den Benutzer, das Konto, den Service oder die sonstige Entität angeben, die die Berechtigungen erhalten soll (gilt nur für ressourcenbasierte Richtlinien). Amazon DocumentDB unterstützt keine ressourcenbasierten Richtlinien.

Weitere Informationen zur Syntax und zu Beschreibungen von IAM-Richtlinien finden Sie in der AWS -IAM-Richtlinienreferenz im IAM-Benutzerhandbuch.

Eine Tabelle mit allen Amazon DocumentDB DocumentDB-API-Aktionen und den Ressourcen, für die sie gelten, finden Sie unterAmazon DocumentDB DocumentDB-API-Berechtigungen: Referenz zu Aktionen, Ressourcen und Bedingungen.

Angeben von Bedingungen in einer Richtlinie

Beim Erteilen von Berechtigungen können Sie mithilfe der IAM-Richtliniensyntax die Bedingungen angeben, unter denen die Richtlinie wirksam werden soll. Beispielsweise kann festgelegt werden, dass eine Richtlinie erst ab einem bestimmten Datum gilt. Weitere Informationen zum Angeben von Bedingungen in einer Richtliniensyntax finden Sie im Thema Bedingung im IAM Benutzerhandbuch.

Bedingungen werden mithilfe vordefinierter Bedingungsschlüssel formuliert. Amazon DocumentDB hat keine dienstspezifischen Kontextschlüssel, die in einer IAM-Richtlinie verwendet werden können. Eine Liste der globalen Kontextschlüssel für Bedingungen, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen im IAM-Benutzerhandbuch.

Verwendung identitätsbasierter Richtlinien (IAM-Richtlinien) für Amazon DocumentDB

> **Important**
>
> Für bestimmte Verwaltungsfunktionen verwendet Amazon DocumentDB Betriebstechnologie, die mit Amazon RDS gemeinsam genutzt wird. Amazon DocumentDB DocumentDB-Konsolen- und API-Aufrufe werden als Aufrufe der Amazon RDS-API protokolliert. AWS CLI Wir empfehlen Ihnen, zunächst die einführenden Themen zu lesen, in denen die grundlegenden Konzepte und Optionen erläutert werden, die Ihnen zur Verwaltung des Zugriffs auf Ihre Amazon DocumentDB DocumentDB-Ressourcen zur Verfügung stehen. Weitere Informationen finden Sie unter Verwaltung der Zugriffsberechtigungen für Ihre Amazon DocumentDB DocumentDB-Ressourcen.

In diesem Thema finden Sie Beispiele für identitätsbasierte Richtlinien, in denen ein Kontoadministrator den IAM-Identitäten (Benutzer, Gruppen und Rollen) Berechtigungsrichtlinien anfügen kann.

Im Folgenden finden Sie ein Beispiel für eine IAM-Richtlinie.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCreateDBInstanceOnly",
            "Effect": "Allow",
            "Action": [
                "rds:CreateDBInstance"
            ],
            "Resource": [
                "arn:aws:rds:*:123456789012:db:test*",
                "arn:aws:rds:*:123456789012:pg:cluster-pg:default*",
                "arn:aws:rds:*:123456789012:subgrp:default"
            ]
        }
```

```
    ]
}
```

Die Richtlinie ist ein einzelnes Statement, das die folgenden Berechtigungen für den IAM-Benutzer bestimmt:

- Die Richtlinie ermöglicht es dem IAM-Benutzer, eine Instanz mithilfe der Aktion CreateDBInstance zu erstellen (dies gilt auch für den Vorgang AWS CLI create-db-instance und die). AWS-Managementkonsole
- Das Element `Resource` gibt an, dass der Benutzer auf oder mit Ressourcen Aktionen ausführen kann. Sie geben Ressourcen über einen Amazon-Ressourcennamen (ARN) an. Dieser ARN enthält den Namen des Dienstes, zu dem die Ressource gehört (`rds`), den AWS-Region (*gibt in diesem Beispiel eine beliebige Region an), die Benutzerkontonummer (123456789012ist in diesem Beispiel die Benutzer-ID) und den Ressourcentyp.

  Das `Resource`-Element im Beispiel gibt für den Benutzer die folgenden richtlinienbezogenen Einschränkungen für die Ressourcen an:

  - Die Instance-Kennung für die neue Instance muss mit `test` beginnen (zum Beispiel `testCustomerData1`, `test-region2-data`).
  - Die Parametergruppe für die neue Instance muss mit `default` beginnen.
  - Die Subnetzgruppe für die neue Instance muss mit `default` beginnen.

Das Element `Principal` ist in der Richtlinie nicht angegeben, da in identitätsbasierten Richtlinien die Angabe des Prinzipals als Empfänger der Berechtigung nicht erforderlich ist. Wenn Sie einem Benutzer eine Richtlinie zuweisen, ist der Benutzer automatisch der Prinzipal. Wird die Berechtigungsrichtlinie einer IAM-Rolle angefügt, erhält der in der Vertrauensrichtlinie der Rolle angegebene Prinzipal die Berechtigungen.

Eine Tabelle mit allen Amazon DocumentDB DocumentDB-API-Vorgängen und den Ressourcen, für die sie gelten, finden Sie unterAmazon DocumentDB DocumentDB-API-Berechtigungen: Referenz zu Aktionen, Ressourcen und Bedingungen.

Für die Verwendung der Amazon DocumentDB DocumentDB-Konsole sind Berechtigungen erforderlich

Damit ein Benutzer mit der Amazon DocumentDB DocumentDB-Konsole arbeiten kann, muss er über Mindestberechtigungen verfügen. Diese Berechtigungen ermöglichen es dem Benutzer, die Amazon DocumentDB DocumentDB-Ressourcen für ihn zu beschreiben AWS-Konto und andere verwandte Informationen bereitzustellen, einschließlich Amazon EC2-Sicherheits- und Netzwerkinformationen.

Wenn Sie eine IAM-Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Benutzer mit dieser IAM-Richtlinie. Um sicherzustellen, dass diese Benutzer die Amazon DocumentDB DocumentDB-Konsole weiterhin verwenden können, fügen Sie dem Benutzer auch die `AmazonDocDBConsoleFullAccess` verwaltete Richtlinie beiAWS verwaltete Richtlinien für Amazon DocumentDB, wie unter beschrieben.

Sie müssen Benutzern, die nur die Amazon DocumentDB-API AWS CLI oder die Amazon DocumentDB DocumentDB-API aufrufen, keine Mindestberechtigungen für die Konsole gewähren.

Beispiele für vom Kunden verwaltete Richtlinien

In diesem Abschnitt finden Sie Beispielbenutzerrichtlinien, die Berechtigungen für verschiedene Amazon DocumentDB DocumentDB-Aktionen gewähren. Diese Richtlinien funktionieren, wenn Sie Amazon DocumentDB DocumentDB-API-Aktionen, AWS SDKs oder die verwenden. AWS CLI Bei Verwendung der Konsole müssen Sie zusätzliche konsolenspezifische Berechtigungen erteilen, die im Abschnitt Für die Verwendung der Amazon DocumentDB DocumentDB-Konsole sind Berechtigungen erforderlich erläutert werden.

Für bestimmte Verwaltungsfunktionen verwendet Amazon DocumentDB Betriebstechnologie, die mit Amazon Relational Database Service (Amazon RDS) und Amazon Neptune gemeinsam genutzt wird.

> **Note**
>
> Alle Beispiele verwenden die Region USA Ost (Nord-Virginia) (`us-east-1`) und enthalten fiktive Konto-IDs.

Beispiele

- Beispiel 1: Erlauben Sie einem Benutzer, eine beliebige Beschreibungsaktion für eine beliebige Amazon DocumentDB DocumentDB-Ressource auszuführen
- Beispiel 2: Verhindern, dass ein Benutzer eine Instance löscht

- Beispiel 3: Verhindern, dass ein Benutzer einen Cluster erstellt, sofern die Speicherverschlüsselung nicht aktiviert ist

Beispiel 1: Erlauben Sie einem Benutzer, eine beliebige Beschreibungsaktion für eine beliebige Amazon DocumentDB DocumentDB-Ressource auszuführen

Die folgende Berechtigungsrichtlinie gewährt Berechtigungen für einen Benutzer, alle Aktionen auszuführen, die mit beginne `Describe`. Diese Aktionen zeigen Informationen über eine Amazon DocumentDB DocumentDB-Ressource, z. B. eine Instance. Das Platzhalterzeichen (*) im `Resource` Element gibt an, dass die Aktionen für alle Amazon DocumentDB DocumentDB-Ressourcen zulässig sind, die dem Konto gehören.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"AllowRDSDescribe",
         "Effect":"Allow",
         "Action":"rds:Describe*",
         "Resource":"*"
      }
   ]
}
```

Beispiel 2: Verhindern, dass ein Benutzer eine Instance löscht

Die folgenden Berechtigungsrichtlinien erteilen Berechtigungen, um einen Benutzer davon abzuhalten, eine bestimmte Instance zu löschen. Beispielsweise möchten Sie jedem Benutzer, der kein Administrator ist, verbieten, Ihre Produktions-Instances zu löschen.

JSON

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

```
            "Sid":"DenyDelete1",
            "Effect":"Deny",
            "Action":"rds:DeleteDBInstance",
            "Resource":"arn:aws:rds:us-east-1:123456789012:db:my-db-instance"
         }
      ]
}
```

Beispiel 3: Verhindern, dass ein Benutzer einen Cluster erstellt, sofern die Speicherverschlüsselung nicht aktiviert ist

Die folgende Berechtigungsrichtlinie verweigert einem Benutzer die Erlaubnis, einen Amazon DocumentDB-Cluster zu erstellen, sofern die Speicherverschlüsselung nicht aktiviert ist.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Sid": "PreventUnencryptedDocumentDB",
         "Effect": "Deny",
         "Action": "RDS:CreateDBCluster",
         "Condition": {
         "Bool": {
         "rds:StorageEncrypted": "false"
      },
         "StringEquals": {
         "rds:DatabaseEngine": "docdb"
         }
      },
      "Resource": "*"
      }
   ]
}
```

AWS verwaltete Richtlinien für Amazon DocumentDB

Um Benutzern, Gruppen und Rollen Berechtigungen hinzuzufügen, ist es einfacher, AWS verwaltete Richtlinien zu verwenden, als Richtlinien selbst zu schreiben. Es erfordert Zeit und Fachwissen,

um von Kunden verwaltete IAM-Richtlinien zu erstellen, die Ihrem Team nur die benötigten Berechtigungen bieten. Um schnell loszulegen, können Sie unsere AWS verwalteten Richtlinien verwenden. Diese Richtlinien decken allgemeine Anwendungsfälle ab und sind in Ihrem AWS Konto verfügbar. Weitere Informationen zu AWS verwalteten Richtlinien finden Sie unter AWS Verwaltete Richtlinien im AWS Identity and Access Management-Benutzerhandbuch.

AWS Dienste verwalten und aktualisieren AWS verwaltete Richtlinien. Sie können die Berechtigungen in AWS verwalteten Richtlinien nicht ändern. Dienste fügen einer AWS verwalteten Richtlinie gelegentlich zusätzliche Berechtigungen hinzu, um neue Funktionen zu unterstützen. Diese Art von Update betrifft alle Identitäten (Benutzer, Gruppen und Rollen), an welche die Richtlinie angehängt ist. Es ist sehr wahrscheinlich, dass Dienste eine AWS verwaltete Richtlinie aktualisieren, wenn eine neue Funktion eingeführt wird oder wenn neue Operationen verfügbar werden. Dienste entfernen keine Berechtigungen aus einer AWS verwalteten Richtlinie, sodass durch Richtlinienaktualisierungen Ihre bestehenden Berechtigungen nicht beeinträchtigt werden.

AWS Unterstützt außerdem verwaltete Richtlinien für Jobfunktionen, die sich über mehrere Dienste erstrecken. Die `ViewOnlyAccess` AWS verwaltete Richtlinie bietet beispielsweise Lesezugriff auf viele AWS Dienste und Ressourcen. Wenn ein Dienst eine neue Funktion startet, werden nur Leseberechtigungen für neue Operationen und Ressourcen AWS hinzugefügt. Eine Liste und eine Beschreibung der Richtlinien für Jobfunktionen finden Sie unter AWS Verwaltete Richtlinien für Jobfunktionen im AWS Identity and Access Management-Benutzerhandbuch.

Die folgenden AWS verwalteten Richtlinien, die Sie Benutzern in Ihrem Konto zuordnen können, sind spezifisch für Amazon DocumentDB:

- AmazonDocDBFullAccess— Gewährt vollen Zugriff auf alle Amazon DocumentDB DocumentDB-Ressourcen für das AWS Root-Konto.
- AmazonDocDBReadOnlyAccess— Gewährt schreibgeschützten Zugriff auf alle Amazon DocumentDB DocumentDB-Ressourcen für das Root-Konto. AWS
- AmazonDocDBConsoleFullAccess— Gewährt vollen Zugriff auf die Verwaltung von Amazon DocumentDB- und Amazon DocumentDB Elastic Cluster-Ressourcen mithilfe von. AWS-Managementkonsole
- AmazonDocDBElasticReadOnlyAccess— Gewährt schreibgeschützten Zugriff auf alle Amazon DocumentDB Elastic Cluster-Ressourcen für das Root-Konto. AWS
- AmazonDocDBElasticFullAccess— Gewährt vollen Zugriff auf alle Amazon DocumentDB Elastic Cluster-Ressourcen für das AWS Root-Konto.

AmazonDocDBFullAccess

Diese Richtlinie gewährt Administratorberechtigungen, die einem Principal vollen Zugriff auf alle Amazon DocumentDB DocumentDB-Aktionen gewähren. Die Berechtigungen in dieser Richtlinie sind wie folgt gruppiert:

- Die Amazon DocumentDB DocumentDB-Berechtigungen ermöglichen alle Amazon DocumentDB DocumentDB-Aktionen.
- Einige der Amazon-EC2-Berechtigungen in dieser Richtlinie sind erforderlich, um die übergebenen Ressourcen in einer API-Anfrage zu validieren. Dadurch wird sichergestellt, dass Amazon DocumentDB die Ressourcen erfolgreich mit einem Cluster nutzen kann. Die übrigen Amazon EC2 EC2-Berechtigungen in dieser Richtlinie ermöglichen es Amazon DocumentDB, AWS Ressourcen zu erstellen, die erforderlich sind, damit Sie eine Verbindung zu Ihren Clustern herstellen können.
- Die Amazon DocumentDB DocumentDB-Berechtigungen werden bei API-Aufrufen verwendet, um die übergebenen Ressourcen in einer Anfrage zu validieren. Sie sind erforderlich, damit Amazon DocumentDB den übergebenen Schlüssel mit dem Amazon DocumentDB-Cluster verwenden kann.
- Die CloudWatch Protokolle sind erforderlich, damit Amazon DocumentDB sicherstellen kann, dass die Protokollzustellungsziele erreichbar sind und dass sie für die Verwendung von Broker-Protokollen gültig sind.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "rds:AddRoleToDBCluster",
                "rds:AddSourceIdentifierToSubscription",
                "rds:AddTagsToResource",
                "rds:ApplyPendingMaintenanceAction",
                "rds:CopyDBClusterParameterGroup",
                "rds:CopyDBClusterSnapshot",
                "rds:CopyDBParameterGroup",
                "rds:CreateDBCluster",
                "rds:CreateDBClusterParameterGroup",
                "rds:CreateDBClusterSnapshot",
                "rds:CreateDBInstance",
```

```
                "rds:CreateDBParameterGroup",
                "rds:CreateDBSubnetGroup",
                "rds:CreateEventSubscription",
                "rds:DeleteDBCluster",
                "rds:DeleteDBClusterParameterGroup",
                "rds:DeleteDBClusterSnapshot",
                "rds:DeleteDBInstance",
                "rds:DeleteDBParameterGroup",
                "rds:DeleteDBSubnetGroup",
                "rds:DeleteEventSubscription",
                "rds:DescribeAccountAttributes",
                "rds:DescribeCertificates",
                "rds:DescribeDBClusterParameterGroups",
                "rds:DescribeDBClusterParameters",
                "rds:DescribeDBClusterSnapshotAttributes",
                "rds:DescribeDBClusterSnapshots",
                "rds:DescribeDBClusters",
                "rds:DescribeDBEngineVersions",
                "rds:DescribeDBInstances",
                "rds:DescribeDBLogFiles",
                "rds:DescribeDBParameterGroups",
                "rds:DescribeDBParameters",
                "rds:DescribeDBSecurityGroups",
                "rds:DescribeDBSubnetGroups",
                "rds:DescribeEngineDefaultClusterParameters",
                "rds:DescribeEngineDefaultParameters",
                "rds:DescribeEventCategories",
                "rds:DescribeEventSubscriptions",
                "rds:DescribeEvents",
                "rds:DescribeOptionGroups",
                "rds:DescribeOrderableDBInstanceOptions",
                "rds:DescribePendingMaintenanceActions",
                "rds:DescribeValidDBInstanceModifications",
                "rds:DownloadDBLogFilePortion",
                "rds:FailoverDBCluster",
                "rds:ListTagsForResource",
                "rds:ModifyDBCluster",
                "rds:ModifyDBClusterParameterGroup",
                "rds:ModifyDBClusterSnapshotAttribute",
                "rds:ModifyDBInstance",
                "rds:ModifyDBParameterGroup",
                "rds:ModifyDBSubnetGroup",
                "rds:ModifyEventSubscription",
                "rds:PromoteReadReplicaDBCluster",
```

```
                "rds:RebootDBInstance",
                "rds:RemoveRoleFromDBCluster",
                "rds:RemoveSourceIdentifierFromSubscription",
                "rds:RemoveTagsFromResource",
                "rds:ResetDBClusterParameterGroup",
                "rds:ResetDBParameterGroup",
                "rds:RestoreDBClusterFromSnapshot",
                "rds:RestoreDBClusterToPointInTime"
            ],
            "Effect": "Allow",
            "Resource": [
                "*"
            ]
        },
        {
            "Action": [
                "cloudwatch:GetMetricStatistics",
                "cloudwatch:ListMetrics",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcAttribute",
                "ec2:DescribeVpcs",
                "kms:ListAliases",
                "kms:ListKeyPolicies",
                "kms:ListKeys",
                "kms:ListRetirableGrants",
                "logs:DescribeLogStreams",
                "logs:GetLogEvents",
                "sns:ListSubscriptions",
                "sns:ListTopics",
                "sns:Publish"
            ],
            "Effect": "Allow",
            "Resource": [
                "*"
            ]
        },
        {
            "Action": "iam:CreateServiceLinkedRole",
            "Effect": "Allow",
            "Resource": "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
```

```
            "Condition": {
                "StringLike": {
                    "iam:AWS ServiceName": "rds.amazonaws.com"
                }
            }
        }
    ]
}
```

AmazonDocDBReadOnlyAccess

Diese Richtlinie gewährt nur Leseberechtigungen, die es Benutzern ermöglichen, Informationen in Amazon DocumentDB einzusehen. Principals, denen diese Richtlinie beigefügt ist, können weder Aktualisierungen vornehmen oder bestehende Ressourcen löschen, noch können sie neue Amazon DocumentDB DocumentDB-Ressourcen erstellen. Prinzipale mit diesen Berechtigungen können beispielsweise die Liste der Cluster und Konfigurationen, die mit ihrem Konto verknüpft sind, einsehen, aber nicht die Konfiguration oder Einstellungen von Clustern ändern. Die Berechtigungen in dieser Richtlinie sind wie folgt gruppiert:

- Mit Amazon DocumentDB DocumentDB-Berechtigungen können Sie Amazon DocumentDB DocumentDB-Ressourcen auflisten, beschreiben und Informationen über sie abrufen.
- Amazon EC2 EC2-Berechtigungen werden verwendet, um die Amazon VPC, Subnetze, Sicherheitsgruppen und ENIs zu beschreiben, die einem Cluster zugeordnet sind.
- Eine Amazon DocumentDB DocumentDB-Berechtigung wird verwendet, um den Schlüssel zu beschreiben, der dem Cluster zugeordnet ist.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "rds:DescribeAccountAttributes",
                "rds:DescribeCertificates",
                "rds:DescribeDBClusterParameterGroups",
                "rds:DescribeDBClusterParameters",
                "rds:DescribeDBClusterSnapshotAttributes",
```

```
                "rds:DescribeDBClusterSnapshots",
                "rds:DescribeDBClusters",
                "rds:DescribeDBEngineVersions",
                "rds:DescribeDBInstances",
                "rds:DescribeDBLogFiles",
                "rds:DescribeDBParameterGroups",
                "rds:DescribeDBParameters",
                "rds:DescribeDBSubnetGroups",
                "rds:DescribeEventCategories",
                "rds:DescribeEventSubscriptions",
                "rds:DescribeEvents",
                "rds:DescribeOrderableDBInstanceOptions",
                "rds:DescribePendingMaintenanceActions",
                "rds:DownloadDBLogFilePortion",
                "rds:ListTagsForResource"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "cloudwatch:GetMetricStatistics",
                "cloudwatch:ListMetrics"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcAttribute",
                "ec2:DescribeVpcs"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "kms:ListKeys",
                "kms:ListRetirableGrants",
```

```
                "kms:ListAliases",
                "kms:ListKeyPolicies"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "logs:DescribeLogStreams",
                "logs:GetLogEvents"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:logs:*:*:log-group:/aws/rds/*:log-stream:*",
                "arn:aws:logs:*:*:log-group:/aws/docdb/*:log-stream:*"
            ]
        }
    ]
}
```

AmazonDocDBConsoleFullAccess

Gewährt vollen Zugriff auf die Verwaltung von Amazon DocumentDB DocumentDB-Ressourcen unter Verwendung der folgenden AWS-Managementkonsole Optionen:

- Die Amazon DocumentDB-Berechtigungen, um alle Amazon DocumentDB- und Amazon DocumentDB-Cluster-Aktionen zuzulassen.
- Einige der Amazon-EC2-Berechtigungen in dieser Richtlinie sind erforderlich, um die übergebenen Ressourcen in einer API-Anfrage zu validieren. Dadurch soll sichergestellt werden, dass Amazon DocumentDB die Ressourcen erfolgreich für die Bereitstellung und Wartung des Clusters nutzen kann. Die restlichen Amazon EC2 EC2-Berechtigungen in dieser Richtlinie ermöglichen es Amazon DocumentDB, AWS Ressourcen zu erstellen, die benötigt werden, damit Sie eine Verbindung zu Ihren Clustern wie vpcEndpoint herstellen können.
- AWS KMS Berechtigungen werden bei API-Aufrufen verwendet, um die übergebenen Ressourcen in einer Anfrage AWS KMS zu validieren. Sie sind erforderlich, damit Amazon DocumentDB den übergebenen Schlüssel verwenden kann, um die Daten im Ruhezustand mit dem Amazon DocumentDB Elastic Cluster zu verschlüsseln und zu entschlüsseln.

- Die CloudWatch Protokolle sind erforderlich, damit Amazon DocumentDB sicherstellen kann, dass die Ziele für die Protokollzustellung erreichbar sind und dass sie für die Verwendung von Prüfungs- und Profilerstellungsprotokollen gültig sind.
- Secrets Manager Manager-Berechtigungen sind erforderlich, um das angegebene Geheimnis zu validieren und es zu verwenden, um den Admin-Benutzer für Amazon DocumentDB Elastic Clusters einzurichten.
- Amazon RDS-Berechtigungen sind für Amazon DocumentDB-Cluster-Management-Aktionen erforderlich. Für bestimmte Verwaltungsfunktionen verwendet Amazon DocumentDB Betriebstechnologie, die mit Amazon RDS gemeinsam genutzt wird.
- Mit SNS-Berechtigungen können Principals Abonnements und Themen für Amazon Simple Notification Service (Amazon SNS) abonnieren und Amazon SNS-Nachrichten veröffentlichen.
- Für die Erstellung der serviceverknüpften Rollen, die für die Veröffentlichung von Metriken und Protokollen erforderlich sind, sind IAM-Berechtigungen erforderlich.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DocdbSids",
            "Effect": "Allow",
            "Action": [
                "docdb-elastic:CreateCluster",
                "docdb-elastic:UpdateCluster",
                "docdb-elastic:GetCluster",
                "docdb-elastic:DeleteCluster",
                "docdb-elastic:ListClusters",
                "docdb-elastic:CreateClusterSnapshot",
                "docdb-elastic:GetClusterSnapshot",
                "docdb-elastic:DeleteClusterSnapshot",
                "docdb-elastic:ListClusterSnapshots",
                "docdb-elastic:RestoreClusterFromSnapshot",
                "docdb-elastic:TagResource",
                "docdb-elastic:UntagResource",
                "docdb-elastic:ListTagsForResource",
                "docdb-elastic:CopyClusterSnapshot",
                "docdb-elastic:StartCluster",
                "docdb-elastic:StopCluster",
```

```
                "docdb-elastic:GetPendingMaintenanceAction",
                "docdb-elastic:ListPendingMaintenanceActions",
                "docdb-elastic:ApplyPendingMaintenanceAction",
                "rds:AddRoleToDBCluster",
                "rds:AddSourceIdentifierToSubscription",
                "rds:AddTagsToResource",
                "rds:ApplyPendingMaintenanceAction",
                "rds:CopyDBClusterParameterGroup",
                "rds:CopyDBClusterSnapshot",
                "rds:CopyDBParameterGroup",
                "rds:CreateDBCluster",
                "rds:CreateDBClusterParameterGroup",
                "rds:CreateDBClusterSnapshot",
                "rds:CreateDBInstance",
                "rds:CreateDBParameterGroup",
                "rds:CreateDBSubnetGroup",
                "rds:CreateEventSubscription",
                "rds:CreateGlobalCluster",
                "rds:DeleteDBCluster",
                "rds:DeleteDBClusterParameterGroup",
                "rds:DeleteDBClusterSnapshot",
                "rds:DeleteDBInstance",
                "rds:DeleteDBParameterGroup",
                "rds:DeleteDBSubnetGroup",
                "rds:DeleteEventSubscription",
                "rds:DeleteGlobalCluster",
                "rds:DescribeAccountAttributes",
                "rds:DescribeCertificates",
                "rds:DescribeDBClusterParameterGroups",
                "rds:DescribeDBClusterParameters",
                "rds:DescribeDBClusterSnapshotAttributes",
                "rds:DescribeDBClusterSnapshots",
                "rds:DescribeDBClusters",
                "rds:DescribeDBEngineVersions",
                "rds:DescribeDBInstances",
                "rds:DescribeDBLogFiles",
                "rds:DescribeDBParameterGroups",
                "rds:DescribeDBParameters",
                "rds:DescribeDBSecurityGroups",
                "rds:DescribeDBSubnetGroups",
                "rds:DescribeEngineDefaultClusterParameters",
                "rds:DescribeEngineDefaultParameters",
                "rds:DescribeEventCategories",
                "rds:DescribeEventSubscriptions",
```

```
                "rds:DescribeEvents",
                "rds:DescribeGlobalClusters",
                "rds:DescribeOptionGroups",
                "rds:DescribeOrderableDBInstanceOptions",
                "rds:DescribePendingMaintenanceActions",
                "rds:DescribeValidDBInstanceModifications",
                "rds:DownloadDBLogFilePortion",
                "rds:FailoverDBCluster",
                "rds:ListTagsForResource",
                "rds:ModifyDBCluster",
                "rds:ModifyDBClusterParameterGroup",
                "rds:ModifyDBClusterSnapshotAttribute",
                "rds:ModifyDBInstance",
                "rds:ModifyDBParameterGroup",
                "rds:ModifyDBSubnetGroup",
                "rds:ModifyEventSubscription",
                "rds:ModifyGlobalCluster",
                "rds:PromoteReadReplicaDBCluster",
                "rds:RebootDBInstance",
                "rds:RemoveFromGlobalCluster",
                "rds:RemoveRoleFromDBCluster",
                "rds:RemoveSourceIdentifierFromSubscription",
                "rds:RemoveTagsFromResource",
                "rds:ResetDBClusterParameterGroup",
                "rds:ResetDBParameterGroup",
                "rds:RestoreDBClusterFromSnapshot",
                "rds:RestoreDBClusterToPointInTime"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "DependencySids",
            "Effect": "Allow",
            "Action": [
                "iam:GetRole",
                "cloudwatch:GetMetricData",
                "cloudwatch:GetMetricStatistics",
                "cloudwatch:ListMetrics",
                "ec2:AllocateAddress",
                "ec2:AssignIpv6Addresses",
                "ec2:AssignPrivateIpAddresses",
                "ec2:AssociateAddress",
```

```
                "ec2:AssociateRouteTable",
                "ec2:AssociateSubnetCidrBlock",
                "ec2:AssociateVpcCidrBlock",
                "ec2:AttachInternetGateway",
                "ec2:AttachNetworkInterface",
                "ec2:CreateCustomerGateway",
                "ec2:CreateDefaultSubnet",
                "ec2:CreateDefaultVpc",
                "ec2:CreateInternetGateway",
                "ec2:CreateNatGateway",
                "ec2:CreateNetworkInterface",
                "ec2:CreateRoute",
                "ec2:CreateRouteTable",
                "ec2:CreateSecurityGroup",
                "ec2:CreateSubnet",
                "ec2:CreateVpc",
                "ec2:CreateVpcEndpoint",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAddresses",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeCustomerGateways",
                "ec2:DescribeInstances",
                "ec2:DescribeNatGateways",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribePrefixLists",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroupReferences",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcAttribute",
                "ec2:DescribeVpcEndpoints",
                "ec2:DescribeVpcs",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:ModifySubnetAttribute",
                "ec2:ModifyVpcAttribute",
                "ec2:ModifyVpcEndpoint",
                "kms:DescribeKey",
                "kms:ListAliases",
                "kms:ListKeyPolicies",
                "kms:ListKeys",
                "kms:ListRetirableGrants",
                "logs:DescribeLogStreams",
                "logs:GetLogEvents",
                "sns:ListSubscriptions",
```

```
                "sns:ListTopics",
                "sns:Publish"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "DocdbSLRSid",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "rds.amazonaws.com"
                }
            }
        },
        {
            "Sid": "DocdbElasticSLRSid",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/docdb-
elastic.amazonaws.com/AWSServiceRoleForDocDB-Elastic",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "docdb-elastic.amazonaws.com"
                }
            }
        }
    ]
}
```

AmazonDocDBElasticReadOnlyAccess

Diese Richtlinie gewährt nur Leseberechtigungen, mit denen Benutzer Elastic Cluster-Informationen in Amazon DocumentDB anzeigen können. Principals, denen diese Richtlinie beigefügt ist, können weder Aktualisierungen vornehmen oder bestehende Ressourcen löschen, noch können sie neue Amazon DocumentDB DocumentDB-Ressourcen erstellen. Prinzipale mit diesen Berechtigungen können beispielsweise die Liste der Cluster und Konfigurationen, die mit ihrem Konto verknüpft sind,

einsehen, aber nicht die Konfiguration oder Einstellungen von Clustern ändern. Die Berechtigungen in dieser Richtlinie sind wie folgt gruppiert:

- Mit Amazon DocumentDB-Elastic-Cluster-Berechtigungen können Sie Elastic Cluster-Ressourcen von Amazon DocumentDB auflisten, beschreiben und Informationen über sie abrufen.
- CloudWatch Berechtigungen werden verwendet, um Servicemetriken zu überprüfen.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "docdb-elastic:ListClusters",
            "docdb-elastic:GetCluster",
            "docdb-elastic:ListClusterSnapshots",
            "docdb-elastic:GetClusterSnapshot",
            "docdb-elastic:ListTagsForResource"
         ],
         "Resource": "*"
      },
      {
         "Effect": "Allow",
         "Action": [
            "cloudwatch:GetMetricData",
            "cloudwatch:ListMetrics",
            "cloudwatch:GetMetricStatistics"
         ],
         "Resource": "*"
      }
   ]
}
```

AmazonDocDBElasticFullAccess

Diese Richtlinie gewährt Administratorberechtigungen, die einem Principal vollen Zugriff auf alle Amazon DocumentDB-Aktionen für Amazon DocumentDB Elastic Cluster gewähren.

Diese Richtlinie verwendet AWS Tags (https://docs.aws.amazon.com/tag-editor/latest/userguide/tagging.html) innerhalb bestimmter Bedingungen, um den Zugriff auf Ressourcen einzuschränken. Wenn Sie ein Geheimnis verwenden, muss es mit einem Tag-Schlüssel `DocDBElasticFullAccess` und einem Tag-Wert gekennzeichnet werden. Wenn Sie einen vom Kunden verwalteten Schlüssel verwenden, muss dieser mit einem Tag-Schlüssel `DocDBElasticFullAccess` und einem Tag-Wert versehen werden.

Die Berechtigungen in dieser Richtlinie sind wie folgt gruppiert:

- Elastische Cluster-Berechtigungen von Amazon DocumentDB ermöglichen alle Amazon DocumentDB DocumentDB-Aktionen.
- Einige der Amazon-EC2-Berechtigungen in dieser Richtlinie sind erforderlich, um die übergebenen Ressourcen in einer API-Anfrage zu validieren. Dadurch soll sichergestellt werden, dass Amazon DocumentDB die Ressourcen erfolgreich für die Bereitstellung und Wartung des Clusters nutzen kann. Die restlichen Amazon EC2 EC2-Berechtigungen in dieser Richtlinie ermöglichen es Amazon DocumentDB, AWS Ressourcen zu erstellen, die erforderlich sind, damit Sie sich mit Ihren Clustern wie einem VPC-Endpunkt verbinden können.
- AWS KMS Für Amazon DocumentDB sind Berechtigungen erforderlich, um den übergebenen Schlüssel zum Verschlüsseln und Entschlüsseln der ruhenden Daten innerhalb des Amazon DocumentDB Elastic Clusters verwenden zu können.

  > **Note**
  >
  > Der vom Kunden verwaltete Schlüssel muss über ein Tag mit Schlüssel `DocDBElasticFullAccess` und Tag-Wert verfügen.

- SecretsManager Berechtigungen sind erforderlich, um das angegebene Geheimnis zu validieren und es zu verwenden, um den Admin-Benutzer für Amazon DocumentDB Elastic Clusters einzurichten.

  > **Note**
  >
  > Das verwendete Geheimnis muss ein Tag mit einem Schlüssel `DocDBElasticFullAccess` und einem Tag-Wert haben.

- Für die Erstellung der serviceverknüpften Rollen, die für die Veröffentlichung von Metriken und Protokollen erforderlich sind, sind IAM-Berechtigungen erforderlich.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DocdbElasticSid",
            "Effect": "Allow",
            "Action": [
                "docdb-elastic:CreateCluster",
                "docdb-elastic:UpdateCluster",
                "docdb-elastic:GetCluster",
                "docdb-elastic:DeleteCluster",
                "docdb-elastic:ListClusters",
                "docdb-elastic:CreateClusterSnapshot",
                "docdb-elastic:GetClusterSnapshot",
                "docdb-elastic:DeleteClusterSnapshot",
                "docdb-elastic:ListClusterSnapshots",
                "docdb-elastic:RestoreClusterFromSnapshot",
                "docdb-elastic:TagResource",
                "docdb-elastic:UntagResource",
                "docdb-elastic:ListTagsForResource",
                "docdb-elastic:CopyClusterSnapshot",
                "docdb-elastic:StartCluster",
                "docdb-elastic:StopCluster",
                "docdb-elastic:GetPendingMaintenanceAction",
                "docdb-elastic:ListPendingMaintenanceActions",
                "docdb-elastic:ApplyPendingMaintenanceAction"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "EC2Sid",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateVpcEndpoint",
                "ec2:DescribeVpcEndpoints",
                "ec2:DeleteVpcEndpoints",
                "ec2:ModifyVpcEndpoint",
                "ec2:DescribeVpcAttribute",
                "ec2:DescribeSecurityGroups",
```

```
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeAvailabilityZones",
                "secretsmanager:ListSecrets"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:CalledViaFirst": "docdb-elastic.amazonaws.com"
                }
            }
        },
        {
            "Sid": "KMSSid",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:DescribeKey",
                "kms:GenerateDataKey"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "kms:ViaService": [
                        "docdb-elastic.*.amazonaws.com"
                    ],
                    "aws:ResourceTag/DocDBElasticFullAccess": "*"
                }
            }
        },
        {
            "Sid": "KMSGrantSid",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/DocDBElasticFullAccess": "*",
                    "kms:ViaService": [
                        "docdb-elastic.*.amazonaws.com"
```

```
                    ]
                },
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        },
        {
            "Sid": "SecretManagerSid",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:ListSecretVersionIds",
                "secretsmanager:DescribeSecret",
                "secretsmanager:GetSecretValue",
                "secretsmanager:GetResourcePolicy"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "secretsmanager:ResourceTag/DocDBElasticFullAccess": "*"
                },
                "StringEquals": {
                    "aws:CalledViaFirst": "docdb-elastic.amazonaws.com"
                }
            }
        },
        {
            "Sid": "CloudwatchSid",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:GetMetricData",
                "cloudwatch:ListMetrics",
                "cloudwatch:GetMetricStatistics"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "SLRSid",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/docdb-
elastic.amazonaws.com/AWSServiceRoleForDocDB-Elastic",
```

```
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "docdb-elastic.amazonaws.com"
                }
            }
        }
    ]
}
```

AmazonDocDB-ElasticServiceRolePolicy

Sie können nichts an Ihre AWS Identity and Access Management Entitäten `AmazonDocDBElasticServiceRolePolicy` anhängen. Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es Amazon DocumentDB ermöglicht, Aktionen in Ihrem Namen durchzuführen. Weitere Informationen finden Sie unter Service-linked Rollen in elastischen Clustern.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": [
                        "AWS/DocDB-Elastic"
                    ]
                }
            }
        }
    ]
}
```

Amazon DocumentDB DocumentDB-Updates für AWS Verwaltete Richtlinien

Änderungen	Beschreibung	Date
AmazonDocDBElasticFullAccess, AmazonDocDBConsoleFullAccess - Ändern	Die Richtlinien wurden aktualisiert, um ausstehende Wartungsaktionen hinzuzufügen.	2/11/2025
AmazonDocDBElasticFullAccess, AmazonDocDBConsoleFullAccess - Veränderung	Die Richtlinien wurden aktualisiert, um start/stop Cluster-Snapshot-Aktionen hinzuzufügen und Cluster-Snapshots zu kopieren.	2/21/2024
AmazonDocDBElasticReadOnlyAccess, AmazonDocDBElasticFullAccess - Veränderung	Richtlinien wurden aktualisiert, um `cloudwatch:GetMetricData` Aktionen hinzuzufügen.	6/21/2023
AmazonDocDBElasticReadOnlyAccess – Neue Richtlinie	Neue verwaltete Richtlinie für elastische Amazon DocumentDB-Cluster.	6/8/2023
AmazonDocDBElasticFullAccess – Neue Richtlinie	Neue verwaltete Richtlinie für elastische Amazon DocumentDB-Cluster.	6/5/2023
AmazonDocDB-ElasticServiceRolePolicy – Neue Richtlinie	Amazon DocumentDB erstellt eine neue AWS ServiceRoleForDocDB-Elastic serviceverknüpfte Rolle für elastische Amazon DocumentDB-Cluster.	11/30/2022
AmazonDocDBConsoleFullAccess- Veränderung	Die Richtlinie wurde aktualisiert, um globale und elastische Cluster-Berechtigungen	11/30/2022

Änderungen	Beschreibung	Date
	für Amazon DocumentDB hinzuzufügen.	
AmazonDocDBConsoleFullAccess,AmazonDocDBFullAccess, AmazonDocDBReadOnlyAccess - Neue Richtlinie	Start des Dienstes.	1/19/2017

Amazon DocumentDB DocumentDB-API-Berechtigungen: Referenz zu Aktionen, Ressourcen und Bedingungen

Verwenden Sie die folgenden Abschnitte als Referenz, wenn Sie Berechtigungsrichtlinien einrichten Verwendung identitätsbasierter Richtlinien (IAM-Richtlinien) für Amazon DocumentDB und schreiben, die Sie einer IAM-Identität zuordnen können (identitätsbasierte Richtlinien).

Im Folgenden werden alle Amazon DocumentDB DocumentDB-API-Operationen aufgeführt. In der Liste sind die entsprechenden Aktionen enthalten, für die Sie Berechtigungen zur Ausführung der Aktion erteilen können, die AWS Ressource, für die Sie die Berechtigungen erteilen können, und Bedingungsschlüssel, die Sie für eine detaillierte Zugriffskontrolle angeben 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. Weitere Informationen über Bedingungen finden Sie unter Angeben von Bedingungen in einer Richtlinie.

Sie können in Ihren Amazon DocumentDB DocumentDB-Richtlinien AWS-weite Bedingungsschlüssel verwenden, um Bedingungen auszudrücken. Eine vollständige Liste der AWS-weiten Schlüssel finden Sie unter Verfügbare Schlüssel im IAM-Benutzerhandbuch.

Sie können IAM-Richtlinien mit dem IAM-Richtliniensimulator testen. Es stellt automatisch eine Liste der Ressourcen und Parameter bereit, die für jede AWS Aktion erforderlich sind, einschließlich Amazon DocumentDB DocumentDB-Aktionen. Der IAM-Richtliniensimulator bestimmt die Berechtigungen, die für jede der von Ihnen angegebenen Aktionen erforderlich sind. Informationen zum IAM-Richtliniensimulator finden Sie unter Testen von IAM-Richtlinien mit dem IAM-Richtliniensimulator im IAM-Benutzerhandbuch.

> **Note**
>
> Um eine Aktion anzugeben, verwenden Sie das Präfix `rds:` gefolgt vom Namen der API-Operation (z. B. `rds:CreateDBInstance`).

Im Folgenden werden Amazon RDS-API-Operationen und die zugehörigen Aktionen, Ressourcen und Bedingungsschlüssel aufgeführt.

Themen

- Amazon DocumentDB DocumentDB-Aktionen, die Berechtigungen auf Ressourcenebene unterstützen
- Amazon DocumentDB DocumentDB-Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen

Amazon DocumentDB DocumentDB-Aktionen, die Berechtigungen auf Ressourcenebene unterstützen

Resource-level Berechtigungen bieten die Möglichkeit, die Ressourcen anzugeben, auf denen Benutzer Aktionen ausführen dürfen. Amazon DocumentDB unterstützt teilweise Berechtigungen auf Ressourcenebene. Das bedeutet, dass Sie für bestimmte Amazon DocumentDB DocumentDB-Aktionen steuern können, wann Benutzer diese Aktionen verwenden dürfen, basierend auf Bedingungen, die erfüllt sein müssen, oder auf bestimmten Ressourcen, die Benutzer verwenden dürfen. Beispielsweise können Sie Benutzern die Berechtigung erteilen, nur bestimmte Instances zu ändern.

Im Folgenden werden Amazon DocumentDB DocumentDB-API-Operationen und die zugehörigen Aktionen, Ressourcen und Bedingungsschlüssel aufgeführt.

> **Note**
>
> Für bestimmte Verwaltungsfunktionen verwendet Amazon DocumentDB Betriebstechnologie, die mit Amazon RDS gemeinsam genutzt wird. Weitere Amazon DocumentDB DocumentDB-Aktionen und -Berechtigungen finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon RDS in der Service Authorization Reference.

Amazon DocumentDB DocumentDB-API-Operationen und -Aktionen	Ressourcen	Bedingungsschlüssel
AddTagsToResource rds:AddTagsToResource	Instance arn:aws:rds: *region*:*account-id* :db:*db-instance-name*	rds:db-tag
	Subnetzgruppe arn:aws:rds: *region*:*account-id* :subgrp:*subnet-group-name*	rds:subgrp-tag
ApplyPendingMaintenanceAction rds:ApplyPendingMaintenanceAction	Instance arn:aws:rds: *region*:*account-id* :db:*db-instance-name*	rds:db-tag
CopyDBClusterSnapshot rds:CopyDBClusterSnapshot	Cluster-Snapshot arn:aws:rds: *region*:*account-id* :cluster-snapshot: *cluster-snapshot-name*	rds:cluster-snapshot-tag
CreateDBCluster rds:CreateDBCluster	Cluster arn:aws:rds: *region*:*account-id* :cluster: *db-cluster-name*	rds:cluster-tag
	Cluster-Parametergruppe	rds:cluster-pg-tag

Amazon DocumentDB DocumentDB-API-Operationen und -Aktionen	Ressourcen	Bedingungsschlüssel
	arn:aws:rds: *region*:*account-id* :cluster-pg: *cluster-parameter-group-name*	
	Subnetzgruppe arn:aws:rds: *region*:*account-id* :subgrp:*subnet-group-name*	rds:subgrp-tag
CreateDBClusterParameterGroup rds:CreateDBClusterParameterGroup	Cluster-Parametergruppe arn:aws:rds: *region*:*account-id* :cluster-pg: *cluster-parameter-group-name*	rds:cluster-pg-tag
CreateDBClusterSnapshot rds:CreateDBClusterSnapshot	Cluster arn:aws:rds: *region*:*account-id* :cluster: *db-cluster-name*	rds:cluster-tag
	Cluster-Snapshot arn:aws:rds: *region*:*account-id* :cluster-snapshot: *cluster-snapshot-name*	rds:cluster-snapshot-tag
CreateDBInstance rds:CreateDBInstance	Instance arn:aws:rds: *region*:*account-id* :db:*db-instance-name*	rds:DatabaseClass rds:db-tag

Amazon DocumentDB DocumentDB-API-Operationen und -Aktionen	Ressourcen	Bedingungsschlüssel
	Cluster arn:aws:rds: *region*:*account-id* :cluster: *db-cluster-name*	rds:cluster-tag
CreateDBSubnetGroup rds:CreateDBSubnetGroup	Subnetzgruppe arn:aws:rds: *region*:*account-id* :subgrp:*subnet-group-name*	rds:subgrp-tag
DeleteDBInstance rds:DeleteDBInstance	Instance arn:aws:rds: *region*:*account-id* :db:*db-instance-name*	rds:db-tag
DeleteDBSubnetGroup rds:DeleteDBSubnetGroup	Subnetzgruppe arn:aws:rds: *region*:*account-id* :subgrp:*subnet-group-name*	rds:subgrp-tag
DescribeDBClusterParameterGroups rds:DescribeDBClusterParameterGroups	Cluster-Parametergruppe arn:aws:rds: *region*:*account-id* :cluster-pg: *cluster-parameter-group-name*	rds:cluster-pg-tag

Amazon DocumentDB DocumentDB-API-Operationen und -Aktionen	Ressourcen	Bedingungsschlüssel
DescribeDBClusterParameters rds:DescribeDBClusterParameters	Cluster-Parametergruppe arn:aws:rds: *region*:*account-id* :cluster-pg: *cluster-parameter-group-name*	rds:cluster-pg-tag
DescribeDBClusters rds:DescribeDBClusters	Cluster arn:aws:rds: *region*:*account-id* :cluster: *db-cluster-instance-name*	rds:cluster-tag
DescribeDBClusterSnapshotAttributes rds:DescribeDBClusterSnapshotAttributes	Cluster-Snapshot arn:aws:rds: *region*:*account-id* :cluster-snapshot: *cluster-snapshot-name*	rds:cluster-snapshot-tag
DescribeDBSubnetGroups rds:DescribeDBSubnetGroups	Subnetzgruppe arn:aws:rds: *region*:*account-id* :subgrp:*subnet-group-name*	rds:subgrp-tag
DescribePendingMaintenanceActions rds:DescribePendingMaintenanceActions	Instance arn:aws:rds: *region*:*account-id* :db:*db-instance-name*	rds:DatabaseClass rds:db-tag

Amazon DocumentDB DocumentDB-API-Operationen und -Aktionen	Ressourcen	Bedingungsschlüssel
FailoverDBCluster rds:FailoverDBCluster	Cluster arn:aws:rds: *region*:*account-id* :cluster: *db-cluster-instance-name*	rds:cluster-tag
ListTagsForResource rds:ListTagsForResource	Instance arn:aws:rds: *region*:*account-id* :db:*db-instance-name*	rds:db-tag
	Subnetzgruppe arn:aws:rds: *region*:*account-id* :subgrp:*subnet-group-name*	rds:subgrp-tag
ModifyDBCluster rds:ModifyDBCluster	Cluster arn:aws:rds: *region*:*account-id* :cluster: *db-cluster-name*	rds:cluster-tag
	Cluster-Parametergruppe arn:aws:rds: *region*:*account-id* :cluster-pg: *cluster-parameter-group-name*	rds:cluster-pg-tag
ModifyDBClusterParameterGroup rds:ModifyDBClusterParameterGroup	Cluster-Parametergruppe arn:aws:rds: *region*:*account-id* :cluster-pg: *cluster-parameter-group-name*	rds:cluster-pg-tag

Amazon DocumentDB DocumentDB-API-Operationen und -Aktionen	Ressourcen	Bedingungsschlüssel
ModifyDBClusterSnapshotAttribute rds:ModifyDBClusterSnapshotAttribute	Cluster-Snapshot arn:aws:rds: *region*:*account-id* :cluster-snapshot: *cluster-snapshot-name*	rds:cluster-snapshot-tag
ModifyDBInstance rds:ModifyDBInstance	Instance arn:aws:rds: *region*:*account-id* :db:*db-instance-name*	rds:DatabaseClass rds:db-tag
RebootDBInstance rds:RebootDBInstance	Instance arn:aws:rds: *region*:*account-id* :db:*db-instance-name*	rds:db-tag
RemoveTagsFromResource rds:RemoveTagsFromResource	Instance arn:aws:rds: *region*:*account-id* :db:*db-instance-name*	rds:db-tag
	Subnetzgruppe arn:aws:rds: *region*:*account-id* :subgrp:*subnet-group-name*	rds:subgrp-tag
ResetDBClusterParameterGroup rds:ResetDBClusterParameterGroup	Cluster-Parametergruppe arn:aws:rds: *region*:*account-id* :cluster-pg: *cluster-parameter-group-name*	rds:cluster-pg-tag

Amazon DocumentDB DocumentDB-API-Operationen und -Aktionen	Ressourcen	Bedingungsschlüssel
RestoreDBClusterFromSnapshot rds:RestoreDBClusterFromSnapshot	Cluster arn:aws:rds: *region*:*account-id* :cluster: *db-cluster-instance-name*	rds:cluster-tag
	Cluster-Snapshot arn:aws:rds: *region*:*account-id* :cluster-snapshot: *cluster-snapshot-name*	rds:cluster-snapshot-tag
RestoreDBClusterToPointInTime rds:RestoreDBClusterToPointInTime	Cluster arn:aws:rds: *region*:*account-id* :cluster: *db-cluster-instance-name*	rds:cluster-tag
	Subnetzgruppe arn:aws:rds: *region*:*account-id* :subgrp:*subnet-group-name*	rds:subgrp-tag

Amazon DocumentDB DocumentDB-Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen

Sie können alle Amazon DocumentDB DocumentDB-Aktionen in einer IAM-Richtlinie verwenden, um Benutzern entweder die Erlaubnis zu erteilen oder zu verweigern, diese Aktion zu verwenden. Allerdings unterstützen nicht alle Amazon DocumentDB DocumentDB-Aktionen Berechtigungen auf Ressourcenebene, mit denen Sie angeben können, für welche Ressourcen eine Aktion ausgeführt werden kann. Die folgenden Amazon DocumentDB DocumentDB-API-Aktionen unterstützen derzeit keine Berechtigungen auf Ressourcenebene. Um diese Aktionen in einer IAM-Richtlinie verwenden

zu können, müssen Sie den Benutzern daher die Erlaubnis erteilen, alle Ressourcen für die Aktion zu verwenden, indem Sie einen * Platzhalter für das Element in Ihrer Anweisung verwenden. `Resource`

- `rds:DescribeDBClusterSnapshots`
- `rds:DescribeDBInstances`

Cross-service verwirrter Stellvertreter, 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. Im AWS Fall eines dienststellenübergreifenden Identitätswechsels kann es zu einem Problem mit verwirrten Stellvertretern kommen. Cross-service Ein Identitätswechsel kann auftreten, wenn ein Dienst (der anrufende Dienst) einen anderen Dienst (den angerufenen Dienst) aufruft. 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 DocumentDB einem anderen Service für die Ressource gewährt. 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 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 Kontextbedingungsschlüssel `aws:SourceArn` mit Platzhalterzeichen (*) für die unbekannten Teile des ARN. Beispiel, `arn:aws:`*`servicename`*`:*:`*`123456789012`*`:*`.

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.

Der Wert von `aws:SourceArn` muss Cluster sein.

Das folgende Beispiel zeigt, wie Sie die Kontextschlüssel `aws:SourceArn` und die `aws:SourceAccount` globalen Bedingungsschlüssel in Amazon DocumentDB verwenden können, um das Problem des verwirrten Stellvertreters zu verhindern.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "servicename.amazonaws.com"
    },
    "Action": "servicename:ActionName",
    "Resource": [
      "arn:aws:servicename:::ResourceName/*"
    ],
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:servicename:*:123456789012:*"
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
  }
}
```

Authentifizierung mit IAM-Identität

Amazon DocumentDB-Benutzer und -Anwendungen können IAM-Benutzer und -Rollen verwenden, um sich in einem Amazon DocumentDB-Cluster zu authentifizieren. Die Amazon DocumentDB IAM-Authentifizierung ist eine kennwortlose Authentifizierungsmethode. Außerdem senden Client-Anwendungen die Kennwortgeheimnisse nicht an den Amazon DocumentDB-Cluster, wenn sie roles/users IAM verwenden. Stattdessen werden Client-Verbindungen AWS STS mithilfe temporärer Sicherheitstoken authentifiziert. Non-administrative Benutzer und Anwendungen können jetzt dieselbe IAM-Identität (ARN) verwenden, wenn sie eine Verbindung zu verschiedenen Amazon DocumentDB-Clustern und anderen AWS Diensten herstellen.

Sie können sich auch dafür entscheiden, sowohl die kennwortbasierte als auch die IAM-Authentifizierung zu verwenden, um Benutzer und Anwendungen in einem Amazon DocumentDB-

Cluster zu authentifizieren. Die IAM-Authentifizierung ist nur in der instanzbasierten Amazon DocumentDB-Cluster-Version 5.0 verfügbar. Die IAM-Authentifizierung mit IAM-IdentitätsARNs wird für den Amazon DocumentDB DocumentDB-Hauptbenutzer nicht unterstützt.

> **Note**
>
> Der Hauptbenutzer kann nur mithilfe einer vorhandenen passwortbasierten Authentifizierung authentifiziert werden.

Topics

- Erste Schritte mit der Authentifizierung mithilfe von IAM-Benutzern und -Rollen
- Konfigurieren AWS Berechnungstypen für die Authentifizierung bei Amazon DocumentDB mithilfe AWS IAM
- Überwachung von IAM-Authentifizierungsanfragen
- Verwenden der IAM-Authentifizierung
- Treiber, die IAM unterstützen
- Häufig gestellte Fragen zur IAM-Identitätsauthentifizierung

Erste Schritte mit der Authentifizierung mithilfe von IAM-Benutzern und -Rollen

Amazon DocumentDB DocumentDB-Benutzer und -Rollen mit IAM-Identitäten werden in einer Datenbank erstellt und verwaltet. `$external`

Einen Benutzer erstellen

Connect als Hauptbenutzer her und erstellen Sie dann einen IAM-Benutzer und eine IAM-Rolle:

```
use $external;
db.createUser(
    {
        user: "arn:aws:iam::123456789123:user/iamuser",
        mechanisms: ["MONGODB-AWS"],
        roles: [ { role: "readWrite", db: "readWriteDB" } ]
    }
```

```
);
```

Alternativ können Sie einen Amazon DocumentDB DocumentDB-Benutzer mithilfe einer IAM-Rolle hinzufügen:

```
use $external;
db.createUser(
    {
        user: "arn:aws:iam::123456789123:role/iamrole",
        mechanisms: ["MONGODB-AWS"],
        roles: [ { role: "readWrite", db: "readWriteDB" } ]
    }
);
```

Ändern eines IAM-Benutzers oder einer IAM-Rolle

Ändern Sie einen vorhandenen IAM-Benutzer:

```
use $external;
db.updateUser(
  "arn:aws:iam::123456789123:user/iamuser",
  {
    roles: [ { role: "read", db: "readDB" } ]
  }
);
```

Ändern Sie eine bestehende IAM-Rolle:

```
use $external;
db.updateUser(
  "arn:aws:iam::123456789123:role/iamrole",
  {
    roles: [ { role: "read", db: "readDB" } ]
  }
);
```

So gewähren oder entziehen Sie einem IAM-Benutzer Rollen:

```
use $external;
db.grantRolesToUser(
  "arn:aws:iam::123456789123:user/iamuser",
  [ { db: "admin", role: "readWriteAnyDatabase" } ]
```

```
);
```

```
use $external;
db.revokeRolesFromUser(
  "arn:aws:iam::123456789123:user/iamuser",
  [ { db: "admin", role: "readWriteAnyDatabase" } ]
);
```

So gewähren oder entziehen Sie Rollen für eine IAM-Rolle:

```
use $external;
db.grantRolesToUser(
  "arn:aws:iam::123456789123:user/iamrole",
  [ { db: "admin", role: "readWriteAnyDatabase" } ]
);
```

```
use $external;
db.revokeRolesFromUser(
  "arn:aws:iam::123456789123:user/iamrole",
  [ { db: "admin", role: "readWriteAnyDatabase" } ]
);
```

Löschen eines IAM-Benutzers oder einer IAM-Rolle

Um einen vorhandenen IAM-Benutzer zu löschen:

```
use $external;
db.dropUser("arn:aws:iam::123456789123:user/iamuser");
```

Um eine bestehende IAM-Rolle zu löschen:

```
use $external;
db.dropUser("arn:aws:iam::123456789123:role/iamrole");
```

Konfigurieren Sie einen Verbindungs-URI für die Authentifizierung mit IAM AWS

Verwenden Sie zur Authentifizierung mit AWS IAM die folgenden URI-Parameter: `authSource` as und as. `$external` `authMechanism` `MONGODB-AWS` Wenn Sie einen IAM-Benutzer verwenden, werden die Felder für den Benutzernamen und das Passwort durch einen Zugriffsschlüssel bzw. einen geheimen Schlüssel ersetzt. Wenn Sie eine IAM-Rolle übernehmen, die der Umgebung

zugeordnet ist, in der Sie sich befinden (z. B. AWS Lambda Funktion, Amazon EC2 EC2-Instance). Sie müssen bei der Authentifizierung mit diesem Mechanismus keine speziellen Anmeldeinformationen angeben. `MONGODB-AWS` Wenn Sie MongoDB-Treiber verwenden, die den `MONGODB-AWS` Authentifizierungsmechanismus unterstützen, können die Treiber auch IAM-Rollenanmeldedaten von der Compute-Instance abrufen (z. B. Amazon EC2, Lambda-Funktion und andere). Im folgenden Beispiel wird eine Mongo-Shell zur Authentifizierung verwendet, `MONGODB-AWS` indem ein Zugriffsschlüssel und ein geheimer Schlüssel (eines IAM-Benutzers) manuell übergeben werden, um die Authentifizierung gegenüber Amazon DocumentDB nachzuweisen.

Im folgenden Beispiel wird Python-Code zur Authentifizierung verwendet, `MONGODB-AWS` ohne dass Anmeldeinformationen explizit übergeben werden (mithilfe einer der Umgebung zugewiesenen IAM-Rolle), um die Authentifizierung gegenüber Amazon DocumentDB zu demonstrieren.

```
##Create a MongoDB client, open a connection to Amazon DocumentDB using an IAM role
    client = pymongo.MongoClient('mongodb://<DocDBEndpoint>:27017/?
tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false&authSource=
%24external&authMechanism=MONGODB-AWS')
```

Im folgenden Beispiel wird eine Mongo-Shell verwendet, um sich mithilfe eines `MONGODB-AWS` Mechanismus zu authentifizieren, indem ein Zugriffsschlüssel und ein geheimer Schlüssel (eines IAM-Benutzers) manuell übergeben werden, um die Authentifizierung gegenüber Amazon DocumentDB nachzuweisen.

```
$ mongo 'mongodb://<access_key>:<secret_key>@<cluster_endpoint>:<db_port>/test?
authSource=%24external&authMechanism=MONGODB-AWS'
```

Im folgenden Beispiel wird eine Mongo-Shell zur Authentifizierung verwendet, `MONGODB-AWS` ohne dass Anmeldeinformationen explizit übergeben werden (mithilfe der der Umgebung zugewiesenen IAM-Rolle), um die Authentifizierung gegenüber Amazon DocumentDB zu demonstrieren.

```
$ mongo 'mongodb://<cluster_endpoint>:<db_port>/test?authSource=
%24external&authMechanism=MONGODB-AWS'
```

Konfigurieren AWS Berechnungstypen für die Authentifizierung bei Amazon DocumentDB mithilfe AWS IAM

Verwenden von Amazon EC2//AWS LambdaAWS Fargate

Amazon EC2 verwendet die folgenden Umgebungsvariablen. Wenn der EC2-Instance eine IAM-Rolle oder eine Ausführungs-IAM-Rolle mit einer Lambda-Funktion oder einer Amazon ECS-Aufgabe verknüpft ist, werden diese Variablen automatisch gefüllt und der Treiber kann diese Werte aus der Umgebung abrufen:

```
AWS_ACCESS_KEY_ID
AWS_SECRET_ACCESS_KEY
AWS_SESSION_TOKEN
```

Weitere Informationen zu Umgebungsvariablen finden Sie unter Verwenden von Lambda-Umgebungsvariablen im AWS Lambda Entwicklerhandbuch.

Amazon EKS verwenden

Wenn Sie Ihren Amazon Elastic Kubernetes Service (Amazon EKS) -Pods eine Rolle zuweisen, werden automatisch die folgenden beiden Umgebungsvariablen eingerichtet:

```
AWS_WEB_IDENTITY_TOKEN_FILE - path of web identity token file
AWS_ROLE_ARN - Name of IAM role to connect with
```

Übernehmen Sie mithilfe dieser Variablen manuell die Rolle aus Ihrem Code mithilfe des AWS SDK-Aufrufs für: `AssumeRoleWithWebIdentity`

- Lassen Sie den `ProviderID` Parameter weg.
- Suchen Sie den Wert des `WebIdentityToken` Parameters in der Datei, die in der `AWS_WEB_IDENTITY_TOKEN_FILE` Umgebungsvariablen beschrieben ist.

Weitere Informationen zu Amazon EKS finden Sie unter Was ist Amazon EKS im Amazon EKS-Benutzerhandbuch.

Überwachung von IAM-Authentifizierungsanfragen

Amazon DocumentDB DocumentDB-Auditing verwenden

Gehen Sie zum Audit-Log-Ordner in Amazon und verwenden Sie verschiedene Suchmuster CloudWatch, um die Protokolle für die IAM-Authentifizierung abzurufen. Verwenden Sie es beispielsweise `{ $.param.mechanism = "MONGODB-AWS" }` als Suchmuster für „Alle Protokollstreams durchsuchen“.

Weitere Informationen zu unterstützten Ereignissen bei der Überwachung finden Sie unterAmazon DocumentDB DocumentDB-Ereignisse prüfen.

Verwenden von CloudWatch Amazon-Metriken

`StsGetCallerIdentityCalls`: Diese Metrik zeigt, wie viele `GetCallerIdentity` Aufrufe eine Amazon DocumentDB DocumentDB-Instance an den regionalized AWS -Security-Token-Service (AWS STS) -Endpunkt tätigt. In der `MONGODB-AWS` Authentifizierungsspezifikation erfahren Sie, warum Datenbank-Instances `GetCallerIdentity` STS-Aufrufe tätigen müssen.

Verwenden der IAM-Authentifizierung

Wenn Sie den Benutzernamen und das Passwort nicht in Ihrer eigenen Datenbank verwalten möchten, können Sie die IAM-Authentifizierung verwenden. Die IAM-Authentifizierung ist nur in der instanzbasierten Amazon DocumentDB-Cluster-Version 5.0 verfügbar.

Die IAM-Authentifizierung ist vom STS-Service abhängig. Wir empfehlen Ihnen, zu prüfen, ob Sie die Verbindungsrate senken können, wenn Sie die IAM-Authentifizierung für die Verbindung verwenden und eine STS-Drosselungsausnahme auftritt.

Informationen zu IAM-Kontingenten finden Sie unter IAM und AWS STS Kontingente im IAM-Benutzerhandbuch.

Treiber, die IAM unterstützen

Treiber, die Amazon DocumentDB 5.0 und den `MONGODB-AWS` Authentifizierungsmechanismus unterstützen, sollten mit der IAM-Authentifizierungsimplementierung in Amazon DocumentDB funktionieren.

> **Important**
>
> Es gibt eine bekannte Einschränkung bei Node.js Treibern, die älter als Version 6.13.1 sind und derzeit nicht von der IAM-Identitätsauthentifizierung für Amazon DocumentDB unterstützt werden. Node.js Treiber und Tools, die Node.js Treiber verwenden (z. B. Mongosh), müssen aktualisiert werden, sodass sie die Node.js Treiberversion 6.13.1 oder höher verwenden.

Häufig gestellte Fragen zur IAM-Identitätsauthentifizierung

Gibt es Beispiele, auf die ich mich beziehen kann?

Auf diesen Seiten finden Sie Beispiele für Anwendungsfälle und Konfigurationen:

- So können sich menschliche Benutzer mithilfe von IAM-Benutzern und IAM-Rollen bei Amazon DocumentDB authentifizieren
- Password-less Authentifizierung bei Amazon DocumentDB mithilfe von IAM-Rollen

Ich erhalte eine Fehlermeldung bei der Verwendung meines Python-Treibers: „pymongo.errors. ConfigurationError: Die AWS MONGODB-Authentifizierung erfordert „pymongo-auth-aws“. Wie kann ich das lösen?

Stellen Sie sicher, dass Sie bei der Installation des Python-Treibers mit IAM-Authentifizierung die folgende Anweisung verwenden:

```
pip install 'pymongo[aws]'
```

Dadurch werden die zusätzlichen AWS Abhängigkeiten installiert, die für das Funktionieren der IAM-Authentifizierung erforderlich sind.

Wird meine Verbindung unterbrochen, wenn meine temporären Anmeldeinformationen für meine IAM-Rolle ablaufen?

Nein, die temporären IAM-Anmeldeinformationen werden nur für den Verbindungsaufbau und die Authentifizierung verwendet. Dann erfolgt die gesamte weitere Autorisierung im Amazon DocumentDB-Cluster. Selbst wenn es sich um IAM-Anmeldeinformationen rotate/expire handelt, wird die Verbindung nicht unterbrochen oder veraltet.

Amazon DocumentDB DocumentDB-Benutzer verwalten

In Amazon DocumentDB authentifizieren sich Benutzer bei einem Cluster in Verbindung mit einem Passwort. Jeder Cluster verfügt über primäre Anmeldeinformationen, die bei der Clustererstellung festgelegt werden.

> **Note**
>
> Allen neuen Benutzern, die vor dem 26. März 2020 erstellt wurden, wurden die `dbAdminAnyDatabase`-, `readWriteAnyDatabase`- und `clusterAdmin`-Rollen erteilt. Es wird empfohlen, alle Benutzer neu zu bewerten und die Rollen nach Bedarf zu ändern, um die geringstmöglichen Berechtigungen für alle Benutzer in Ihren Clustern zu erzwingen.

Weitere Informationen finden Sie unter Datenbankzugriff mit Role-Based Access Control.

Primär- und `Serviceadmin-Benutzer`

Ein neu erstellter Amazon DocumentDB-Cluster hat zwei Benutzer: den Hauptbenutzer und den `serviceadmin` Benutzer.

Der Hauptbenutzer ist ein einzelner, privilegierter Benutzer, der administrative Aufgaben ausführen und zusätzliche Benutzer mit Rollen erstellen kann. Wenn Sie sich zum ersten Mal mit einem Amazon DocumentDB-Cluster verbinden, müssen Sie sich mit den primären Anmeldeinformationen authentifizieren. Der Hauptbenutzer erhält diese Administratorberechtigungen für einen Amazon DocumentDB-Cluster, wenn dieser Cluster erstellt wird, und ihm wird die Rolle von `root` zugewiesen.

Der `serviceadmin`-Benutzer wird implizit beim Erstellen des Clusters erstellt. Jeder Amazon DocumentDB-Cluster hat einen `serviceadmin` Benutzer, AWS der die Möglichkeit bietet, Ihren Cluster zu verwalten. Sie können sich mit `serviceadmin` nicht anmelden, den Benutzer löschen oder umbenennen, sein Passwort ändern oder die Berechtigungen ändern. Jeder Versuch, das zu tun, führt zu einem Fehler.

> **Note**
>
> Die primären `serviceadmin` Benutzer und Benutzer für einen Amazon DocumentDB-Cluster können nicht gelöscht werden, und die Rolle des `root` Hauptbenutzers kann nicht entzogen werden.
> Wenn Sie Ihr primäres Benutzerkennwort vergessen haben, können Sie es mit dem AWS-Managementkonsole oder dem zurücksetzen. AWS CLI

Zusätzliche Benutzer erstellen

Nachdem Sie sich als Hauptbenutzer (oder als beliebiger Benutzer mit dieser Rolle`createUser`) verbunden haben, können Sie einen neuen Benutzer erstellen, wie unten gezeigt.

```
db.createUser(
    {
        user: "sample-user-1",
        pwd: "password123",
        roles:
```

```
            [{"db":"admin", "role":"dbAdminAnyDatabase" }]
    }
)
```

Um Benutzerdetails anzuzeigen, können Sie den Befehl `show users` wie folgt verwenden. Sie können Benutzer zusätzlich mit dem Befehl `dropUser` entfernen. Weitere Informationen finden Sie unter Allgemeine Befehle.

```
show users
{
    "_id" : "serviceadmin",
    "user" : "serviceadmin",
    "db" : "admin",
    "roles" : [
     {
            "role" : "root",
            "db" : "admin"
        }
    ]
},

{
    "_id" : "myPrimaryUser",
    "user" : "myPrimaryUser",
    "db" : "admin",
    "roles" : [
     {
            "role" : "root",
            "db" : "admin"
        }
    ]
},

{
    "_id" : "sample-user-1",
    "user" : "sample-user-1",
    "db" : "admin",
    "roles" : [
     {
            "role" : "dbAdminAnyDatabase",
            "db" : "admin"
     }
```

```
    ]
}
```

Im obigen Beispiel wird der neue Benutzer `sample-user-1` der `admin`-Datenbank zugewiesen. Dies ist bei einem neuen Benutzer immer der Fall. Amazon DocumentDB hat nicht das Konzept einer `authenticationDatabase` und daher wird die gesamte Authentifizierung im Kontext der `admin` Datenbank durchgeführt.

Wenn Sie beim Erstellen von Benutzern das db Feld bei der Angabe der Rolle weglassen, ordnet Amazon DocumentDB die Rolle implizit der Datenbank zu, für die die Verbindung hergestellt wird. Wenn Ihre Verbindung beispielsweise für die Datenbank `sample-database` hergestellt wird und Sie den folgenden Befehl ausführen, wird der Benutzer `sample-user-2` in der Datenbank `admin` erstellt und verfügt über `readWrite`-Berechtigungen für die Datenbank `sample-database`.

```
db.createUser(
    {
        user: "sample-user-2",
        pwd: "password123",
        roles:
            ["readWrite"]
    }
)
```

Wenn Sie Benutzer mit Rollen erstellen, die über alle Datenbanken hinweg erfasst sind (z. B. `readInAnyDatabase`), müssen Sie sich beim Erstellen des Benutzers entweder im Kontext der `admin`-Datenbank befinden oder beim Erstellen des Benutzers explizit die Datenbank für die Rolle angeben.

Um den Kontext Ihrer Datenbank zu wechseln, können Sie den folgenden Befehl verwenden.

```
use admin
```

Weitere Informationen zur rollenbasierten Zugriffssteuerung und zum Erzwingen geringstmöglicher Berechtigungen unter den Benutzern im Cluster finden Sie unter Datenbankzugriff mit Role-Based Access Control.

Automatisch rotierende Passwörter für Amazon DocumentDB

Mit AWS Secrets Manager können Sie hartcodierte Anmeldeinformationen in Ihrem Code (einschließlich Kennwörtern) durch einen API-Aufruf an Secrets Manager ersetzen, um das Geheimnis programmgesteuert abzurufen. Dadurch wird sichergestellt, dass das Secret nicht kompromittiert werden kann, wenn jemand Ihren Code durchsucht, da es sich gar nicht dort befindet. Außerdem können Sie Secrets Manager so konfigurieren, dass er das Secret automatisch nach einem von Ihnen festgelegten Zeitplan rotiert. So können Sie Secrets mit langer Einsatzdauer durch Secrets mit kurzer Einsatzdauer ersetzen und damit das Risiko einer Kompromittierung erheblich verringern.

Mit Secrets Manager können Sie Ihre Amazon DocumentDB-Passwörter (d. h. Secrets) mithilfe einer von Secrets Manager AWS Lambda bereitgestellten Funktion automatisch rotieren.

Weitere Informationen AWS Secrets Manager zur systemeigenen Integration mit Amazon DocumentDB finden Sie im Folgenden:

- Blog: So wechseln Sie Amazon DocumentDB- und Amazon Redshift Redshift-Anmeldeinformationen in Secrets Manager AWS
- Was ist AWS Secrets Manager?
- AWS Secrets Manager Geheimnisse rotieren
- Amazon DocumentDB DocumentDB-Anmeldeinformationen in Secrets Manager

Datenbankzugriff mit Role-Based Access Control

Mithilfe der rollenbasierten Zugriffskontrolle (RBAC) in Amazon DocumentDB (mit MongoDB-Kompatibilität) können Sie den Zugriff auf die Aktionen einschränken, die Benutzer an Datenbanken ausführen können. Bei RBAC werden einem Benutzer eine oder mehrere Rollen gewährt. Diese Rollen bestimmen die Operationen, die ein Benutzer mit Datenbankressourcen ausführen kann. Amazon DocumentDB unterstützt derzeit sowohl integrierte Rollen, die auf Datenbankebene begrenzt sind, wie,,,,,,,,,`read`,,,`readWrite`,`readAnyDatabase`,`clusterAdmin`, als auch benutzerdefinierte Rollen, die auf bestimmte Aktionen beschränkt werden können, und granulare Ressourcen wie Sammlungen, die auf Ihre Anforderungen zugeschnitten sind.

Zu den häufigsten Anwendungsfällen für RBAC gehören die Durchsetzung der geringsten Rechte durch die Erstellung von Benutzern mit schreibgeschütztem Zugriff auf die Datenbanken oder

Sammlungen in einem Cluster sowie mandantenfähige Anwendungsdesigns, die es einem einzelnen Benutzer ermöglichen, auf eine bestimmte Datenbank oder Sammlung in einem Cluster zuzugreifen.

> **Note**
>
> Allen neuen Benutzern, die vor dem 26. März 2020 erstellt wurden, wurden die `dbAdminAnyDatabase`-, `readWriteAnyDatabase`- und `clusterAdmin`-Rollen erteilt. Es wird empfohlen, alle vorhandenen Benutzer neu zu bewerten und die Rollen nach Bedarf zu ändern, um die geringstmöglichen Berechtigungen für Ihre Cluster zu erzwingen.

Themen

- RBAC-Konzepte
- Erste Schritte mit den integrierten RBAC-Rollen
- Erste Schritte mit benutzerdefinierten RBAC-Rollen
- Als Benutzer eine Verbindung zu Amazon DocumentDB herstellen
- Allgemeine Befehle
- Funktionelle Unterschiede
- Einschränkungen
- Datenbankzugriff mit Role-Based Access Control

RBAC-Konzepte

Im Folgenden finden Sie wichtige Begriffe und Konzepte zur rollenbasierten Zugriffssteuerung. Weitere Informationen zu Amazon DocumentDB DocumentDB-Benutzern finden Sie unterAmazon DocumentDB DocumentDB-Benutzer verwalten.

- Benutzer — Eine einzelne Entität, die sich bei der Datenbank authentifizieren und Operationen ausführen kann.
- Passwort — Ein Geheimnis, das zur Authentifizierung des Benutzers verwendet wird.
- Rolle — Autorisiert einen Benutzer, Aktionen an einer oder mehreren Datenbanken durchzuführen.
- Admin-Datenbank — Die Datenbank, in der Benutzer gespeichert sind und für die sie autorisiert sind.
- Datenbank (**db**) — Der Namespace innerhalb von Clustern, der Sammlungen zum Speichern von Dokumenten enthält.

Der folgende Befehl erstellt einen Benutzer mit Namen `sample-user`.

```
db.createUser({user: "sample-user", pwd: "abc123", roles: [{role: "read", db: "sample-database"}]})
```

In diesem Beispiel:

- `user: "sample-user"`— Gibt den Benutzernamen an.
- `pwd: "abc123"`— Zeigt das Benutzerkennwort an.
- `role: "read", "db: "sample-database"`— Zeigt an, dass der Benutzer Leseberechtigungen für haben `sample-user` wird`sample-database`.

Das folgende Beispiel zeigt die Ausgabe, nachdem Sie den Benutzer `sample-user` mit `db.getUser(sample-user)` erhalten. In diesem Beispiel befindet sich der Benutzer `sample-user` in der Datenbank `admin`, besitzt jedoch die „read“-Rolle für die Datenbank `sample-database`.

Wenn Sie beim Erstellen von Benutzern das db Feld bei der Angabe der Rolle weglassen, ordnet Amazon DocumentDB die Rolle implizit der Datenbank zu, für die die Verbindung hergestellt wird. Wenn Ihre Verbindung beispielsweise für die Datenbank `sample-database` hergestellt wird und Sie den folgenden Befehl ausführen, wird der Benutzer `sample-user` in der Datenbank `admin` erstellt und verfügt über `readWrite`-Berechtigungen für die Datenbank `sample-database`.

```
db.createUser({user: "sample-user", pwd: "abc123", roles: ["readWrite"]})
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus.

```
{
   "user":"sample-user",
   "roles":[
      {
         "db":"sample-database",
         "role":"readWrite"
      }
   ]
}
```

Wenn Sie Benutzer mit Rollen erstellen, die über alle Datenbanken hinweg erfasst sind (z. B. `readAnyDatabase`), müssen Sie sich beim Erstellen des Benutzers entweder im Kontext der Datenbank `admin` befinden oder beim Erstellen des Benutzers explizit die Datenbank für die Rolle angeben. Um Befehle für die Datenbank `admin` auszugeben, können Sie den Befehl `use admin` verwenden. Weitere Informationen finden Sie unter Allgemeine Befehle.

Erste Schritte mit den integrierten RBAC-Rollen

Um Ihnen den Einstieg in die rollenbasierte Zugriffssteuerung zu erleichtern, führen Sie in diesem Abschnitt ein Beispielszenario zum Erzwingen der geringstmöglichen Berechtigungen durch das Erstellen von Rollen für drei Benutzer mit unterschiedlichen Auftragsfunktionen durch.

- `user1` ist ein neuer Manager, der in der Lage sein muss, alle Datenbanken in einem Cluster anzuzeigen und darauf zuzugreifen.
- `user2` ist ein neuer Mitarbeiter, der Zugriff auf nur eine Datenbank, `sample-database-1`, in demselben Cluster benötigt.
- `user3` ist ein vorhandener Mitarbeiter, der im selben Cluster eine andere Datenbank, `sample-database-2`, anzeigen und darauf zugreifen muss, auf die er vorher keinen Zugriff hatten.

Zu einem späteren Zeitpunkt verlassen sowohl `user1` als auch `user2` das Unternehmen, so dass ihr Zugang widerrufen werden muss.

Um Benutzer zu erstellen und Rollen zu erteilen, muss der Benutzer, mit dem Sie sich beim Cluster authentifizieren, über eine zugeordnete Rolle verfügen, die Aktionen für `createUser` und `grantRole` ausführen kann. Zum Beispiel können die Rollen `admin` und `userAdminAnyDatabase` beide solche Fähigkeiten gewähren. Informationen zu Aktionen pro Rolle finden Sie unter Datenbankzugriff mit Role-Based Access Control.

> **Note**
>
> In Amazon DocumentDB werden alle Benutzer- und Rollenoperationen (z. B.`create`,`get`,`drop`, `grantrevoke`, usw.) implizit in der `admin` Datenbank ausgeführt, unabhängig davon, ob Sie Befehle für die `admin` Datenbank ausgeben oder nicht.

Um zunächst zu verstehen, was die aktuellen Benutzer und Rollen im Cluster sind, können Sie den Befehl `show users` ausführen, wie im folgenden Beispiel. Sie sehen zwei Benutzer `serviceadmin` und den Hauptbenutzer für den Cluster. Diese beiden Benutzer sind immer vorhanden und können nicht gelöscht werden. Weitere Informationen finden Sie unter Amazon DocumentDB DocumentDB-Benutzer verwalten.

```
show users
```

Erstellen Sie für `user1` eine Rolle mit Lese- und Schreibzugriff auf alle Datenbanken im gesamten Cluster mit dem folgenden Befehl.

```
db.createUser({user: "user1", pwd: "abc123", roles: [{role: "readWriteAnyDatabase", db:
 "admin"}]})
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus.

```
{
   "user":"user1",
   "roles":[
      {
         "role":"readWriteAnyDatabase",
         "db":"admin"
      }
   ]
}
```

Erstellen Sie für `user2` eine Rolle mit schreibgeschütztem Zugriff auf die Datenbank `sample-database-1` mit dem folgenden Befehl.

```
db.createUser({user: "user2", pwd: "abc123", roles: [{role: "read", db: "sample-
database-1"}]})
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus.

```
{
   "user":"user2",
   "roles":[
      {
         "role":"read",
         "db":"sample-database-1"
      }
   ]
}
```

Um das Szenario zu simulieren, dass `user3` ein vorhandener Benutzer ist, erstellen Sie zuerst den Benutzer `user3` und weisen Sie dann `user3` eine neue Rolle zu.

```
db.createUser({user: "user3", pwd: "abc123", roles: [{role: "readWrite", db: "sample-
database-1"}]})
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus.

```
{
   "user":"user3",
   "roles":[
      {
         "role":"readWrite",
         "db":"sample-database-1"
      }
   ]
}
```

Nachdem der Benutzer `user3` erstellt wurde, weisen Sie `user3` die `read`-Rolle für `sample-database-2` zu.

```
db.grantRolesToUser("user3", [{role: "read", db: "sample-database-2"}])
```

Schließlich verlassen sowohl `user1` als auch `user2` das Unternehmen und ihr Zugriff auf den Cluster muss widerrufen werden. Sie können dies tun, indem Sie die Benutzer wie folgt löschen.

```
db.dropUser("user1")
db.dropUser("user2")
```

Um sicherzustellen, dass alle Benutzer über die entsprechenden Rollen verfügen, können Sie alle Benutzer mit dem folgenden Befehl auflisten.

```
show users
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus.

```
{
   "_id":"serviceadmin",
   "user":"serviceadmin",
   "db":"admin",
   "roles":[
      {
         "db":"admin",
         "role":"root"
      }
   ]
}
{
   "_id":"master-user",
   "user":"master-user",
   "db":"admin",
   "roles":[
      {
         "db":"admin",
         "role":"root"
      }
   ]
}
{
   "_id":"user3",
   "user":"user3",
   "db":"admin",
   "roles":[
      {
         "db":"sample-database-2",
         "role":"read"
      },
      {
         "db":"sample-database-1",
         "role":"readWrite"
      }
   ]
```

```
}
```

Erste Schritte mit benutzerdefinierten RBAC-Rollen

Um Ihnen den Einstieg in benutzerdefinierte Rollen zu erleichtern, führt Sie dieser Abschnitt durch ein Beispielszenario zur Durchsetzung der geringsten Rechte durch die Erstellung von Rollen für drei Benutzer mit unterschiedlichen Aufgabenfunktionen.

In diesem Beispiel gilt Folgendes:

- `user1` ist ein neuer Manager, der in der Lage sein muss, alle Datenbanken in einem Cluster anzuzeigen und darauf zuzugreifen.
- `user2`ist ein neuer Mitarbeiter, der nur die Aktion „Suchen“ für nur eine Datenbank im selben Cluster benötigt. `sample-database-1`
- `user3`ist ein vorhandener Mitarbeiter, der eine bestimmte Sammlung (Spalte 2) in einer anderen Datenbank, auf `sample-database-2` die er zuvor keinen Zugriff hatte, im selben Cluster anzeigen und darauf zugreifen muss.
- Erstellen Sie für `user1` eine Rolle mit Lese- und Schreibzugriff auf alle Datenbanken im gesamten Cluster mit dem folgenden Befehl.

```
db.createUser(
 {
     user: "user1", pwd: "abc123",
     roles: [{role: "readWriteAnyDatabase", db: "admin"}]
 }
 )
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus.

```
{
   "user":"user1",
   "roles":[
      {
         "role":"readWriteAnyDatabase",
         "db":"admin"
      }
   ]
}
```

Erstellen Sie für `user2` mit dem folgenden Befehl eine Rolle mit Find-Rechten für alle Sammlungen in der Datenbank`sample-database-1`. Beachten Sie, dass diese Rolle sicherstellen würde, dass alle zugehörigen Benutzer nur Suchabfragen ausführen können.

```
db.createRole(
{
    role: "findRole",
    privileges: [
    {
        resource: {db: "sample-database-1", collection: ""}, actions: ["find"]
    }],
    roles: []
}
)
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus.

```
{
   "role":"findRole",
   "privileges":[
      {
         "resource":{
            "db":"sample-database-1",
            "collection":""
         },
         "actions":[
            "find"
         ]
      }
   ],
   "roles":[

   ]
}
```

Erstellen Sie als Nächstes den Benutzer (`user2`) und fügen Sie dem Benutzer die kürzlich erstellte Rolle `findRole` hinzu.

```
db.createUser(
{
    user: "user2",
    pwd: "abc123",
```

```
    roles: []
})

 db.grantRolesToUser("user2",["findRole"])
```

Um das `user3` Szenario eines vorhandenen Benutzers zu simulieren, erstellen Sie zuerst den Benutzer `user3` und dann eine neue Rolle namens CollectionRole, der wir im nächsten Schritt zuweisen werden. `user3`

Jetzt können Sie eine neue Rolle zuweisen. `user3` Diese neue Rolle ermöglicht es `user3` Ihnen, eine bestimmte Sammlung einzufügen, zu aktualisieren, zu löschen und Zugriff auf diese zu finden. `sample-database-2`

```
db.createUser(
{
    user: "user3",
    pwd: "abc123",
    roles: []
})

db.createRole(
{
    role: "collectionRole",
    privileges: [
    {
        resource: {db: "sample-database-2", collection: "col2"}, actions: ["find",
 "update", "insert", "remove"]
    }],
    roles: []
}
)
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus.

```
{
   "role":"collectionRole",
   "privileges":[
      {
         "resource":{
            "db":"sample-database-2",
            "collection":"col2"
         },
```

```
         "actions":[
            "find",
            "update",
            "insert",
            "remove"
         ]
      }
   ],
   "roles":[

   ]
}
```

Nachdem der Benutzer erstellt `user3` wurde, können Sie ihm `user3` die Rolle `collectionFind` zuweisen.

```
db.grantRolesToUser("user3",["collectionRole"])
```

Schließlich verlassen sowohl `user1` als auch `user2` das Unternehmen und ihr Zugriff auf den Cluster muss widerrufen werden. Sie können dies tun, indem Sie die Benutzer wie folgt löschen.

```
db.dropUser("user1")
db.dropUser("user2")
```

Um sicherzustellen, dass alle Benutzer über die entsprechenden Rollen verfügen, können Sie alle Benutzer mit dem folgenden Befehl auflisten.

```
show users
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus.

```
{
   "_id":"serviceadmin",
   "user":"serviceadmin",
   "db":"admin",
   "roles":[
      {
         "db":"admin",
         "role":"root"
      }
```

```
   ]
}
{
   "_id":"master-user",
   "user":"master-user",
   "db":"admin",
   "roles":[
      {
         "db":"admin",
         "role":"root"
      }
   ]
}
{
   "_id":"user3",
   "user":"user3",
   "db":"admin",
   "roles":[
      {
         "db":"admin",
         "role":"collectionRole"
      }
   ]
}
```

Als Benutzer eine Verbindung zu Amazon DocumentDB herstellen

Wenn Sie eine Verbindung zu einem Amazon DocumentDB-Cluster herstellen, stellen Sie eine Verbindung im Kontext einer bestimmten Datenbank her. Wenn Sie in der Verbindungszeichenfolge keine Datenbank angeben, werden Sie standardmäßig automatisch im Kontext der Datenbank `test` mit dem Cluster verbunden. Alle Befehle auf Sammlungsebene wie `insert` und `find` werden für Sammlungen in der Datenbank `test` ausgegeben.

Um die Datenbank zu sehen, in der Sie sich befinden, oder — mit anderen Worten — Befehle für die Sie ausführen, verwenden Sie den db Befehl in der Mongo-Shell wie folgt.

Abfrage:

```
db
```

Ausgabe:

```
test
```

Obwohl sich die Standardverbindung möglicherweise im Kontext der Datenbank `test` befindet, bedeutet dies nicht unbedingt, dass der Benutzer, der der Verbindung zugeordnet ist, berechtigt ist, Aktionen für die Datenbank `test` auszuführen. Wenn Sie sich im vorangegangenen Beispielszenario als Benutzer `user3` authentifizieren, der die `readWrite`-Rolle für die Datenbank `sample-database-1` besitzt, ist der Standardkontext Ihrer Verbindung die Datenbank `test`. Wenn Sie jedoch versuchen, ein Dokument in eine Sammlung in der Datenbank `test` einzufügen, erhalten Sie die Fehlermeldung Autorisierungsfehler. Dies liegt daran, dass dieser Benutzer nicht berechtigt ist, diesen Befehl in dieser Datenbank auszuführen, wie unten gezeigt.

Abfrage:

```
db
```

Ausgabe:

```
test
```

Abfrage:

```
db.col.insert({x:1})
```

Ausgabe:

```
WriteCommandError({ "ok" : 0, "code" : 13, "errmsg" : "Authorization failure" })
```

Wenn Sie den Kontext Ihrer Verbindung zur Datenbank `sample-database-1` ändern, können Sie in die Sammlung schreiben, für die der Benutzer die Berechtigung dazu hat.

Abfrage:

```
use sample-database-1
```

Ausgabe:

```
switched to db sample-database-1
```

Abfrage:

```
db.col.insert({x:1})
```

Ausgabe:

```
WriteResult({ "nInserted" : 1})
```

Wenn Sie sich bei einem Cluster mit einem bestimmten Benutzer authentifizieren, können Sie die Datenbank auch in der Verbindungszeichenfolge angeben. Dadurch entfällt die Notwendigkeit, den Befehl `use` auszuführen, nachdem der Benutzer in der Datenbank `admin` authentifiziert wurde.

Die folgende Verbindungszeichenfolge authentifiziert den Benutzer für die Datenbank `admin`, aber der Kontext der Verbindung wird für die Datenbank `sample-database-1` verwendet.

```
mongo "mongodb://user3:abc123@sample-cluster.node.us-east-1.docdb.amazonaws.com:27017/
sample-database-2"
```

Allgemeine Befehle

Dieser Abschnitt enthält Beispiele für häufig verwendete Befehle, die die rollenbasierte Zugriffskontrolle in Amazon DocumentDB verwenden. Sie müssen sich im Kontext der Datenbank `admin` befinden, um Benutzer und Rollen zu erstellen und zu ändern. Sie können den Befehl `use admin` verwenden, um zur Datenbank `admin` zu wechseln.

> **Note**
>
> Änderungen an den Benutzern und Rollen erfolgen implizit in der Datenbank `admin`. Wenn Sie Benutzer mit Rollen erstellen, die über alle Datenbanken hinweg erfasst sind (z. B. `readAnyDatabase`), müssen Sie sich beim Erstellen des Benutzers entweder im Kontext der Datenbank `admin` befinden (d. h. `use admin`) oder beim Erstellen des Benutzers explizit die Datenbank für die Rolle angeben (wie in Beispiel 2 in diesem Abschnitt gezeigt).

Beispiel 1: Erstellen Sie einen Benutzer mit `read` Rolle für die Datenbank. `foo`

```
db.createUser({user: "readInFooBar", pwd: "abc123", roles: [{role: "read", db:
 "foo"}]})
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus.

```
{
   "user":"readInFooBar",
   "roles":[
      {
         "role":"read",
         "db":"foo"
      }
   ]
}
```

Beispiel 2: Erstellen Sie einen Benutzer mit Lesezugriff auf alle Datenbanken.

```
db.createUser({user: "readAllDBs", pwd: "abc123", roles: [{role: "readAnyDatabase", db:
 "admin"}]})
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus.

```
{
   "user":"readAllDBs",
   "roles":[
      {
         "role":"readAnyDatabase",
         "db":"admin"
      }
   ]
}
```

Beispiel 3: Erteilen Sie einem vorhandenen Benutzer eine `read` Rolle in einer neuen Datenbank.

```
db.grantRolesToUser("readInFooBar", [{role: "read", db: "bar"}])
```

Beispiel 4: Aktualisieren Sie die Rolle eines Benutzers.

```
db.updateUser("readInFooBar", {roles: [{role: "read", db: "foo"}, {role: "read", db:
 "baz"}]})
```

Beispiel 5: Widerrufen Sie einem Benutzer den Zugriff auf eine Datenbank.

```
db.revokeRolesFromUser("readInFooBar", [{role: "read", db: "baz"}])
```

Beispiel 6: Beschreiben Sie eine integrierte Rolle.

```
db.getRole("read", {showPrivileges:true})
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus.

```
{
   "role":"read",
   "db":"sample-database-1",
   "isBuiltin":true,
   "roles":[

   ],
   "inheritedRoles":[

   ],
   "privileges":[
      {
         "resource":{
            "db":"sample-database-1",
            "collection":""
         },
         "actions":[
            "changeStream",
            "collStats",
            "dbStats",
            "find",
            "killCursors",
            "listCollections",
            "listIndexes"
         ]
      }
   ],
   "inheritedPrivileges":[
      {
         "resource":{
            "db":"sample-database-1",
            "collection":""
         },
         "actions":[
            "changeStream",
            "collStats",
            "dbStats",
```

```
            "find",
            "killCursors",
            "listCollections",
            "listIndexes"
         ]
      }
   }
```

Beispiel 7: Einen Benutzer aus dem Cluster löschen.

```
db.dropUser("readInFooBar")
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus.

```
true
```

Beispiel 8: Erstellen Sie eine Rolle mit Lese- und Schreibzugriff auf eine bestimmte Sammlung

```
db.createRole(
{
    role: "collectionRole",
    privileges: [
    {
        resource: {db: "sample-database-2", collection: "col2"}, actions: ["find",
 "update", "insert", "remove"]
    }],
    roles: []
}
)
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus.

```
{
   "role":"collectionRole",
   "privileges":[
      {
         "resource":{
            "db":"sample-database-2",
            "collection":"col2"
         },
         "actions":[
            "find",
```

```
            "update",
            "insert",
            "remove"
         ]
      }
   ],
   "roles":[

   ]
}
```

Beispiel 9: Erstellen Sie einen Benutzer und weisen Sie ihm eine benutzerdefinierte Rolle zu

```
db.createUser(
{
    user: "user3",
    pwd: "abc123",
    roles: []
})

db.grantRolesToUser("user3",["collectionRole"])
```

Beispiel 10: Erteilen Sie einer benutzerdefinierten Rolle zusätzliche Rechte

```
db.grantPrivilegesToRole(
  "collectionRole",
  [
    {
      resource: { db: "sample-database-1", collection: "col1" },
      actions: ["find", "update", "insert", "remove"]
    }
  ]
)
```

Beispiel 11: Entfernen Sie Rechte aus einer benutzerdefinierten Rolle

```
db.revokePrivilegesFromRole(
  "collectionRole",
  [
    {
      resource: { db: "sample-database-1", collection: "col2" },
      actions: ["find", "update", "insert", "remove"]
```

```
    }
  ]
)
```

Beispiel 12: Aktualisieren Sie eine bestehende benutzerdefinierte Rolle

```
db.updateRole(
  "collectionRole",
  {
    privileges: [
    {
        resource: {db: "sample-database-3", collection: "sample-collection-3"},
 actions: ["find", "update", "insert", "remove"]
    }],
    roles: []
  }
)
```

Funktionelle Unterschiede

In Amazon DocumentDB werden Benutzer- und Rollendefinitionen in der `admin` Datenbank gespeichert und Benutzer werden anhand der `admin` Datenbank authentifiziert. Diese Funktionalität unterscheidet sich von der MongoDB Community Edition, ist aber konsistent mit MongoDB Atlas.

Amazon DocumentDB unterstützt auch Change-Streams, die eine zeitlich geordnete Abfolge von Änderungsereignissen bereitstellen, die in den Sammlungen Ihres Clusters auftreten. Die `listChangeStreams` Aktion wird auf Clusterebene (d. h. auf alle Datenbanken) angewendet, und die `modifyChangeStreams` Aktion kann auf Datenbank- und Clusterebene angewendet werden.

Einschränkungen

Die folgende Tabelle enthält die Beschränkungen für die Role-Based Zugriffskontrolle in Amazon DocumentDB.

Description	Limit
Anzahl Benutzer pro Cluster	1000
Anzahl der Rollen, die einem Benutzer zugeordnet sind	1000

Description	Limit
Anzahl der benutzerdefinierten Rollen	100
Anzahl der Ressourcen, die einer Berechtigung zugeordnet sind	100

Datenbankzugriff mit Role-Based Access Control

Mit der rollenbasierten Zugriffssteuerung können Sie einen Benutzer erstellen und ihm eine oder mehrere Rollen erteilen, um zu bestimmen, welche Operationen der Benutzer in einer Datenbank oder einem Cluster ausführen kann.

Im Folgenden finden Sie eine Liste der integrierten Rollen, die derzeit in Amazon DocumentDB unterstützt werden.

> **Note**
>
> In Amazon DocumentDB 4.0 und 5.0 können die `ListDatabase` Befehle `ListCollection` und optional die `authorizedDatabases` Parameter `authorizedCollections` und verwenden, um die Sammlungen und Datenbanken aufzulisten, auf die der Benutzer zugreifen darf, wobei er die jeweiligen `listDatabase` Rollen `listCollections` und benötigt. Außerdem haben Benutzer jetzt die Möglichkeit, ihre eigenen Cursor zu beenden, ohne die `KillCursor` Rolle zu benötigen.

Database user

Rollenname	Description	Aktionen

`read`	Gewährt einem Benutzer Lesezugriff auf die angegebene Datenbank.	`changeStreams`
		`collStats`
		`dbStats`
		`find`
		`killCursors`

Rollenname	Description	Aktionen

		`listIndexes`
		
		`listColle ctions`

`readWrite`	Gewährt dem Benutzer Lese- und Schreibzu griff auf die angegebene Datenbank.	Alle Aktionen von `read`-Berechti gungen.
		
		`createCol lection`
		
		`dropCollection`
		
		`createIndex`
		
		`dropIndex`
		
		`insert`
		
		`killCursors`
		
		`listIndexes`
		
		`listColle ctions`
		
		`remove`
		
		`update`

Cluster user

Rollenname	Description	Aktionen
lesen AnyDatabase	Gewährt einem Benutzer Lesezugriff auf alle Datenbanken im Cluster.	Alle Aktionen von `read`-Berechti gungen.

Rollenname	Description	Aktionen
		`listChangeStreams` `listDatabases`

`readWriteAnyDatabase`	Gewährt einem Benutzer Lese- und Schreibzugriff auf alle Datenbanken im Cluster.	Alle Aktionen von `readWrite` - Berechtigungen.
		`listChangeStreams`
		`listDatabases`

`userAdminAnyDatabase`	Gewährt einem Benutzer die Möglichkeit, die Rollen oder Berechtigungen, die ein Benutzer hat, der angegebenen Datenbank zuzuweisen und zu ändern.	`changeCustomData`
		`changePassword`
		`createUser`
		`dropRole`
		`dropUser`
		`grantRole`
		`listDatabases`
		`revokeRole`
		`viewRole`
		`viewUser`

Rollenname	Description	Aktionen

`dbAdminAnyDatabase`	Gewährt einem Benutzer die Möglichkeit, Datenbankverwaltungsrollen für jede angegebene Datenbank auszuführen.	Alle Aktionen von `dbAdmin`-Berechtigungen.
		`dropCollection`
		`listDatabases`
		`listChangeStreams`
		`modifyChangeStreams`

Superuser

Rollenname	Description	Aktionen
`root`	Gewährt einem Benutzer Zugriff auf die Ressourcen und Operationen aller folgenden Rollen zusammen: `readWriteAnyDatabase` , `dbAdminAnyDatabase` , `userAdminAnyDatabase` , `clusterAdmin` , `restore` und `backup`.	Alle Aktionen von `readWriteAnyDatabase` , `dbAdminAnyDatabase` , `userAdminAnyDatabase` , `clusterAdmin` , `restore` und `backup`.

Database administrator

Rollenname	Description	Aktionen

`dbAdmin`	Gewährt einem Benutzer die Möglichkeit, administrative Aufgaben für die angegebene Datenbank auszuführen.	`bypassDocumentValidation`
		`collMod`
		`collStats`
		`createCollection`
		`createIndex`
		`dropCollection`
		`dropDatabase`
		`dropIndex`
		`dbStats`
		`find`
		`killCursors`
		`listIndexes`
		`listCollections`
		`modifyChangeStreams`

`dbOwner`	Gewährt einem Benutzer die Möglichkeit, alle administrativen Aufgaben für die angegebenen Datenbank auszuführen, indem die Rollen	Alle Aktionen von `dbAdmin` und `readWrite` .

Rollenname	Description	Aktionen
	dbAdmin und readWrite kombiniert werden.	

Cluster administrator

Name der Rolle	Description	Aktionen
clusterAdmin	Gewährt einem Benutzer den größtmöglichen Zugriff auf die Cluster-Verwaltung durch Kombination der Rollen clusterManager , clusterMonitor und hostManager .	Alle Aktionen von clusterManager , clusterMonitor und hostManager . listChangeStreams dropDatabase modifyChangeStreams
clusterManager	Gewährt einem Benutzer die Möglichkeit, Verwaltungs- und Überwachungsaktionen für den angegebenen Cluster durchzuführen.	listChangeStreams listSessions modifyChangeStreams replSetGetConfig
clusterMonitor	Gewährt einem Benutzer die Möglichkeit, schreibgeschützten Zugriff auf Überwachungstools zu haben.	collStats dbStats find getParameter

Name der Rolle	Description	Aktionen

		`hostInfo`
		`indexStats`
		`killCursors`
		`listChangeStreams`
		`listCollections`
		`listDatabases`
		`listIndexes`
		`listSessions`
		`replSetGetConfig`
		`serverStatus`
		`top`

`hostManager`	Gewährt einem Benutzer die Möglichkeit, Server zu überwachen und zu verwalten.	`auditConfigure`
		`killCursors`
		`killAnyCursor`
		`killAnySession`
		`killop`

Backup administrator

Rollenname	Description	Aktionen

`backup`	Gewährt einem Benutzer den erforderlichen Zugriff zum Sichern von Daten.	`getParameter`
		`insert`
		`find`
		`listChangeStreams`
		`listCollections`
		`listDatabases`
		`listIndexes`
		`update`

`restore`	Gewährt einem Benutzer den erforderlichen Zugriff zum Wiederherstellen von Daten.	`bypassDocumentValidation`
		`changeCustomData`
		`changePassword`
		`collMod`
		`createCollection`
		`createIndex`
		`createUser`
		`dropCollection`

Rollenname	Description	Aktionen

		`dropRole`
		`dropUser`
		`getParameter`
		`grantRole`
		`find`
		`insert`
		`listCollections`
		`modifyChangeStreams`
		`revokeRole`
		`remove`
		`viewRole`
		`viewUser`
		`update`

Protokollierung und Überwachung in Amazon DocumentDB

Amazon DocumentDB (mit MongoDB-Kompatibilität) bietet eine Vielzahl von CloudWatch Amazon-Metriken, die Sie überwachen können, um den Zustand und die Leistung Ihrer Amazon DocumentDB-Cluster und -Instances zu ermitteln. Sie können Amazon DocumentDB-Metriken mithilfe verschiedener Tools anzeigen, darunter die Amazon DocumentDB DocumentDB-Konsole, die AWS CLI, die CloudWatch Amazon-Konsole und die CloudWatch API. Weitere Informationen zur Überwachung finden Sie unter Amazon DocumentDB überwachen.

Zusätzlich zu den CloudWatch Amazon-Metriken können Sie den Profiler verwenden, um die Ausführungszeit und Details der Operationen zu protokollieren, die auf Ihrem Cluster ausgeführt wurden. Profiler ist nützlich für die Überwachung der langsamsten Operationen in Ihrem Cluster, um die Leistung einzelner Abfragen und die allgemeine Cluster-Leistung zu verbessern. Wenn diese Option aktiviert ist, werden Vorgänge in Amazon CloudWatch Logs protokolliert, und Sie können CloudWatch Insight verwenden, um Ihre Amazon DocumentDB DocumentDB-Profilerstellungsdaten zu analysieren, zu überwachen und zu archivieren. Weitere Informationen finden Sie unter Profilierung von Amazon DocumentDB DocumentDB-Vorgängen.

Amazon DocumentDB ist auch in einen Service integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen von Benutzern, Rollen oder einem AWS Service in Amazon DocumentDB (mit MongoDB-Kompatibilität) bereitstellt. CloudTrail erfasst alle AWS CLI API-Aufrufe für Amazon DocumentDB als Ereignisse, einschließlich Aufrufe von Amazon DocumentDB AWS-Managementkonsole und von Codeaufrufen an das Amazon DocumentDB-SDK. Weitere Informationen finden Sie unter Protokollieren Amazon DocumentDB DocumentDB-API-Aufrufen mit AWS CloudTrail.

Mit Amazon DocumentDB können Sie Ereignisse prüfen, die in Ihrem Cluster durchgeführt wurden. Beispiele für protokollierte Ereignisse sind erfolgreiche und fehlgeschlagene Authentifizierungsversuche, Drop-Ereignisse für Sammlungen in einer Datenbank oder das Erstellen eines Index. Standardmäßig ist die Prüfung in Amazon DocumentDB deaktiviert und erfordert, dass Sie sich für diese Funktion anmelden. Weitere Informationen finden Sie unter Amazon DocumentDB DocumentDB-Ereignisse prüfen.

Aktualisierung Ihrer Amazon DocumentDB-TLS-Zertifikate

Topics

- Aktualisierung Ihrer Anwendung und Ihres Amazon DocumentDB-Clusters
- Automatische Rotation von Serverzertifikaten
- Fehlerbehebung
- Häufig gestellte Fragen

Das Zertifikat der Zertifizierungsstelle (CA) für Amazon DocumentDB-Cluster wurde im August 2024 aktualisiert. Wenn Sie Amazon DocumentDB-Cluster mit aktiviertem Transport Layer Security (TLS) verwenden (Standardeinstellung) und Sie Ihre Client-Anwendungs- und Serverzertifikate nicht rotiert haben, sind die folgenden Schritte erforderlich, um Verbindungsprobleme zwischen Ihrer Anwendung und Ihren Amazon DocumentDB-Clustern zu beheben.

- Schritt 1: Herunterladen des neuen CA-Zertifikats und Aktualisieren Ihrer Anwendung
- Schritt 2: Aktualisieren des Serverzertifikats

Die CA- und Serverzertifikate wurden im Rahmen der bewährten Standardmethoden für Wartung und Sicherheit für Amazon DocumentDB aktualisiert. Client-Anwendungen müssen die neuen CA-Zertifikate zu ihren Trust Stores hinzufügen, und bestehende Amazon DocumentDB DocumentDB-Instances müssen aktualisiert werden, sodass sie die neuen CA-Zertifikate vor diesem Ablaufdatum verwenden können.

Aktualisierung Ihrer Anwendung und Ihres Amazon DocumentDB-Clusters

Führen Sie die Schritte in diesem Abschnitt aus, um das CA-Zertifikatspaket Ihrer Anwendung (Schritt 1) und die Serverzertifikate Ihres Clusters (Schritt 2) zu aktualisieren. Bevor Sie die Änderungen auf Ihre Produktionsumgebungen anwenden, empfehlen wir dringend, diese Schritte in einer Entwicklungs- oder Stagingumgebung zu testen.

> **Note**
>
> Sie müssen die Schritte 1 und 2 jeweils AWS-Region ausführen, wenn Sie Amazon DocumentDB-Cluster haben.

Schritt 1: Herunterladen des neuen CA-Zertifikats und Aktualisieren Ihrer Anwendung

Laden Sie das neue CA-Zertifikat herunter und aktualisieren Sie Ihre Anwendung so, dass sie das neue CA-Zertifikat verwendet, um TLS-Verbindungen zu Amazon DocumentDB herzustellen. Laden Sie das neue CA-Zertifikatpaket von https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem herunter. Diese Operation lädt die Datei mit dem Namen `global-bundle.pem` herunter.

> **Note**
>
> Wenn Sie auf den Keystore zugreifen, der sowohl das alte CA-Zertifikat (`rds-ca-2019-root.pem`) als auch die neuen CA-Zertifikate (`rds-ca-rsa2048-g1`,,) enthält, stellen Sie sicher`rds-ca-rsa4096-g1`, `rds-ca-ecc384-g1` dass der Keystore auswählt. `global-bundle`

```
wget https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem
```

Aktualisieren Sie als Nächstes Ihre Anwendungen, um das neue Zertifikatpaket zu verwenden. Das neue CA-Paket enthält sowohl das alte CA-Zertifikat (rds-ca-2019) als auch die neuen CA-Zertifikate (rds-ca-rsa2048-g1, rds-ca-rsa4096-g1, rds-ca-ecc384-g1). Wenn beide CA-Zertifikate im neuen CA-Paket enthalten sind, können Sie Ihre Anwendung und Ihren Cluster in zwei Schritten aktualisieren.

Für Java-Anwendungen müssen Sie einen neuen Trust Store mit dem neuen CA-Zertifikat erstellen. Anweisungen finden Sie auf der Registerkarte Java im Verbindung bei aktiviertem TLS herstellen Thema.

Informationen dazu, wie Sie überprüfen, ob Ihre Anwendung das neueste CA-Zertifikatspaket verwendet, finden Sie unter Wie kann ich sicher sein, dass ich das neueste Zertifizierungsstellenpaket verwende?. Wenn Sie das neueste CA-Zertifikatspaket in Ihrer Anwendung bereits verwenden, können Sie mit Schritt 2 fortfahren.

Beispiele für die Verwendung eines Zertifizierungsstellenpakets mit Ihrer Anwendung finden Sie unter Verschlüsseln von Daten während der Übertragung und Verbindung bei aktiviertem TLS herstellen.

> **Note**
>
> Zurzeit akzeptiert der MongoDB Go Driver 1.2.1 nur ein einzelnes CA-Serverzertifikat in `sslcertificateauthorityfile`. Informationen Verbindung bei aktiviertem TLS herstellen zum Herstellen einer Verbindung zu Amazon DocumentDB mithilfe von Go, wenn TLS aktiviert ist, finden Sie unter.

Schritt 2: Aktualisieren des Serverzertifikats

Nachdem die Anwendung für die Verwendung des neuen CA-Bundles aktualisiert wurde, besteht der nächste Schritt darin, das Serverzertifikat zu aktualisieren, indem jede Instance in einem Amazon DocumentDB-Cluster geändert wird. Informationen zum Ändern von Instances zur Verwendung des neuen Serverzertifikats finden Sie in den folgenden Anweisungen.

Amazon DocumentDB bietet die folgenden Zertifizierungsstellen zum Signieren des DB-Serverzertifikats für eine DB-Instance:

- rds-ca-ecc384-g1 — Verwendet eine Zertifizierungsstelle mit dem ECC 384-Algorithmus für private Schlüssel und dem SHA384-Signaturalgorithmus. Diese CA unterstützt die automatische Rotation von Serverzertifikaten. Dies wird nur auf Amazon DocumentDB 4.0 und 5.0 unterstützt.
- rds-ca-rsa2048-g1 — Verwendet in den meisten Regionen eine Zertifizierungsstelle mit dem RSA 2048-Algorithmus für private Schlüssel und dem SHA256-Signaturalgorithmus. AWS Diese CA unterstützt die automatische Rotation von Serverzertifikaten.
- rds-ca-rsa4096-g1 — Verwendet eine Zertifizierungsstelle mit dem RSA 4096-Algorithmus für private Schlüssel und dem SHA384-Signaturalgorithmus. Diese CA unterstützt die automatische Rotation von Serverzertifikaten.

> **Note**
>
> Wenn Sie den verwenden, können Sie die Gültigkeitsdauer der im AWS CLI vorherigen Abschnitt aufgeführten Zertifizierungsstellen mithilfe von Describe-Zertifikaten überprüfen.

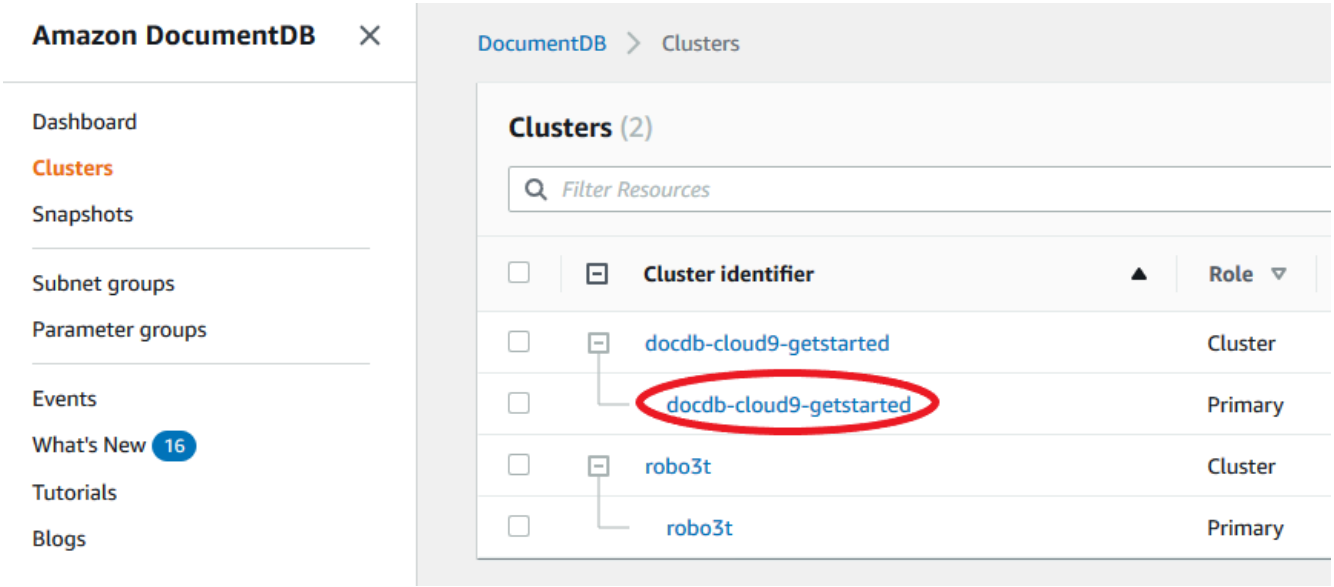
Diese CA-Zertifikate sind im regionalen und globalen Zertifikatpakets enthalten. Wenn Sie die Zertifizierungsstelle rds-ca-rsa2048-g1, rds-ca-rsa4096-g1 oder rds-ca-ecc384-g1 mit einer Datenbank verwenden, verwaltet Amazon DocumentDB das DB-Serverzertifikat in der Datenbank. Amazon DocumentDB rotiert das DB-Serverzertifikat automatisch, bevor es abläuft.

> **Note**
>
> Amazon DocumentDB erfordert keinen Neustart für die Zertifikatsrotation, wenn Ihr Cluster auf den folgenden Engine-Patch-Versionen läuft:
>
> - Amazon DocumentDB 3.6:1.0.208662 oder höher
> - Amazon DocumentDB 4.0:2.0.10179 oder höher
> - Amazon DocumentDB 5.0:3.0.4780 oder höher
>
> Sie können die aktuelle Patch-Version der Amazon DocumentDB DocumentDB-Engine ermitteln, indem Sie den folgenden Befehl ausführen:`db.runCommand({getEngineVersion: 1})`.
> Bevor Sie das Serverzertifikat aktualisieren, stellen Sie sicher, dass Sie den Vorgang abgeschlossen Schritt 1 haben.

Using the AWS-Managementkonsole

Gehen Sie wie folgt vor, um das alte Serverzertifikat für Ihre vorhandenen Amazon DocumentDB DocumentDB-Instances mithilfe von zu identifizieren und zu rotieren. AWS-Managementkonsole

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Wählen Sie in der Liste der Regionen in der oberen rechten Ecke des Bildschirms die Region aus, AWS-Region in der sich Ihre Cluster befinden.
3. Wählen Sie im Navigationsbereich auf der linken Seite der Konsole die Option Cluster aus.
4. Möglicherweise müssen Sie herausfinden, welche Instanzen sich noch auf dem alten Serverzertifikat befinden (). `rds-ca-2019` Sie können dies in der Spalte Zertifizierungsstelle tun, die sich ganz rechts in der Cluster-Tabelle befindet.
5. In der Cluster-Tabelle sehen Sie ganz links die Spalte Cluster-ID. Ihre Instances werden unter Clustern aufgeführt, ähnlich wie im folgenden Screenshot.



6. Markieren Sie das Kästchen links neben der Instanz, an der Sie interessiert sind.
7. Wählen Sie Aktionen und dann Ändern.
8. Wählen Sie unter Certificate authority (Zertifizierungsstelle) das neue Serverzertifikat (d. h. `rds-ca-rsa2048-g1`) für diese Instance aus.
9. Sie können eine Zusammenfassung der Änderungen auf der nächsten Seite sehen. Beachten Sie, dass es eine zusätzliche Warnung gibt, die Sie daran erinnert, dass Ihre Anwendung das neueste Zertifizierungsstellenpaket verwendet, bevor Sie die Instance ändern, um eine Unterbrechung der Konnektivität zu vermeiden.

10. Sie können die Änderung während Ihres nächsten Wartungsfensters oder sofort anwenden. Wenn Sie beabsichtigen, das Serverzertifikat sofort zu ändern, verwenden Sie die Option Apply Immediately (Sofort anwenden) .
11. Wählen Sie Modify instance (Instance ändern), um die Aktualisierung abzuschließen.

Using the AWS CLI

Gehen Sie wie folgt vor, um das alte Serverzertifikat für Ihre vorhandenen Amazon DocumentDB DocumentDB-Instances mithilfe von zu identifizieren und zu rotieren. AWS CLI

1. Um die Instances sofort zu ändern, führen Sie für jede Instance im Cluster den folgenden Befehl aus.

```
aws docdb modify-db-instance --db-instance-identifier <yourInstanceIdentifier>
 --ca-certificate-identifier rds-ca-rsa2048-g1 --apply-immediately
```

2. Um die Instances in Ihren Clustern so zu ändern, dass sie während des nächsten Wartungsfensters Ihres Clusters das neue CA-Zertifikat verwenden, führen Sie für jede Instance im Cluster den folgenden Befehl aus.

```
aws docdb modify-db-instance --db-instance-identifier <yourInstanceIdentifier>
 --ca-certificate-identifier rds-ca-rsa2048-g1 --no-apply-immediately
```

Automatische Rotation von Serverzertifikaten

Amazon DocumentDB unterstützt die automatische Rotation von Serverzertifikaten. Das Serverzertifikat ist das Blattzertifikat, das für jede Cluster-Instance ausgestellt wurde. Im Gegensatz zu den Root-CA-Zertifikaten haben die Serverzertifikate eine kurze Gültigkeitsdauer (12 Monate) und Amazon DocumentDB führt ihre Rotation automatisch durch, ohne dass Sie etwas unternehmen müssen. Amazon DocumentDB verwendet dieselbe Root-CA für diese automatische Rotation, sodass Sie kein neues CA-Bundle herunterladen müssen.

> **Important**
>
> Wenn Sie eine Verbindung zu Ihrem Amazon DocumentDB-Cluster herstellen, empfehlen wir, dass Sie dem Root-CA-Bundle vertrauen, anstatt jedem Serverzertifikat direkt zu vertrauen.

Dadurch werden Verbindungsfehler vermieden, nachdem das Serverzertifikat rotiert wurde. Siehe Verbindung bei aktiviertem TLS herstellen.

Amazon DocumentDB versucht, Ihr Serverzertifikat in Ihrem bevorzugten Wartungsfenster mit der Halbwertszeit des Serverzertifikats zu rotieren. Das neue Serverzertifikat ist 12 Monate gültig.

Verwenden Sie den `describe-db-engine-versions`Befehl und überprüfen Sie das `SupportsCertificateRotationWithoutRestart` Kennzeichen, um festzustellen, ob die Engine-Version das Rotieren des Zertifikats ohne Neustart unterstützt.

Note

Amazon DocumentDB unterstützt die Rotation von Serverzertifikaten ohne Neustarts, wenn Ihr Cluster auf den folgenden Engine-Patch-Versionen läuft:

- Amazon DocumentDB 3.6:1.0.208662 oder höher
- Amazon DocumentDB 4.0:2.0.10179 oder höher
- Amazon DocumentDB 5.0:3.0.4780 oder höher

Sie können die aktuelle Patch-Version der Amazon DocumentDB DocumentDB-Engine ermitteln, indem Sie diesen Befehl ausführen:`db.runCommand({getEngineVersion: 1})`.
Wenn Sie eine ältere Engine-Patch-Version verwenden, rotiert Amazon DocumentDB das Serverzertifikat und plant einen Datenbank-Neustart in Ihrem bevorzugten Wartungsfenster.

Fehlerbehebung

Wenn im Rahmen der Zertifikatrotation Probleme beim Herstellen einer Verbindung mit dem Cluster auftreten, empfehlen wir Folgendes:

- Stellen Sie sicher, dass Ihre Clients das neueste Zertifikatpaket verwenden. Siehe Wie kann ich sicher sein, dass ich das neueste Zertifizierungsstellenpaket verwende?.
- Stellen Sie sicher, dass Ihre Instances das neueste Zertifikat verwenden. Siehe Woher weiß ich, welche meiner Amazon DocumentDB DocumentDB-Instances das old/new Serverzertifikat verwenden?.

- Stellen Sie sicher, dass die neueste Zertifizierungsstelle von Ihrer Anwendung verwendet wird. Einige Treiber, wie Java und Go, benötigen zusätzlichen Code, um mehrere Zertifikate aus einem Zertifikatpaket in den Vertrauensspeicher zu importieren. Weitere Informationen zur Verbindung mit Amazon DocumentDB mit TLS finden Sie unterProgrammgesteuertes Herstellen einer Verbindung zu Amazon DocumentDB.
- Wenden Sie sich an den Support. Wenn Sie Fragen oder Probleme haben, wenden Sie sich an Support.

Häufig gestellte Fragen

Im Folgenden finden Sie Antworten auf einige häufig gestellte Fragen zu TLS-Zertifikaten.

Was passiert, wenn ich Fragen oder Probleme habe?

Wenn Sie Fragen oder Probleme haben, wenden Sie sich an Support.

Woher weiß ich, ob ich TLS verwende, um eine Verbindung zu meinem Amazon DocumentDB-Cluster herzustellen?

Sie können bestimmen, ob Ihr Cluster TLS verwendet, indem Sie den `tls`-Parameter für die Clusterparametergruppe Ihres Clusters untersuchen. Wenn der `tls`-Parameter auf `enabled` festgelegt ist, verwenden Sie das TLS-Zertifikat, um eine Verbindung mit dem Cluster herzustellen. Weitere Informationen finden Sie unter Verwaltung von Amazon DocumentDB-Cluster-Parametergruppen.

Warum aktualisieren Sie die Zertifizierungsstellen- und Serverzertifikate?

Die Amazon DocumentDB-CA- und Serverzertifikate werden im Rahmen der bewährten Standardmethoden für Wartung und Sicherheit für Amazon DocumentDB aktualisiert.

Was passiert, wenn ich bis zum Ablaufdatum nichts unternehme?

Wenn Sie TLS verwenden, um mit einem abgelaufenen CA-Zertifikat eine Verbindung zu Ihrem Amazon DocumentDB-Cluster herzustellen, können Ihre Anwendungen, die eine Verbindung über TLS herstellen, nicht mehr mit dem Amazon DocumentDB-Cluster kommunizieren.

Amazon DocumentDB rotiert Ihre Datenbankzertifikate vor Ablauf nicht automatisch. Sie müssen Ihre Anwendungen und Cluster aktualisieren, um die neuen CA-Zertifikate vor oder nach dem Ablaufdatum verwenden zu können.

Woher weiß ich, welche meiner Amazon DocumentDB DocumentDB-Instances das old/new Serverzertifikat verwenden?

Um die Amazon DocumentDB-Instances zu identifizieren, die noch das alte Serverzertifikat verwenden, können Sie entweder die Amazon DocumentDB AWS-Managementkonsole oder die verwenden. AWS CLI

Verwendung der AWS-Managementkonsole

So identifizieren Sie die Instances in Ihren Clustern, die das ältere Zertifikat verwenden

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Wählen Sie in der Liste der Regionen in der oberen rechten Ecke des Bildschirms die Region aus, AWS-Region in der sich Ihre Instances befinden.
3. Wählen Sie im Navigationsbereich auf der linken Seite der Konsole die Option Cluster aus.
4. In der Spalte Zertifizierungsstelle (ganz rechts in der Tabelle) wird angezeigt, welche Instanzen sich noch auf dem alten Serverzertifikat (`rds-ca-2019`) und dem neuen Serverzertifikat () befinden. `rds-ca-rsa2048-g1`

Verwendung der AWS CLI

Um die Instances in Ihren Clustern zu identifizieren, die das ältere Serverzertifikat verwenden, verwenden Sie den Befehl `describe-db-clusters` mit Folgendem:

```
aws docdb describe-db-instances \
    --filters Name=engine,Values=docdb \
    --query 'DBInstances[*].
{CertificateVersion:CACertificateIdentifier,InstanceID:DBInstanceIdentifier}'
```

Wie ändere ich einzelne Instances in meinem Amazon DocumentDB-Cluster, um das Serverzertifikat zu aktualisieren?

Sie sollten die Serverzertifikate für alle Instances in einem Cluster gleichzeitig aktualisieren. Um die Instances im Cluster zu ändern, können Sie die Konsole oder die AWS CLI verwenden.

> **Note**
>
> Sie müssen Schritt 1 abschließen, bevor Sie das Serverzertifikat aktualisieren.

Verwendung der AWS-Managementkonsole

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Wählen Sie in der Liste der Regionen in der oberen rechten Ecke des Bildschirms die Region aus, AWS-Region in der sich Ihre Cluster befinden.
3. Wählen Sie im Navigationsbereich auf der linken Seite der Konsole die Option Cluster aus.
4. In der Spalte Zertifizierungsstelle (ganz rechts in der Tabelle) wird angezeigt, welche Instanzen sich noch auf dem alten Serverzertifikat befinden (). `rds-ca-2019`
5. Wählen Sie in der Cluster-Tabelle unter Cluster-ID eine Instanz aus, die geändert werden soll.
6. Wählen Sie Aktionen und dann Ändern.
7. Wählen Sie unter Certificate authority (Zertifizierungsstelle) das neue Serverzertifikat (d. h. `rds-ca-rsa2048-g1`) für diese Instance aus.
8. Sie können eine Zusammenfassung der Änderungen auf der nächsten Seite sehen. Beachten Sie, dass es eine zusätzliche Warnung gibt, die Sie daran erinnert, dass Ihre Anwendung das neueste Zertifizierungsstellenpaket verwendet, bevor Sie die Instance ändern, um eine Unterbrechung der Konnektivität zu vermeiden.
9. Sie können die Änderung während Ihres nächsten Wartungsfensters oder sofort anwenden.
10. Wählen Sie Modify instance (Instance ändern), um die Aktualisierung abzuschließen.

Verwendung der AWS CLI

Gehen Sie wie folgt vor, um das alte Serverzertifikat für Ihre vorhandenen Amazon DocumentDB DocumentDB-Instances mithilfe von zu identifizieren und zu rotieren. AWS CLI

1. Um die Instances sofort zu ändern, führen Sie für jede Instance im Cluster den folgenden Befehl aus.

```
aws docdb modify-db-instance --db-instance-identifier <yourInstanceIdentifier> --
ca-certificate-identifier rds-ca-rsa2048-g1 --apply-immediately
```

2. Um die Instances in Ihren Clustern so zu ändern, dass sie während des nächsten Wartungsfensters Ihres Clusters das neue CA-Zertifikat verwenden, führen Sie für jede Instance im Cluster den folgenden Befehl aus.

```
aws docdb modify-db-instance --db-instance-identifier <yourInstanceIdentifier> --
ca-certificate-identifier rds-ca-rsa2048-g1 --no-apply-immediately
```

Was passiert, wenn ich einem vorhandenen Cluster eine neue Instance hinzufüge?

Alle neu erstellten Instances verwenden das alte Serverzertifikat und erfordern TLS-Verbindungen über das alte CA-Zertifikat. Alle neuen Amazon DocumentDB DocumentDB-Instances, die nach dem 25. Januar 2024 erstellt wurden, verwenden standardmäßig das neue Zertifikat rds-ca-rsa2048-g1.

Was passiert, wenn ein Instance-Ersatz oder ein Failover auf meinem Cluster vorhanden ist?

Wenn ein Instance-Ersatz in Ihrem Cluster vorhanden ist, verwendet die neu erstellte Instance weiterhin dasselbe Serverzertifikat wie die Instance davor. Es wird empfohlen, Serverzertifikate für alle Instances gleichzeitig zu aktualisieren. Wenn ein Failover im Cluster auftritt, wird das Serverzertifikat auf dem neuen Primärserver verwendet.

Wenn ich keine TLS für die Verbindung mit meinem Cluster verwende, muss ich trotzdem jede meiner Instances aktualisieren?

Wir empfehlen dringend, TLS zu aktivieren. Für den Fall, dass Sie TLS nicht aktivieren, empfehlen wir dennoch, die Zertifikate auf Ihren Amazon DocumentDB DocumentDB-Instances zu rotieren, falls Sie in future TLS für die Verbindung mit Ihren Clustern verwenden möchten. Wenn Sie nie planen, TLS für die Verbindung zu Ihren Amazon DocumentDB-Clustern zu verwenden, sind keine Maßnahmen erforderlich.

Was soll ich tun, wenn ich derzeit nicht TLS für die Verbindung mit meinem Cluster verwende, dies zukünftig aber vorhabe?

Wenn Sie vor Januar 2024 einen Cluster erstellt haben, folgen Sie Schritt 1 und Schritt 2 im vorherigen Abschnitt, um sicherzustellen, dass Ihre Anwendung das aktualisierte CA-Bundle verwendet und dass jede Amazon DocumentDB DocumentDB-Instance das neueste Serverzertifikat verwendet. Wenn Sie nach dem 25. Januar 2024 einen Cluster erstellen, verfügt Ihr Cluster

bereits über das neueste Serverzertifikat (rds-ca-rsa2048-g1). Informationen zum Überprüfen, ob Ihre Anwendung das neueste CA-Paket verwendet, finden Sie unter Wenn ich keine TLS für die Verbindung mit meinem Cluster verwende, muss ich trotzdem jede meiner Instances aktualisieren?.

Kann die Frist über den August 2024 hinaus verlängert werden?

Wenn Ihre Anwendungen eine Verbindung über TLS herstellen, kann die Frist nicht verlängert werden.

Wie kann ich sicher sein, dass ich das neueste Zertifizierungsstellenpaket verwende?

Verwenden Sie den folgenden Befehl, um zu überprüfen, ob Sie das neueste Paket haben. Um diesen Befehl ausführen zu können, muss Java installiert sein und die Java-Tools müssen sich in der PATH-Variablen Ihrer Shell befinden. Weitere Informationen finden Sie unter Java verwenden

macOS und Amazon Linux

```
keytool -printcert -v -file global-bundle.pem
```

Windows

```
keytool -printcert -v -file global-bundle.p7b
```

Warum sehe ich „RDS“ im Namen des Zertifizierungsstellenpakets?

Für bestimmte Verwaltungsfunktionen, wie z. B. die Zertifikatsverwaltung, verwendet Amazon DocumentDB Betriebstechnologie, die mit Amazon Relational Database Service (Amazon RDS) gemeinsam genutzt wird.

Wann läuft das neue Zertifikat ab?

Das neue Serverzertifikat läuft (in der Regel) wie folgt ab:

- rds-ca-rsa2048-g1 — Läuft 2061 ab
- rds-ca-rsa4096-g1 — Läuft 2121 ab
- rds-ca-ecc384-g1 — Läuft 2121 ab

Welche Fehler treten auf, wenn ich vor Ablauf des Zertifikats keine Maßnahmen ergreife?

Die Fehlermeldungen variieren je nach Treiber. Im Allgemeinen werden Ihnen Fehler bei der Zertifikatsvalidierung angezeigt, die die Zeichenfolge „Zertifikat ist abgelaufen“ enthalten.

Kann ich nach der Anwendung des neuen Serverzertifikats wieder zum alten Zertifikat zurückkehren?

Wenn Sie eine Instance auf das alte Serverzertifikat zurücksetzen müssen, sollten Sie alle Instances im Cluster zurücksetzen. Sie können das Serverzertifikat für jede Instanz in einem Cluster rückgängig machen, indem Sie den AWS-Managementkonsole oder den AWS CLI verwenden.

Verwendung der AWS-Managementkonsole

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Wählen Sie in der Liste der Regionen in der oberen rechten Ecke des Bildschirms die Region aus, AWS-Region in der sich Ihre Cluster befinden.
3. Wählen Sie im Navigationsbereich auf der linken Seite der Konsole die Option Cluster aus.
4. Wählen Sie in der Cluster-Tabelle unter Cluster-ID eine Instanz aus, die Sie ändern möchten. Wählen Sie Actions (Aktionen) und dann Modify (Ändern) aus.
5. Unter Certificate authority (Zertifizierungsstelle) können Sie das alte Serverzertifikat (`rds-ca-2019`) auswählen.
6. Wählen Sie Continue (Weiter) aus, um eine Übersicht Ihrer Änderungen anzuzeigen.
7. Auf dieser resultierenden Seite können Sie festlegen, dass Ihre Änderungen im nächsten Wartungsfenster oder sofort angewendet werden sollen. Wählen Sie die gewünschte Option und anschließend Modify instance (Instance ändern) aus.

> **Note**
>
> Wenn Sie Ihre Änderungen sofort anwenden möchten, werden alle Änderungen in der Warteschlange für ausstehende Änderungen ebenfalls angewendet. Wenn eine der ausstehenden Änderungen eine Ausfallszeit erfordert, kann die Auswahl dieser Option einen unerwarteten Ausfall verursachen.

Verwendung der AWS CLI

```
aws docdb modify-db-instance --db-instance-identifier <db_instance_name> ca-
certificate-identifier rds-ca-2019 <--apply-immediately | --no-apply-immediately>
```

Wenn Sie `--no-apply-immediately` wählen, werden die Änderungen während des nächsten Wartungsfensters des Clusters angewendet.

Wird bei einer Wiederherstellung, die ich aus einem Snapshot oder zeitpunktbezogen ausführe, das neue Serverzertifikat verwendet?

Wenn Sie nach August 2024 einen Snapshot wiederherstellen oder eine Point-in-Time-Wiederherstellung durchführen, verwendet der neue Cluster, der erstellt wird, das neue CA-Zertifikat.

Was ist, wenn ich Probleme habe, von einem beliebigen Mac OS aus eine direkte Verbindung zu meinem Amazon DocumentDB-Cluster herzustellen?

Mac OS hat die Anforderungen für vertrauenswürdige Zertifikate aktualisiert. Vertrauenswürdige Zertifikate müssen jetzt 397 Tage oder weniger gültig sein (siehehttps://support.apple.com/en-us/HT211025).

> **Note**
>
> Diese Einschränkung gilt für neuere Versionen von Mac OS.

Amazon DocumentDB DocumentDB-Instance-Zertifikate sind über vier Jahre gültig und damit länger als das Mac OS-Maximum. Um von einem Computer mit Mac OS aus eine direkte Verbindung zu einem Amazon DocumentDB-Cluster herzustellen, müssen Sie beim Erstellen der TLS-Verbindung ungültige Zertifikate zulassen. In diesem Fall bedeuten ungültige Zertifikate, dass die Gültigkeitsdauer mehr als 397 Tage beträgt. Sie sollten die Risiken verstehen, bevor Sie ungültige Zertifikate zulassen, wenn Sie eine Verbindung zu Ihrem Amazon DocumentDB-Cluster herstellen.

Verwenden Sie den Parameter, um von Mac OS aus eine Verbindung zu einem Amazon DocumentDB-Cluster herzustellen AWS CLI, indem Sie den `tlsAllowInvalidCertificates` Parameter verwenden.

```
mongo --tls --host <hostname> --username <username> --password <password> --port 27017
 --tlsAllowInvalidCertificates
```

Konformitätsprüfung in Amazon DocumentDB

Die Sicherheit und Konformität von Amazon DocumentDB wird von externen Prüfern im Rahmen mehrerer AWS Compliance-Programme bewertet, darunter die folgenden:

- System and Organization Controls (SOC) 1, 2 und 3. Weitere Informationen finden Sie unter SOC.
- Föderales Risiko- und Autorisierungsmanagementprogramm (FedRAMP). Weitere Informationen finden Sie unterAWS -Services im Rahmen des Compliance-Programms.
- Payment Card Industry Data Security Standard (PCI DSS). Weitere Informationen finden Sie unter PCI DSS.
- ISO 9001, 27001, 27017 und 27018. Weitere Informationen finden Sie unter ISO-zertifiziert.
- Health Insurance Portability and Accountability Act Business Associate Agreement (HIPAA BAA). Weitere Informationen finden Sie unter HIPAA-Compliance.

AWS bietet unter AWS Services in Scope by Compliance Program eine häufig aktualisierte Liste der AWS Services im Rahmen bestimmter Compliance-Programme.

Third-party Prüfberichte stehen Ihnen zum Herunterladen zur Verfügung unter AWS Artifact. Weitere Informationen finden Sie unter Berichte in AWS Artifact herunterladen.

Weitere Informationen zu AWS Compliance-Programmen finden Sie unter AWS Compliance-Programme.

Ihre Compliance-Verantwortung bei der Verwendung von Amazon DocumentDB richtet sich nach der Sensibilität Ihrer Daten, den Compliance-Zielen Ihrer Organisation und den geltenden Gesetzen und Vorschriften. Wenn Ihre Nutzung von Amazon DocumentDB der Einhaltung von Standards wie HIPAA oder PCI unterliegt, AWS bietet Ihnen folgende Ressourcen:

- AWS Ressourcen zur Einhaltung von Vorschriften — Eine Sammlung von Arbeitsmappen und Leitfäden, die möglicherweise auf Ihre Branche und Ihren Standort zutreffen.
- Schnellstartanleitungen zu Sicherheit und Compliance — Implementierungsleitfäden, in denen architektonische Überlegungen erörtert und Schritte für die Implementierung von Umgebungen beschrieben werden, auf denen Sicherheit und Compliance im Vordergrund stehen. AWS
- AWS Config — Ein Service, der bewertet, wie gut Ihre Ressourcenkonfigurationen internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.

- AWS Security Hub — Ein umfassender Überblick über Ihren Sicherheitsstatus innerhalb AWS , anhand dessen Sie überprüfen können, ob Sie die Sicherheitsstandards und Best Practices der Sicherheitsbranche einhalten.
- Whitepaper „Architecting for HIPAA Security and Compliance“ — Ein Whitepaper, das beschreibt, wie Unternehmen Anwendungen entwickeln können. AWS HIPAA-compliant

Resilienz in Amazon DocumentDB

Die AWS globale Infrastruktur basiert auf AWS-Regionen Availability Zones. AWS-Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander 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.

Ein Amazon DocumentDB-Cluster kann nur in einer Amazon VPC erstellt werden, die über mindestens zwei Subnetze in mindestens zwei Availability Zones verfügt. Durch die Verteilung Ihrer Cluster-Instances auf mindestens zwei Availability Zones trägt Amazon DocumentDB dazu bei, dass für den unwahrscheinlichen Fall eines Ausfalls der Availability Zone Instances in Ihrem Cluster verfügbar sind. Das Cluster-Volume für Ihren Amazon DocumentDB-Cluster erstreckt sich immer über drei Availability Zones, um dauerhaften Speicher mit geringerer Wahrscheinlichkeit von Datenverlusten bereitzustellen.

Weitere Informationen zu AWS-Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

Zusätzlich zur AWS globalen Infrastruktur bietet Amazon DocumentDB mehrere Funktionen, um Ihre Anforderungen an Datenstabilität und Datensicherung zu erfüllen.

Fault-tolerant und selbstheilendes Speichersystem

> Jeder 10-GB-Teil Ihres Speichervolumens wird auf sechs Arten in drei Availability Zones repliziert. Amazon DocumentDB verwendet fehlertoleranten Speicher, der den Verlust von bis zu zwei Datenkopien transparent handhabt, ohne die Schreibverfügbarkeit der Datenbank zu beeinträchtigen, und von bis zu drei Kopien, ohne die Leseverfügbarkeit zu beeinträchtigen. Der Amazon DocumentDB DocumentDB-Speicher repariert sich ebenfalls selbst. Datenblöcke und Festplatten werden kontinuierlich auf Fehler überprüft und automatisch ersetzt.

Manuelle Sicherungen und Wiederherstellung

Amazon DocumentDB bietet die Möglichkeit, vollständige Backups Ihres Clusters für die langfristige Aufbewahrung und Wiederherstellung zu erstellen. Weitere Informationen finden Sie unter Sichern und Wiederherstellen in Amazon DocumentDB.

Point-in-time Wiederherstellung

Point-in-time Recovery schützt Ihre Amazon DocumentDB-Cluster vor versehentlichen Schreib- oder Löschvorgängen. Mit der zeitpunktbezogenen Wiederherstellung müssen Sie sich keine Gedanken über das Erstellen, Warten oder Planen von On-Demand-Backups machen. Weitere Informationen finden Sie unter Zu einem bestimmten Zeitpunkt wiederherstellen.

Infrastruktursicherheit in Amazon DocumentDB

Als verwalteter Service ist Amazon DocumentDB 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 DocumentDB zuzugreifen. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Cipher-Suites mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Diffie-Hellman Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Sie können diese API-Vorgänge von einem beliebigen Netzwerkstandort aus aufrufen. Sie können Amazon DocumentDB DocumentDB-Richtlinien verwenden, um den Zugriff von bestimmten Amazon Virtual Private Cloud (Amazon VPC) -Endpunkten oder bestimmten VPCs aus zu kontrollieren. Dadurch wird der Netzwerkzugriff auf eine bestimmte Amazon DocumentDB DocumentDB-Ressource effektiv nur von der spezifischen VPC innerhalb des Netzwerks isoliert. AWS

> **Note**
>
> Amazon DocumentDB unterstützt keine ressourcenbasierten Zugriffsrichtlinien.

Amazon DocumentDB DocumentDB-API und VPC-Schnittstellen-Endpunkte (AWS PrivateLink)

> **Note**
>
> Elastische Amazon DocumentDB DocumentDB-Cluster unterstützen keine AWS PrivateLink VPC-Endpunkte.

Sie können eine private Verbindung zwischen Ihrer VPC und den Amazon DocumentDB DocumentDB-API-Endpunkten herstellen, indem Sie einen VPC-Schnittstellen-Endpunkt erstellen. Schnittstellen-Endpunkte werden betrieben von. AWS PrivateLink

Instanzbasierte Cluster von Amazon DocumentDB benötigen zwar keine VPC-Endpunktverbindung mit einer Schnittstelle, AWS PrivateLink ermöglichen Ihnen aber den privaten Zugriff auf Amazon DocumentDB DocumentDB-API-Operationen ohne Internet-Gateway, NAT-Gerät, VPN-Verbindung oder Verbindung. Direct Connect Amazon DocumentDB DocumentDB-Instances in Ihrer VPC benötigen keine öffentlichen IP-Adressen, um mit Amazon DocumentDB DocumentDB-API-Endpunkten zu kommunizieren und Datenbank-Instances und Datenbankcluster zu starten, zu ändern oder zu beenden. Ihre Amazon DocumentDB DocumentDB-Instances benötigen auch keine öffentlichen IP-Adressen, um die verfügbaren Amazon DocumentDB DocumentDB-API-Operationen nutzen zu können. Der Datenverkehr zwischen Ihrer VPC und Amazon DocumentDB verlässt das Amazon-Netzwerk nicht.

Jeder Schnittstellenendpunkt wird durch eine oder mehrere Elastic Network-Schnittstellen in Ihren Subnetzen dargestellt. Weitere Informationen finden Sie unter Elastic Network-Schnittstellen im Benutzerhandbuch für Amazon EC2.

Weitere Informationen zu VPC-Endpunkten finden Sie unter Zugreifen und AWS-Service Verwenden eines VPC-Endpunkts mit einer Schnittstelle im Amazon Virtual Private Cloud (AWS PrivateLink) - Benutzerhandbuch. Weitere Informationen zu Amazon DocumentDB DocumentDB-Vorgängen finden Sie in der Amazon DocumentDB DocumentDB-API-Referenz.

Topics

- Überlegungen zu VPC-Endpunkten
- Verfügbarkeit in Regionen

- Erstellen eines VPC-Schnittstellen-Endpunkts für die Amazon DocumentDB DocumentDB-API
- Erstellen einer VPC-Endpunktrichtlinie für die Amazon DocumentDB DocumentDB-API

Überlegungen zu VPC-Endpunkten

Bevor Sie einen VPC-Schnittstellen-Endpunkt für Amazon DocumentDB DocumentDB-API-Endpunkte einrichten, stellen Sie sicher, dass Sie die Voraussetzungen für Schnittstellen-Endpunkte im Amazon Virtual Private Cloud (AWS PrivateLink) -Benutzerhandbuch lesen.

Alle Amazon DocumentDB DocumentDB-API-Operationen, die für die Verwaltung von Amazon DocumentDB DocumentDB-Ressourcen relevant sind, sind über Ihre VPC verfügbar unter. AWS PrivateLink

VPC-Endpunktrichtlinien werden für Amazon DocumentDB DocumentDB-API-Endpunkte unterstützt. Standardmäßig ist der vollständige Zugriff auf Amazon DocumentDB DocumentDB-API-Operationen über den Endpunkt erlaubt. Weitere Informationen finden Sie unter Steuern des Zugriffs auf VPC-Endpunkte mithilfe von Endpunktrichtlinien im Amazon Virtual Private Cloud (AWS PrivateLink) -Benutzerhandbuch.

Verfügbarkeit in Regionen

Die Amazon DocumentDB DocumentDB-API unterstützt derzeit VPC-Endpunkte in den folgenden Bereichen: AWS-Regionen

- US East (Ohio)
- USA Ost (Nord-Virginia)
- USA West (Oregon)
- Africa (Cape Town)
- Asia Pacific (Hong Kong)
- Asien-Pazifik (Mumbai)
- Asien-Pazifik (Hyderabad)
- Asien-Pazifik (Osaka)
- Asien-Pazifik (Seoul)
- Asien-Pazifik (Singapur)
- Asien-Pazifik (Sydney)
- Asien-Pazifik (Tokio)

- Canada (Central)
- China (Peking)
- China (Ningxia)
- Europe (Frankfurt)
- Europa (Irland)
- Europa (London)
- Europa (Paris)
- Europa (Spain)
- Europa (Milan)
- Naher Osten (VAE)
- Südamerika (São Paulo)
- AWS GovCloud (US-East)
- AWS GovCloud (US-West)

Erstellen eines VPC-Schnittstellen-Endpunkts für die Amazon DocumentDB DocumentDB-API

Sie können einen VPC-Endpunkt für die Amazon DocumentDB DocumentDB-API entweder mit der Amazon VPC-Konsole oder mit () erstellen. AWS Command Line Interface AWS CLI Weitere Informationen finden Sie unter Zugreifen und AWS-Service Verwenden eines VPC-Endpunkts mit einer Schnittstelle im Amazon Virtual Private Cloud (AWS PrivateLink) -Benutzerhandbuch.

Erstellen Sie mithilfe des Servicenamens einen VPC-Endpunkt für die Amazon DocumentDB DocumentDB-API. `com.amazonaws.region.rds`

Mit Ausnahme AWS-Regionen von China können Sie, wenn Sie privates DNS für den Endpunkt aktivieren, API-Anfragen an Amazon DocumentDB stellen, wobei der VPC-Endpunkt seinen Standard-DNS-Namen für den verwendet AWS-Regionen, zum Beispiel rds.us-east-1.amazonaws.com. Für China (Peking) und China (Ningxia) AWS-Regionen können Sie API-Anfragen mit dem VPC-Endpunkt über rds-api.cn-north-1.amazonaws.com .cn bzw. rds-api.cn-northwest-1.amazonaws.com .cn stellen.

Weitere Informationen finden Sie unter Zugreifen und AWS-Service Verwenden eines VPC-Endpunkts mit einer Schnittstelle im Amazon Virtual Private Cloud (AWS PrivateLink) -Benutzerhandbuch.

Erstellen einer VPC-Endpunktrichtlinie für die Amazon DocumentDB DocumentDB-API

Sie können Ihrem VPC-Endpunkt eine Endpunktrichtlinie hinzufügen, die den Zugriff auf die Amazon DocumentDB DocumentDB-API steuert. Die Richtlinie gibt die folgenden Informationen an:

- Prinzipal, der die Aktionen ausführen kann.
- Aktionen, die ausgeführt werden können
- Die Ressourcen, für die Aktionen ausgeführt werden können.

Weitere Informationen finden Sie unter Steuern des Zugriffs auf VPC-Endpunkte mithilfe von Endpunktrichtlinien im Amazon Virtual Private Cloud (AWS PrivateLink) -Benutzerhandbuch.

Beispiel: VPC-Endpunktrichtlinie für Amazon DocumentDB DocumentDB-API-Aktionen

Im Folgenden finden Sie ein Beispiel für eine Endpunktrichtlinie für die Amazon DocumentDB DocumentDB-API. Wenn diese Richtlinie an einen Endpunkt angehängt ist, gewährt sie allen Prinzipalen auf allen Ressourcen Zugriff auf die aufgelisteten Amazon DocumentDB DocumentDB-API-Aktionen.

```
{
"Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "docdb:CreateDBInstance",
            "docdb:ModifyDBInstance",
            "docdb:CreateDBSnapshot"
         ],
         "Resource":"*"
      }
   ]
}
```

Beispiel: VPC-Endpunktrichtlinie, die jeglichen Zugriff von einem bestimmten Konto aus verweigert AWS

Die folgende VPC-Endpunktrichtlinie verweigert dem AWS Konto 123456789012 jeglichen Zugriff auf Ressourcen, die den Endpunkt verwenden. Die Richtlinie erlaubt alle Aktionen von anderen Konten.

```
{
  "Statement": [
    {
      "Action": "*",
      "Effect": "Allow",
      "Resource": "*",
      "Principal": "*"
    },
    {
      "Action": "*",
      "Effect": "Deny",
      "Resource": "*",
      "Principal": { "AWS": [ "123456789012" ] }
     }
   ]
}
```

Bewährte Sicherheitsmethoden für Amazon DocumentDB

Aus Sicherheitsgründen müssen Sie AWS Identity and Access Management (IAM-) Konten verwenden, um den Zugriff auf Amazon DocumentDB DocumentDB-API-Operationen zu kontrollieren, insbesondere Operationen, die Amazon DocumentDB DocumentDB-Ressourcen erstellen, ändern oder löschen. Zu solchen Ressourcen gehören Cluster, Sicherheitsgruppen und Parametergruppen. Sie müssen IAM auch zur Steuerung von Aktionen verwenden, mit denen allgemeine Verwaltungsaktionen wie das Sichern und Wiederherstellen von Clustern ausgeführt werden. Verwenden Sie bei der Erstellung von IAM-Rollen das Prinzip der geringsten Rechte.

- Erzwingen Sie die geringste Berechtigung mit rollenbasierter Zugriffssteuerung.
- Weisen Sie jeder Person, die Amazon DocumentDB DocumentDB-Ressourcen verwaltet, ein individuelles IAM-Konto zu. Verwenden Sie den AWS-Konto Root-Benutzer nicht zur Verwaltung von Amazon DocumentDB DocumentDB-Ressourcen. Erstellen Sie einen IAM-Benutzer für jede Person einschließlich Sie selbst.
- Gewähren Sie jedem -Benutzer nur den Mindestsatz an Berechtigungen, die für die Ausführung seiner Aufgaben erforderlich sind.
- Verwenden Sie IAM-Gruppen, um Berechtigungen für mehrere Benutzer effektiv zu verwalten. Weitere Informationen zu IAM finden Sie im IAM-Benutzerhandbuch. Weitere Informationen zu bewährten Methoden für IAM finden Sie unter Bewährte Methoden für IAM.
- Wechseln Sie regelmäßig die IAM-Anmeldeinformationen.

- Konfigurieren Sie AWS Secrets Manager so, dass die Secrets für Amazon DocumentDB automatisch rotiert werden. Weitere Informationen finden Sie unter Rotating Your AWS Secrets Manager Secrets und Rotating Secrets for Amazon DocumentDB im AWS Secrets Manager User Guide.
- Verwenden Sie Transport Layer Security (TLS) und die Verschlüsselung ruhender Daten, um Ihre Daten zu verschlüsseln.

Amazon DocumentDB DocumentDB-Ereignisse prüfen

Mit Amazon DocumentDB (mit MongoDB-Kompatibilität) können Sie Ereignisse überprüfen, die in Ihrem Cluster durchgeführt wurden. Beispiele für protokollierte Ereignisse sind erfolgreiche und fehlgeschlagene Authentifizierungsversuche, Drop-Ereignisse für Sammlungen in einer Datenbank oder das Erstellen eines Index. Standardmäßig ist die Prüfung in Amazon DocumentDB deaktiviert und erfordert, dass Sie sich für die Nutzung dieser Funktion anmelden.

Wenn die Prüfung aktiviert ist, zeichnet Amazon DocumentDB Ereignisse in Data Definition Language (DDL), Data Manipulation Language (DML), Authentifizierung, Autorisierung und Benutzerverwaltung in Amazon Logs auf. CloudWatch Wenn Auditing aktiviert ist, exportiert Amazon DocumentDB die Auditing-Datensätze (JSON-Dokumente) Ihres Clusters nach Amazon CloudWatch Logs. Sie können Amazon CloudWatch Logs verwenden, um Ihre Amazon DocumentDB-Prüfungsereignisse zu analysieren, zu überwachen und zu archivieren.

Amazon DocumentDB berechnet zwar keine zusätzlichen Kosten für die Aktivierung der Prüfung, Ihnen werden jedoch Standardtarife für die Nutzung von CloudWatch Logs berechnet. Informationen zu den Preisen für CloudWatch Logs finden Sie unter CloudWatch Amazon-Preise.

Die Amazon DocumentDB-Prüfungsfunktion unterscheidet sich deutlich von der Nutzung der Serviceressourcen, mit der überwacht wird. AWS CloudTrail CloudTrail zeichnet Operationen AWS-Managementkonsole auf, die mit AWS Command Line Interface (AWS CLI) oder mit Ressourcen wie Clustern, Instances, Parametergruppen und Snapshots ausgeführt werden. Die Überwachung von Ressourcen mit CloudTrail ist standardmäßig aktiviert und kann nicht deaktiviert werden. Die Amazon DocumentDB-Prüfungsfunktion ist eine optionale Funktion. Sie zeichnet Operationen auf, die innerhalb Ihres Clusters für Objekte, wie z. B. Datenbanken, Sammlungen, Indizes und Benutzer ausgeführt werden.

Themen

- Unterstützte Ereignisse

- Auditing wird aktiviert
- Auditing wird deaktiviert
- Zugriff auf Ihre Prüfereignisse
- DML-Auditereignisse filtern

Unterstützte Ereignisse

Amazon DocumentDB DocumentDB-Auditing unterstützt die folgenden Ereigniskategorien:

- Data Definition Language (DDL) — umfasst Datenbankverwaltungsvorgänge, Verbindungen, Benutzerverwaltung und Autorisierung.
- Leseereignisse (DML-Lesevorgänge) in der Data Manipulation Language — umfasst die verschiedenen Aggregationsoperatoren, arithmetischen Operatoren, booleschen Operatoren `find()` und andere Leseabfrageoperatoren.
- Schreibereignisse (DML-Schreibvorgänge) in der Data Manipulation Language — beinhaltet Operatoren `insert(), update(), delete(), bulkWrite()`

Folgende Ereignistypen werden unterstützt:

Ereignistyp	Kategorie	Description
`authCheck`	Autorisierung	Ergebniscode 0: Erfolg
		Ergebniscode 13: Unbefugte Versuche, einen Vorgang auszuführen.
`authenticate`	Connection (Verbindung)	Erfolgreiche oder fehlgeschlagene Authentifizierungsversuche bei einer neuen Verbindung.

Ereignistyp	Kategorie	Description
`auditConfigure`	DDL	Überprüfen Sie die Filterkonfiguration.
`createDatabase`	DDL	Erstellung einer neuen Datenbank.
`createCollection`	DDL	Erstellung einer neuen Sammlung innerhalb einer Datenbank.
`createIndex`	DDL	Erstellung eines neuen Index innerhalb einer Sammlung.
`dropCollection`	DDL	Löschen einer Sammlung in einer Datenbank.
`dropDatabase`	DDL	Löschen einer Datenbank.
`dropIndex`	DDL	Löschen eines Index innerhalb einer Sammlung.
`modifyChangeStreams`	DDL	Der Change-Stream wurde erstellt.
`renameCollection`	DDL	Umbenennen einer Sammlung innerhalb einer Datenbank.
`createRole`	Rollenverwaltung	Eine Rolle erstellen.

Ereignistyp	Kategorie	Description
`dropAllRolesFromDatabase`	Rollenverwaltung	Alle Rollen innerhalb einer Datenbank löschen.
`dropRole`	Rollenverwaltung	Eine Rolle löschen.
`grantPrivilegesToRole`	Rollenverwaltung	Einer Rolle Rechte gewähren.
`grantRolesToRole`	Rollenverwaltung	Einer benutzerd efinierten Rolle Rollen zuweisen
`revokePrivilegesFromRole`	Rollenverwaltung	Rechte einer Rolle entziehen
`revokeRolesFromRole`	Rollenverwaltung	Sperren von Rollen aus einer benutzerd efinierten Rolle.
`updateRole`	Rollenverwaltung	Eine Rolle aktualisi eren.
`createUser`	Benutzerverwaltung	Anlegen eines neuen Benutzers.
`dropAllUsersFromDatabase`	Benutzerverwaltung	Löschen aller Benutzer innerhalb einer Datenbank.
`dropUser`	Benutzerverwaltung	Löschen eines bestehenden Benutzers.
`grantRolesToUser`	Benutzerverwaltung	Einem Benutzer Rollen zuweisen.

Ereignistyp	Kategorie	Description
`revokeRolesFromUser`	Benutzerverwaltung	Einem Benutzer Rollen entziehen.
`updateUser`	UserManagement	Aktualisierung eines bestehenden Benutzers.
`insert`	DML schreiben	Fügt ein oder mehrere Dokumente in eine Sammlung ein.
`delete`	DML schreiben	Löscht ein oder mehrere Dokumente aus einer Sammlung.
`update`	DML, schreiben	Ändert ein vorhanden es Dokument oder Dokumente in einer Sammlung.
`bulkWrite`	DML-Schreiben	Führt mehrere Schreiboperationen mit Steuerung der Ausführungsreihenf olge aus.
`setAuditConfig`	DML-Schreiben	Legen Sie einen neuen Filter für die DML-Überwachung fest.

Ereignistyp	Kategorie	Description
`count`	DML gelesen	Gibt die Anzahl der Dokumente zurück, die einer find () -Abfrage für die Sammlung oder Ansicht entsprechen würden.
`countDocuments`	DML gelesen	Gibt die Anzahl der Dokumente zurück, die der Abfrage für eine Sammlung oder Ansicht entsprechen.
`find`	DML gelesen	Wählt Dokumente in einer Sammlung oder Ansicht aus und bringt einen Cursor zu den ausgewählten Dokumenten zurück.
`getAuditConfig`	DML gelesen	Ruft den aktuellen Filter für die DML-Überwachung ab.
`findAndModify`	DML lesen und DML schreiben	Ändert ein einzelnes Dokument und gibt es zurück.
`findOneAndDelete`	DML lesen und DML schreiben	Löscht ein einzelnes Dokument auf der Grundlage der Filter- und Sortierkr iterien und gibt das gelöschte Dokument zurück.

Ereignistyp	Kategorie	Description
`findOneAndReplace`	DML lesen und DML schreiben	Ersetzt ein einzelnes Dokument auf der Grundlage des angegebenen Filters.
`findOneAndUpdate`	DML lesen und DML schreiben	Aktualisiert ein einzelnes Dokument auf der Grundlage der Filter- und Sortierkr iterien.
`aggregate`	DML lesen und DML schreiben	Unterstützt APIs in der Aggregationspipeli ne.
`distinct`	DML gelesen	Findet die unterschi edlichen Werte für ein bestimmtes Feld in einer einzelnen Sammlung oder Ansicht und gibt die Ergebnisse in einem Array zurück.

> **Note**
>
> Die Werte im Parameterfeld des DML-Ereignisdokuments haben eine Größenbeschränkung von 1 KB. Amazon DocumentDB kürzt den Wert, wenn er 1 KB überschreitet.

> **Note**
>
> TTL-Löschereignisse werden derzeit nicht geprüft.

Auditing wird aktiviert

Die Aktivierung des Prüfens für einen Cluster ist ein zweistufiger Prozess. Stellen Sie sicher, dass beide Schritte abgeschlossen sind, da andernfalls keine Auditprotokolle an CloudWatch Logs gesendet werden.

Schritt 1. Aktivieren Sie den Clusterparameter audit_logs

Um die Überwachung zu aktivieren, müssen Sie den `audit_logs` Parameter in der Parametergruppe ändern. `audit_logs`ist eine durch Kommas getrennte Liste von Ereignissen, die protokolliert werden sollen. Ereignisse müssen in Kleinbuchstaben angegeben werden und es darf kein Leerzeichen zwischen den Listenelementen sein.

Sie können die folgenden Werte für die Parametergruppe festlegen:

Wert	Description	
`ddl`	Diese Einstellung ermöglicht die Überwachung von DDL-Ereignissen wie CreateDatabase, DropDatabase, CreateCollection, DropCollection, CreateIndex, DropIndex, AuthCheck, authenticate, createUser, DropUser, grant, revoke, updateUser und drop RolesToUser RolesFromUser AllUsersFromDatabase	
`dml_read`	Diese Einstellung ermöglicht die	

Wert	Description	
	Prüfung von DML-Leseereignissen wie find, sort count, distinct, group, projecta, unwind, GeoNear, GeoIntersects, GeoWithin und anderen MongoDB-Leseabfrageoperatoren.	
`dml_write`	Diese Einstellung ermöglicht die Überwachung von DML-Schreibereignissen wie insert (), update (), delete () und bulkWrite ()	
`all`	Wenn Sie diese Einstellung festlegen, wird die Überwachung Ihrer Datenbankereignisse wie Leseabfragen, Schreibabfragen, Datenbankaktionen und Administratoraktionen aktiviert.	
`none`	Wenn Sie diese Einstellung festlegen, wird die Überwachung deaktiviert	

Wert	Description	
`enabled` (veraltet)	Dies ist eine ältere Parametereinstellung, die 'ddl' entspricht. Diese Einstellung ermöglicht die Überwachung von DDL-Ereignissen wie CreateDatabase, DropDatabase, CreateCollection, DropCollection, CreateIndex, DropIndex, AuthCheck, AuthCheck, authenticate, createUser, DropUser, grant, revoke, updateUser und drop. RolesToUser RolesFromUser AllUsersFromDatabase Es wird nicht empfohlen, diese Einstellung zu verwenden, da es sich um eine ältere Einstellung handelt.	

Wert	Description	
`disabled` (veraltet)	Dies ist eine ältere Parametereinstellung, die „none“ entspricht. Wir empfehlen, diese Einstellung nicht zu verwenden, da es sich um eine ältere Einstellung handelt.	

> **Note**
>
> Der Standardwert für den Clusterparameter audit_logs ist `none` (legacy "`disabled`„).

Sie können die oben genannten Werte auch in Kombinationen verwenden.

Wert	Description	
`ddl, dml_read`	Wenn Sie diese Einstellung festlegen, wird die Überwachung von DDL-Ereignissen und DML-Lesee reignissen aktiviert.	
`ddl, dml_write`	Wenn Sie diese Einstellung festlegen , wird die Überwachu ng von DDL-Ereig nissen und DML-Schreibvorgängen aktiviert	
`dml_read, dml_write`	Wenn Sie diese Einstellung festlegen	

Wert	Description	
	, wird die Überwachung für alle DML-Ereignisse aktiviert	

> **Note**
>
> Eine Standardparametergruppe kann nicht abgeändert werden.

Weitere Informationen finden Sie hier:

- Amazon DocumentDB-Cluster-Parametergruppen erstellen

  Nach dem Erstellen einer Parametergruppe ändern Sie diese, indem Sie den `audit_logs`-Parameterwert auf `all` ändern.
- Amazon DocumentDB-Cluster-Parametergruppen ändern

Schritt 2. Amazon CloudWatch Logs-Export aktivieren

Wenn der Wert des `audit_logs` Cluster-Parameters`enabled`,, oder `dml_write` ist `ddl`,`dml_read`, müssen Sie Amazon DocumentDB auch für den Export von Protokollen nach Amazon CloudWatch aktivieren. Wenn Sie einen dieser Schritte auslassen, werden keine Audit-Logs an gesendet. CloudWatch

Wenn Sie einen Cluster erstellen, eine Point-in-Time-Wiederherstellung durchführen oder einen Snapshot wiederherstellen, können Sie CloudWatch Logs aktivieren, indem Sie die folgenden Schritte ausführen.

Using the AWS-Managementkonsole

Informationen zum Exportieren von Protokollen durch Amazon DocumentDB in die CloudWatch Konsole finden Sie in den folgenden Themen:

- Beim Erstellen eines Clusters — siehe Cluster erstellen: Zusätzliche Konfigurationen (Schritt 5, Protokollexporte) Erstellen eines Clusters und einer primären Instance mit dem AWS-Managementkonsole

- Beim Ändern eines vorhandenen Clusters — Ändern eines Amazon DocumentDB-Clusters
- Bei der Durchführung einer Cluster-Snapshot-Wiederherstellung — Wiederherstellung aus einem Cluster-Snapshot
- Bei der Durchführung einer Point-in-Time-Wiederherstellung — Zu einem bestimmten Zeitpunkt wiederherstellen

Using the AWS CLI

So aktivieren Sie Prüfungsprotokolle beim Erstellen eines neuen Clusters

Der folgende Code erstellt den Cluster `sample-cluster` und aktiviert CloudWatch Audit-Logs.

Example

Für Linux, macOS oder Unix:

```
aws docdb create-db-cluster \
    --db-cluster-identifier sample-cluster \
    --port 27017 \
    --engine docdb \
    --master-username master-username \
    --master-user-password password \
    --db-subnet-group-name default \
    --enable-cloudwatch-logs-exports audit
```

Für Windows:

```
aws docdb create-db-cluster ^
    --db-cluster-identifier sample-cluster ^
    --port 27017 ^
    --engine docdb ^
    --master-username master-username ^
    --master-user-password password ^
    --db-subnet-group-name default ^
    --enable-cloudwatch-logs-exports audit
```

So aktivieren Sie Prüfungsprotokolle beim Ändern eines vorhandenen Clusters

Der folgende Code ändert den Cluster `sample-cluster` und aktiviert CloudWatch Auditprotokolle.

Example

Für Linux, macOS oder Unix:

```
aws docdb modify-db-cluster \
   --db-cluster-identifier sample-cluster \
   --cloudwatch-logs-export-configuration '{"EnableLogTypes":["audit"]}'
```

Für Windows:

```
aws docdb modify-db-cluster ^
   --db-cluster-identifier sample-cluster ^
   --cloudwatch-logs-export-configuration '{"EnableLogTypes":["audit"]}'
```

Die Ausgabe dieser Operationen sieht in etwa wie folgt aus (JSON-Format).

```
{
    "DBCluster": {
        "HostedZoneId": "ZNKXH85TT8WVW",
        "StorageEncrypted": false,
        "DBClusterParameterGroup": "default.docdb4.0",
        "MasterUsername": "<user-name>",
        "BackupRetentionPeriod": 1,
        "Port": 27017,
        "VpcSecurityGroups": [
            {
                "Status": "active",
                "VpcSecurityGroupId": "sg-77186e0d"
            }
        ],
        "DBClusterArn": "arn:aws:rds:us-east-1:900083794985:cluster:sample-cluster",
        "Status": "creating",
        "Engine": "docdb",
        "EngineVersion": "4.0.0",
        "MultiAZ": false,
        "AvailabilityZones": [
            "us-east-1a",
            "us-east-1c",
            "us-east-1f"
        ],
        "DBSubnetGroup": "default",
        "DBClusterMembers": [],
```

```
        "ReaderEndpoint": "sample-cluster.cluster-ro-corcjozrlsfc.us-
east-1.docdb.amazonaws.com",
        "EnabledCloudwatchLogsExports": [
            "audit"
        ],
        "PreferredMaintenanceWindow": "wed:03:08-wed:03:38",
        "AssociatedRoles": [],
        "ClusterCreateTime": "2019-02-13T16:35:04.756Z",
        "DbClusterResourceId": "cluster-YOS52CUXGDTNKDQ7DH72I4LED4",
        "Endpoint": "sample-cluster.cluster-corcjozrlsfc.us-
east-1.docdb.amazonaws.com",
        "PreferredBackupWindow": "07:16-07:46",
        "DBClusterIdentifier": "sample-cluster"
    }
}
```

Auditing wird deaktiviert

Sie können die Überwachung deaktivieren, indem Sie den CloudWatch Protokollexport und den `audit_logs` Parameter deaktivieren.

Den Export von Protokollen deaktivieren CloudWatch

Sie können den Export von Auditprotokollen entweder mit dem AWS-Managementkonsole oder dem AWS CLI deaktivieren.

Using the AWS-Managementkonsole

Das folgende Verfahren verwendet die AWS-Managementkonsole , um den Export von Protokollen durch Amazon DocumentDB zu CloudWatch deaktivieren.

So deaktivieren Sie Prüfungsprotokolle

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Klicken Sie im Navigationsbereich auf Cluster. Wählen Sie anschließend die Schaltfläche links neben dem Namen des Clusters aus, für den Sie das Exportieren von Protokollen deaktivieren möchten.
3. Wählen Sie Actions (Aktionen) und dann Modify (Ändern) aus.

4. Scrollen Sie nach unten zum Abschnitt Log exports (Protokollexporte) und wählen Sie Disabled (Deaktiviert) aus.
5. Klicken Sie auf Weiter.
6. Überprüfen Sie Ihre Änderungen. Wählen Sie anschließend den Zeitpunkt aus, an dem diese Änderung auf Ihren Cluster angewendet werden soll.
   - Apply during the next scheduled maintenance window (Anwendung während des nächsten geplanten Wartungsfensters)
   - Apply immediately (Sofort anwenden)
7. Wählen Sie Cluster bearbeiten aus.

Using the AWS CLI

Der folgende Code ändert den Cluster `sample-cluster` und deaktiviert CloudWatch Audit-Logs.

Example

Für Linux, macOS oder Unix:

```
aws docdb modify-db-cluster \
   --db-cluster-identifier sample-cluster \
   --cloudwatch-logs-export-configuration '{"DisableLogTypes":["audit"]}'
```

Für Windows:

```
aws docdb modify-db-cluster ^
   --db-cluster-identifier sample-cluster ^
   --cloudwatch-logs-export-configuration '{"DisableLogTypes":["audit"]}'
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus (JSON-Format).

```
{
    "DBCluster": {
        "DBClusterParameterGroup": "default.docdb4.0",
        "HostedZoneId": "ZNKXH85TT8WVW",
        "MasterUsername": "<user-name>",
        "Status": "available",
        "Engine": "docdb",
        "Port": 27017,
```

```
        "AvailabilityZones": [
            "us-east-1a",
            "us-east-1c",
            "us-east-1f"
        ],
        "EarliestRestorableTime": "2019-02-13T16:35:50.387Z",
        "DBSubnetGroup": "default",
        "LatestRestorableTime": "2019-02-13T16:35:50.387Z",
        "DBClusterArn": "arn:aws:rds:us-east-1:900083794985:cluster:sample-
cluster2",
        "Endpoint": "sample-cluster2.cluster-corcjozrlsfc.us-
east-1.docdb.amazonaws.com",
        "ReaderEndpoint": "sample-cluster2.cluster-ro-corcjozrlsfc.us-
east-1.docdb.amazonaws.com",
        "BackupRetentionPeriod": 1,
        "EngineVersion": "4.0.0",
        "MultiAZ": false,
        "ClusterCreateTime": "2019-02-13T16:35:04.756Z",
        "DBClusterIdentifier": "sample-cluster2",
        "AssociatedRoles": [],
        "PreferredBackupWindow": "07:16-07:46",
        "DbClusterResourceId": "cluster-YOS52CUXGDTNKDQ7DH72I4LED4",
        "StorageEncrypted": false,
        "PreferredMaintenanceWindow": "wed:03:08-wed:03:38",
        "DBClusterMembers": [],
        "VpcSecurityGroups": [
            {
                "Status": "active",
                "VpcSecurityGroupId": "sg-77186e0d"
            }
        ]
    }
}
```

Deaktivierung des Parameters audit_logs

Um den Parameter `audit_logs` für Ihren Cluster zu deaktivieren, können Sie den Cluster so ändern, dass er eine Parametergruppe mit dem Wert `disabled` für den Parameter `audit_logs` verwendet. Sie können auch den Wert des Parameters `audit_logs` in der Parametergruppe des Clusters in `disabled` ändern.

Weitere Informationen finden Sie unter den folgenden Themen:

- Ändern eines Amazon DocumentDB-Clusters
- Amazon DocumentDB-Cluster-Parametergruppen ändern

Zugriff auf Ihre Prüfereignisse

Gehen Sie wie folgt vor, um auf Ihre Prüfereignisse bei Amazon zuzugreifen CloudWatch.

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Stellen Sie sicher, dass Sie sich in derselben Region wie Ihr Amazon DocumentDB-Cluster befinden.
3. Wählen Sie im Navigationsbereich Protokolle aus.
4. Um die Prüfprotokolle für Ihren Cluster zu finden, suchen Sie in der Liste und wählen Sie **`/aws/docdb/`*`yourClusterName`*`/audit`** aus.

   Die Prüfereignisse für Ihre Instances sind unter dem jeweiligen Instance-Namen verfügbar.

DML-Auditereignisse filtern

Erste Schritte mit der DML-Auditfilterung

DML-Prüfereignisse können gefiltert werden, bevor sie an Amazon CloudWatch geschrieben werden. Um diese Funktion nutzen zu können, müssen das Auditprotokoll und die DML-Protokollierung aktiviert sein. Amazon DocumentDB unterstützt das Filtern nach `atypecommand`,`user`,`namespace`, und`auditAuthorizationSuccess`.

> **Note**
>
> DDL-Ereignisse werden nicht gefiltert.

Sie können die Überwachungsfilterung jederzeit aktivieren, indem Sie den Überwachungsfilter mithilfe der `auditAuthorizationSuccess` Parameter `setAuditConfigfilter`, und im `db.adminCommand( { command } )` Vorgang angeben:

```
db.admin.runCommand(
   {
```

```
      setAuditConfig: 1,
      filter:
         {
            //filter conditions
         },
      auditAuthorizationSuccess: true | false
   }
)
```

Sie können die Auditfiltereinstellungen auch abrufen, indem Sie den folgenden Befehl ausführen:

```
db.admin.runCommand( { getAuditConfig: 1})
```

Sicherheitsanforderungen

Nur Datenbanken users/roles mit privilegierten Aktionen `auditConfigure` können die oben genannten Befehle ausführen, `admin`db wenn sie DML-Auditfilter setzen oder auflisten. Sie können entweder eine der integrierten Rollen von [`clusterAdmin`,`hostManager`,`root`] verwenden oder benutzerdefinierte Rollen mit `auditConfigure` Rechten erstellen. Im Folgenden finden Sie ein Beispiel für die Verwendung vorhandener Rollen mit dieser `auditConfigure` Berechtigung und ein Beispiel für benutzerdefinierte Rollen.

Benutzer mit integrierter Rolle:

```
use admin
db.createUser(
  {
    user: "myClusterAdmin",
    pwd: "password123",
    roles: [ { role: "clusterAdmin", db: "admin" } ]
  }
)
```

Benutzer mit benutzerdefinierten Rollen:

```
use admin
db.createRole(
   {
     role: "myRole",
     privileges: [
```

```
       { resource: { cluster: true }, actions: [ "auditConfigure" ] }
     ],
     roles: []
   }
)
db.createUser(
  {
    user: "myUser",
    pwd: "myPassword",
    roles: [ { role: "myRole", db: "admin" } ]
  }
)
```

Anwendungsfälle filtern

Beispiel: Ereignisse nach Befehlen filtern

```
db.admin.runCommand(
   {
      setAuditConfig: 1,
      filter: {
        "$and": [
         {
            "param.command":
               {
                  $in: [ "find","count", "insert", "delete", "update",
 "findandmodify" ]
               }
         }
         ]
      },
      auditAuthorizationSuccess: true
   }
)
```

Beispiel: Ereignisse nach Benutzernamen filtern

In diesem Beispiel wird nur der Benutzer „MyUser“ protokolliert:

```
db.admin.runCommand(
   {
      setAuditConfig: 1,
      filter: {
```

```
      "$and": [
         {
            "param.user":
               {
                  $in: [ "myUser" ]
               }
         }
         ]},
      auditAuthorizationSuccess: true})
```

Beispiel: Filtern nach **`atype`**

```
db.admin.runCommand(
   {
      setAuditConfig: 1,
      filter: {atype: "authCheck"},
      auditAuthorizationSuccess: true
   })
```

> **Note**
>
> Alle DML-Protokolle haben `authCheck` als`atype`. Nur DDL hat eine andere. `atype` Wenn Sie einen anderen Wert als `authCheck` in den eingeben`filter`, wird kein DML-Login erzeugt. CloudWatch

Beispiel: Filterung mithilfe mehrerer Filter, die durch Operatoren miteinander verbunden sind

```
db.admin.runCommand(
   {
      setAuditConfig: 1,
      filter: {
      "$and": [
         {
            "param.command":
               {
                  $in: [ "find","count", "insert", "delete", "update",
 "findandmodify" ]
               }
         }
         ],
```

```
       "$nor": [
         {
            "param.command":
               {
                  $in: ["count", "insert", "delete", "update", "findandmodify" ]
               }
         }]
       },
      auditAuthorizationSuccess: true})
```

> **Note**
>
> Auf der obersten Ebene `$nor` werden nur `$and``$or`, und unterstützt. Alle anderen Operatoren werden nicht unterstützt und verursachen einen Fehler.

Beispiel: Filterung nach Ereignissen nach **`auditAuthorizationSuccess`**

In diesem Filter werden alle Befehle, die die Autorisierung erfolgreich bestanden haben, nicht protokolliert:

```
db.admin.runCommand(
   {
      setAuditConfig: 1,
      filter: {},
      auditAuthorizationSuccess: false
   }
)
```

Beispiel: Filtern mit **`$in`** und **`$nin`** Bedingungen

Wenn `$in` sowohl in als auch verwendet wird`$nin`, wird der Befehl nicht protokolliert, da zwischen den Bedingungen ein implizites „und“ steht. In diesem Beispiel blockiert Regex den `find` Befehl, sodass nichts protokolliert wird:

```
db.admin.runCommand(
   {
      setAuditConfig: 1,
      filter: {
      "$and": [
         {
```

```
            atype: "authCheck",
            "param.command":
               {
                  $in: [ "find", "insert", "delete", "update", "findandmodify" ],
                  $nin: ["count", "insert", "delete", "update", "findandmodify" ],
                  $not: /^^find.*/
               }
         },
         ],
       "$or": [
         {
            "param.command":
               {
                  $nin: ["count", "insert", "delete", "update", "findandmodify" ]
               }
         }]
       },
      auditAuthorizationSuccess: true})
```

Beispiel: Filtern nach **`namespace`**

```
db.admin.runCommand(
   {
      setAuditConfig: 1,
      filter: {
      "$and": [
         {
            "param.ns":
               {
                  $in: [ "test.foo" ]
               }
         }
         ]},
      auditAuthorizationSuccess: true})
```

Beispiel: Auf den Standardfilter zurücksetzen

Das Zurücksetzen auf den Standardwert bedeutet, dass jedes DML-Auditereignis protokolliert wird. Führen Sie den folgenden Befehl aus, um die Filterung auf den Standardwert zurückzusetzen:

```
db.admin.runCommand(
   {
```

```
      setAuditConfig: 1,
      filter: {},
      auditAuthorizationSuccess: true
   }
)
```

Amazon VPC und Amazon DocumentDB

Amazon Virtual Private Cloud (Amazon VPC) ermöglicht es Ihnen, AWS Ressourcen wie Amazon DocumentDB DocumentDB-Instances in einer Virtual Private Cloud (VPC) zu starten.

Wenn Sie eine VPC verwenden, haben Sie die Kontrolle über Ihre virtuelle Netzwerkumgebung. Sie können Ihren eigenen IP-Adressbereich auswählen, Subnetze erstellen sowie Routing-Tabellen und Zugriffskontrolllisten konfigurieren. Für den Betrieb Ihres Clusters in einer VPC fallen keine zusätzlichen Kosten an.

Konten haben eine Standard-VPC. Alle neuen Cluster werden in der Standard-VPC erstellt, sofern Sie nichts anderes angeben.

Topics

- DocumentDB-Cluster in einer VPC
- Zugreifen auf einen Amazon DocumentDB-Cluster in einer VPC
- Erstellen Sie eine IPv4-only VPC zur Verwendung mit einem DocumentDB-Cluster
- Erstellen Sie eine Dual-Stack-VPC zur Verwendung mit einem DocumentDB-Cluster

Im Folgenden finden Sie eine Diskussion über VPC-Funktionen, die für Amazon DocumentDB-Cluster relevant sind. Weitere Informationen zur Amazon VPC-Sicherheit finden Sie unter Sicherheit im Amazon VPC-Benutzerhandbuch.

DocumentDB-Cluster in einer VPC

Ihr Amazon DocumentDB-Cluster befindet sich in einer Virtual Private Cloud (VPC). Eine VPC ist ein virtuelles Netzwerk, das logisch von anderen virtuellen Netzwerken in der isoliert ist. AWS Cloud Amazon VPC ermöglicht es Ihnen, AWS Ressourcen wie einen Amazon DocumentDB-Cluster oder eine Amazon EC2 EC2-Instance in einer VPC zu starten. Bei der VPC kann es sich um die mit Ihrem Konto verknüpfte Standard-VPC oder eine von Ihnen erstellte VPC handeln. Alle VPCs sind mit Ihrem Konto verknüpft. AWS

Die Standard-VPC besitzt drei Subnetze, mit denen Sie Ressourcen innerhalb der VPC separieren können. Zudem verfügt die Standard-VPC über ein Internet-Gateway, mit dem Sie den externen Zugriff auf Ressourcen in der VPC gewähren können.

Szenarien mit Amazon DocumentDB-Clustern in einer VPC und außerhalb einer VPC finden Sie unter. Zugreifen auf einen Amazon DocumentDB-Cluster in einer VPC

Topics

- Arbeiten mit Clustern in einer VPC
- Arbeiten mit Subnetzgruppen
- Amazon DocumentDB DocumentDB-IP-Adressierung
- Erstellen eines Clusters in einer VPC

Arbeiten mit Clustern in einer VPC

Hier sind einige Tipps zur Arbeit mit einem Cluster in einer VPC:

- Ihre VPC muss mindestens zwei Subnetze besitzen. Diese Subnetze müssen sich in zwei verschiedenen Availability Zones in dem Bereich befinden AWS-Region , in dem Sie Ihren Cluster bereitstellen möchten. Ein Subnetz ist ein Segment des IP-Adressbereichs einer VPC, das Sie angeben und das Sie verwenden können, um Cluster auf der Grundlage Ihrer Sicherheits- und Betriebsanforderungen zu gruppieren.
- Wenn Sie möchten, dass Ihr Cluster in der VPC öffentlich zugänglich ist, stellen Sie sicher, dass Sie die VPC-Attribute `DNS hostnames` und aktivieren. `DNS resolution`
- Ihre VPC muss über eine Subnetzgruppe verfügen, die Sie erstellen. Sie erstellen eine Subnetzgruppe, indem Sie die von Ihnen erstellten Subnetze angeben. Amazon DocumentDB wählt ein Subnetz und eine IP-Adresse innerhalb dieser Subnetzgruppe aus, um sie der primären Instance in Ihrem Cluster zuzuordnen. Die primäre Instance verwendet die Availability Zone, die das Subnetz enthält.
- Ihre VPC muss über eine VPC-Sicherheitsgruppe verfügen, die den Zugriff auf den Cluster ermöglicht.

  Weitere Informationen finden Sie unter Zugreifen auf einen Amazon DocumentDB-Cluster in einer VPC.
- Die CIDR-Blöcke in jedem Ihrer Subnetze müssen groß genug sein, um Reserve-IP-Adressen aufzunehmen, die Amazon DocumentDB bei Wartungsaktivitäten, einschließlich Failover und

Rechenskalierung, verwenden kann. Zum Beispiel ein Bereich wie 10.0.0. 0/24 und 10.0.1. 0/24 ist normalerweise groß genug.

- Eine VPC kann das `instance tenancy` Attribut entweder `default` oder `dedicated` haben. Bei allen Standard-VPCs ist das `instance tenancy` Attribut auf default gesetzt, und eine Standard-VPC kann jede Instance-Klasse unterstützen.

  Wenn Sie sich dafür entscheiden, Ihren Cluster in einer dedizierten VPC zu haben, auf die das `instance tenancy` Attribut gesetzt ist`dedicated`, muss die Instance-Klasse Ihres Clusters einer der zugelassenen Amazon EC2 EC2-Dedicated Instance-Typen sein. Beispielsweise entspricht die dedizierte `r5.large` EC2-Instance der `db.r5.large` Instance-Klasse. Informationen zur Instance-Tenancy in einer VPC finden Sie unter Amazon EC2 EC2-Instances im Amazon Elastic Compute Cloud-Benutzerhandbuch.

  Weitere Informationen zu Instance-Typen, die in einer Dedicated Instance enthalten sein dürfen, finden Sie unter Amazon EC2 Dedicated Instances auf der Preisseite für Amazon EC2.

  > **Note**
  >
  > Wenn Sie das `instance tenancy` Attribut `dedicated` für einen Cluster auf setzen, garantiert dies nicht, dass der Cluster auf einem dedizierten Host ausgeführt wird.

Arbeiten mit Subnetzgruppen

Subnetze sind Segmente eines IP-Adressbereichs der VPC, die Sie festlegen und mit denen Sie basierend auf Ihren Sicherheits- und Betriebsanforderungen Ressourcen gruppieren können. Eine Subnetzgruppe ist eine Sammlung von Subnetzen (normalerweise privat), die Sie in einer VPC erstellen und die Sie dann für Ihre Cluster festlegen. Durch die Verwendung einer Subnetzgruppe können Sie eine bestimmte VPC angeben, wenn Sie Cluster mit der AWS CLI oder der Amazon DocumentDB DocumentDB-API erstellen. Wenn Sie die Konsole verwenden, können Sie die VPC und Subnetze auswählen, die Sie verwenden möchten.

Jede Subnetzgruppe sollte Subnetze in mindestens zwei Availability Zones in einer bestimmten Zone haben. AWS-Region Wenn Sie einen Cluster in einer VPC erstellen, wählen Sie eine Subnetzgruppe dafür aus. Aus der Subnetzgruppe wählt Amazon DocumentDB ein Subnetz und eine IP-Adresse innerhalb dieses Subnetzes aus, um sie der primären Instance in Ihrem Cluster zuzuordnen. Die Datenbank verwendet die Availability Zone, die das Subnetz enthält. DocumentDB weist immer eine IP-Adresse aus einem Subnetz zu, das über freien IP-Adressraum verfügt.

Die Subnetze in einer Subnetzgruppe sind entweder öffentlich oder privat, abhängig von der Konfiguration, die Sie für ihre Netzwerkzugriffskontrolllisten (Netzwerk-ACLs) und Routingtabellen festgelegt haben. Damit ein Cluster öffentlich zugänglich ist, müssen alle Subnetze in seiner Subnetzgruppe öffentlich sein. Wenn ein Subnetz, das einem öffentlich zugänglichen Cluster zugeordnet ist, von öffentlich zu privat wechselt, kann sich dies auf die Clusterverfügbarkeit auswirken.

Um eine Subnetzgruppe zu erstellen, die den Dual-Stack-Modus unterstützt, stellen Sie sicher, dass jedem Subnetz, das Sie der Subnetzgruppe hinzufügen, ein IPv6-CIDR-Block (Internet Protocol Version 6) zugeordnet ist. Weitere Informationen finden Sie unter Amazon DocumentDB DocumentDB-IP-Adressierung und IPv6-Unterstützung für Ihre VPC im Amazon Virtual Private Cloud Cloud-Benutzerhandbuch.

Wenn Amazon DocumentDB einen Cluster in einer VPC erstellt, weist es dem Cluster mithilfe einer IP-Adresse aus Ihrer Subnetzgruppe eine Netzwerkschnittstelle zu. Wir empfehlen jedoch dringend, den DNS-Namen (Domain Name System) zu verwenden, um eine Verbindung zu Ihrem Cluster herzustellen. Wir empfehlen dies, da sich die zugrunde liegende IP-Adresse während des Failovers ändert.

> **Note**
>
> Stellen Sie sicher, dass Sie für jeden Cluster, den Sie in einer VPC ausführen, mindestens eine Adresse in jedem Subnetz der Subnetzgruppe für die Verwendung durch Amazon DocumentDB für Wiederherstellungsaktionen reservieren.

Gemeinsam genutzte Subnetze

Sie können einen Cluster in einer gemeinsam genutzten VPC erstellen.

Einige Aspekte, die Sie bei der Verwendung gemeinsam genutzter VPCs beachten sollten:

- Sie können einen Cluster von einem gemeinsam genutzten VPC-Subnetz in ein nicht gemeinsam genutztes VPC-Subnetz verschieben und umgekehrt.
- Teilnehmer einer gemeinsam genutzten VPC müssen eine Sicherheitsgruppe in der VPC erstellen, damit sie einen Cluster erstellen können.
- Besitzer und Teilnehmer einer gemeinsam genutzten VPC können mithilfe von DocumentDB-Abfragen auf die Datenbank zugreifen. Allerdings kann nur der Ersteller einer Ressource beliebige API-Aufrufe für die Ressource tätigen.

Amazon DocumentDB DocumentDB-IP-Adressierung

IP-Adressen ermöglichen es Ressourcen in Ihrer VPC untereinander und mit Ressourcen im Internet zu kommunizieren. Amazon DocumentDB unterstützt sowohl IPv4- als auch IPv6-Adressierungsprotokolle. Standardmäßig verwenden Amazon DocumentDB und Amazon VPC das IPv4-Adressierungsprotokoll. Sie können dieses Standardverhalten nicht deaktivieren. Wenn Sie eine VPC erstellen, müssen Sie einen IPv4 CIDR-Block (einen privaten IPv4-Adressenbereich) angeben. Sie können Ihrer VPC und Ihren Subnetzen optional einen IPv6-CIDR-Block und Clustern in Ihrem Subnetz IPv6-Adressen aus diesem Block zuweisen.

> **Note**
>
> Dual-stack Modus (IPv6-Adressierung) wird nur in den Amazon DocumentDB DocumentDB-Versionen 4.0 und 5.0 unterstützt.

Durch die Unterstützung des IPv6-Protokolls wird die Anzahl der unterstützten IP-Adressen erweitert. Durch die Verwendung des IPv6-Protokolls stellen Sie sicher, dass Sie über ausreichende verfügbare Adressen für das künftige Wachstum des Internets verfügen. Neue und bestehende DocumentDB-Ressourcen können IPv4- und IPv6-Adressen in Ihrer VPC verwenden. Das Konfigurieren, Sichern und Übersetzen des Netzwerkverkehrs zwischen den beiden Protokollen, die in verschiedenen Teilen einer Anwendung verwendet werden, können den Betriebsaufwand erhöhen. Sie können das IPv6-Protokoll für Amazon DocumentDB DocumentDB-Ressourcen standardisieren, um Ihre Netzwerkkonfiguration zu vereinfachen.

Topics

- IPv4-Adressen
- IPv6-Adressen
- Dual-stack Modus

IPv4-Adressen

Beim Erstellen einer VPC müssen Sie für diese einen IPv4-Adressbereich in Form eines CIDR-Blocks wie `10.0.0.0/16` festlegen. Eine Subnetzgruppe definiert den Bereich von IP-Adressen in diesem CIDR-Block, den ein Cluster verwenden kann. Diese IP-Adressen können privat oder öffentlich sein.

Eine private IPv4-Adresse ist eine IP-Adresse, die nicht über das Internet erreichbar ist. Sie können private IPv4-Adressen für die Kommunikation zwischen Ihrem Cluster und anderen Ressourcen wie

Amazon EC2 EC2-Instances in derselben VPC verwenden. Jeder Cluster hat eine private IP-Adresse für die Kommunikation in der VPC.

Eine öffentliche IP-Adresse ist eine IPv4-Adresse, die über das Internet erreichbar ist. Öffentliche IP-Adressierung ist für Ihren DocumentDB-Cluster nicht zulässig. Jede öffentliche IP-Adresse sollte vom Internet-Gateway und von EC2 im öffentlichen Subnetz aufgelöst werden.

Informationen zum Erstellen einer VPC mit nur privaten IPv4-Adressen, die Sie für ein gängiges Amazon DocumentDB-Szenario verwenden können, finden Sie unter. Erstellen Sie eine IPv4-only VPC zur Verwendung mit einem DocumentDB-Cluster

IPv6-Adressen

Optional können Sie Ihrer VPC und den Subnetzen einen IPv6 CIDR-Block zuordnen und den Ressourcen in Ihrer VPC IPv6-Adressen von diesem Block zuweisen. Jede IPv6-Adresse ist global eindeutig.

Der IPv6 CIDR-Block für Ihre VPC wird automatisch aus dem Amazon-Pool mit IPv6-Adressen zugewiesen. Sie können den Bereich nicht selbst auswählen.

Stellen Sie beim Herstellen einer Verbindung mit einer IPv6-Adresse sicher, dass die folgenden Bedingungen erfüllt sind:

- Der Client ist so konfiguriert, dass der Datenverkehr zwischen Client und Datenbank über IPv6 erlaubt ist.
- Die vom Cluster verwendeten DocumentDB-Sicherheitsgruppen sind korrekt konfiguriert, sodass Datenverkehr zwischen Clients und Datenbanken über IPv6 zulässig ist.
- Der Client-Betriebssystemstapel ermöglicht den Datenverkehr über die IPv6-Adresse, und die Betriebssystemtreiber und Bibliotheken sind so konfiguriert, dass sie den richtigen Standard-Cluster-Endpunkt (entweder IPv4 oder IPv6) auswählen.

Weitere Informationen zu IPv6 finden Sie unter IP-Adressierung im Amazon Virtual Private Cloud Cloud-Benutzerhandbuch.

Dual-stack Modus

Wenn ein Cluster sowohl über die IPv4- als auch über die IPv6-Adressierungsprotokolle kommunizieren kann, wird er im Dual-Stack-Modus ausgeführt. Ressourcen können also über IPv4, IPv6 oder beides mit dem Cluster kommunizieren. DocumentDB deaktiviert den Internet-Gateway-

Zugriff für IPv6-Endpunkte von privaten Clustern im Dual-Stack-Modus. DocumentDB tut dies, um sicherzustellen, dass Ihre IPv6-Endpunkte privat sind und nur von Ihrer VPC aus darauf zugegriffen werden kann.

Topics

- Dual-stack Modus und Subnetzgruppen
- Arbeiten mit Clustern im Dual-Stack-Modus
- Ändern von IPv4-only Clustern für die Verwendung des Dual-Stack-Modus
- Dual-stack Modus, Region und Verfügbarkeit der Version
- Einschränkungen für Dual-Stack-Netzwerkcluster

Dual-stack Modus und Subnetzgruppen

Um den Dual-Stack-Modus zu verwenden, stellen Sie sicher, dass jedem Subnetz in der Subnetzgruppe, die Sie dem Cluster zuordnen, ein IPv6-CIDR-Block zugeordnet ist. Sie können eine neue Subnetzgruppe erstellen oder eine bestehende Subnetzgruppe ändern, um diese Anforderung zu erfüllen. Sobald sich ein Cluster im Dual-Stack-Modus befindet, können sich Clients normal mit ihm verbinden. Stellen Sie sicher, dass Client Security-Firewalls und DocumentDB-Cluster-Sicherheitsgruppen korrekt konfiguriert sind, um Datenverkehr über IPv6 zuzulassen. Um eine Verbindung herzustellen, verwenden die Clients den Endpunkt des Clusters. Clientanwendungen können angeben, welches Protokoll bevorzugt wird, wenn eine Verbindung mit einer Datenbank hergestellt wird. Im Dual-Stack-Modus erkennt der Cluster das bevorzugte Netzwerkprotokoll des Clients, entweder IPv4 oder IPv6, und verwendet dieses Protokoll für die Verbindung.

Wenn eine Subnetzgruppe den Dual-Stack-Modus nicht mehr unterstützt, weil das Subnetz gelöscht oder die CIDR-Verbindung getrennt wurde, besteht das Risiko eines inkompatiblen Netzwerkstatus für Cluster, die der Subnetzgruppe zugeordnet sind. Außerdem können Sie die Subnetzgruppe nicht verwenden, wenn Sie einen neuen Cluster im Dual-Stack-Modus erstellen.

Um mithilfe von festzustellen, ob eine Subnetzgruppe den Dual-Stack-Modus unterstützt AWS-Managementkonsole, sehen Sie sich den Netzwerktyp auf der Detailseite der Subnetzgruppe an. Um mithilfe von zu ermitteln, ob eine Subnetzgruppe den Dual-Stack-Modus unterstützt AWS CLI, führen Sie den `describe-db-subnet-groups`Befehl aus und sehen Sie sich die Ausgabe an. `SupportedNetworkTypes`

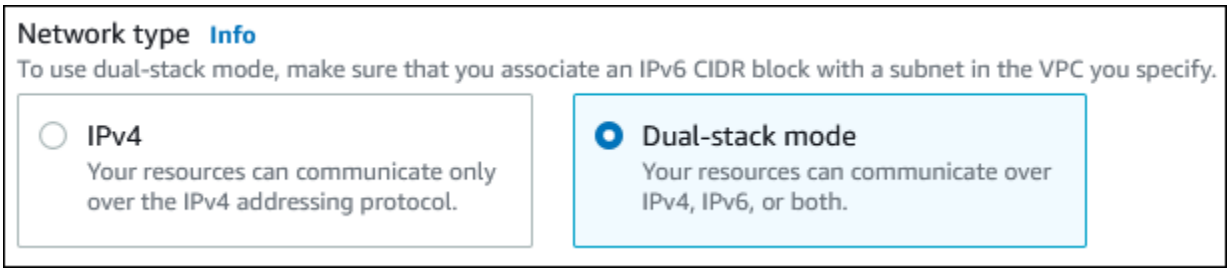
Read Replicas werden als unabhängige Cluster behandelt und können einen anderen Netzwerktyp als der primäre Cluster haben. Wenn Sie den Netzwerktyp des primären Clusters einer Read Replica

ändern, ist die Read Replica davon nicht betroffen. Wenn Sie einen Cluster wiederherstellen, können Sie ihn auf jedem unterstützten Netzwerktyp wiederherstellen.

Arbeiten mit Clustern im Dual-Stack-Modus

Wenn Sie einen Cluster erstellen oder ändern, können Sie den Dual-Stack-Modus angeben, damit Ihre Ressourcen über IPv4, IPv6 oder beides mit Ihrem Cluster kommunizieren können.

Wenn Sie den verwenden AWS-Managementkonsole , um einen Cluster zu erstellen oder zu ändern, können Sie den Dual-Stack-Modus im Abschnitt Netzwerktyp angeben. Die folgende Abbildung zeigt den Abschnitt Netzwerktyp in der Konsole:



Wenn Sie den AWS CLI zum Erstellen oder Ändern eines Clusters verwenden, stellen Sie die `--network-type` Option `DUAL` auf Dual-Stack-Modus ein. Wenn Sie die DocumentDB-API verwenden, um einen Cluster zu erstellen oder zu ändern, setzen Sie den `NetworkType` Parameter auf, um den Dual-Stack-Modus `DUAL` zu verwenden. Wenn der Dual-Stack-Modus von der angegebenen DocumentDB-Engine-Version oder Subnetzgruppe nicht unterstützt wird, wird der `NetworkTypeNotSupported` Fehler zurückgegeben.

Weitere Informationen zum Erstellen eines Clusters finden Sie unter. Einen Amazon DocumentDB-Cluster erstellen Weitere Informationen zum Ändern eines Clusters finden Sie unterÄndern eines Amazon DocumentDB-Clusters.

Um mithilfe der Konsole festzustellen, ob sich ein Cluster im Dual-Stack-Modus befindet, sehen Sie sich den Netzwerktyp auf der Registerkarte Konnektivität und Sicherheit für den Cluster an.

Ändern von IPv4-only Clustern für die Verwendung des Dual-Stack-Modus

Sie können einen IPv4-only Cluster so ändern, dass er den Dual-Stack-Modus verwendet. Ändern Sie dazu den Netzwerktyp des Clusters.

Es wird empfohlen, den Netzwerktyp Ihres Amazon DocumentDB-Clusters während eines Wartungsfensters zu ändern. Sie können den Netzwerktyp manuell festlegen, indem Sie den `modify-db-cluster`Befehl verwenden.

Bevor Sie einen Cluster für den Dual-Stack-Modus ändern, stellen Sie sicher, dass seine Subnetzgruppe den Dual-Stack-Modus unterstützt. Wenn die dem Cluster zugeordnete Subnetzgruppe den Dual-Stack-Modus nicht unterstützt, geben Sie bei der Änderung des Clusters eine andere Subnetzgruppe an, die ihn unterstützt. Das Ändern der Subnetzgruppe eines Clusters kann zu Ausfallzeiten führen.

Wenn Sie die Subnetzgruppe eines Clusters ändern, bevor Sie den Cluster auf den Dual-Stack-Modus umstellen, stellen Sie sicher, dass die Subnetzgruppe vor und nach der Änderung für den Cluster gültig ist.

Es wird empfohlen, den `ModifyDBCluster` Anruf nur mit dem `NetworkType` Parameter auf auszuführen, um das Netzwerk in den Dual-Stack-Modus `DUAL` zu ändern. Das Hinzufügen weiterer Parameter zusammen mit `NetworkType` demselben API-Aufruf kann zu Ausfallzeiten führen. Wenn Sie mehrere Parameter ändern möchten, stellen Sie sicher, dass die Änderung des Netzwerktyps erfolgreich abgeschlossen wurde, bevor Sie eine weitere `ModifyDBCluster`-Anforderung mit anderen Parametern senden.

Wenn Sie nach der Änderung keine Verbindung zum Cluster herstellen können, stellen Sie sicher, dass die Client- und Datenbanksicherheitsfirewalls und Routing-Tabellen korrekt konfiguriert sind, sodass der Datenverkehr zur Datenbank im ausgewählten Netzwerk (entweder IPv4 oder IPv6) zugelassen wird. Möglicherweise müssen Sie auch Betriebssystemparameter, Bibliotheken oder Treiber ändern, um eine Verbindung mithilfe einer IPv6-Adresse herzustellen.

Um einen IPv4-only Cluster so zu ändern, dass er den Dual-Stack-Modus verwendet

1. Ändern Sie eine Subnetzgruppe, sodass sie den Dual-Stack-Modus unterstützt, oder erstellen Sie eine Subnetzgruppe, die den Dual-Stack-Modus unterstützt:

   a. Ordnen Sie Ihrer VPC einen IPv6-CIDR-Block zu.

      Anweisungen finden Sie unter Hinzufügen oder Entfernen eines CIDR-Blocks zu Ihrer VPC im Amazon VPC-Benutzerhandbuch.

   b. Hängen Sie den IPv6-CIDR-Block an alle Subnetze in Ihrer Subnetzgruppe an.

      Anweisungen finden Sie unter Hinzufügen oder Entfernen eines IPv6-CIDR-Blocks zu Ihrem Subnetz im Amazon Virtual Private Cloud Cloud-Benutzerhandbuch.

   c. Vergewissern Sie sich, dass die Subnetzgruppe den Dual-Stack-Modus unterstützt.

      Wenn Sie den verwenden AWS-Managementkonsole, wählen Sie die Subnetzgruppe aus und stellen Sie sicher, dass der Wert Unterstützte Netzwerktypen auf Dual gesetzt ist.

Wenn Sie den verwenden AWS CLI, führen Sie den `describe-db-subnet-groups`Befehl aus und stellen Sie sicher, dass der `SupportedNetworkType` Wert für den Cluster lautet`Dual`.

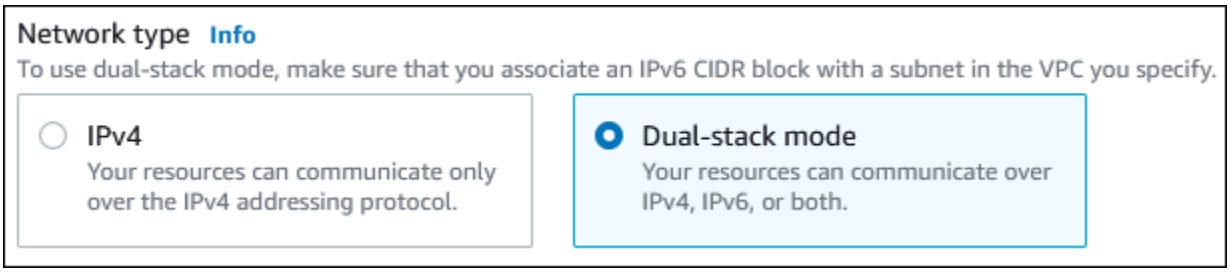
2. Ändern Sie die dem Cluster zugeordnete Sicherheitsgruppe, um IPv6-Verbindungen zur Datenbank zuzulassen, oder erstellen Sie eine neue Sicherheitsgruppe, die IPv6-Verbindungen zulässt.

   Anweisungen finden Sie unter Sicherheitsgruppenregeln im Amazon Virtual Private Cloud Cloud-Benutzerhandbuch.

3. Ändern Sie den Cluster so, dass er den Dual-Stack-Modus unterstützt. Stellen Sie dazu den Netzwerktyp auf Dual-stack Modus ein.

   Wenn Sie die Konsole verwenden, stellen Sie sicher, dass die folgenden Einstellungen korrekt sind:

   - Netzwerktyp — Dual-stack Modus

   - Subnetzgruppe — Die Subnetzgruppe, die Sie in einem vorherigen Schritt konfiguriert haben
   - Sicherheitsgruppe — Die Sicherheit, die Sie in einem vorherigen Schritt konfiguriert haben

   Wenn Sie die verwenden AWS CLI, stellen Sie sicher, dass die folgenden Einstellungen korrekt sind:

   - `--network-type` — `dual`
   - `--db-subnet-group-name`— Die Subnetzgruppe, die Sie in einem vorherigen Schritt konfiguriert haben
   - `--vpc-security-group-ids`— Die VPC-Sicherheitsgruppe, die Sie in einem vorherigen Schritt konfiguriert haben

   Beispiel:

```
aws docdb modify-db-cluster --db-cluster-identifier <cluster-name> --network-type
 "DUAL"
```

4. Vergewissern Sie sich, dass der Cluster den Dual-Stack-Modus unterstützt.

   Wenn Sie die Konsole verwenden, wählen Sie die Registerkarte Konnektivität und Sicherheit für den Cluster und stellen Sie sicher, dass der Wert Netzwerktyp auf Dual-stack Modus gesetzt ist.

   Wenn Sie die verwenden AWS CLI, führen Sie den `describe-db-cluster` Befehl aus und stellen Sie sicher, dass der `NetworkType` Wert für den Cluster lautet`dual`.

   Führen Sie den `dig` Befehl auf dem Cluster-Endpunkt aus, um die zugehörige IPv6-Adresse zu ermitteln:

   ```
   dig <db-cluster-endpoint> AAAA
   ```

   Verwenden Sie den Cluster-Endpunkt, nicht die IPv6-Adresse, um eine Verbindung zum Cluster herzustellen.

Dual-stack Modus, Region und Verfügbarkeit der Version

Die Verfügbarkeit und der Support von Funktionen sind von Land zu Land unterschiedlich AWS-Regionen.

Regionsunterstützung

Der Dual-Stack-Modus für Amazon DocumentDB ist derzeit in allen kommerziellen AWS-Regionen Anwendungen verfügbar.

Unterstützung von Versionen

Dual-stack Der Modus wird auf Amazon DocumentDB Version 4.0, 5.0 und 8.0 unterstützt. Wenn Sie auf keiner dieser Versionen auf den Dual-Stack-Modus zugreifen können, stellen Sie sicher, dass Sie die neueste Engine-Patch-Version auf Ihrem Cluster ausführen.

Einschränkungen für Dual-Stack-Netzwerkcluster

Die folgenden Einschränkungen gelten für Dual-Stack-Netzwerkcluster:

- Cluster können das IPv6-Protokoll nicht ausschließlich verwenden. Sie können ausschließlich IPv4 oder das IPv4- und das IPv6-Protokoll (Dual-Stack-Modus) verwenden.
- Amazon DocumentDB unterstützt keine systemeigenen IPv6-Subnetze.
- Cluster, die den Dual-Stack-Modus verwenden, müssen privat sein. Sie dürfen nicht öffentlich zugänglich sein.

Erstellen eines Clusters in einer VPC

Die folgenden Verfahren helfen Ihnen beim Erstellen eines Clusters in einer VPC. Um die Standard-VPC zu verwenden, können Sie mit Schritt 2 beginnen und die VPC und die Subnetzgruppe verwenden, die bereits für Sie erstellt wurden. Bei Bedarf können Sie auch zusätzliche VPCs erstellen.

> **Note**
>
> Wenn Sie möchten, dass Ihr Cluster in der VPC öffentlich zugänglich ist, müssen Sie die DNS-Informationen für die VPC aktualisieren, indem Sie die VPC-Attribute und aktivieren. `DNS hostnames` `DNS resolution` Informationen zur Aktualisierung des DNS für eine VPC-Instance finden Sie unter DNS-Attribute für Ihre VPC anzeigen und aktualisieren im Amazon Virtual Private Cloud Cloud-Benutzerhandbuch.

Gehen Sie wie folgt vor, um einen Cluster in einer VPC zu erstellen:

- Schritt 1: Erstellen einer VPC
- Schritt 2: Erstellung einer Subnetzgruppe
- Schritt 3: Erstellen einer VPC-Sicherheitsgruppe
- Schritt 4: Erstellen Sie einen Cluster in der VPC

Schritt 1: Erstellen einer VPC

Erstellen Sie eine VPC mit Subnetzen in mindestens zwei Availability Zones. Sie verwenden diese Subnetze, wenn Sie eine Subnetzgruppe erstellen. Wenn Sie eine Standard-VPC verwenden, wird automatisch ein Subnetz in jeder Availability Zone der AWS-Region für Sie erstellt.

Weitere Informationen finden Sie unter Erstellen Sie eine IPv4-only VPC zur Verwendung mit einem DocumentDB-Cluster oder unter Erstellen einer VPC im Amazon Virtual Private Cloud Cloud-Benutzerhandbuch.

Schritt 2: Erstellung einer Subnetzgruppe

Eine Subnetzgruppe ist eine Sammlung von Subnetzen (normalerweise privat), die Sie für eine VPC erstellen und die Sie dann für Ihre Cluster festlegen. Mit einer Subnetzgruppe können Sie eine bestimmte VPC angeben, wenn Sie Cluster mithilfe der AWS CLI oder DocumentDB-API erstellen. Wenn Sie die verwenden AWS-Managementkonsole, können Sie einfach die VPC und die Subnetze auswählen, die Sie verwenden möchten. Jede Subnetzgruppe muss mindestens ein Subnetz in mindestens zwei Availability Zones in der haben. AWS-Region Als bewährte Methode sollte jede Subnetzgruppe mindestens ein Subnetz für jede Availability Zone in der haben. AWS-Region

Damit ein Cluster öffentlich zugänglich ist, müssen die Subnetze in der Subnetzgruppe über ein Internet-Gateway verfügen. Weitere Informationen zu Internet-Gateways für Subnetze finden Sie unter Aktivieren des Internetzugangs für eine VPC mithilfe eines Internet-Gateways im Amazon Virtual Private Cloud Cloud-Benutzerhandbuch.

> **Note**
>
> Die Subnetzgruppe für eine lokale Zone kann nur ein Subnetz haben.

Wenn Sie einen Cluster in einer VPC erstellen, können Sie eine Subnetzgruppe auswählen. Amazon DocumentDB wählt ein Subnetz und eine IP-Adresse (innerhalb dieses Subnetzes) aus, die Ihrem Cluster zugeordnet werden sollen. Wenn keine Subnetzgruppen vorhanden sind, erstellt Amazon DocumentDB bei der Erstellung des Clusters eine Standard-Subnetzgruppe. DocumentDB erstellt ein Elastic Network Interface und ordnet es Ihrem Cluster mit dieser IP-Adresse zu. Der Cluster verwendet die Availability Zone, die das Subnetz enthält.

In diesem Schritt erstellen Sie eine Subnetzgruppe und fügen die Subnetze hinzu, die Sie für Ihre VPC erstellt haben.

Um eine Subnetzgruppe zu erstellen

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Wählen Sie im Navigationsbereich Subnetzgruppe aus.

3. Wählen Sie Erstellen aus.
4. Geben Sie unter Name den Namen Ihrer Subnetzgruppe ein.
5. Geben Sie unter Beschreibung eine Beschreibung für Ihre Subnetzgruppe ein.
6. Wählen Sie im Abschnitt Subnetze hinzufügen für VPC die Standard-VPC oder die von Ihnen erstellte VPC aus. Wählen Sie dann die Availability Zones aus, die die Subnetze aus Availability Zones enthalten, und wählen Sie dann die Subnetze aus Subnets aus.
7. Wählen Sie Erstellen aus.

   Ihre neue Subnetzgruppe wird in der Liste der Subnetzgruppen auf der DocumentDB-Konsole angezeigt. Sie können die Subnetzgruppe auswählen, um Details, einschließlich aller mit der Gruppe verknüpften Subnetze, im Detailbereich unten im Fenster zu sehen.

Schritt 3: Erstellen einer VPC-Sicherheitsgruppe

Bevor Sie Ihren Cluster erstellen, erstellen Sie eine VPC-Sicherheitsgruppe, die Sie ihm zuordnen möchten. Wenn Sie keine VPC-Sicherheitsgruppe erstellen, können Sie bei der Erstellung des Clusters die Standardsicherheitsgruppe verwenden. Anweisungen zum Erstellen einer Sicherheitsgruppe für Ihren Cluster finden Sie unter oder unter Erstellen Sie eine IPv4-only VPC zur Verwendung mit einem DocumentDB-Cluster Steuern des Datenverkehrs zu Ihren AWS Ressourcen mithilfe von Sicherheitsgruppen im Amazon Virtual Private Cloud Cloud-Benutzerhandbuch.

Schritt 4: Erstellen Sie einen Cluster in der VPC

In diesem Schritt erstellen Sie einen Cluster mit dem VPC-Namen, der Subnetzgruppe und der VPC-Sicherheitsgruppe, die Sie in den vorherigen Schritten erstellt haben.

> **Note**
>
> Wenn Sie möchten, dass Ihr Cluster in der VPC öffentlich zugänglich ist, müssen Sie die VPC-Attribute `DNS hostnames` und aktivieren. `DNS resolution` Weitere Informationen finden Sie unter DNS-Attribute für Ihre VPC anzeigen und aktualisieren im Amazon Virtual Private Cloud Cloud-Benutzerhandbuch.

Einzelheiten zum Erstellen eines Clusters finden Sie unterEinen Amazon DocumentDB-Cluster erstellen.

Wenn Sie im Abschnitt Konnektivität dazu aufgefordert werden, geben Sie den VPC-Namen, die Subnetzgruppe und die VPC-Sicherheitsgruppe ein.

> **Note**
>
> Das Aktualisieren von VPCs wird derzeit für DocumentDBDocumentDB-Cluster nicht unterstützt.

Zugreifen auf einen Amazon DocumentDB-Cluster in einer VPC

Amazon DocumentDB unterstützt die folgenden Szenarien für den Zugriff auf einen Cluster in einer VPC:

Topics

- Ein Cluster in einer VPC, auf den eine Amazon EC2 EC2-Instance in derselben VPC zugreift
- Ein Cluster in einer VPC, auf den eine Amazon EC2 EC2-Instance in einer anderen VPC zugreift

Ein Cluster in einer VPC, auf den eine Amazon EC2 EC2-Instance in derselben VPC zugreift

Ein Cluster in einer VPC wird häufig verwendet, um Daten mit einem Anwendungsserver gemeinsam zu nutzen, der in einer Amazon EC2 EC2-Instance in derselben VPC ausgeführt wird.

Nachfolgend finden Sie den einfachsten Weg für die Verwaltung des Zugriffs zwischen EC2-Instances und DB-Instances in derselben VPC:

- Erstellen Sie eine VPC-Sicherheitsgruppe, in der sich Ihre Cluster befinden sollen. Diese Sicherheitsgruppe kann verwendet werden, um den Zugriff auf die Cluster einzuschränken. Sie können beispielsweise eine benutzerdefinierte Regel für diese Sicherheitsgruppe erstellen. Dies ermöglicht möglicherweise den TCP-Zugriff über den Port, den Sie dem Cluster bei der Erstellung zugewiesen haben, und über eine IP-Adresse, mit der Sie zu Entwicklungs- oder anderen Zwecken auf den Cluster zugreifen.
- Erstellen Sie eine VPC-Sicherheitsgruppe, der sich Ihre EC2-Instances (Webserver und Clients) befinden. Mithilfe dieser Sicherheitsgruppe können Sie bei Bedarf den Internetzugriff auf die EC2-Instance über die Routing-Tabelle der VPC zulassen. Sie können beispielsweise Regeln für diese Sicherheitsgruppe festlegen, damit der TCP-Zugriff auf die EC2-Instance über Port 22 möglich ist.

- Erstellen Sie in der Sicherheitsgruppe für Ihre Cluster benutzerdefinierte Regeln, die Verbindungen von der Sicherheitsgruppe aus zulassen, die Sie für Ihre EC2-Instances erstellt haben. Diese Regeln können jedem Mitglied der Sicherheitsgruppe den Zugriff auf die Cluster ermöglichen.

Es gibt ein zusätzliches öffentliches und privates Subnetz in einer separaten Availability Zone. Eine DocumentDB-Subnetzgruppe erfordert ein Subnetz in mindestens zwei Availability Zones. Das zusätzliche Subnetz macht es einfach, in future auf eine Multi-AZ-Cluster-Bereitstellung umzusteigen.

Anweisungen zum Erstellen einer VPC mit öffentlichen und privaten Subnetzen für dieses Szenario finden Sie unter. Erstellen Sie eine IPv4-only VPC zur Verwendung mit einem DocumentDB-Cluster

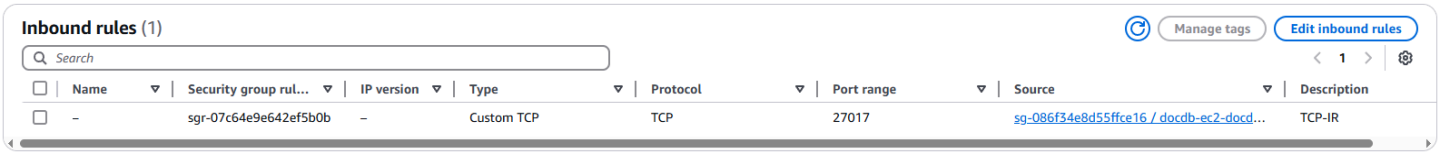
> **Tip**
>
> Sie können die Netzwerkkonnektivität zwischen einer Amazon EC2 EC2-Instance und einem DocumentDB-Cluster automatisch einrichten, wenn Sie den Cluster erstellen. Weitere Informationen finden Sie unter Amazon EC2 automatisch Connect.

Gehen Sie wie folgt vor, um eine Regel in einer VPC-Sicherheitsgruppe zu erstellen, die Verbindungen von einer anderen Sicherheitsgruppe zulässt:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc.
2. Suchen Sie im Navigationsbereich nach Sicherheitsgruppen und wählen Sie diese aus.
3. Erstellen oder wählen Sie eine Sicherheitsgruppe aus, der Sie den Zugriff zu Teilen einer anderen Sicherheitsgruppe erlauben möchten. Dies ist die Sicherheitsgruppe, die Sie für Ihre Cluster verwenden. Wählen Sie die Registerkarte Inbound Rules (Eingehende Regeln) und anschließend Edit Inbound Rules (Eingehende Regeln bearbeiten) aus.
4. Wählen Sie auf der Seite Edit inbound rules (Regeln für eingehenden Datenverkehr bearbeiten) die Option Add Rule (Regel hinzufügen).
5. Wählen Sie unter Typ den Eintrag aus, der dem Port entspricht, den Sie bei der Erstellung Ihres Clusters verwendet haben, z. B. Custom TCP.
6. Beginnen Sie im Feld Quelle mit der Eingabe der ID der Sicherheitsgruppe, in der die entsprechenden Sicherheitsgruppen aufgeführt sind. Wählen Sie die Sicherheitsgruppe mit den Mitgliedern aus, die Zugriff auf die durch diese Sicherheitsgruppe geschützten Ressourcen erhalten sollen. Im vorhergehenden Szenario ist dies die Sicherheitsgruppe, die Sie für Ihre EC2-Instance verwenden.

7. Falls erforderlich, wiederholen Sie die Schritte für das TCP-Protokoll, indem Sie eine Regel mit All TCP als Typ und Ihrer Sicherheitsgruppe im Feld Quelle erstellen. Wenn Sie das UDP-Protokoll verwenden möchten, erstellen Sie eine Regel mit Alle UDP als Typ und Ihrer Sicherheitsgruppe im Quelle.
8. Wählen Sie Regeln speichern aus.

Der folgende Bildschirm zeigt eine eingehende Regel mit einer Sicherheitsgruppe für ihre Quelle.



Weitere Informationen zum Herstellen einer Verbindung zu einem Cluster von Ihrer EC2-Instance aus finden Sie unter. Amazon EC2 automatisch Connect

Ein Cluster in einer VPC, auf den eine Amazon EC2 EC2-Instance in einer anderen VPC zugreift

Wenn sich Ihr Cluster in einer anderen VPC befindet als die EC2-Instance, die Sie für den Zugriff verwenden, können Sie VPC-Peering verwenden, um auf den Cluster zuzugreifen.

Peering: Eine VPC-Peering-Verbindung ist eine Netzwerkverbindung zwischen zwei VPCs. Diese ermöglicht die Weiterleitung des Datenverkehrs zwischen den VPCs mithilfe von privaten IP-Adressen. Ressourcen in jeder der VPCs können so miteinander kommunizieren, als befänden sie sich im selben Netzwerk. Sie können eine VPC-Peering-Verbindung zwischen Ihren eigenen VPCs, mit einer VPC in einem anderen AWS Konto oder mit einer VPC in einem anderen Konto herstellen. AWS-Region Weitere Informationen über VPC-Peering finden Sie unter VPC-Peering im Amazon Virtual Private Cloud-Benutzerhandbuch.

Erstellen Sie eine IPv4-only VPC zur Verwendung mit einem DocumentDB-Cluster

Ein gängiges Szenario beinhaltet einen Cluster in einer Virtual Private Cloud (VPC), der auf dem Amazon VPC-Service basiert. Diese VPC könnte beispielsweise Daten mit einem Dienst oder einer Anwendung teilen, die in derselben VPC ausgeführt wird. In diesem Thema erstellen Sie die VPC für dieses Szenario.

Topics

- Schritt 1: Erstellen Sie eine VPC mit privaten und öffentlichen Subnetzen
- Schritt 2: Erstellen Sie eine VPC-Sicherheitsgruppe für eine öffentliche Anwendung
- Schritt 3: Erstellen Sie eine VPC-Sicherheitsgruppe für einen privaten Cluster
- Schritt 4: Erstellen Sie eine Subnetzgruppe
- Löschen einer VPC

Ihr Cluster muss nur für Ihre Anwendung und nicht für das öffentliche Internet verfügbar sein. Daher erstellen Sie eine VPC sowohl mit öffentlichen als auch mit privaten Subnetzen. Die Anwendung wird im öffentlichen Subnetz gehostet, sodass sie das öffentliche Internet erreichen kann. Der Cluster wird in einem privaten Subnetz gehostet. Die Anwendung kann eine Verbindung zum Cluster herstellen, da sie in derselben VPC gehostet wird. Der Cluster ist jedoch nicht für das öffentliche Internet verfügbar, was für mehr Sicherheit sorgt.

Mit dem Verfahren in diesem Thema wird ein zusätzliches öffentliches und ein privates Subnetz in einer separaten Availability Zone konfiguriert. Diese Subnetze werden von dem Verfahren nicht verwendet. Eine DocumentDB-Subnetzgruppe erfordert ein Subnetz in mindestens zwei Availability Zones. Das zusätzliche Subnetz macht es einfacher, mehr als eine DocumentDB-Instanz zu konfigurieren.

In diesem Thema wird die Konfiguration einer VPC für Amazon DocumentDB-Cluster beschrieben. Weitere Informationen zur Amazon VPC-Sicherheit finden Sie unter Sicherheit im Amazon VPC-Benutzerhandbuch.

> **Tip**
>
> Sie können die Netzwerkkonnektivität zwischen einer Amazon EC2 EC2-Instance und einem DocumentDB-Cluster automatisch einrichten, wenn Sie den Cluster erstellen. Die Netzwerkkonfiguration ähnelt der in diesem Szenario beschriebenen. Weitere Informationen finden Sie unter Amazon EC2 automatisch Connect.

Schritt 1: Erstellen Sie eine VPC mit privaten und öffentlichen Subnetzen

Verwenden sie die folgenden Vorgänge, um eine VPC sowohl mit öffentlichen als auch mit privaten Subnetzen zu erstellen.

So erstellen Sie eine VPC und Subnetze

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc.
2. Wählen Sie in der oberen rechten Ecke von die Region aus AWS-Managementkonsole, in der Sie Ihre VPC erstellen möchten. In diesem Beispiel wird die Region USA West (Oregon) verwendet.
3. Wählen Sie links oben die Option VPC-Dashboard aus. Wählen Sie Create VPC (VPC erstellen) aus, um mit dem Erstellen einer VPC zu beginnen.
4. Wählen Sie unter VPC Settings (VPC-Einstellungen) für Resources to create (Zu erstellende Ressourcen) VPC and more (VPC und mehr) aus.
5. Legen Sie für VPC settings (VPC-Einstellungen) folgende Werte fest:
   - Automatische Generierung von Namensschildern — **`example`**
   - IPv4-CIDR-Block — **`10.0.0.0/16`**
   - IPv6-CIDR-Block — Kein IPv6-CIDR-Block
   - Tenancy — Standard
   - Anzahl der Availability Zones (AZs) — 2
   - AZs anpassen — Behalten Sie die Standardwerte bei
   - Anzahl der öffentlichen Subnetze — 2
   - Anzahl der privaten Subnetze — 2
   - CIDR-Blöcke der Subnetze anpassen — Behalten Sie die Standardwerte bei
   - NAT-Gateways ($) — Keine
   - VPC-Endpunkte — Keine
   - DNS-Optionen — Behalten Sie die Standardwerte bei
6. Wählen Sie VPC erstellen aus.

Schritt 2: Erstellen Sie eine VPC-Sicherheitsgruppe für eine öffentliche Anwendung

Erstellen Sie als Nächstes eine Sicherheitsgruppe für den öffentlichen Zugriff. Wenn Sie eine Verbindung mit öffentlichen EC2-Instances in Ihrer VPC herstellen möchten, fügen Sie Ihrer VPC-Sicherheitsgruppe Regeln für eingehenden Datenverkehr hinzu. Diese ermöglichen die Verbindung des Datenverkehrs aus dem Internet.

So erstellen Sie eine VPC-Sicherheitsgruppe

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc.

2. Wählen Sie VPC Dashboard (VPC-Dashboard), Security Groups (Sicherheitsgruppen) und anschließend Create security group (Sicherheitsgruppe erstellen).
3. Legen Sie auf der Seite Create security group (Sicherheitsgruppe erstellen) die folgenden Werte fest:

   - Name der Sicherheitsgruppe — **`example-securitygroup`**
   - Beschreibung — **`Application security group`**
   - VPC — Wählen Sie die VPC aus, die Sie zuvor erstellt haben, zum Beispiel: vpc-example.
4. Fügen Sie der Sicherheitsgruppe Regeln für den eingehenden Datenverkehr hinzu.

   a. Legen Sie die IP-Adresse fest, die für die Verbindung mit EC2-Instances in Ihrer VPC mit Secure Shell (SSH) verwendet werden soll. Um Ihre öffentliche IP-Adresse in einem anderen Browserfenster oder einer anderen Registerkarte zu ermitteln, können Sie den Dienst unter verwenden. https://checkip.amazonaws.com Ein Beispiel für eine IP-Adresse ist `203.0.113.25/32`.

   In vielen Fällen können Sie eine Verbindung über einen Internetdienstanbieter (ISP) oder hinter Ihrer Firewall ohne statische IP-Adresse herstellen. Suchen Sie in diesem Fall den Bereich der IP-Adressen, die von Client-Computern verwendet werden.

   > ⚠ Warning
   >
   > Wenn Sie `0.0.0.0/0` für SSH-Zugriff verwenden, ermöglichen Sie für alle IP-Adressen den Zugriff auf Ihre öffentlichen Instances. Dieser Ansatz ist zwar für kurze Zeit in einer Testumgebung zulässig, aber für Produktionsumgebungen sehr unsicher. Für die Produktion wird nur eine bestimmte IP-Adresse bzw. ein bestimmter Adressbereich für den Zugriff auf Ihre Instances autorisiert.

   b. Wählen Sie im Abschnitt Eingehende Regeln die Option Regel hinzufügen aus.

   c. Legen Sie die folgenden Werte für Ihre neue eingehende Regel fest, um SSH den Zugriff auf Ihre Amazon-EC2-Instance zu erlauben. Nachdem Sie dies getan haben, können Sie eine Verbindung zu Ihrer EC2-Instance herstellen, um die Anwendung und andere Dienstprogramme zu installieren. Sie stellen auch eine Verbindung zu Ihrer EC2-Instance her, um Inhalte für Ihre Anwendung hochzuladen.

      - Geben Sie — ein **`SSH`**

- Quelle — Die IP-Adresse oder der Bereich, die Sie in Schritt a erstellt haben, zum Beispiel: **`203.0.113.25/32`**

d. Wählen Sie Regel hinzufügen aus.

e. Legen Sie die folgenden Werte für Ihre neue Regel für eingehende Nachrichten fest, um den HTTP-Zugriff auf Ihre Anwendung zu ermöglichen:

- Geben Sie — ein **`HTTP`**
- Quelle — **`0.0.0.0/0`**

5. Wählen Sie Create security group (Sicherheitsgruppe erstellen) aus, um die Sicherheitsgruppe zu erstellen.

   Notieren Sie sich die Sicherheitsgruppen-ID, da Sie sie später in einem anderen Verfahren benötigen.

Schritt 3: Erstellen Sie eine VPC-Sicherheitsgruppe für einen privaten Cluster

Um Ihren Cluster privat zu halten, erstellen Sie eine zweite Sicherheitsgruppe für den privaten Zugriff. Um eine Verbindung zu privaten Clustern in Ihrer VPC herzustellen, fügen Sie Ihrer VPC-Sicherheitsgruppe Regeln für eingehenden Datenverkehr hinzu, die nur Datenverkehr von Ihrer Anwendung zulassen.

So erstellen Sie eine VPC-Sicherheitsgruppe

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc.
2. Wählen Sie VPC Dashboard (VPC-Dashboard), Security Groups (Sicherheitsgruppen) und anschließend Create security group (Sicherheitsgruppe erstellen).
3. Legen Sie auf der Seite Create security group (Sicherheitsgruppe erstellen) die folgenden Werte fest:

   - Name der Sicherheitsgruppe — **`example-securitygroup`**
   - Beschreibung — **`Instance security group`**
   - VPC — Wählen Sie die VPC aus, die Sie zuvor erstellt haben, zum Beispiel: vpc-example

4. Fügen Sie der Sicherheitsgruppe Regeln für den eingehenden Datenverkehr hinzu.

   a. Wählen Sie im Abschnitt Eingehende Regeln die Option Regel hinzufügen aus.

b. Legen Sie die folgenden Werte für Ihre neue eingehende Regel fest, um DocumentDB-Verkehr auf Port 27017 von Ihrer Amazon EC2 EC2-Instance aus zuzulassen. Nachdem Sie dies getan haben, können Sie von Ihrer Anwendung aus eine Verbindung zu Ihrem Cluster herstellen. Auf diese Weise können Sie Daten aus Ihrer Anwendung in Ihrer Datenbank speichern und abrufen.

   - Geben Sie — ein **`Custom TCP`**
   - Quelle — Die ID der Anwendungssicherheitsgruppe, die Sie zuvor in diesem Thema erstellt haben, z. B.: sg-9edd5cfb.

c. Wählen Sie Regel hinzufügen aus.

d. Legen Sie die folgenden Werte für Ihre neue Regel für eingehende Zugriffe fest, um den HTTP-Zugriff auf Ihre Anwendung zu ermöglichen:

   - Geben Sie — ein **`HTTP`**
   - Quelle — **`0.0.0.0/0`**

5. Wählen Sie Create security group (Sicherheitsgruppe erstellen) aus, um die Sicherheitsgruppe zu erstellen.

Schritt 4: Erstellen Sie eine Subnetzgruppe

Eine Subnetzgruppe ist eine Sammlung von Subnetzen, die Sie in einer VPC erstellen und die Sie dann für Ihre Cluster festlegen. Eine Subnetzgruppe ermöglicht es Ihnen, beim Erstellen von Clustern eine bestimmte VPC anzugeben.

Um eine Subnetzgruppe zu erstellen

1. Identifizieren Sie die privaten Subnetze für Ihre Datenbank in der VPC.

   a. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc.

   b. Wählen Sie VPC Dashboard (VPC-Dashboard) und dann Subnets (Subnetze) aus.

   c. Notieren Sie sich die Subnetz-IDs der Subnetze, die Sie in Schritt 1 erstellt haben, mit den folgenden Namen: example-subnet-private1-us-west-2a und example-subnet-private2-us-west-2b. Sie benötigen die Subnetz-IDs, wenn Sie Ihre Subnetzgruppe erstellen.

2. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.

Stellen Sie sicher, dass Sie eine Verbindung zur Amazon DocumentDB DocumentDB-Konsole herstellen, nicht zur Amazon VPC-Konsole.

3. Wählen Sie im Navigationsbereich Subnetzgruppe aus.
4. Wählen Sie Erstellen aus.
5. Legen Sie auf der Seite Subnetzgruppe erstellen im Abschnitt Subnetzgruppendetails die folgenden Werte fest:
   - Name — **`example-db-subnet-group`**
   - Beschreibung — **`Instance security group`**
6. Legen Sie im Abschnitt Subnetze hinzufügen die folgenden Werte fest:
   - VPC — Wählen Sie die VPC aus, die Sie zuvor erstellt haben, zum Beispiel: vpc-example
   - Availability Zones — Wählen Sie beide Availability Zones aus, die in Schritt 1 erstellt wurden. Beispiel: us-west-2a und us-west-2b
   - Subnetze — Wählen Sie die privaten Subnetze aus, die Sie in Schritt 1 erstellt haben.
7. Wählen Sie Erstellen aus.

Ihre neue Subnetzgruppe wird in der Liste der Subnetzgruppen auf der DocumentDB-Konsole angezeigt. Sie können die Subnetzgruppe auswählen, um Details im Detailbereich anzuzeigen. Diese Informationen umfassen alle Subnetze, die der Gruppe zugeordnet sind.

> **Note**
>
> Wenn Sie diese VPC erstellt haben, um sie mit einem DocumentDB-Cluster zu verknüpfen, erstellen Sie den Cluster, indem Sie den Anweisungen unter folgen. Einen Amazon DocumentDB-Cluster erstellen

Löschen einer VPC

Sie können eine VPC und die anderen Ressourcen, die darin verwendet werden, löschen, wenn sie nicht mehr benötigt werden.

> **Note**
>
> Wenn Sie der VPC, die Sie in diesem Thema erstellt haben, Ressourcen hinzugefügt haben, müssen Sie diese möglicherweise löschen, bevor Sie die VPC löschen können. Zu diesen Ressourcen können beispielsweise Amazon EC2 EC2-Instances oder DocumentDB-Cluster gehören. Weitere Informationen finden Sie unter Löschen Ihrer VPC im Amazon VPC User Guide.

So löschen Sie eine VPC und zugehörige Ressourcen

1. Löschen Sie die Subnetzgruppe:
   a. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
   b. Wählen Sie im Navigationsbereich Subnetzgruppe aus.
   c. Wählen Sie die Subnetzgruppe aus, die Sie löschen möchten, z. B. example-db-subnet-group.
   d. Wählen Sie Löschen, und wählen Sie dann im Bestätigungsfenster Löschen.
2. Notieren Sie sich die VPC-ID.
   a. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc.
   b. Wählen Sie VPC Dashboard und dann Your VPCs aus.
   c. Identifizieren Sie in der Liste die VPC, die Sie erstellt haben, z. B. vpc-example.
   d. Notieren Sie die VPC ID (VPC-ID) der VPC, die Sie erstellt haben. Sie benötigen die VPC-ID in späteren Schritten.
3. Löschen der Sicherheitsgruppen:
   a. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc.
   b. Wählen Sie VPC Dashboard und dann Sicherheitsgruppen.
   c. Wählen Sie die Sicherheitsgruppe für den Amazon DocumentDB-Cluster aus, z. B. example-securitygroup.
   d. Wählen Sie für Aktionen die Option Sicherheitsgruppen löschen und wählen Sie dann im Bestätigungsdialogfeld Löschen aus.
   e. Zurück auf der Seite Sicherheitsgruppen wählen Sie die Sicherheitsgruppe für die Amazon EC2 EC2-Instance aus, z. B. example-securitygroup.

f. Wählen Sie für Aktionen die Option Sicherheitsgruppen löschen und wählen Sie dann im Bestätigungsdialogfeld Löschen aus.

4. Löschen der VPC:

   a. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc.

   b. Wählen Sie VPC Dashboard und dann Your VPCs aus.

   c. Wählen Sie die VPC aus, die Sie löschen möchten, z. B. vpc-example.

   d. Wählen Sie für Aktionen die Option VPC löschen aus.

      Auf der Bestätigungsseite werden weitere Ressourcen angezeigt, die der VPC zugeordnet sind, die ebenfalls gelöscht werden, einschließlich der damit verknüpften Subnetze.

   e. Geben Sie im Bestätigungsdialogfeld die Eingabetaste ein **`delete`** und wählen Sie dann Löschen aus.

Erstellen Sie eine Dual-Stack-VPC zur Verwendung mit einem DocumentDB-Cluster

Ein gängiges Szenario beinhaltet einen Cluster in einer Virtual Private Cloud (VPC), der auf dem Amazon VPC-Service basiert. Diese VPC teilt Daten mit einer öffentlichen Amazon-EC2-Instance, die in derselben VPC ausgeführt wird. In diesem Thema erstellen Sie die VPC für dieses Szenario.

Topics

- Schritt 1: Erstellen Sie eine VPC mit privaten und öffentlichen Subnetzen
- Schritt 2: Erstellen Sie eine VPC-Sicherheitsgruppe für eine öffentliche Amazon EC2 EC2-Instance
- Schritt 3: Erstellen Sie eine VPC-Sicherheitsgruppe für einen privaten Cluster
- Schritt 4: Erstellen Sie eine Subnetzgruppe
- Schritt 5: Erstellen Sie eine Amazon EC2 EC2-Instance im Dual-Stack-Modus
- Schritt 6: Erstellen Sie einen Cluster im Dual-Stack-Modus
- Schritt 7: Connect zu Ihrer Amazon EC2 EC2-Instance und Ihrem DB-Cluster her
- Löschen der VPC

In diesem Verfahren erstellen Sie die VPC für dieses Szenario, das mit einer Datenbank funktioniert, die im Dual-Stack-Modus ausgeführt wird. Dual-stack Der Modus ermöglicht die Verbindung über

das IPv6-Adressierungsprotokoll. Weitere Informationen über die IP-Adressierung finden Sie unter Amazon DocumentDB DocumentDB-IP-Adressierung.

Dual-stack Netzwerkcluster werden in den meisten Regionen unterstützt. Weitere Informationen finden Sie unter Dual-stack Modus, Region und Verfügbarkeit der Version. Informationen zu den Einschränkungen des Dual-Stack-Modus finden Sie unter Einschränkungen für Dual-Stack-Netzwerkcluster.

Dieses Thema und das IPv4-only Thema erstellen die öffentlichen und privaten Subnetze in derselben VPC. Informationen zum Erstellen des Amazon DocumentDB-Clusters in einer VPC und der Amazon EC2 EC2-Instance in einer anderen VPC finden Sie unter. Zugreifen auf einen Amazon DocumentDB-Cluster in einer VPC

Ihr DocumentDB-Cluster muss nur für Ihre Amazon EC2 EC2-Instance und nicht für das öffentliche Internet verfügbar sein. Daher erstellen Sie eine VPC sowohl mit öffentlichen als auch mit privaten Subnetzen. Die EC2-Instance wird im öffentlichen Subnetz gehostet, sodass sie das öffentliche Internet erreichen kann. Der Cluster wird in einem privaten Subnetz gehostet. Die EC2-Instance kann eine Verbindung zum Cluster herstellen, da sie in derselben VPC gehostet wird. Der Cluster ist jedoch nicht für das öffentliche Internet verfügbar, was für mehr Sicherheit sorgt.

Mit den Verfahren in diesem Thema wird ein zusätzliches öffentliches und ein privates Subnetz in einer separaten Availability Zone konfiguriert. Diese Subnetze werden von dem Verfahren nicht verwendet. Eine DocumentDB-Subnetzgruppe erfordert ein Subnetz in mindestens zwei Availability Zones. Das zusätzliche Subnetz macht es einfach, mehr als eine DocumentDB-Instanz zu konfigurieren.

Um einen Cluster zu erstellen, der den Dual-Stack-Modus verwendet, geben Sie Dual-stack mode e für die Einstellung Netzwerktyp an. Sie können einen Cluster auch mit derselben Einstellung ändern. Weitere Informationen zum Erstellen eines Clusters finden Sie unterEinen Amazon DocumentDB-Cluster erstellen. Weitere Informationen über das Ändern eines DB-Clusters finden Sie unter Ändern eines Amazon DocumentDB-Clusters.

In diesem Thema wird die Konfiguration einer VPC für Amazon DocumentDB-Cluster beschrieben. Weitere Informationen zur Amazon VPC-Sicherheit finden Sie unter Sicherheit im Amazon VPC-Benutzerhandbuch.

Schritt 1: Erstellen Sie eine VPC mit privaten und öffentlichen Subnetzen

Verwenden sie die folgenden Vorgänge, um eine VPC sowohl mit öffentlichen als auch mit privaten Subnetzen zu erstellen.

So erstellen Sie eine VPC und Subnetze

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc.
2. Wählen Sie in der oberen rechten Ecke von die Region aus AWS-Managementkonsole, in der Sie Ihre VPC erstellen möchten. In diesem Beispiel wird die Region USA West (Oregon) verwendet.
3. Wählen Sie links oben die Option VPC-Dashboard aus. Wählen Sie Create VPC (VPC erstellen) aus, um mit dem Erstellen einer VPC zu beginnen.
4. Wählen Sie unter VPC Settings (VPC-Einstellungen) für Resources to create (Zu erstellende Ressourcen) VPC and more (VPC und mehr) aus.
5. Legen Sie für VPC settings (VPC-Einstellungen) folgende Werte fest:
   - Automatische Generierung von Namensschildern — **`example-dual-stack`**
   - IPv4-CIDR-Block — **`10.0.0.0/16`**
   - IPv6-CIDR-Block — IPv6-CIDR-Block Amazon-provided
   - Tenancy — Standard
   - Anzahl der Availability Zones (AZs) — 2
   - AZs anpassen — Behalten Sie die Standardwerte bei
   - Anzahl der öffentlichen Subnetze — 2
   - Anzahl der privaten Subnetze — 2
   - CIDR-Blöcke der Subnetze anpassen — Behalten Sie die Standardwerte bei
   - NAT-Gateways ($) — Keine
   - Internet-Gateway nur für ausgehenden Datenverkehr — Nein
   - VPC-Endpunkte — Keine
   - DNS-Optionen — Behalten Sie die Standardwerte bei
6. Wählen Sie VPC erstellen aus.

Schritt 2: Erstellen Sie eine VPC-Sicherheitsgruppe für eine öffentliche Amazon EC2 EC2-Instance

Als Nächstes erstellen Sie eine Sicherheitsgruppe für öffentlichen Zugriff. Wenn Sie eine Verbindung mit öffentlichen EC2-Instances in Ihrer VPC herstellen möchten, fügen Sie Ihrer VPC-Sicherheitsgruppe eingehende Regeln hinzu, die Verbindungen aus dem Internet zulassen.

So erstellen Sie eine VPC-Sicherheitsgruppe

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc.
2. Wählen Sie VPC Dashboard (VPC-Dashboard), Security Groups (Sicherheitsgruppen) und anschließend Create security group (Sicherheitsgruppe erstellen).
3. Legen Sie auf der Seite Create security group (Sicherheitsgruppe erstellen) die folgenden Werte fest:

   - Name der Sicherheitsgruppe — **`example-dual-stack-securitygroup`**
   - Beschreibung — **`Dual-stack security group`**
   - VPC — Wählen Sie die VPC aus, die Sie zuvor erstellt haben, zum Beispiel: vpc-example-dual-stack.
4. Fügen Sie der Sicherheitsgruppe Regeln für den eingehenden Datenverkehr hinzu.

   a. Legen Sie die IP-Adresse fest, die für die Verbindung mit EC2-Instances in Ihrer VPC mit Secure Shell (SSH) verwendet werden soll. Um Ihre öffentliche IP-Adresse in einem anderen Browserfenster oder einer anderen Registerkarte zu ermitteln, können Sie den Dienst unter verwenden. https://checkip.amazonaws.com

      Ein Beispiel für einen IPv4-Adressbereich (Internet Protocol Version 4) ist`203.0.113.25/32`. Ein Beispiel für einen Internet Protocol Version 6 (IPv6)-Adressbereich ist `2001:db8:1234:1a00::/64`.

      In vielen Fällen können Sie eine Verbindung über einen Internetdienstanbieter (ISP) oder hinter Ihrer Firewall ohne statische IP-Adresse herstellen. Suchen Sie in diesem Fall den Bereich der IP-Adressen, die von Client-Computern verwendet werden.

      > **Warning**
      >
      > Wenn Sie `0.0.0.0/0` für IPv4 oder `::0` für IPv6 verwenden, lassen Sie für alle IP-Adressen den Zugriff auf Ihre öffentlichen Instances mit SSH zu. Dieser Ansatz ist zwar für kurze Zeit in einer Testumgebung zulässig, aber für Produktionsumgebungen sehr unsicher. Autorisieren Sie in Produktionsumgebungen nur eine bestimmte IP-Adresse bzw. einen bestimmten Adressbereich für den Zugriff auf Ihre Instances.

   b. Wählen Sie im Abschnitt Eingehende Regeln die Option Regel hinzufügen aus.

c. Legen Sie die folgenden Werte für Ihre neue eingehende Regel fest, um SSH den Zugriff auf Ihre Amazon-EC2-Instance zu erlauben. Nachdem Sie dies getan haben, können Sie eine Verbindung zu Ihrer EC2-Instance herstellen, um Anwendungen oder andere Dienstprogramme zu installieren. Geben Sie eine IP-Adresse an, damit Sie auf Ihre EC2-Instance zugreifen können:

   - Geben Sie — ein **`SSH`**
   - Quelle — Die IP-Adresse oder der Bereich, die Sie in Schritt a erstellt haben. Ein Beispiel für einen IPv4-Adressbereich ist **`203.0.113.25/3`** 2. Ein Beispiel für einen IPv6-Adressbereich ist. **`2001:DB8::/32`**

d. Wählen Sie Regel hinzufügen aus.

5. Wählen Sie Create security group (Sicherheitsgruppe erstellen) aus, um die Sicherheitsgruppe zu erstellen.

   Notieren Sie sich die Sicherheitsgruppen-ID, da Sie sie später in einem anderen Verfahren benötigen.

Schritt 3: Erstellen Sie eine VPC-Sicherheitsgruppe für einen privaten Cluster

Um Ihren Cluster privat zu halten, erstellen Sie eine zweite Sicherheitsgruppe für den privaten Zugriff. Um eine Verbindung zu privaten Clustern in Ihrer VPC herzustellen, fügen Sie Ihrer VPC-Sicherheitsgruppe Regeln für eingehenden Datenverkehr hinzu. Diese lassen ausschließlich Datenverkehr von Ihrer Amazon-EC2-Instance zu.

So erstellen Sie eine VPC-Sicherheitsgruppe

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc.
2. Wählen Sie VPC Dashboard (VPC-Dashboard), Security Groups (Sicherheitsgruppen) und anschließend Create security group (Sicherheitsgruppe erstellen).
3. Legen Sie auf der Seite Create security group (Sicherheitsgruppe erstellen) die folgenden Werte fest:

   - Name der Sicherheitsgruppe — **`example-dual-stack-cluster-securitygroup`**
   - Beschreibung — **`Dual-stack cluster security group`**
   - VPC — Wählen Sie die VPC aus, die Sie zuvor erstellt haben, zum Beispiel: vpc-example-dual-stack

4. Fügen Sie der Sicherheitsgruppe Regeln für den eingehenden Datenverkehr hinzu.

    a. Wählen Sie im Abschnitt Eingehende Regeln die Option Regel hinzufügen aus.

    b. Legen Sie die folgenden Werte für Ihre neue eingehende Regel fest, um DocumentDB-Verkehr auf Port 27017 von Ihrer Amazon EC2 EC2-Instance aus zuzulassen. Nachdem Sie dies getan haben, können Sie von Ihrer EC2-Instance aus eine Verbindung zu Ihrem Cluster herstellen. Auf diese Weise können Sie Daten von Ihrer EC2-Instance an Ihre Datenbank senden.

    - Geben Sie — ein **`Custom TCP`**
    - Quelle — Die ID der EC2-Sicherheitsgruppe, die Sie zuvor in diesem Thema erstellt haben, z. B.: sg-9edd5cfb.

5. Wählen Sie Create security group (Sicherheitsgruppe erstellen) aus, um die Sicherheitsgruppe zu erstellen.

Schritt 4: Erstellen Sie eine Subnetzgruppe

Eine Subnetzgruppe ist eine Sammlung von Subnetzen, die Sie in einer VPC erstellen und die Sie dann für Ihre Cluster festlegen. Mithilfe einer Subnetzgruppe können Sie beim Erstellen von Clustern eine bestimmte VPC angeben. Um eine kompatible Subnetzgruppe zu erstellen, müssen alle Subnetze `DUAL` kompatibel sein. `DUAL` Um mit `DUAL` kompatibel zu sein, muss einem Subnetz ein IPv6 CIDR zugeordnet sein.

Um eine Subnetzgruppe zu erstellen

1. Identifizieren Sie die privaten Subnetze für Ihre Datenbank in der VPC.

    a. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc.

    b. Wählen Sie VPC Dashboard (VPC-Dashboard) und dann Subnets (Subnetze) aus.

    c. Notieren Sie sich die Subnetz-IDs der Subnetze, die Sie in Schritt 1 erstellt haben, mit den folgenden Namen: example-dual-stack-subnet-subnet-private1-us-west-2a und example-dual-stack-subnet-private2-us-west-2b. Sie benötigen die Subnetz-IDs, wenn Sie Ihre Subnetzgruppe erstellen.

2. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.

Stellen Sie sicher, dass Sie eine Verbindung zur Amazon DocumentDB DocumentDB-Konsole herstellen, nicht zur Amazon VPC-Konsole.

3. Wählen Sie im Navigationsbereich Subnetzgruppe aus.
4. Wählen Sie Erstellen aus.
5. Legen Sie auf der Seite Subnetzgruppe erstellen im Abschnitt Subnetzgruppendetails die folgenden Werte fest:
   - Name — **`example-dual-stack-cluster-subnet-group`**
   - Beschreibung — **`Dual-stack cluster subnet group`**
6. Legen Sie im Abschnitt Subnetze hinzufügen die folgenden Werte fest:
   - VPC — Wählen Sie die VPC aus, die Sie zuvor erstellt haben, zum Beispiel: vpc-example-dual-stack
   - Availability Zones — Wählen Sie beide Availability Zones aus, die in Schritt 1 erstellt wurden. Beispiel: us-west-2a und us-west-2b
   - Subnetze — Wählen Sie die privaten Subnetze aus, die Sie in Schritt 1 erstellt haben.
7. Wählen Sie Erstellen aus.

Ihre neue Subnetzgruppe wird in der Liste der Subnetzgruppen auf der DocumentDB-Konsole angezeigt. Sie können die Subnetzgruppe auswählen, um Details im Detailbereich anzuzeigen. Diese Informationen umfassen alle Subnetze, die der Gruppe zugeordnet sind.

Schritt 5: Erstellen Sie eine Amazon EC2 EC2-Instance im Dual-Stack-Modus

Um eine Amazon EC2 EC2-Instance zu erstellen, folgen Sie den Anweisungen unter Starten einer EC2-Instance mithilfe des Launch-Instance-Assistenten in der Konsole im Amazon Elastic Compute Cloud-Benutzerhandbuch.

Legen Sie auf der Seite Configure Instance Details (Konfigurieren von Instance-Detail)s wie im Folgenden gezeigt die folgenden Werte fest und behalten Sie die Standardwerte für die anderen Werte bei:

- Netzwerk — Wählen Sie eine vorhandene VPC mit öffentlichen und privaten Subnetzen aus, z. B. vpc-example-dual-stack-vpc (vpc- identifier), die in erstellt wurde. Schritt 1: Erstellen Sie eine VPC mit privaten und öffentlichen Subnetzen

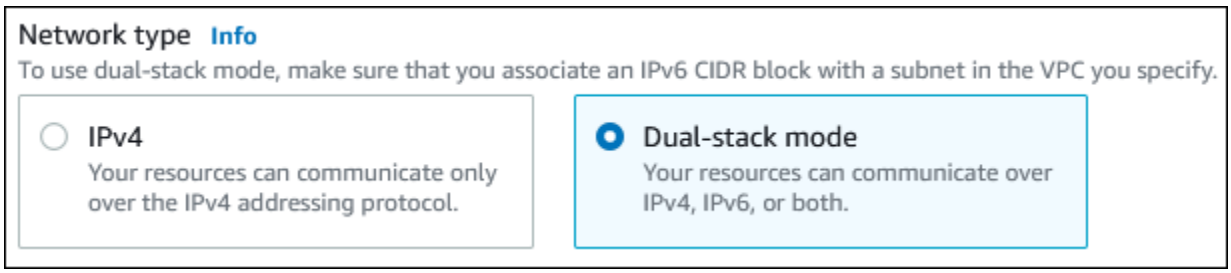
- Subnetz — Wählen Sie ein vorhandenes öffentliches Subnetz aus, z. B. subnet - identifier | example-dual-stack-subnet-public1-us-east-2a | us-east-2a, erstellt in. Schritt 2: Erstellen Sie eine VPC-Sicherheitsgruppe für eine öffentliche Amazon EC2 EC2-Instance
- Auto-assign Öffentliche IP — Wählen Sie Aktivieren.
- Auto-assign IPv6-IP — Wählen Sie Aktivieren.
- Firewall (Sicherheitsgruppen) Wählen Sie eine vorhandene Sicherheitsgruppe aus. —
- Allgemeine Sicherheitsgruppen — Wählen Sie eine vorhandene Sicherheitsgruppe aus, z. B. die in erstellte Example-Dual-Stack-SecurityGroup. Schritt 2: Erstellen Sie eine VPC-Sicherheitsgruppe für eine öffentliche Amazon EC2 EC2-Instance Stellen Sie sicher, dass die von Ihnen gewählte Sicherheitsgruppe Regeln für eingehenden Datenverkehr für Secure Shell (SSH) und HTTP-Zugriff enthält.

Schritt 6: Erstellen Sie einen Cluster im Dual-Stack-Modus

In diesem Schritt erstellen Sie einen DB-Cluster, der im Dual-Stack-Modus ausgeführt wird. !!! Hinweis: Dieser Abschnitt muss bearbeitet werden, sobald die IPv6-Updates an der Konsole vorgenommen wurden!!!

Um einen Cluster im Dual-Stack-Modus zu erstellen

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Wählen Sie in der oberen rechten Ecke der Konsole den Ort aus, an AWS-Region dem Sie den DocumentDB-Cluster erstellen möchten. In diesem Beispiel wird die Region USA Ost (Ohio) verwendet.
3. Klicken Sie im Navigationsbereich auf Cluster.
4. Wählen Sie auf der Cluster-Listenseite die Option Create aus.
5. Stellen Sie auf der Seite Amazon DocumentDB-Cluster erstellen sicher, dass die Instance-based Cluster-Option ausgewählt ist.
6. Wählen Sie im Abschnitt Konnektivität unter Netzwerktyp die Option Dual-stack Modus aus.



7. Aktivieren Sie unten auf der Seite die Option Erweiterte Einstellungen anzeigen.
8. Stellen Sie im Bereich Netzwerkeinstellungen die folgenden Werte ein:

   - Virtual Private Cloud (VPC) — Wählen Sie eine bestehende VPC mit öffentlichen und privaten Subnetzen aus, z. B. vpc-example-dual-stack (vpc- identifier), die in erstellt wurde. Schritt 1: Erstellen Sie eine VPC mit privaten und öffentlichen Subnetzen

     Die VPC muss Subnetze in verschiedenen Availability Zones haben.
   - Subnetzgruppe — Wählen Sie eine Subnetzgruppe für die VPC aus, z. B. example-dual-stack-cluster-subnet-group created in. Schritt 4: Erstellen Sie eine Subnetzgruppe
   - Öffentlicher Zugriff — Wählen Sie Nein.
   - VPC-Sicherheitsgruppe (Firewall) — Wählen Sie Bestehende auswählen aus.
   - Bestehende VPC-Sicherheitsgruppen — Wählen Sie eine vorhandene VPC-Sicherheitsgruppe aus, die für privaten Zugriff konfiguriert ist, z. B. example-dual-stack-cluster-securitygroup, die in erstellt wurde. Schritt 3: Erstellen Sie eine VPC-Sicherheitsgruppe für einen privaten Cluster

     Entfernen Sie andere Sicherheitsgruppen wie die Standardsicherheitsgruppe, indem Sie das jeweilige X wählen.
   - Availability Zone — Wählen Sie die Availability Zone aus, die Sie in Schritt 1 erstellt haben. Beispiel: us-west-2a.

     Um AZ-übergreifenden Verkehr zu vermeiden, stellen Sie sicher, dass sich der Cluster und die EC2-Instance in derselben Availability Zone befinden.
9. Geben Sie für die verbleibenden Abschnitte Ihre Clustereinstellungen an. Weitere Informationen zu den einzelnen Einstellungen finden Sie unter Einen Amazon DocumentDB-Cluster erstellen.

Schritt 7: Connect zu Ihrer Amazon EC2 EC2-Instance und Ihrem DB-Cluster her

Nachdem Sie Ihre Amazon EC2 EC2-Instance und Ihren DocumentDB-Cluster im Dual-Stack-Modus erstellt haben, können Sie über das IPv6-Protokoll eine Verbindung zu beiden herstellen. Um mithilfe

des IPv6-Protokolls eine Connect zu einer EC2-Instance herzustellen, folgen Sie den Anweisungen unter Verbinden Sie Ihre EC2-Instance im Amazon Elastic Compute Cloud-Benutzerhandbuch.

Um von der EC2-Instance aus eine Verbindung zu Ihrem DocumentDB-Cluster herzustellenSchritt 5: Installieren Sie die MongoDB-Shell, folgen Sie den Anweisungen im Thema Amazon EC2 manuell Connect (und fahren Sie mit den nachfolgenden Schritten 6 und 7 im gleichen Verfahren fort).

Löschen der VPC

Sie können eine VPC und die anderen Ressourcen, die darin verwendet werden, löschen, wenn sie nicht mehr benötigt werden.

> **Note**
>
> Wenn Sie der VPC, die Sie in diesem Thema erstellt haben, Ressourcen hinzugefügt haben, müssen Sie diese möglicherweise löschen, bevor Sie die VPC löschen können. Zu diesen Ressourcen können beispielsweise Amazon EC2 EC2-Instances oder DocumentDB-Cluster gehören. Weitere Informationen finden Sie unter Löschen Ihrer VPC im Amazon VPC User Guide.

So löschen Sie eine VPC und zugehörige Ressourcen

1. Löschen Sie die Subnetzgruppe:
   a. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
   b. Wählen Sie im Navigationsbereich Subnetzgruppe aus.
   c. Wählen Sie die Subnetzgruppe aus, die Sie löschen möchten, z. B. example-dual-stack-cluster-subnet-group.
   d. Wählen Sie Löschen, und wählen Sie dann im Bestätigungsfenster Löschen.
2. Notieren Sie sich die VPC-ID.
   a. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc.
   b. Wählen Sie VPC Dashboard und dann Your VPCs aus.
   c. Identifizieren Sie in der Liste die VPC, die Sie erstellt haben, z. B. vpc-example-dual-stack.
   d. Notieren Sie die VPC ID (VPC-ID) der VPC, die Sie erstellt haben. Sie benötigen die VPC-ID in späteren Schritten.

3. Löschen der Sicherheitsgruppen:

    a. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc.

    b. Wählen Sie VPC Dashboard und dann Sicherheitsgruppen.

    c. Wählen Sie die Sicherheitsgruppe für den Amazon DocumentDB-Cluster aus, z. B. example-dual-stack-securitygroup.

    d. Wählen Sie für Aktionen die Option Sicherheitsgruppen löschen und wählen Sie dann im Bestätigungsdialogfeld Löschen aus.

    e. Zurück auf der Seite Sicherheitsgruppen wählen Sie die Sicherheitsgruppe für die Amazon EC2 EC2-Instance aus, z. B. example-securitygroup.

    f. Wählen Sie für Aktionen die Option Sicherheitsgruppen löschen und wählen Sie dann im Bestätigungsdialogfeld Löschen aus.

4. Löschen des NAT-Gateways:

    a. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc.

    b. Wählen Sie VPC Dashboard und dann Sicherheitsgruppen.

    c. Wählen Sie das NAT-Gateway der VPC aus, die Sie erstellt haben. Verwenden Sie die VPC-ID, um das richtige NAT-Gateway zu identifizieren.

    d. Wählen Sie unter Actions (Aktionen) die Option Delete NAT gateway (NAT-Gateway löschen) aus.

    e. Geben Sie im Bestätigungsdialogfeld die Eingabetaste ein**`delete`**, und wählen Sie dann Löschen aus.

5. Löschen der VPC:

    a. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc.

    b. Wählen Sie VPC Dashboard und dann Your VPCs aus.

    c. Wählen Sie die VPC aus, die Sie löschen möchten, z. B. vpc-example-dual-stack.

    d. Wählen Sie für Aktionen die Option VPC löschen aus.

    Auf der Bestätigungsseite werden weitere Ressourcen angezeigt, die der VPC zugeordnet sind, die ebenfalls gelöscht werden, einschließlich der damit verknüpften Subnetze.

    e. Geben Sie im Bestätigungsdialogfeld die Eingabetaste ein **`delete`** und wählen Sie dann Löschen aus.

6. Geben Sie die elastische IP-Adresse frei:

a. Öffnen Sie die EC2-Konsole unter https://console.aws.amazon.com/ec2.
b. Klicken Sie aufEC2-DashboardKlicken Sie auf und danach aufElastische IP-Adressenaus.
c. Wählen Sie die Elastic-IP-Adresse aus, die Sie freigeben möchten.
d. Wählen Sie unter Actions (Aktionen) die Option Release Elastic IP addresses (Elastic-IP-Adressenfreigeben) aus.
e. Wählen Sie im Bestätigungsdialogfeld die Option Release aus.

Sichern und Wiederherstellen in Amazon DocumentDB

Amazon DocumentDB (mit MongoDB-Kompatibilität) sichert Ihre Daten kontinuierlich 1—35 Tage lang auf Amazon Simple Storage Service (Amazon S3), sodass Sie sie an jedem beliebigen Punkt innerhalb der Aufbewahrungsfrist für Backups schnell wiederherstellen können. Amazon DocumentDB erstellt im Rahmen dieses kontinuierlichen Backup-Prozesses auch automatische Schnappschüsse Ihrer Daten.

> **Note**
>
> Dies sind vom Service verwaltete Amazon S3 S3-Buckets, und Sie haben keinen Zugriff auf die Sicherungsdateien. Wenn Sie Ihre eigenen Backups kontrollieren möchten, folgen Sie den Anweisungen zum Dumping, Wiederherstellen, Importieren und Exportieren von Daten.

Sie können Backup-Daten auch über die Aufbewahrungsfrist hinaus aufbewahren, indem Sie einen manuellen Snapshot der Daten Ihres Clusters erstellen. Der Backup-Prozess hat keinen Einfluss auf die Leistung Ihres Clusters.

In diesem Abschnitt werden die Anwendungsfälle für die Backup-Funktionen in Amazon DocumentDB beschrieben und es wird gezeigt, wie Sie Backups für Ihre Amazon DocumentDB-Cluster verwalten.

Themen

- Sichern und Wiederherstellen: Konzepte
- Grundlegendes zur Sicherungsspeicher-Nutzung in
- Daten speichern, wiederherstellen, importieren und exportieren
- Überlegungen zu Cluster-Snapshots
- Vergleich von automatischen und manuellen Snapshots
- Einen manuellen Cluster-Snapshot erstellen
- Amazon DocumentDB-Cluster-Snapshots kopieren
- Amazon DocumentDB-Cluster-Snapshots teilen
- Wiederherstellung aus einem Cluster-Snapshot
- Zu einem bestimmten Zeitpunkt wiederherstellen
- Löschen eines Cluster-Snapshots

Sichern und Wiederherstellen: Konzepte

Substantiv	Description	APIs (Verben)

Aufbewahrungszeitraum für Backups	Ein Zeitraum zwischen 1 und 35 Tagen, für den Sie eine Point-in-Time Wiederherstellung durchführen können.	`create-db-cluster`
		`modify-db-cluster`
		`restore-db-cluster-to-point-in-time`

Amazon DocumentDB DocumentDB-Speichervolumen	Hochverfügbares und sehr robustes Speichervolume, das Daten auf sechs Arten in drei Availability Zones repliziert. Ein Amazon DocumentDB-Cluster ist unabhängi	`create-db-cluster` `delete-db-cluster`

Substantiv	Description	APIs (Verben)
	g von der Anzahl der Instances im Cluster äußerst robust.	

Backup window	Zeitspanne an dem Tag, an dem automatische Snapshots gemacht werden.	`create-db-cluster`
		`describe-db-cluster`
		`modify-db-cluster`

Substantiv	Description	APIs (Verben)

Automatischer Snapshot	Tägliche Snapshots, bei denen es sich um vollständige Backups des Clusters handelt, die automatisch durch den kontinuierlichen Backup-Prozess in Amazon DocumentDB erstellt werden.	`restore-db-cluster-from-snapshot`
		
		`describe-db-cluster-snapshot-attributes`
		
		`describe-db-cluster-snapshots`

Substantiv	Description	APIs (Verben)

Manueller Snapshot	Snapshots, die Sie manuell erstellen, um Vollsicherungen eines Clusters über den Sicherungszeitraum hinaus aufzubewahren.	`create-db-cluster-snapshot`
		`copy-db-cluster-snapshot`
		`delete-db-cluster-snapshot`
		`describe-db-cluster-snapshot-attributes`
		`describe-db-cluster-snapshots`
		`modify-db-cluster-snapshot-attribute`

Grundlegendes zur Sicherungsspeicher-Nutzung in

Der Amazon DocumentDB-Backup-Speicher besteht aus kontinuierlichen Backups innerhalb des Aufbewahrungszeitraums für Backups und manuellen Snapshots außerhalb des Aufbewahrungszeitraums. Wenn Sie Ihren Sicherungsspeicher kontrollieren möchten, können Sie das Aufbewahrungsintervall für Sicherungen verringern, alte (nicht mehr benötigte) manuelle Snapshots entfernen oder beides. Allgemeine Informationen zu Amazon DocumentDB-Backups finden Sie unterSichern und Wiederherstellen in Amazon DocumentDB. Preisinformationen zum Amazon DocumentDB-Backup-Speicher finden Sie unter Amazon DocumentDB DocumentDB-Preise.

Wenn Sie Ihre Kosten kontrollieren möchten, können Sie die Menge des Speichers überwachen, der nach Ablauf des Aufbewahrungszeitraums noch von kontinuierlichen Sicherungen und manuellen Snapshots belegt wird. Anschließend können Sie den Aufbewahrungszeitraum für Backups verringern und manuelle Snapshots entfernen, wenn sie nicht mehr benötigt werden.

Sie können die CloudWatch Amazon-Metriken`TotalBackupStorageBilled`,, wie folgt verwenden`SnapshotStorageUsed`, `BackupRetentionPeriodStorageUsed` um die Menge an Speicherplatz zu überprüfen und zu überwachen, die von Ihren Amazon DocumentDB-Backups verwendet wird:

- `BackupRetentionPeriodStorageUsed` stellt den Umfang des Backup-Speichers zum Speichern von kontinuierlichen Backups zur aktuellen Zeit dar. Dieser Metrikwert hängt von der Größe des Cluster-Volumens und der Menge der von Ihnen während des Aufbewahrungszeitraums vorgenommenen Änderungen ab. Für Fakturierungszwecke übersteigt die Metrik die kumulative Cluster-Volume-Größe während des Aufbewahrungszeitraums nicht. Beispiel: Wenn Ihr Cluster 100 GiB groß ist und Ihr Aufbewahrungszeitraum zwei Tage beträgt, hat `BackRetentionPeriodStorageUsed` einen Maximalwert von 200 GiB (100 GiB+100 GiB).

- `SnapshotStorageUsed` stellt den Umfang des Backup-Speichers zum Speichern von manuellen Snapshots außerhalb des Aufbewahrungszeitraums für Backups dar. Innerhalb des Aufbewahrungszeitraums manuell aufgenommene Snapshots zählen nicht zu Ihrem Backup-Speicher. Ebenso werden automatische Snapshots nicht zu Ihrem Backup-Speicher gezählt. Die Größe einzelner Snapshots entspricht der Größe des Cluster-Volumes zum Zeitpunkt der Snapshot-Erstellung. Der `SnapshotStorageUsed`-Wert hängt von der Anzahl der Snapshots ab, die Sie aufbewahren, und von der Größe der einzelnen Snapshots. Beispiel: Angenommen, Sie haben einen Snapshot außerhalb des Aufbewahrungszeitraums und die Cluster-Volume-Größe betrug 100 GiB, als der Snapshot erstellt wurde. Dann beträgt die `SnapshotStorageUsed`-Menge 100 GiB.

- `TotalBackupStorageBilled` stellt die Summe von `BackupRetentionPeriodStorageUsed` und `SnapshotStorageUsed` abzüglich des freien Backup-Speichers gleich der Größe des Cluster-Volumes für einen Tag dar. Wenn Ihre Clustergröße beispielsweise 100 GiB beträgt, haben Sie einen Aufbewahrungstag und Sie haben einen Snapshot außerhalb des Aufbewahrungszeitraums, dieser `TotalBackupStorageBilled` beträgt 100 GiB (100 GiB + 100 GiB — 100 GiB).

- Diese Metriken werden unabhängig für jeden Amazon DocumentDB-Cluster berechnet.

Sie können Ihre Amazon DocumentDB-Cluster überwachen und Berichte mithilfe von CloudWatch Metriken über die CloudWatch Konsole erstellen. Weitere Informationen zur Verwendung von CloudWatch Metriken finden Sie unterAmazon DocumentDB überwachen.

Daten speichern, wiederherstellen, importieren und exportieren

Sie können die `mongoimport` Dienstprogramme`mongodump`,`mongorestore`, und verwenden`mongoexport`, um Daten in und aus Ihrem Amazon DocumentDB-Cluster zu verschieben. In diesem Abschnitt wird der Zweck der einzelnen Tools und Konfigurationen beschrieben, damit Sie die Leistung verbessern können.

Themen

- Mongodump
- mongorestore
- mongoexport
- Mongoimport
- Tutorial

Mongodump

Das Dienstprogramm `mongodump` erstellt eine binäre (BSON)-Sicherung einer MongoDB-Datenbank. Das `mongodump` Tool ist aufgrund der Größeneffizienz, die durch das Speichern der Daten in einem Binärformat erzielt wird, die bevorzugte Methode zum Dumping von Daten aus Ihrer MongoDB-Quellbereitstellung, wenn Sie sie in Ihrem Amazon DocumentDB-Cluster wiederherstellen möchten.

Abhängig von den Ressourcen, die auf der Instanz oder dem Computer verfügbar sind, den Sie für die Ausführung des Befehls verwenden, können Sie Ihren Vorgang beschleunigen, `mongodump` indem Sie die Anzahl der parallel Sammlungen erhöhen, die von der Standardeinstellung 1 abgerufen werden, indem Sie die `--numParallelCollections` Option verwenden. Eine gute Faustregel lautet, mit einem Worker pro vCPU auf der primären Instance Ihres Amazon DocumentDB-Clusters zu beginnen.

> **Note**
>
> Wir empfehlen MongoDB Database Tools bis einschließlich Version 100.6.1 für Amazon DocumentDB. Sie können hier auf die Downloads der MongoDB Database Tools zugreifen.

Beispielverwendung

Im Folgenden finden Sie ein Beispiel für die Verwendung des mongodump Dienstprogramms im Amazon DocumentDB-Cluster,`sample-cluster`.

```
mongodump --ssl \
    --host="sample-cluster.node.us-east-1.docdb.amazonaws.com:27017" \
    --collection=sample-collection \
    --db=sample-database \
    --out=sample-output-file \
    --numParallelCollections 4  \
    --username=sample-user \
    --password=abc0123 \
    --sslCAFile global-bundle.pem
```

`mongorestore`

Mit dem Dienstprogramm `mongorestore` können Sie eine Binärsicherung (BSON) einer Datenbank wiederherstellen, die mit dem Dienstprogramm `mongodump` erstellt wurde. Sie können die Wiederherstellungsleistung verbessern, indem Sie die Anzahl der Worker für jede Sammlung während der Wiederherstellung mit der Option `--numInsertionWorkersPerCollection` erhöhen. (Der Standardwert ist 1.) Eine gute Faustregel lautet, mit einem Worker pro vCPU auf der primären Instance Ihres Amazon DocumentDB-Clusters zu beginnen.

Beispielverwendung

Im Folgenden finden Sie ein Beispiel für die Verwendung des `mongorestore` Dienstprogramms im Amazon DocumentDB-Cluster,`sample-cluster`.

```
mongorestore --ssl \
    --host="sample-cluster.node.us-east-1.docdb.amazonaws.com:27017" \
    --username=sample-user \
    --password=abc0123 \
    --sslCAFile global-bundle.pem <fileToBeRestored>
```

`mongoexport`

Das `mongoexport` Tool exportiert Daten in Amazon DocumentDB in die Dateiformate JSON, CSV oder TSV. Das `mongoexport`-Tool ist die bevorzugte Methode für den Export von Daten, die für Menschen oder Maschinen lesbar sein müssen.

> **Note**
>
> `mongoexport` unterstützt parallele Exporte nicht direkt. Es ist jedoch möglich, die Leistung zu steigern, indem mehrere `mongoexport`-Aufgaben gleichzeitig für verschiedene Sammlungen ausgeführt werden.

Beispielverwendung

Im Folgenden finden Sie ein Beispiel für die Verwendung des `mongoexport` Tools im Amazon DocumentDB-Cluster,`sample-cluster`.

```
mongoexport --ssl \
    --host="sample-cluster.node.us-east-1.docdb.amazonaws.com:27017" \
    --collection=sample-collection \
    --db=sample-database \
    --out=sample-output-file \
    --username=sample-user \
    --password=abc0123 \
    --sslCAFile global-bundle.pem
```

Mongoimport

Das `mongoimport` Tool importiert den Inhalt von JSON-, CSV- oder TSV-Dateien in einen Amazon DocumentDB-Cluster. Mithilfe des Parameters `--numInsertionWorkers` können Sie den Import parallelisieren und beschleunigen. (Der Standardwert ist 1.)

Beispielverwendung

Im Folgenden finden Sie ein Beispiel für die Verwendung des `mongoimport` Tools im Amazon DocumentDB-Cluster,`sample-cluster`.

```
mongoimport --ssl \
    --host="sample-cluster.node.us-east-1.docdb.amazonaws.com:27017" \
    --collection=sample-collection \
    --db=sample-database \
    --file=<yourFile> \
    --numInsertionWorkers 4 \
    --username=sample-user \
    --password=abc0123 \
```

```
    --sslCAFile global-bundle.pem
```

Tutorial

Das folgende Tutorial beschreibt, wie Sie die `mongoimport` Dienstprogramme`mongodump`,`mongorestore`, und verwenden`mongoexport`, um Daten in und aus einem Amazon DocumentDB-Cluster zu verschieben.

1. Voraussetzungen — Bevor Sie beginnen, stellen Sie sicher, dass Ihr Amazon DocumentDB-Cluster bereitgestellt ist und dass Sie Zugriff auf eine Amazon EC2 EC2-Instance in derselben VPC wie Ihr Cluster haben. Weitere Informationen finden Sie unter Stellen Sie mithilfe von Amazon EC2 eine Verbindung her.

   Um die mongo-Dienstprogrammtools verwenden zu können, muss das mongodb-org-tools-Paket wie folgt in Ihrer EC2-Instance installiert sein.

   ```
   sudo yum install mongodb-org-tools-4.0.18
   ```

   Da Amazon DocumentDB standardmäßig die Transport Layer Security (TLS) -Verschlüsselung verwendet, müssen Sie auch die Datei der Amazon RDS-Zertifizierungsstelle (CA) herunterladen, um die Mongo-Shell für die Verbindung zu verwenden. Gehen Sie dazu wie folgt vor.

   ```
   wget https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem
   ```

2. Beispieldaten herunterladen — Für dieses Tutorial laden Sie einige Beispieldaten herunter, die Informationen über Restaurants enthalten.

   ```
   wget https://raw.githubusercontent.com/ozlerhakan/mongodb-json-files/master/
   datasets/restaurant.json
   ```

3. Importieren Sie die Beispieldaten in Amazon DocumentDB — Da die Daten in einem logischen JSON-Format vorliegen, verwenden Sie das `mongoimport` Hilfsprogramm, um die Daten in Ihren Amazon DocumentDB-Cluster zu importieren.

   ```
   mongoimport --ssl \
       --host="tutorialCluster.amazonaws.com:27017" \
       --collection=restaurants \
       --db=business \
   ```

```
    --file=restaurant.json \
    --numInsertionWorkers 4 \
    --username=<yourUsername> \
    --password=<yourPassword> \
    --sslCAFile global-bundle.pem
```

4. Daten ausgeben mit **`mongodump`** — Da Sie nun Daten in Ihrem Amazon DocumentDB-Cluster haben, können Sie mit dem Hilfsprogramm einen binären Speicherauszug dieser Daten erstellen. `mongodump`

```
mongodump --ssl \
    --host="tutorialCluster.us-east-1.docdb.amazonaws.com:27017"\
    --collection=restaurants \
    --db=business \
    --out=restaurantDump.bson \
    --numParallelCollections 4 \
    --username=<yourUsername> \
    --password=<yourPassword> \
    --sslCAFile global-bundle.pem
```

5. **`restaurants`**Sammlung löschen — Bevor Sie die `restaurants` Sammlung in der `business` Datenbank wiederherstellen, müssen Sie zunächst die Sammlung löschen, die bereits in dieser Datenbank vorhanden ist, und zwar wie folgt.

```
use business
```

```
db.restaurants.drop()
```

6. Daten wiederherstellen mit **`mongorestore`** — Mit dem binären Speicherauszug der Daten aus Schritt 3 können Sie jetzt das `mongorestore` Hilfsprogramm verwenden, um Ihre Daten in Ihrem Amazon DocumentDB-Cluster wiederherzustellen.

```
mongorestore --ssl \
    --host="tutorialCluster.us-east-1.docdb.amazonaws.com:27017" \
    --numParallelCollections 4 \
    --username=<yourUsername> \
    --password=<yourPassword> \
    --sslCAFile global-bundle.pem restaurantDump.bson
```

7. Daten exportieren mit **`mongoexport`** — Um das Tutorial abzuschließen, exportieren Sie die Daten aus Ihrem Cluster im Format einer JSON-Datei, die sich nicht von der Datei unterscheidet, die Sie in Schritt 1 importiert haben.

```
mongoexport --ssl \
    --host="tutorialCluster.node.us-east-1.docdb.amazonaws.com:27017" \
    --collection=restaurants \
    --db=business \
    --out=restaurant2.json \
    --username=<yourUsername> \
    --password=<yourPassword> \
    --sslCAFile global-bundle.pem
```

8. Validierung — Mit den folgenden Befehlen können Sie überprüfen, ob die Ausgabe von Schritt 5 dasselbe Ergebnis wie Schritt 1 liefert.

```
wc -l restaurant.json
```

Ausgabe dieses Befehls:

```
2548 restaurant.json
```

```
wc -l restaurant2.json
```

Ausgabe dieses Befehls:

```
2548 restaurant2.json
```

Überlegungen zu Cluster-Snapshots

Amazon DocumentDB erstellt täglich automatische Snapshots Ihres Clusters während des Backup-Fensters Ihres Clusters. Amazon DocumentDB speichert die automatischen Snapshots Ihres Clusters entsprechend dem von Ihnen angegebenen Aufbewahrungszeitraum für Backups. Bei Bedarf können Sie Ihren Cluster zu einem beliebigen Zeitpunkt während der Aufbewahrungsdauer des Backups wiederherstellen. Automatische Snapshots treten nicht auf, während ein Kopiervorgang in derselben Region für denselben Cluster ausgeführt wird.

Themen

- Backup-Speicher
- Backup window
- Aufbewahrungszeitraum für Backups
- Kopieren Sie die Cluster-Snapshot-

Zusätzlich zu den automatischen Cluster-Snapshots können Sie auch manuell einen Cluster-Snapshot erstellen. Sie können sowohl automatische als auch manuelle Snapshots kopieren. Weitere Informationen erhalten Sie unter Einen manuellen Cluster-Snapshot erstellen und Amazon DocumentDB-Cluster-Snapshots kopieren.

> **Note**
>
> Ihr Cluster muss sich im Status verfügbar befinden, damit ein automatischer Snapshot erstellt werden kann.
> Sie können keinen automatisierten Amazon DocumentDB-Cluster-Snapshot teilen. Als Problemumgehung können Sie einen manuellen Snapshot erstellen, indem Sie den automatisierten Snapshot kopieren und dann diese Kopie freigeben. Weitere Informationen zum Kopieren eines Snapshots finden Sie unter Amazon DocumentDB-Cluster-Snapshots kopieren. Weitere Informationen zum Wiederherstellen eines Clusters aus einem Snapshot finden Sie unter Wiederherstellung aus einem Cluster-Snapshot.

Backup-Speicher

Ihr Amazon DocumentDB-Backup-Speicher AWS-Region besteht aus dem Backup-Speicher, der für Ihren Backup-Aufbewahrungszeitraum benötigt wird, einschließlich automatischer und manueller Cluster-Snapshots in dieser Region. Der standardmäßige Aufbewahrungszeitraum für Backups beträgt 1 Tag. Weitere Informationen zu den Preisen für Backup-Speicher finden Sie unter Amazon DocumentDB DocumentDB-Preise.

Wenn Sie einen Cluster löschen, werden alle seine automatischen Snapshots gelöscht und können nicht wiederhergestellt werden. Manuelle Snapshots werden jedoch nicht gelöscht, wenn Sie einen Cluster löschen. Wenn Sie Amazon DocumentDB einen endgültigen Snapshot (manueller Snapshot) erstellen lassen möchten, bevor Ihr Cluster gelöscht wird, können Sie den endgültigen Snapshot verwenden, um Ihren Cluster wiederherzustellen.

Weitere Informationen zu Snapshots und Speicher finden Sie unter Grundlegendes zur Sicherungsspeicher-Nutzung in.

Backup window

Automatische Snapshots erfolgen täglich während des bevorzugten Backup-Fensters. Wenn der Snapshot mehr Zeit benötigt, als dem Backup-Fenster zugewiesen wurde, wird der Backup-Prozess bis zum Ende fortgesetzt, auch wenn das Backup-Fenster beendet ist. Das Backup-Fenster kann sich nicht mit dem wöchentlichen Wartungsfenster für den Cluster überschneiden.

Wenn Sie bei der Erstellung des Clusters kein bevorzugtes Backup-Fenster angeben, weist Amazon DocumentDB ein standardmäßiges 30-minütiges Backup-Fenster zu. Dieses Fenster wird nach dem Zufallsprinzip aus einem 8-stündigen Zeitblock ausgewählt, der mit der Region Ihres Clusters verknüpft ist. Sie können Ihr bevorzugtes Backup-Fenster ändern, indem Sie den Cluster ändern. Weitere Informationen finden Sie unter Ändern eines Amazon DocumentDB-Clusters.

Name der Region	Region	UTC-Zeitblock
USA Ost (Ohio)	us-east-2	03:00-11:00
USA Ost (Nord-Virginia)	us-east-1	03:00-11:00
USA West (Oregon)	us-west-2	06:00-14:00
Afrika (Kapstadt)	af-south-1	03:00 — 11:00
Asien-Pazifik (Hongkong)	ap-east-1	06:00-14:00
Asien-Pazifik (Hyderabad)	ap-south-2	06:30 — 14:30
Asien-Pazifik (Malaysia)	ap-southeast-5	13:00-21:00
Asien-Pazifik (Mumbai)	ap-south-1	06:00-14:00
Asia Pacific (Osaka)	ap-northeast-3	12:00-20:00
Asien-Pazifik (Seoul)	ap-northeast-2	13:00-21:00
Asien-Pazifik (Singapur)	ap-southeast-1	14:00-22:00
Asien-Pazifik (Sydney)	ap-southeast-2	12:00-20:00

Name der Region	Region	UTC-Zeitblock
Asien-Pazifik (Jakarta)	ap-southeast-3	08:00-16:00
Asien-Pazifik (Melbourne)	ap-southeast-4	11:00-19:00
Asien-Pazifik (Thailand)	ap-southeast-7	15:00-23:00
Asien-Pazifik (Tokio)	ap-northeast-1	13:00-21:00
Kanada (Zentral)	ca-central-1	03:00-11:00
Kanada West (Calgary)	ca-west-1	18:00-02:00
China (Beijing)	cn-north-1	06:00-14:00
China (Ningxia)	cn-northwest-1	06:00-14:00
Europa (Frankfurt)	eu-central-1	21:00-05:00
Europa (Zürich)	eu-central-2	02:00-10:00
Europa (Irland)	eu-west-1	22:00-06:00
Europa (London)	eu-west-2	22:00-06:00
Europa (Milan)	eu-south-1	02:00-10:00
Europa (Paris)	eu-west-3	23:59-07:29
Europa (Spain)	eu-south-2	02:00 — 10:00
Europa (Stockholm)	eu-north-1	04:00 — 12:00
Mexiko (Zentral)	mx-central-1	03:00-11:00
Naher Osten (VAE)	me-central-1	05:00 — 13:00
Südamerika (São Paulo)	sa-east-1	00:00-08:00
Israel (Tel Aviv)	il-central-1	04:00-12:00

Name der Region	Region	UTC-Zeitblock
AWS GovCloud (US-East)	us-gov-east-1	17:00-01:00
AWS GovCloud (US-West)	us-gov-west-1	06:00-14:00

Aufbewahrungszeitraum für Backups

Die Aufbewahrungsfrist für Backups gibt an, wie viele Tage ein automatisches Backup aufbewahrt wird, bevor es automatisch gelöscht wird. Amazon DocumentDB unterstützt eine Aufbewahrungsdauer von Backups von 1—35 Tagen.

Sie können die Aufbewahrungsdauer des Backups beim Anlegen eines Clusters festlegen. Wenn Sie die Aufbewahrungsdauer für das Backup nicht explizit festlegen, wird Ihrem Cluster die standardmäßige Aufbewahrungsdauer für das Backup von 1 Tag zugewiesen. Nachdem Sie einen Cluster erstellt haben, können Sie den Aufbewahrungszeitraum für Backups ändern, indem Sie den Cluster entweder mit AWS-Managementkonsole oder dem ändern. AWS CLI Weitere Informationen finden Sie unter Ändern eines Amazon DocumentDB-Clusters.

Kopieren Sie die Cluster-Snapshot-

Die Cluster- und Snapshot-Verschlüsselung basiert auf einem KMS-Verschlüsselungsschlüssel. Die KMS-Schlüssel-ID ist der Amazon-Ressourcenname (ARN), der KMS-Schlüsselbezeichner oder der KMS-Schlüsselalias für den KMS-Verschlüsselungsschlüssel.

Es gelten die folgenden Richtlinien und Einschränkungen:

- Bei der Erstellung eines Snapshots wird die Verschlüsselung aus dem Cluster abgeleitet. Wenn der Cluster verschlüsselt ist, wird der Snapshot dieses Clusters mit demselben KMS-Schlüssel verschlüsselt. Wenn der Cluster nicht verschlüsselt ist, ist der Snapshot nicht verschlüsselt.
- Wenn Sie einen verschlüsselten Cluster-Snapshot von Ihrem Amazon Web Services Services-Konto kopieren, können Sie einen Wert angeben, `KmsKeyId` um die Kopie mit einem neuen KMS-Verschlüsselungsschlüssel zu verschlüsseln. Wenn Sie keinen Wert für angeben`KmsKeyId`, wird die Kopie des Cluster-Snapshots mit demselben KMS-Schlüssel verschlüsselt wie der Quell-Cluster-Snapshot.
- Wenn Sie einen verschlüsselten Cluster-Snapshot kopieren, der von einem anderen Amazon Web Services Services-Konto gemeinsam genutzt wird, müssen Sie einen Wert für angeben`KmsKeyId`.

- Um einen verschlüsselten Cluster-Snapshot in eine andere Amazon Web Services Services-Region `KmsKeyId` zu kopieren, legen Sie die KMS-Schlüssel-ID fest, mit der Sie die Kopie des Cluster-Snapshots in der Zielregion verschlüsseln möchten. KMS-Verschlüsselungsschlüssel sind spezifisch für die Amazon Web Services Services-Region, in der sie erstellt wurden, und Sie können keine Verschlüsselungsschlüssel aus einer Amazon Web Services Services-Region in einer anderen Amazon Web Services Services-Region verwenden.
- Wenn Sie einen unverschlüsselten Cluster-Snapshot kopieren und einen Wert für den `KmsKeyId` Parameter angeben, wird ein Fehler zurückgegeben.

Vergleich von automatischen und manuellen Snapshots

Im Folgenden sind die wichtigsten Funktionen der automatischen und manuellen Snapshots von Amazon DocumentDB (mit MongoDB-Kompatibilität) aufgeführt.

Automatische Amazon DocumentDB-Snapshots haben die folgenden Hauptfunktionen:

- Automatische Snapshot-Benennung — Automatische Snapshot-Namen folgen dem Muster `rds:<cluster-name>-yyyy-mm-dd-hh-mm` und geben das `yyyy-mm-dd-hh-mm` Datum und die Uhrzeit der Snapshot-Erstellung an.
- Automatisch nach einem Zeitplan erstellt — Wenn Sie einen Cluster erstellen oder ändern, können Sie den Aufbewahrungszeitraum für Backups auf einen ganzzahligen Wert zwischen 1 und 35 Tagen festlegen. Standardmäßig haben neue Cluster eine Aufbewahrungsdauer von 1 Tag. Die Aufbewahrungsdauer für Backups definiert die Anzahl der Tage, die automatische Snapshots aufbewahrt werden, bevor sie automatisch gelöscht werden. Sie können automatische Backups auf Amazon DocumentDB-Clustern nicht deaktivieren.

  Zusätzlich zur Einstellung der Aufbewahrungsdauer für das Backup legen Sie auch das Backup-Fenster fest (die Tageszeit, zu der automatische Snapshots erstellt werden).
- Automatische Snapshots löschen — Automatische Snapshots werden gelöscht, wenn Sie den Cluster des automatischen Snapshots löschen. Sie können einen automatischen Snapshot nicht manuell löschen.
- Inkrementell — Während der Aufbewahrungszeit der Backups werden Datenbankaktualisierungen aufgezeichnet, sodass eine inkrementelle Aufzeichnung der Änderungen erfolgt.
- Wiederherstellung aus einem automatischen Snapshot — Sie können die Wiederherstellung aus einem automatischen Snapshot mit dem AWS-Managementkonsole oder dem durchführen. AWS

CLI Wenn Sie mithilfe von aus einem Snapshot wiederherstellen AWS CLI, müssen Sie Instanzen separat hinzufügen, sobald der Cluster verfügbar ist.

- Teilen — Sie können einen automatisierten Amazon DocumentDB-Cluster-Snapshot nicht teilen. Als Problemumgehung können Sie einen manuellen Snapshot erstellen, indem Sie den automatisierten Snapshot kopieren und dann diese Kopie freigeben. Weitere Informationen zum Kopieren eines Snapshots finden Sie unter Amazon DocumentDB-Cluster-Snapshots kopieren. Weitere Informationen zum Wiederherstellen eines Clusters aus einem Snapshot finden Sie unter Wiederherstellung aus einem Cluster-Snapshot.
- Sie können von jedem beliebigen Zeitpunkt innerhalb der Aufbewahrungsfrist für Backups aus wiederherstellen — Da Datenbankaktualisierungen inkrementell aufgezeichnet werden, können Sie Ihren Cluster zu jedem beliebigen Zeitpunkt innerhalb der Aufbewahrungsfrist für Backups wiederherstellen.

  Wenn Sie die Wiederherstellung aus einem automatischen Snapshot oder aus einer Point-in-Time-Wiederherstellung mit dem durchführen AWS CLI, müssen Sie Instanzen separat hinzufügen, sobald der Cluster verfügbar ist.

Manuelle Amazon DocumentDB-Snapshots haben die folgenden Hauptfunktionen:

- Auf Anfrage erstellt — Manuelle Amazon DocumentDB-Snapshots werden bei Bedarf mit der Amazon DocumentDB-Managementkonsole oder erstellt. AWS CLI
- Löschen eines manuellen Snapshots — Ein manueller Snapshot wird nur gelöscht, wenn Sie ihn explizit mit der Amazon DocumentDB DocumentDB-Konsole oder AWS CLI löschen. Ein manueller Snapshot wird nicht gelöscht, wenn Sie seinen Cluster löschen.
- Vollständige Backups — Wenn ein manueller Snapshot erstellt wird, wird eine vollständige Sicherung der Daten Ihres Clusters erstellt und gespeichert.
- Manuelle Snapshot-Benennung — Sie geben den Namen des manuellen Snapshots an. Amazon DocumentDB fügt dem Namen keinen `datetime` Stempel hinzu. Sie müssen diese Informationen also hinzufügen, wenn Sie möchten, dass sie in den Namen aufgenommen werden.
- Wiederherstellung aus einem manuellen Snapshot — Sie können die Wiederherstellung aus einem manuellen Snapshot mit der Konsole oder dem durchführen. AWS CLI Bei der Wiederherstellung aus einem Snapshot mit dem müssen Sie Instanzen separat hinzufügen AWS CLI, sobald der Cluster verfügbar ist.
- Servicekontingente — Sie sind auf maximal 100 manuelle Snapshots pro Person AWS-Region beschränkt.

- Teilen — Sie können manuelle Cluster-Snapshots teilen, die von autorisierten Personen kopiert werden können. AWS-Konten Sie können verschlüsselte oder unverschlüsselte manuelle Snapshots freigeben. Weitere Informationen zum Kopieren eines Snapshots finden Sie unter Amazon DocumentDB-Cluster-Snapshots kopieren.
- Sie stellen den Zeitpunkt wieder her, zu dem der manuelle Snapshot erstellt wurde — Wenn Sie eine Wiederherstellung von einem manuellen Snapshot durchführen, stellen Sie den Zeitpunkt wieder her, zu dem der manuelle Snapshot erstellt wurde.

  Wenn Sie die Wiederherstellung aus einem Snapshot mithilfe von AWS CLI durchführen, müssen Sie Instanzen separat hinzufügen, sobald der Cluster verfügbar ist.

Einen manuellen Cluster-Snapshot erstellen

Sie können einen manuellen Snapshot entweder mit AWS-Managementkonsole oder AWS CLI erstellen. Die Zeit, die für die Erstellung eines Snapshots benötigt wird, hängt von der Größe Ihrer Datenbanken ab. Wenn Sie einen Snapshot erstellen, müssen Sie Folgendes tun:

1. Identifizieren Sie den zu sichernden Cluster.
2. Geben Sie Ihrem Snapshot einen Namen. Dies ermöglicht es Ihnen, ihn später wiederherzustellen.

Using the AWS-Managementkonsole

Um einen manuellen Snapshot mit dem zu erstellen AWS-Managementkonsole, können Sie eine der folgenden Methoden verwenden.

1. Methode 1:

   1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
   2. Wählen Sie im Navigationsbereich die Option Snapshots.

      > **Tip**
      >
      > Wenn der Navigationsbereich auf der linken Seite des Bildschirms nicht angezeigt wird, wählen Sie links oben auf der Seite das Menüsymbol (≡) aus.

3. Wählen Sie auf der Seite Snapshots die Option Create (Erstellen) aus.
4. Auf der Seite Create cluster snapshot (Cluster-Snapshot erstellen):
   a. Cluster-ID — Wählen Sie aus der Drop-down-Liste der Cluster den Cluster aus, von dem Sie einen Snapshot erstellen möchten.
   b. Snapshot-ID — Geben Sie einen Namen für Ihren Snapshot ein.

      Einschränkungen bei der Snapshot-Benennung:

      - Die Länge beträgt [1—255] Buchstaben, Zahlen oder Bindestriche.
      - Muss mit einem Buchstaben beginnen.
      - Darf nicht mit einem Bindestrich enden oder zwei aufeinanderfolgende Bindestriche enthalten.
      - Muss für alle Cluster (in Amazon RDS, Amazon Neptune und Amazon DocumentDB) pro AWS Konto und Region eindeutig sein.

   c. Wählen Sie Erstellen aus.

2. Methode 2:

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Klicken Sie im Navigationsbereich auf Cluster.

   > **Tip**
   >
   > Wenn der Navigationsbereich auf der linken Seite des Bildschirms nicht angezeigt wird, wählen Sie links oben auf der Seite das Menüsymbol (≡) aus.

3. Wählen Sie auf der Seite Cluster die Schaltfläche links neben dem Cluster aus, den Sie als Snapshot aufnehmen möchten.
4. Wählen Sie im Menü Actions (Aktionen) die Option Take snapshot (Snapshot erstellen) aus.
5. Auf der Seite Create cluster snapshot (Cluster-Snapshot erstellen):
   a. Snapshot-ID — Geben Sie einen Namen für Ihren Snapshot ein.

      Einschränkungen bei der Snapshot-Benennung:

      - Die Länge beträgt [1—63] Buchstaben, Zahlen oder Bindestriche.

- Muss mit einem Buchstaben beginnen.
- Darf nicht mit einem Bindestrich enden oder zwei aufeinanderfolgende Bindestriche enthalten.
- Muss für alle Cluster (in Amazon RDS, Amazon Neptune und Amazon DocumentDB) pro AWS Konto und Region eindeutig sein.

b. Wählen Sie Erstellen aus.

Using the AWS CLI

Um einen Cluster-Snapshot mit dem zu erstellen AWS CLI, verwenden Sie den `create-db-cluster-snapshot` Vorgang mit den folgenden Parametern.

Parameters

- **`--db-cluster-identifier`** – Erforderlich. Der Name des Clusters, von dem Sie einen Snapshot machen. Dieser Cluster muss vorhanden sein und verfügbar sein.
- **`--db-cluster-snapshot-identifier`** – Erforderlich. Der Name des manuellen Snapshots, den Sie erstellen.

Im folgenden Beispiel wird ein Snapshot mit dem Namen `sample-cluster-snapshot` für einen Clusters namens `sample-cluster` erstellt.

Für Linux, macOS oder Unix:

```
aws docdb create-db-cluster-snapshot \
    --db-cluster-identifier sample-cluster \
    --db-cluster-snapshot-identifier sample-cluster-snapshot
```

Für Windows:

```
aws docdb create-db-cluster-snapshot ^
    --db-cluster-identifier sample-cluster ^
    --db-cluster-snapshot-identifier sample-cluster-snapshot
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus.

```
{
    "DBClusterSnapshot": {
```

```
        "AvailabilityZones": [
            "us-east-1a",
            "us-east-1b",
            "us-east-1c"
        ],
        "DBClusterSnapshotIdentifier": "sample-cluster-snapshot",
        "DBClusterIdentifier": "sample-cluster",
        "SnapshotCreateTime": "2020-04-24T04:59:08.475Z",
        "Engine": "docdb",
        "Status": "creating",
        "Port": 0,
        "VpcId": "vpc-abc0123",
        "ClusterCreateTime": "2020-01-10T22:13:38.261Z",
        "MasterUsername": "master-user",
        "EngineVersion": "4.0.0",
        "SnapshotType": "manual",
        "PercentProgress": 0,
        "StorageEncrypted": true,
        "KmsKeyId": "arn:aws:kms:us-east-1:<accountID>:key/sample-key",
        "DBClusterSnapshotArn": "arn:aws:rds:us-east-1:<accountID>:cluster-
snapshot:sample-cluster-snapshot"
    }
}
```

Amazon DocumentDB-Cluster-Snapshots kopieren

In Amazon DocumentDB können Sie Snapshots innerhalb desselben AWS-Region oder in ein anderes kopieren. AWS-Region Sie können geteilte Snapshots auch auf Ihr Konto in demselben AWS-Region oder in einem anderen Konto kopieren. AWS-Region Weitere Informationen zum Freigeben von Snapshots finden Sie unter Amazon DocumentDB-Cluster-Snapshots teilen.

> **Note**
>
> Amazon DocumentDB berechnet Ihnen auf der Grundlage der Menge der Sicherungs- und Snapshot-Daten, die Sie aufbewahren, und des Zeitraums, in dem Sie sie aufbewahren. Weitere Informationen zum Speicher im Zusammenhang mit Amazon DocumentDB-Backups und -Snapshots finden Sie unter. Grundlegendes zur Sicherungsspeicher-Nutzung in Preisinformationen zum Amazon DocumentDB DocumentDB-Speicher finden Sie unter Amazon DocumentDB DocumentDB-Preise.

Themen

- Kopieren freigegebener Snapshots
- Schnappschüsse werden kopiert AWS-Regionen
- Einschränkungen
- Umgang mit Verschlüsselungen
- Überlegungen zu Parametergruppen
- Einen Cluster-Snapshot kopieren

Kopieren freigegebener Snapshots

Sie können Schnappschüsse kopieren, die Ihnen von anderen Konten zur Verfügung gestellt wurden. AWS Wenn Sie einen verschlüsselten Snapshot kopieren, der von einem anderen AWS Konto geteilt wurde, müssen Sie Zugriff auf den AWS KMS Verschlüsselungsschlüssel haben, mit dem der Snapshot verschlüsselt wurde. Weitere Informationen finden Sie unter Umgang mit Verschlüsselungen.

Schnappschüsse werden kopiert AWS-Regionen

Wenn Sie einen Snapshot in einen Snapshot kopieren AWS-Region , der sich von dem des Quell-Snapshots unterscheidet AWS-Region, ist jede Kopie ein vollständiger Snapshot. Eine vollständige Snapshot-Kopie enthält alle Daten und Metadaten, die für die Wiederherstellung des Amazon DocumentDB-Clusters erforderlich sind.

Einschränkungen

Im folgenden werden einige Einschränkungen beim Kopieren von Snapshots aufgeführt:

- Wenn Sie einen Quell-Snapshot löschen, bevor der Ziel-Snapshot verfügbar ist, kann das Kopieren des Snapshots fehlschlagen. Verifizieren Sie, dass der Ziel-Snapshot den Status `AVAILABLE` hat, bevor Sie einen Quell-Snapshot löschen.
- Pro Konto können bis zu fünf Snapshot-Kopieranforderungen an eine einzelne Zielregion aktiv sein.
- Je nach Umfang und AWS-Regionen Menge der zu kopierenden Daten kann es Stunden dauern, bis eine regionsübergreifende Snapshot-Kopie abgeschlossen ist. In einigen Fällen kann es zu einer großen Anzahl von regionsübergreifenden Snapshot-Kopieranfragen aus einer bestimmten Quelle kommen. AWS-Region In diesen Fällen kann Amazon DocumentDB neue

regionsübergreifende Kopieranfragen von dieser Quelle AWS-Region in eine Warteschlange stellen, bis einige in Bearbeitung befindliche Kopien abgeschlossen sind. Zu Kopieranforderungen, die sich in der Warteschlange befinden, werden keine Fortschrittsinformationen angezeigt. Fortschrittsinformationen werden angezeigt, sobald der Kopiervorgang gestartet wird.

Umgang mit Verschlüsselungen

Sie können einen Snapshot kopieren, der mit einem AWS KMS -Verschlüsselungsschlüssel verschlüsselt wurde. Wenn Sie einen verschlüsselten Snapshot kopieren, muss auch die Kopie des Snapshots verschlüsselt werden. Wenn Sie einen verschlüsselten Snapshot innerhalb desselben kopieren AWS-Region, können Sie die Kopie mit demselben AWS KMS Verschlüsselungsschlüssel wie den ursprünglichen Snapshot verschlüsseln, oder Sie können einen anderen Verschlüsselungsschlüssel angeben. AWS KMS Wenn Sie einen verschlüsselten Snapshot regionsübergreifend kopieren, können Sie für die Kopie nicht denselben AWS KMS Verschlüsselungsschlüssel verwenden wie für den Quell-Snapshot, weil es die AWS KMS Schlüssel sind Region-specific. Stattdessen müssen Sie einen AWS KMS Schlüssel angeben, der für das Ziel AWS-Region n gültig ist.

Der Quell-Snapshot bleibt den gesamten Kopiervorgang über verschlüsselt. Weitere Informationen finden Sie unter Datenschutz in Amazon DocumentDB.

> **Note**
>
> Bei Amazon DocumentDB-Cluster-Snapshots können Sie einen unverschlüsselten Cluster-Snapshot nicht verschlüsseln, wenn Sie den Snapshot kopieren.

Überlegungen zu Parametergruppen

Wenn Sie einen Snapshot regionsübergreifend kopieren, enthält die Kopie nicht die Parametergruppe, die vom ursprünglichen Amazon DocumentDB-Cluster verwendet wurde. Wenn Sie einen Snapshot wiederherstellen, um einen neuen Cluster zu erstellen, erhält dieser Cluster die Standardparametergruppe für den Cluster, in dem AWS-Region er erstellt wurde. Um dem neuen Cluster dieselben Parameter wie dem Original zuzuweisen, müssen Sie wie folgt vorgehen:

1. Erstellen Sie im Ziel AWS-Region eine Amazon DocumentDB-Cluster-Parametergruppe mit denselben Einstellungen wie der ursprüngliche Cluster. Wenn im neuen System bereits eine vorhanden ist AWS-Region, können Sie diese verwenden.

2. Nachdem Sie den Snapshot im Ziel wiederhergestellt haben AWS-Region, ändern Sie den neuen Amazon DocumentDB-Cluster und fügen Sie die neue oder bestehende Parametergruppe aus dem vorherigen Schritt hinzu. Weitere Informationen finden Sie unter Ändern eines Amazon DocumentDB-Clusters.

Einen Cluster-Snapshot kopieren

Sie können einen Amazon DocumentDB-Cluster mit dem AWS-Managementkonsole oder dem AWS CLI wie folgt kopieren.

Using the AWS-Managementkonsole

Gehen Sie wie folgt vor, um mit dem AWS-Managementkonsole eine Kopie eines Cluster-Snapshots zu erstellen. Dieses Verfahren eignet sich für das Kopieren von verschlüsselten oder unverschlüsselten Cluster-Snapshots in derselben Region AWS-Region oder in mehreren Regionen.

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Wählen Sie im Navigationsbereich Snapshots und dann die Schaltfläche links neben dem Snapshot, den Sie kopieren möchten.

   > **Tip**
   >
   > Wenn der Navigationsbereich auf der linken Seite des Bildschirms nicht angezeigt wird, wählen Sie links oben auf der Seite das Menüsymbol (≡) aus.

3. Wählen Sie im Menü Actions die Option Copy aus.
4. Füllen Sie auf der daraufhin angezeigten Seite „Kopie des Cluster-Snapshots erstellen“ den Abschnitt Einstellungen aus.

   a. Zielregion — Optional. Um den Cluster-Snapshot in eine andere zu kopieren AWS-Region, wählen Sie diese Option AWS-Region für Zielregion aus.

   b. Neue Snapshot-ID — Geben Sie einen Namen für den neuen Snapshot ein.

      Einschränkungen bei der Benennung von Ziel-Snapshots:

- Kann nicht der Namen eines vorhandenen Snapshots sein.
- Die Länge beträgt [1—63] Buchstaben, Zahlen oder Bindestriche.
- Muss mit einem Buchstaben beginnen.
- Darf nicht mit einem Bindestrich enden oder zwei aufeinanderfolgende Bindestriche enthalten.
- Muss für alle Cluster in Amazon RDS, Neptune und Amazon DocumentDB pro AWS-Konto Region eindeutig sein.

c. Tags kopieren — Um alle Tags, die Sie in Ihrem Quell-Snapshot haben, in Ihre Snapshot-Kopie zu kopieren, wählen Sie Tags kopieren.

5. Füllen Sie den Encryption-at-restAbschnitt aus.

   a. Verschlüsselung im Ruhezustand — Wenn Ihr Snapshot nicht verschlüsselt ist, stehen Ihnen diese Optionen nicht zur Verfügung, da Sie aus einem unverschlüsselten Snapshot keine verschlüsselte Kopie erstellen können. Wenn Ihr Snapshot verschlüsselt ist, können Sie die während der Verschlüsselung im Ruhezustand AWS KMS key verwendete Einstellung ändern.

      Weitere Hinweise zur Verschlüsselung von Snapshot-Kopien finden Sie unterKopieren Sie die Cluster-Snapshot-.

      Weitere Informationen zur Verschlüsselung im Ruhezustand finden Sie unter Verschlüsselung von Amazon DocumentDB DocumentDB-Daten im Ruhezustand.

   b. AWS KMS Schlüssel — Wählen Sie aus der Dropdownliste eine der folgenden Optionen aus:

      - (Standard) aws/rds — Die Kontonummer und die AWS KMS Schlüssel-ID werden nach dieser Option aufgeführt.
      - <some-key-name>— Wenn Sie einen Schlüssel erstellt haben, wird er aufgelistet und steht Ihnen zur Auswahl zur Verfügung.
      - Geben Sie einen Schlüssel-ARN ein — Geben Sie im Feld ARN den Amazon-Ressourcennamen (ARN) für Ihren AWS KMS Schlüssel ein. Das ARN-Format lautet `arn:aws:kms:<region>:<accountID>:key/<key-id>` .

6. Wenn Sie eine Kopie des ausgewählten Snapshots erstellen möchten, wählen Sie Copy Snapshot (Snapshot kopieren). Alternativ können Sie Abbrechen wählen, um keine Kopie des Snapshots zu erstellen.

Using the AWS CLI

Um mit dem eine Kopie eines unverschlüsselten Cluster-Snapshots zu erstellen AWS CLI, verwenden Sie den `copy-db-cluster-snapshot` Vorgang mit den folgenden Parametern. Wenn Sie den Snapshot in einen anderen kopieren AWS-Region, führen Sie den Befehl aus, in AWS-Region den der Snapshot kopiert werden soll.

- **`--source-db-cluster-snapshot-identifier`** – Erforderlich. Die ID des zu kopierenden Cluster-Snapshots, der kopiert werden soll. Der Cluster-Snapshot muss vorhanden sein und muss sich im verfügbaren Zustand befindet. Wenn Sie den Snapshot in einen anderen kopieren AWS-Region oder wenn Sie einen gemeinsam genutzten Cluster-Snapshot kopieren, muss dieser Bezeichner im ARN-Format des Quell-Cluster-Snapshots vorliegen. Bei diesem Parameter wird nicht zwischen Groß- und Kleinschreibung unterschieden.
- **`--target-db-cluster-snapshot-identifier`** – Erforderlich. Die ID des neuen Cluster-Snapshots, der aus dem Quell-Cluster-Snapshot erstellt werden soll. Bei diesem Parameter wird nicht zwischen Groß- und Kleinschreibung unterschieden.

  Einschränkungen bei der Benennung von Ziel-Snapshots:

  - Kann nicht der Namen eines vorhandenen Snapshots sein.
  - Die Länge beträgt [1—63] Buchstaben, Zahlen oder Bindestriche.
  - Muss mit einem Buchstaben beginnen.
  - Darf nicht mit einem Bindestrich enden oder zwei aufeinanderfolgende Bindestriche enthalten.
  - Muss für alle Cluster in Amazon RDS, Neptune und Amazon DocumentDB pro AWS-Konto Region eindeutig sein.
- **`--source-region`**— Wenn Sie den Snapshot in einen anderen kopieren AWS-Region, geben Sie an, von welchem der AWS-Region verschlüsselte Cluster-Snapshot kopiert werden soll.

  Wenn Sie den Snapshot in einen anderen kopieren AWS-Region und nichts angeben`--source-region`, müssen Sie stattdessen die `pre-signed-url` Option angeben. Der `pre-signed-url` Wert muss eine URL sein, die eine mit Signature Version 4 signierte Anforderung enthält, damit die `CopyDBClusterSnapshot` Aktion in der Quelle AWS-Region aufgerufen wird, aus der der Cluster-Snapshot kopiert wurde. Weitere Informationen über das finden `pre-signed-url` Sie unter CopyDBClusterSnapshot.
- **`--kms-key-id`**— Die KMS-Schlüssel-ID für den Schlüssel, der zum Verschlüsseln der Kopie des Cluster-Snapshots verwendet werden soll.

Wenn Sie einen verschlüsselten Cluster-Snapshot in einen anderen kopieren AWS-Region, ist dieser Parameter erforderlich. Sie müssen einen KMS-Schlüssel für das Ziel angeben AWS-Region.

Wenn Sie einen verschlüsselten Cluster-Snapshot in dasselbe kopieren AWS-Region, ist der AWS KMS Schlüsselparameter optional. Die Kopie des Cluster-Snapshots wird mit demselben AWS KMS Schlüssel verschlüsselt wie der Quell-Cluster-Snapshot. Wenn Sie einen neuen AWS KMS Verschlüsselungsschlüssel angeben möchten, der zum Verschlüsseln der Kopie verwendet werden soll, können Sie dies mit diesem Parameter tun.

- **`--copy-tags`**— Fakultativ. Die Tags und Werte, die kopiert werden sollen.

Um einen laufenden Kopiervorgang abzubrechen, können Sie den Ziel-Cluster-Snapshot löschen, der dadurch identifiziert wurde, `--target-db-cluster-snapshot-identifier` oder `TargetDBClusterSnapshotIdentifier` während sich der Cluster-Snapshot im Kopierstatus befindet.

Example

Beispiel 1: Kopieren Sie einen unverschlüsselten Snapshot in dieselbe Region

Im folgenden AWS CLI Beispiel wird eine Kopie von `sample-cluster-snapshot` named `sample-cluster-snapshot-copy` in derselben Datei AWS-Region wie der Quell-Snapshot erstellt. Beim Erstellen der Kopie werden alle Tags des ursprünglichen Snapshots in die Snapshot-Kopie übernommen.

Für Linux, macOS oder Unix:

```
aws docdb copy-db-cluster-snapshot \
    --source-db-cluster-snapshot-identifier sample-cluster-snapshot \
    --target-db-cluster-snapshot-identifier sample-cluster-snapshot-copy \
    --copy-tags
```

Für Windows:

```
aws docdb copy-db-cluster-snapshot ^
    --source-db-cluster-snapshot-identifier sample-cluster-snapshot ^
    --target-db-cluster-snapshot-identifier sample-cluster-snapshot-copy ^
    --copy-tags
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus.

```
{
    "DBClusterSnapshot": {
        "AvailabilityZones": [
            "us-east-1a",
            "us-east-1b",
            "us-east-1c"
        ],
        "DBClusterSnapshotIdentifier": "sample-cluster-snapshot-copy",
        "DBClusterIdentifier": "sample-cluster",
        "SnapshotCreateTime": "2020-03-27T08:40:24.805Z",
        "Engine": "docdb",
        "Status": "copying",
        "Port": 0,
        "VpcId": "vpc-abcd0123",
        "ClusterCreateTime": "2020-01-10T22:13:38.261Z",
        "MasterUsername": "master-user",
        "EngineVersion": "4.0.0",
        "SnapshotType": "manual",
        "PercentProgress": 0,
        "StorageEncrypted": true,
        "KmsKeyId": "arn:aws:kms:us-east-1:111122223333:key/sample-key-id",
        "DBClusterSnapshotArn": "arn:aws:rds:us-east-1:111122223333:cluster-
snapshot:sample-cluster-snapshot-copy",
        "SourceDBClusterSnapshotArn": "arn:aws:rds:us-east-1:111122223333:cluster-
snapshot:sample-cluster-snapshot"
    }
}
```

Example

Beispiel 2: Kopieren Sie einen unverschlüsselten Snapshot AWS-Regionen

Das folgende AWS CLI Beispiel erstellt eine Kopie von`sample-cluster-snapshot`, die den ARN hat`arn:aws:rds:us-east-1:123456789012:cluster-snapshot:sample-cluster-snapshot`. Diese Kopie trägt den Namen named `sample-cluster-snapshot-copy` und befindet sich in der AWS-Region Datei, in der der Befehl ausgeführt wird.

Für Linux, macOS oder Unix:

```
aws docdb copy-db-cluster-snapshot \
```

```
    --source-db-cluster-snapshot-identifier arn:aws:rds:us-
east-1:123456789012:cluster-snapshot:sample-cluster-snapshot \
    --target-db-cluster-snapshot-identifier sample-cluster-snapshot-copy
```

Für Windows:

```
aws docdb copy-db-cluster-snapshot ^
    --source-db-cluster-snapshot-identifier arn:aws:rds:us-
east-1:123456789012:cluster-snapshot:sample-cluster-snapshot ^
    --target-db-cluster-snapshot-identifier sample-cluster-snapshot-copy
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus.

```
{
    "DBClusterSnapshot": {
        "AvailabilityZones": [
            "us-east-1a",
            "us-east-1b",
            "us-east-1c"
        ],
        "DBClusterSnapshotIdentifier": "sample-cluster-snapshot-copy",
        "DBClusterIdentifier": "sample-cluster",
        "SnapshotCreateTime": "2020-04-29T16:45:51.239Z",
        "Engine": "docdb",
        "AllocatedStorage": 0,
        "Status": "copying",
        "Port": 0,
        "VpcId": "vpc-abc0123",
        "ClusterCreateTime": "2020-04-28T16:43:00.294Z",
        "MasterUsername": "master-user",
        "EngineVersion": "4.0.0",
        "LicenseModel": "docdb",
        "SnapshotType": "manual",
        "PercentProgress": 0,
        "StorageEncrypted": false,
        "DBClusterSnapshotArn": "arn:aws:rds:us-east-1:123456789012:cluster-
snapshot:sample-cluster-snapshot-copy",
        "SourceDBClusterSnapshotArn": "arn:aws:rds:us-east-1:123456789012:cluster-
snapshot:sample-cluster-snapshot",
    }
}
```

Example

Beispiel 3: Kopieren Sie einen verschlüsselten Snapshot AWS-Regionen

Im folgenden AWS CLI Beispiel wird eine Kopie `sample-cluster-snapshot` von von der Region us-west-2 in die Region us-east-1 erstellt. Dieser Befehl wird in der Region us-east-1 aufgerufen.

Für Linux, macOS oder Unix:

```
aws docdb copy-db-cluster-snapshot \
    --source-db-cluster-snapshot-identifier arn:aws:rds:us-
west-2:123456789012:cluster-snapshot:sample-cluster-snapshot \
    --target-db-cluster-snapshot-identifier sample-cluster-snapshot-copy \
    --source-region us-west-2 \
    --kms-key-id sample-us-east-1-key
```

Für Windows:

```
aws docdb copy-db-cluster-snapshot ^
    --source-db-cluster-snapshot-identifier arn:aws:rds:us-
west-2:123456789012:cluster-snapshot:sample-cluster-snapshot ^
    --target-db-cluster-snapshot-identifier sample-cluster-snapshot-copy ^
    --source-region us-west-2 ^
    --kms-key-id sample-us-east-1-key
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus.

```
{
    "DBClusterSnapshot": {
        "AvailabilityZones": [],
        "DBClusterSnapshotIdentifier": "sample-cluster-snapshot-copy",
        "DBClusterIdentifier": "sample-cluster",
        "SnapshotCreateTime": "2020-04-29T16:45:53.159Z",
        "Engine": "docdb",
        "AllocatedStorage": 0,
        "Status": "copying",
        "Port": 0,
        "ClusterCreateTime": "2020-04-28T16:43:07.129Z",
        "MasterUsername": "chimera",
        "EngineVersion": "4.0.0",
        "LicenseModel": "docdb",
        "SnapshotType": "manual",
```

```
        "PercentProgress": 0,
        "StorageEncrypted": true,
        "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/0846496a-
d48e-41c4-9353-86d8301d7e35",
        "DBClusterSnapshotArn": "arn:aws:rds:us-east-1:123456789012:cluster-
snapshot:sample-cluster-snapshot-copy",
        "SourceDBClusterSnapshotArn": "arn:aws:rds:us-west-2:123456789012:cluster-
snapshot:sample-cluster-snapshot",
    }
}
```

Example

Beispiel 4: Kopieren Sie einen unverschlüsselten gemeinsamen Snapshot nach AWS-Regionen

Das folgende AWS CLI Beispiel, account -123456789012, erstellt eine Kopie eines unverschlüsselten Cluster-Snapshots, der von account - `sample-cluster-snapshot` gemeinsam genutzt wird, 999999999999 von der Region us-east-1 in die Region us-west-2. Dieser Befehl wird in der Region us-west-2 aufgerufen. Weitere Informationen zum Freigeben von Snapshots finden Sie unter Freigeben eines Snapshots.

Für Linux, macOS oder Unix:

```
aws docdb copy-db-cluster-snapshot \
--region us-west-2 \
--source-db-cluster-snapshot-identifier arn:aws:rds:us-east-1:999999999999:cluster-
snapshot:sample-cluster-snapshot \
--target-db-cluster-snapshot-identifier sample-cluster-snapshot-copy
```

Für Windows:

```
aws docdb copy-db-cluster-snapshot ^
--region us-west-2 ^
--source-db-cluster-snapshot-identifier arn:aws:rds:us-east-1:999999999999:cluster-
snapshot:sample-cluster-snapshot ^
--target-db-cluster-snapshot-identifier sample-cluster-snapshot-copy
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus.

```
{
 "DBClusterSnapshots": [
 {
```

```
 "AvailabilityZones": [],
 "DBClusterSnapshotIdentifier": "sample-cluster-snapshot-copy",
 "DBClusterIdentifier": "sample-cluster",
 "SnapshotCreateTime": "2025-08-22T11:27:00.497000+00:00",
 "Engine": "docdb",
 "Status": "copying",
 "Port": 0,
 "ClusterCreateTime": "2024-07-02T16:44:50.246000+00:00",
 "MasterUsername": "master-user",
 "EngineVersion": "5.0.0",
 "SnapshotType": "manual",
 "PercentProgress": 0,
 "StorageEncrypted": false,
 "DBClusterSnapshotArn": "arn:aws:rds:us-west-2:123456789012:cluster-
snapshot:sample-cluster-snapshot-copy",
 "SourceDBClusterSnapshotArn": "arn:aws:rds:us-east-1:999999999999:cluster-
snapshot:sample-cluster-snapshot"
 }
 ]
}
```

Example

Beispiel 5: Kopieren Sie einen verschlüsselten, gemeinsam genutzten Snapshot AWS-Regionen

Das folgende AWS CLI Beispiel, account — `123456789012` erstellt eine Kopie eines verschlüsselten Cluster-Snapshots, der von einem Konto `sample-cluster-snapshot` gemeinsam genutzt wird — `999999999999` von der Region us-east-1 in die Region us-west-2. Der Ziel-Snapshot ist mit einem vom Kunden verwalteten KMS-Schlüssel verschlüsselt -. `arn:aws:kms:us-west-2:123456789012:key/6c1f3264-1797-472b-ba37-03011e682d28` Dieser Befehl wird in der Region us-west-2 aufgerufen. Weitere Informationen zum Freigeben von Snapshots finden Sie unter Freigeben eines Snapshots.

Für Linux, macOS oder Unix:

```
aws docdb copy-db-cluster-snapshot \
--region us-west-2 \
--source-db-cluster-snapshot-identifier arn:aws:rds:us-east-1:999999999999:cluster-
snapshot:sample-cluster-snapshot \
--target-db-cluster-snapshot-identifier sample-cluster-snapshot-copy \
--kms-key-id arn:aws:kms:us-west-2:123456789012:key/6c1f3264-1797-472b-
ba37-03011e682d28
```

Für Windows:

```
aws docdb copy-db-cluster-snapshot ^
--region us-west-2 ^
--source-db-cluster-snapshot-identifier arn:aws:rds:us-east-1:999999999999:cluster-
snapshot:sample-cluster-snapshot ^
--target-db-cluster-snapshot-identifier sample-cluster-snapshot-copy ^
--kms-key-id arn:aws:kms:us-west-2:123456789012:key/6c1f3264-1797-472b-
ba37-03011e682d28
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus.

```
{
 "DBClusterSnapshots": [
 {
 "AvailabilityZones": [],
 "DBClusterSnapshotIdentifier": "sample-cluster-snapshot-copy",
 "DBClusterIdentifier": "sample-cluster",
 "SnapshotCreateTime": "2025-08-22T11:27:00.497000+00:00",
 "Engine": "docdb",
 "Status": "copying",
 "Port": 0,
 "ClusterCreateTime": "2024-07-02T16:44:50.246000+00:00",
 "MasterUsername": "master-user",
 "EngineVersion": "5.0.0",
 "SnapshotType": "manual",
 "PercentProgress": 0,
 "StorageEncrypted": true,
 "KmsKeyId": "arn:aws:kms:us-west-2:123456789012:key/6c1f3264-1797-472b-
ba37-03011e682d28",
 "DBClusterSnapshotArn": "arn:aws:rds:us-west-2:123456789012:cluster-
snapshot:sample-cluster-snapshot-copy",
 "SourceDBClusterSnapshotArn": "arn:aws:rds:us-east-1:999999999999:cluster-
snapshot:sample-cluster-snapshot"
 }
 ]
}
```

> **Note**
>
> Weitere Hinweise zur Verschlüsselung von Snapshot-Kopien finden Sie unter. Kopieren Sie die Cluster-Snapshot-

Weitere Informationen zur Verschlüsselung im Ruhezustand finden Sie unter Verschlüsselung von Amazon DocumentDB DocumentDB-Daten im Ruhezustand.

Amazon DocumentDB-Cluster-Snapshots teilen

Mit Amazon DocumentDB können Sie einen manuellen Cluster-Snapshot auf folgende Weise teilen:

- Durch die gemeinsame Nutzung eines manuellen Cluster-Snapshots, ob verschlüsselt oder unverschlüsselt, können autorisierte AWS Konten den Snapshot kopieren.
- Durch die gemeinsame Nutzung eines manuellen Cluster-Snapshots, ob verschlüsselt oder unverschlüsselt, können autorisierte AWS Konten einen Cluster direkt aus dem Snapshot wiederherstellen, anstatt eine Kopie davon zu erstellen und die Wiederherstellung von dort aus durchzuführen.

> **Note**
>
> Um einen automatisierten Cluster-Snapshot gemeinsam zu nutzen, erstellen Sie einen manuellen Cluster-Snapshot, indem Sie den automatisierten Snapshot kopieren, und teilen Sie diese Kopie dann. Dieser Prozess gilt auch für durch AWS Backup generierte Ressourcen.

Sie können einen manuellen Snapshot mit bis zu 20 anderen teilen. AWS-Konten Sie können darüber hinaus einen nicht verschlüsselten Snapshot als öffentlich freigeben. Damit ist der Snapshot für alle -Konten verfügbar. Vergewissern Sie sich bei der Freigabe eines Snapshots als öffentlich darauf, dass in Ihren öffentlichen Snapshots keine privaten Informationen enthalten sind.

Wenn Sie manuelle Snapshots mit anderen AWS-Konten teilen und einen Cluster aus einem gemeinsam genutzten Snapshot mithilfe der AWS CLI oder der Amazon DocumentDB DocumentDB-API wiederherstellen, müssen Sie den Amazon-Ressourcennamen (ARN) des gemeinsam genutzten Snapshots als Snapshot-ID angeben.

Freigeben eines verschlüsselten Snapshots

Die folgenden Einschränkungen gelten für die Freigabe verschlüsselter Snapshots:

- Sie können verschlüsselte Snapshots nicht als öffentlich freigeben.

- Sie können keinen Snapshot teilen, der mit dem AWS KMS Standardverschlüsselungsschlüssel des Kontos verschlüsselt wurde, das den Snapshot geteilt hat.

Führen Sie die folgenden Schritte aus, um verschlüsselte Snapshots freizugeben.

1. Teilen Sie den Verschlüsselungsschlüssel AWS Key Management Service (AWS KMS), der zum Verschlüsseln des Snapshots verwendet wurde, mit allen Konten, die auf den Snapshot zugreifen möchten.

   Sie können AWS KMS Verschlüsselungsschlüssel mit anderen AWS Konten teilen, indem Sie die anderen Konten zur AWS KMS Schlüsselrichtlinie hinzufügen. Einzelheiten zur Aktualisierung einer Schlüsselrichtlinie finden Sie unter Verwenden von Schlüsselrichtlinien in AWS KMS im AWS Key Management Service Entwicklerhandbuch. Ein Beispiel für die Erstellung einer Schlüsselrichtlinie finden Sie unter Erstellen einer IAM-Richtlinie, um das Kopieren des verschlüsselten Snapshots zu erlauben an späterer Stelle in diesem Thema.
2. Verwenden Sie AWS CLI, wie unten gezeigt, um den verschlüsselten Snapshot mit den anderen Konten zu teilen.

Erlaubt den Zugriff auf ein AWS KMS Verschlüsselungsschlüssel

Damit ein anderer AWS-Konto einen verschlüsselten Snapshot kopieren kann, der von Ihrem Konto geteilt wurde, muss das Konto, mit dem Sie Ihren Snapshot teilen, Zugriff auf den AWS KMS Schlüssel haben, mit dem der Snapshot verschlüsselt wurde. Um einem anderen Konto Zugriff auf einen AWS KMS Schlüssel zu gewähren, aktualisieren Sie die Schlüsselrichtlinie für den AWS KMS Schlüssel mit dem ARN des Kontos, das Sie als Principal teilen, in der AWS KMS Schlüsselrichtlinie. Lassen Sie anschließend die Aktion `kms:CreateGrant` zu.

Nachdem Sie einem Konto Zugriff auf Ihren AWS KMS Verschlüsselungsschlüssel gewährt haben, muss dieses Konto, um Ihren verschlüsselten Snapshot zu kopieren, einen AWS Identity and Access Management (IAM-) Benutzer erstellen, falls es noch keinen hat. Darüber hinaus muss dieses Konto diesem IAM-Benutzer eine IAM-Richtlinie zuordnen, die es dem Benutzer ermöglicht, mithilfe Ihres Schlüssels einen verschlüsselten Snapshot zu kopieren. AWS KMS Das Konto muss ein IAM-Benutzer sein und darf aufgrund von Sicherheitseinschränkungen keine AWS-Konto Root-Identität sein. AWS KMS

Im folgenden Beispiel für eine Schlüsselrichtlinie ist der Benutzer 123451234512 der Besitzer des Verschlüsselungsschlüssels. AWS KMS Bei Benutzer 123456789012 handelt es sich um das Konto,

für das der Schlüssel freigegeben wird. Diese aktualisierte Schlüsselrichtlinie gewährt dem Konto Zugriff auf den Schlüssel. AWS KMS Dazu wird der ARN für die AWS-Konto Root-Identität für den Benutzer 123456789012 als Principal für die Richtlinie aufgenommen und die Aktion zugelassen. `kms:CreateGrant`

JSON

```
{
    "Id": "key-policy-1",
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "Allow use of the key",
            "Effect": "Allow",
            "Principal": {"AWS": [
                "arn:aws:iam::123451234512:user/KeyUser",
                "arn:aws:iam::123456789012:root"
            ]},
            "Action": [
                "kms:CreateGrant",
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": "*"},
            {
            "Sid": "Allow attachment of persistent resources",
            "Effect": "Allow",
            "Principal": {"AWS": [
                "arn:aws:iam::123451234512:user/KeyUser",
                "arn:aws:iam::123456789012:root"
            ]},
            "Action": [
                "kms:CreateGrant",
                "kms:ListGrants",
                "kms:RevokeGrant"
            ],
            "Resource": "*",
            "Condition": {"Bool": {"kms:GrantIsForAWSResource": true}}
        }
```

```
    ]
}
```

Erstellen einer IAM-Richtlinie, um das Kopieren des verschlüsselten Snapshots zu erlauben

Wenn der externe Benutzer Zugriff auf Ihren AWS KMS Schlüssel AWS-Konto hat, kann der Besitzer dieses Kontos eine Richtlinie erstellen, die es einem IAM-Benutzer, der für das Konto erstellt wurde, ermöglicht, einen verschlüsselten Snapshot zu kopieren, der mit diesem Schlüssel verschlüsselt ist. AWS KMS

Das folgende Beispiel zeigt eine Richtlinie, die einem IAM-Benutzer für AWS-Konto 123456789012 zugewiesen werden kann. Die Richtlinie ermöglicht es dem IAM-Benutzer, einen gemeinsam genutzten Snapshot aus dem Konto 123451234512 zu kopieren, der mit dem AWS KMS Schlüssel `c989c1dd-a3f2-4a5d-8d96-e793d082ab26` in der Region us-west-2 verschlüsselt wurde.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowUseOfTheKey",
            "Effect": "Allow",
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey",
                "kms:CreateGrant",
                "kms:RetireGrant"
            ],
            "Resource": ["arn:aws:kms:us-west-2:123451234512:key/c989c1dd-
a3f2-4a5d-8d96-e793d082ab26"]
        },
        {
            "Sid": "AllowAttachmentOfPersistentResources",
            "Effect": "Allow",
            "Action": [
```

```
                "kms:CreateGrant",
                "kms:ListGrants",
                "kms:RevokeGrant"
            ],
            "Resource": ["arn:aws:kms:us-west-2:123451234512:key/c989c1dd-
a3f2-4a5d-8d96-e793d082ab26"],
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
    ]
}
```

Einzelheiten zur Aktualisierung einer Schlüsselrichtlinie finden Sie unter Verwenden von Schlüsselrichtlinien im Entwicklerhandbuch. AWS KMSAWS Key Management Service

Freigeben eines Snapshots

Sie können einen manuellen Amazon DocumentDB-Cluster-Snapshot (oder eine Kopie eines automatisierten Snapshots) mit dem AWS-Managementkonsole oder dem AWS CLI teilen:

Using the AWS-Managementkonsole

Gehen Sie wie folgt vor AWS-Managementkonsole, um einen Snapshot mit dem zu teilen:

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Wählen Sie im Navigationsbereich die Option Snapshots.
3. Wählen Sie den manuellen Snapshot, den Sie freigeben möchten.
4. Wählen Sie im Drop-down-Menü Aktionen die Option Teilen aus.
5. Wählen Sie eine der folgenden Optionen für die Sichtbarkeit von DB-Snapshots:

   - Wenn die Quelle unverschlüsselt ist, wählen Sie Öffentlich, damit alle AWS Konten einen Cluster aus Ihrem manuellen Snapshot wiederherstellen können. Oder wählen Sie Privat, um nur von Ihnen angegebene AWS Konten die Wiederherstellung eines Clusters aus Ihrem manuellen Snapshot zuzulassen.

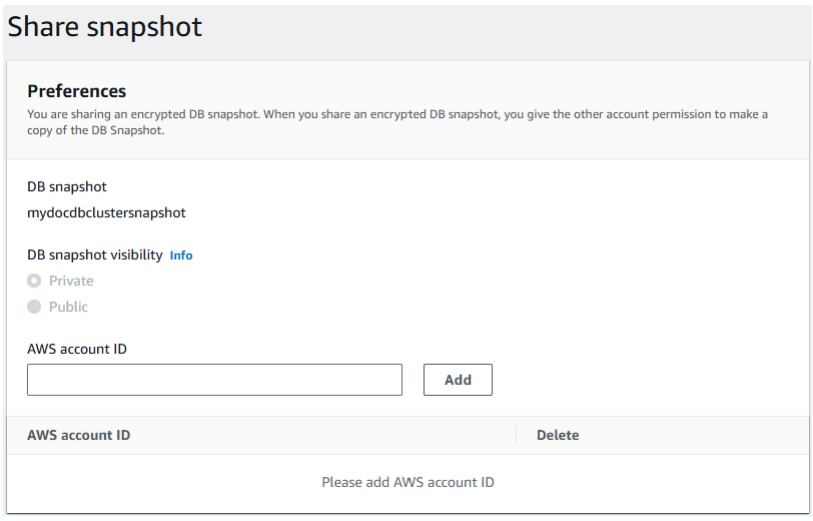
> **Warning**
>
> Wenn Sie die Sichtbarkeit von DB-Snapshots auf Öffentlich setzen, können alle AWS Konten einen Cluster aus Ihrem manuellen Snapshot wiederherstellen und haben Zugriff auf Ihre Daten. Geben Sie keine manuellen Cluster-Snapshots, die private Informationen enthalten, als öffentlich frei.

- Ist die Quelle verschlüsselt, ist DB Snapshot Visibility (Sichtbarkeit des DB-Snapshots) auf Private (Privat) festgelegt, da verschlüsselte Snapshots nicht als öffentlich freigegeben werden können.

> **Note**
>
> Snapshots, die mit der Standardeinstellung verschlüsselt wurden, AWS KMS key können nicht geteilt werden.

6. Geben Sie AWS unter Konto-ID die AWS Konto-ID für ein Konto ein, dem Sie die Wiederherstellung eines Clusters aus Ihrem manuellen Snapshot erlauben möchten, und wählen Sie dann Hinzufügen aus. Wiederholen Sie den Vorgang, um weitere AWS Kontokennungen hinzuzufügen, bis zu 20 AWS Konten.

   Wenn Ihnen beim Hinzufügen einer AWS Konto-ID zur Liste der zulässigen Konten ein Fehler unterläuft, können Sie diese aus der Liste löschen, indem Sie rechts neben der falschen AWS Konto-ID die Option Löschen auswählen.



7. Nachdem Sie Kennungen für alle AWS Konten hinzugefügt haben, denen Sie die Wiederherstellung des manuellen Snapshots erlauben möchten, wählen Sie Speichern, um Ihre Änderungen zu speichern.

Using the AWS CLI

Um einen Snapshot mit dem zu teilen AWS CLI, verwenden Sie den Amazon DocumentDB `modify-db-snapshot-attribute` DocumentDB-Vorgang. Verwenden Sie den `--values-to-add` Parameter, um eine Liste der IDs hinzuzufügen AWS-Konten , die berechtigt sind, den manuellen Snapshot wiederherzustellen.

Im folgenden Beispiel sind zwei AWS-Konto Kennungen, 123451234512 und 123456789012, für die Wiederherstellung des genannten Snapshots zulässig. `manual-snapshot1` Außerdem wird der `all`-Attributwert entfernt, um den Snapshot als privat zu markieren.

Für Linux, macOS oder Unix:

```
aws docdb modify-db-cluster-snapshot-attribute \
    --db-cluster-snapshot-identifier sample-cluster-snapshot \
    --attribute-name restore \
    --values-to-add '["123451234512","123456789012"]'
```

Für Windows:

```
aws docdb modify-db-cluster-snapshot-attribute ^
    --db-cluster-snapshot-identifier sample-cluster-snapshot ^
    --attribute-name restore ^
    --values-to-add '["123451234512","123456789012"]'
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus.

```
{
    "DBClusterSnapshotAttributesResult": {
        "DBClusterSnapshotIdentifier": "sample-cluster-snapshot",
        "DBClusterSnapshotAttributes": [
            {
                "AttributeName": "restore",
                "AttributeValues": [
                    "123451234512",
```

```
                    "123456789012"
                ]
            }
        ]
    }
}
```

Verwenden Sie den Parameter, um einen AWS-Konto Bezeichner aus der Liste zu entfernen. `--values-to-remove` Das folgende Beispiel verhindert, dass AWS-Konto ID 123456789012 den Snapshot wiederherstellt.

Für Linux, macOS oder Unix:

```
aws docdb modify-db-cluster-snapshot-attribute \
    --db-cluster-snapshot-identifier sample-cluster-snapshot \
    --attribute-name restore \
    --values-to-remove '["123456789012"]'
```

Für Windows:

```
aws docdb modify-db-cluster-snapshot-attribute ^
    --db-cluster-snapshot-identifier sample-cluster-snapshot ^
    --attribute-name restore ^
    --values-to-remove '["123456789012"]'
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus.

```
{
    "DBClusterSnapshotAttributesResult": {
        "DBClusterSnapshotIdentifier": "sample-cluster-snapshot",
        "DBClusterSnapshotAttributes": [
            {
                "AttributeName": "restore",
                "AttributeValues": [
                    "123451234512"
                ]
            }
        ]
    }
}
```

Wiederherstellung aus einem Cluster-Snapshot

Amazon DocumentDB (mit MongoDB-Kompatibilität) erstellt einen Cluster-Snapshot Ihres Speichervolumes. Sie können einen neuen Cluster erstellen, indem Sie ihn aus einem Cluster-Snapshot wiederherstellen. Wenn Sie den Cluster wiederherstellen, geben Sie den Namen des wiederherzustellenden Cluster-Snapshots und einen Namen für den neuen Cluster an, der durch die Wiederherstellung erstellt wird. Sie können nicht von einem Snapshot auf einen bestehenden Cluster wiederherstellen, da bei der Wiederherstellung ein neuer Cluster erstellt wird.

Wenn Sie einen Cluster aus einem Cluster-Snapshot wiederherstellen:

- Diese Aktion stellt nur den Cluster wieder her, nicht die Instances für diesen Cluster. Sie müssen die Aktion `create-db-instance` aufrufen, um Instances für den wiederhergestellten Cluster zu erstellen, wobei Sie in `--db-cluster-identifier` die ID des wiederhergestellten Clusters angeben. Sie können Instances erst erstellen, nachdem der Cluster den Status available hat.
- Sie können einen verschlüsselten Snapshot nicht in einem unverschlüsselten Cluster wiederherstellen. Sie können jedoch einen unverschlüsselten Snapshot in einem verschlüsselten Cluster wiederherstellen, indem Sie den Schlüssel angeben. AWS KMS
- Um einen Cluster aus einem verschlüsselten Snapshot wiederherzustellen, müssen Sie Zugriff auf den AWS KMS Schlüssel haben.

> **Note**
>
> Sie können einen 3.6-Cluster nicht auf einem 4.0-Cluster wiederherstellen, aber Sie können von einer Clusterversion zu einer anderen migrieren. Weitere Informationen finden Sie unter Migration zu Amazon DocumentDB.

Using the AWS-Managementkonsole

Das folgende Verfahren zeigt, wie Sie mit der Amazon DocumentDB Management Console einen Amazon DocumentDB-Cluster aus einem Cluster-Snapshot wiederherstellen.

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Wählen Sie im Navigationsbereich Snapshots und dann die Schaltfläche links neben dem Snapshot aus, mit der Sie einen Cluster wiederherstellen möchten.

> **Tip**
>
> Wenn der Navigationsbereich auf der linken Seite des Bildschirms nicht angezeigt wird, wählen Sie links oben auf der Seite das Menüsymbol (≡) aus.

3. Wählen Sie im Menü Aktionen die Option Restore (Wiederherstellen).
4. Füllen Sie auf der Seite Restore snapshot (Snapshot wiederherstellen) den Abschnitt Configuration (Konfiguration) aus.

   a. Cluster-ID — Der Name für den neuen Cluster. Sie können den von Amazon DocumentDB angegebenen Namen akzeptieren oder einen Namen eingeben, den Sie bevorzugen. Der von Amazon DocumentDB bereitgestellte Name hat das Format `docdb-` plus einen UTC-Zeitstempel, zum Beispiel. `docdb-yyyy-mm-dd-hh-mm-ss`

   b. Instance-Klasse — Die Instance-Klasse für den neuen Cluster. Sie können die Standard-Instance-Klasse akzeptieren oder eine Instance-Klasse aus der Dropdown-Liste auswählen.

   c. Anzahl der Instanzen — Die Anzahl der Instanzen, die Sie mit diesem Cluster erstellen möchten. Sie können den Standard von 3 Instanzen (1 primäres read/write und 2 schreibgeschützte Replikate) akzeptieren oder die Anzahl der Instanzen aus der Drop-down-Liste wählen.
5. Wählen Sie für die Cluster-Speicherkonfiguration eine Speicheroption.

> **Note**
>
> Die Amazon I/O-Optimized DocumentDB-Speicherkonfiguration ist nur in den Engine-Versionen Amazon DocumentDB 5.0 und 8.0 verfügbar.

6. Wenn Sie mit der Cluster-Konfiguration zufrieden sind, wählen Sie Restore cluster (Cluster wiederherstellen) aus und warten Sie, bis Ihr Cluster wiederhergestellt ist.
7. Wenn Sie es vorziehen, einige Konfigurationen zu ändern, z. B. eine nicht standardmäßige Amazon VPC oder Sicherheitsgruppe anzugeben, wählen Sie unten links auf der Seite Erweiterte Einstellungen anzeigen aus und fahren Sie dann mit den folgenden Schritten fort.

   a. Vervollständigen Sie den Bereich Network settings (Netzwerkeinstellungen).

- Virtual Private Cloud (VPC) — Akzeptieren Sie die aktuelle VPC oder wählen Sie eine VPC aus der Drop-down-Liste aus.
- Subnetzgruppe — Akzeptieren Sie die `default` Subnetzgruppe oder wählen Sie eine aus der Drop-down-Liste aus.
- VPC-Sicherheitsgruppen — Akzeptieren Sie die `default (VPC)` Sicherheitsgruppe oder wählen Sie eine aus der Liste aus.

b. Vervollständigen Sie den Abschnitt Cluster options (Cluster-Optionen).

- Datenbankport — Akzeptieren Sie den Standardport`27017`, oder verwenden Sie den Aufwärts- oder Abwärtspfeil, um den Port festzulegen, den Sie für Anwendungsverbindungen verwenden möchten.

c. Vervollständigen Sie den Abschnitt Encryption (Verschlüsselung).

- Verschlüsselung im Ruhezustand — Wenn Ihr Snapshot verschlüsselt ist, stehen Ihnen diese Optionen nicht zur Verfügung. Wenn er nicht verschlüsselt ist, können Sie eine der folgenden Optionen auswählen:
  - Um alle Daten Ihres Clusters zu verschlüsseln, wählen Sie Enable encryption-at-rest (Verschlüsselung im Ruhezustand aktivieren) aus. Wenn Sie diese Option wählen, müssen Sie einen KMS-Schlüssel angeben.
  - Um die Daten Ihres Clusters nicht zu verschlüsseln, wählen Sie Disable encryption-at-rest (Verschlüsselung im Ruhezustand deaktivieren) aus. Wenn Sie diese Option wählen, sind Sie mit dem Abschnitt "Verschlüsselung" fertig.
- AWS KMS Schlüssel — Wählen Sie eine der folgenden Optionen aus der Dropdownliste aus:
  - (Standard) aws/rds — Die Kontonummer und die AWS KMS Schlüssel-ID werden nach dieser Option aufgeführt.
  - Customer-managed Schlüssel — Diese Option ist nur verfügbar, wenn Sie einen IAM-Verschlüsselungsschlüssel in der AWS Identity and Access Management (IAM-) Konsole erstellt haben. Sie können den Schlüssel für die Verschlüsselung Ihres Clusters auswählen.
  - Geben Sie einen Schlüssel-ARN ein — Geben Sie im Feld ARN den Amazon-Ressourcennamen (ARN) für Ihren AWS KMS Schlüssel ein. Das ARN-Format lautet `arn:aws:kms:<region>:<accountID>:key/<key-id>`.

d. Füllen sie den Abschnitt Log exports (Protokollexporte) aus.

- Wählen Sie die Protokolltypen aus, in denen veröffentlicht werden soll CloudWatch — Wählen Sie eine der folgenden Optionen:
  - Aktiviert — Ermöglicht Ihrem Cluster den Export von DDL-Protokollen nach Amazon CloudWatch Logs.
  - Deaktiviert — Verhindert, dass Ihr Cluster DDL-Logs nach Amazon CloudWatch Logs exportiert. Disabled (Deaktiviert) ist die Voreinstellung.
- IAM-Rolle — Wählen Sie aus der Liste die Option RDS Service Linked Role aus.

e. Füllen Sie den Abschnitt Tags aus.

- Tag hinzufügen — Geben Sie im Feld Schlüssel den Namen für das Tag für Ihren Cluster ein. Geben Sie optional im Feld Value (Wert) den Tag-Wert ein. Tags werden zusammen mit AWS Identity and Access Management (IAM-) Richtlinien verwendet, um den Zugriff auf Amazon DocumentDB DocumentDB-Ressourcen zu verwalten und zu kontrollieren, welche Aktionen auf die Ressourcen angewendet werden können.

f. Füllen Sie den Abschnitt Deletion protection (Löschschutz) aus.

- Löschschutz aktivieren — Schützt den Cluster davor, versehentlich gelöscht zu werden. Wenn diese Option aktiviert ist, können Sie den Cluster nicht löschen.

8. Wählen Sie Restore cluster (Cluster wiederherstellen) aus.

Using the AWS CLI

Um einen Cluster mithilfe von aus einem Snapshot wiederherzustellen AWS CLI, verwenden Sie den `restore-db-cluster-from-snapshot` Vorgang mit den folgenden Parametern. Weitere Informationen finden Sie unter RestoreDBClusterFromSnapshot.

- **`--db-cluster-identifier`** – Erforderlich. Der Name des Clusters, der von der Operation erstellt wird. Ein Cluster mit diesem Namen darf vor dieser Operation nicht vorhanden sein.

  Einschränkungen bei der Benennung von Clustern:

  - Die Länge beträgt [1—63] Buchstaben, Zahlen oder Bindestriche.
  - Muss mit einem Buchstaben beginnen.
  - Darf nicht mit einem Bindestrich enden oder zwei aufeinanderfolgende Bindestriche enthalten.

  - Muss für alle Cluster in Amazon RDS, Neptune und Amazon DocumentDB pro AWS-Konto Region eindeutig sein.
- **`--snapshot-identifier`** – Erforderlich. Der Name des Snapshots, der für die Wiederherstellung verwendet wird. Ein Snapshot mit diesem Namen muss vorhanden sein und sich im verfügbaren Zustand befindet.
- **`--engine`** – Erforderlich. Der Wert muss `docdb` sein.
- **`--storage-type standard | iopt1`**— Fakultativ. Standard: `standard`.
- **`--kms-key-id`**— Fakultativ. Der ARN der AWS KMS Schlüssel-ID, die beim Wiederherstellen eines verschlüsselten Snapshots oder beim Verschlüsseln eines Clusters bei der Wiederherstellung aus einem unverschlüsselten Snapshot verwendet werden soll. Die Angabe der AWS KMS Schlüssel-ID führt dazu, dass der wiederhergestellte Cluster mit dem AWS KMS Schlüssel verschlüsselt wird, unabhängig davon, ob der Snapshot verschlüsselt wurde oder nicht.

  Das Format der `--kms-key-id` ist `arn:aws:kms:<region>:<accountID>:key/<key-id>`. Wenn Sie keinen Wert für den `--kms-key-id`-Parameter angeben, geschieht folgendes:

  - Wenn der Snapshot verschlüsselt `--snapshot-identifier` ist, wird der wiederhergestellte Cluster mit demselben AWS KMS Schlüssel verschlüsselt, der zum Verschlüsseln des Snapshots verwendet wurde.
  - Wenn der Snapshot in `--snapshot-identifier` nicht verschlüsselt ist, dann ist der wiederhergestellte Cluster nicht verschlüsselt.

Für Linux, macOS oder Unix:

```
aws docdb restore-db-cluster-from-snapshot \
    --db-cluster-identifier sample-cluster-restore \
    --snapshot-identifier sample-cluster-snapshot \
    --engine docdb \
    --kms-key-id arn:aws:kms:us-east-1:123456789012:key/SAMPLE-KMS-KEY-ID
```

Für Windows:

```
aws docdb restore-db-cluster-from-snapshot ^
    --db-cluster-identifier sample-cluster-restore ^
    --snapshot-identifier sample-cluster-snapshot ^
    --engine docdb ^
```

```
    --kms-key-id arn:aws:kms:us-east-1:123456789012:key/SAMPLE-KMS-KEY-ID
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus.

```
{
    "DBCluster": {
        "AvailabilityZones": [
            "us-east-1c",
            "us-east-1b",
            "us-east-1a"
        ],
        "BackupRetentionPeriod": 1,
        "DBClusterIdentifier": "sample-cluster-restore",
        "DBClusterParameterGroup": "default.docdb4.0",
        "DBSubnetGroup": "default",
        "Status": "creating",
        "Endpoint": "sample-cluster-restore.cluster-node.us-
east-1.docdb.amazonaws.com",
        "ReaderEndpoint": "sample-cluster-restore.cluster-node.us-
east-1.docdb.amazonaws.com",
        "MultiAZ": false,
        "Engine": "docdb",
        "EngineVersion": "4.0.0",
        "Port": 27017,
        "MasterUsername": "<master-user>",
        "PreferredBackupWindow": "02:00-02:30",
        "PreferredMaintenanceWindow": "tue:09:50-tue:10:20",
        "DBClusterMembers": [],
        "VpcSecurityGroups": [
            {
                "VpcSecurityGroupId": "sg-abcdefgh",
                "Status": "active"
            }
        ],
        "HostedZoneId": "ABCDEFGHIJKLM",
        "StorageEncrypted": true,
        "KmsKeyId": "arn:aws:kms:us-east-1:<accountID>:key/<sample-key-id>",
        "DbClusterResourceId": "cluster-ABCDEFGHIJKLMNOPQRSTUVWXYZ",
        "DBClusterArn": "arn:aws:rds:us-east-1:<accountID>:cluster:sample-cluster-
restore",
        "AssociatedRoles": [],
        "ClusterCreateTime": "2020-04-01T01:43:40.871Z",
        "DeletionProtection": true
```

```
    }
}
```

Nachdem der Clusterstatus available lautet, erstellen Sie mindestens eine Instance für den Cluster.

Für Linux, macOS oder Unix:

```
aws docdb create-db-instance \
    --db-cluster-identifier sample-cluster-restore  \
    --db-instance-identifier sample-cluster-restore-instance \
    --availability-zone us-east-1b \
    --promotion-tier 2 \
    --db-instance-class db.r5.large \
    --engine docdb
```

Für Windows:

```
aws docdb create-db-instance ^
    --db-cluster-identifier sample-cluster-restore  ^
    --db-instance-identifier sample-cluster-restore-instance ^
    --availability-zone us-east-1b ^
    --promotion-tier 2 ^
    --db-instance-class db.r5.large ^
    --engine docdb
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus.

```
{
    "DBInstance": {
        "DBInstanceIdentifier": "sample-cluster-restore-instance",
        "DBInstanceClass": "db.r5.large",
        "Engine": "docdb",
        "DBInstanceStatus": "creating",
        "PreferredBackupWindow": "02:00-02:30",
        "BackupRetentionPeriod": 1,
        "VpcSecurityGroups": [
            {
                "VpcSecurityGroupId": "sg-abcdefgh",
                "Status": "active"
            }
```

```
        ],
        "AvailabilityZone": "us-west-2b",
        "DBSubnetGroup": {
            "DBSubnetGroupName": "default",
            "DBSubnetGroupDescription": "default",
            "VpcId": "vpc-6242c31a",
            "SubnetGroupStatus": "Complete",
            "Subnets": [
                {
                    "SubnetIdentifier": "subnet-abcdefgh",
                    "SubnetAvailabilityZone": {
                        "Name": "us-west-2a"
                    },
                    "SubnetStatus": "Active"
                },
                {
                    ...
                }
            ]
        },
        "PreferredMaintenanceWindow": "fri:09:43-fri:10:13",
        "PendingModifiedValues": {},
        "EngineVersion": "4.0.0",
        "AutoMinorVersionUpgrade": true,
        "PubliclyAccessible": false,
        "DBClusterIdentifier": "sample-cluster-restore",
        "StorageEncrypted": true,
        "KmsKeyId": "arn:aws:kms:us-east-1:<accountID>:key/<sample-key-id>",
        "DbiResourceId": "db-ABCDEFGHIJKLMNOPQRSTUVWXYZ",
        "CACertificateIdentifier": "rds-ca-2019",
        "PromotionTier": 2,
        "DBInstanceArn": "arn:aws:rds:us-east-1:<accountID>:db:sample-cluster-
restore-instance"
    }
}
```

Zu einem bestimmten Zeitpunkt wiederherstellen

Sie können einen Cluster zu einem beliebigen Zeitpunkt innerhalb der Aufbewahrungsfrist für Backups des Clusters wiederherstellen, indem Sie AWS-Managementkonsole oder AWS Command Line Interface (AWS CLI) verwenden.

> **Note**
>
> Sie können keine Point-in-Time-Wiederherstellung eines 3.6-Clusters auf einen 4.0-Cluster durchführen, aber Sie können von einer Clusterversion zu einer anderen migrieren. Weitere Informationen finden Sie unter Migration zu Amazon DocumentDB.

Beachten Sie Folgendes, wenn Sie einen Cluster zu einem bestimmten Zeitpunkt wiederherstellen.

- Der neue Cluster wird mit der gleichen Konfiguration wie der Quell-Cluster erstellt, nur dass der neue Cluster mit der Standard-Parametergruppe erstellt wird. Um die Parametergruppe des neuen Clusters auf die Parametergruppe des Quellclusters festzulegen, ändern Sie den Cluster, nachdem er den Status available (verfügbar) hat. Weitere Informationen zum Ändern eines Clusters finden Sie unter Ändern eines Amazon DocumentDB-Clusters.

Using the AWS-Managementkonsole

Sie können einen Cluster innerhalb des Aufbewahrungszeitraums für Backups zu einem bestimmten Zeitpunkt wiederherstellen, indem Sie in der AWS-Managementkonsole Folgendes ausführen.

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Klicken Sie im Navigationsbereich auf Cluster. Wählen Sie in der Liste der Cluster die Schaltfläche links neben dem Cluster, den Sie wiederherstellen möchten.

   > **Tip**
   >
   > Wenn der Navigationsbereich auf der linken Seite des Bildschirms nicht angezeigt wird, wählen Sie links oben auf der Seite das Menüsymbol (≡) aus.

3. Wählen Sie im Menü Actions (Aktionen) die Option Restore to point in time (Zu einem bestimmten Zeitpunkt wiederherstellen).
4. Geben Sie im Bereich Restore time (Wiederherstellungszeit) Datum und Uhrzeit für die zeitpunktbezogene Wiederherstellung an.

a. Wiederherstellungsdatum — Wählen oder geben Sie ein Datum ein, das zwischen der frühesten Wiederherstellungszeit und der spätesten Wiederherstellungszeit liegt.

b. Wiederherstellungszeit — Wählen Sie die Stunde, Minute und Sekunden, die zwischen der frühesten Wiederherstellungszeit und der spätesten Wiederherstellungszeit liegen, oder geben Sie sie ein.

5. Füllen Sie den Bereich Configuration (Konfiguration) aus.

a. Cluster-ID — Akzeptieren Sie die Standard-ID, oder geben Sie eine von Ihnen bevorzugte ID ein.

Einschränkungen bei der Benennung von Clustern:

- Die Länge beträgt [1—63] Buchstaben, Zahlen oder Bindestriche.
- Muss mit einem Buchstaben beginnen.
- Darf nicht mit einem Bindestrich enden oder zwei aufeinanderfolgende Bindestriche enthalten.
- Muss für alle Cluster in Amazon RDS, Neptune und Amazon DocumentDB pro AWS-Konto Region eindeutig sein.

b. Instance-Klasse — Wählen Sie aus der Drop-down-Liste die Instance-Klasse aus, die Sie für die Instances des Clusters verwenden möchten.

c. Anzahl der Instanzen — Wählen Sie aus der Drop-down-Liste die Anzahl der Instanzen aus, die bei der Wiederherstellung des Clusters erstellt werden sollen.

6. Wählen Sie für die Cluster-Speicherkonfiguration eine Speicheroption aus.

> **Note**
>
> Die Amazon I/O-Optimized DocumentDB-Speicherkonfiguration ist nur in den Engine-Versionen Amazon DocumentDB 5.0 und 8.0 verfügbar.

7. Optional. Um die Netzwerkeinstellungen, Cluster-Optionen und die Aktivierung von Protokollexporten zu konfigurieren, wählen Sie Show advanced settings (Erweiterte Einstellungen anzeigen) aus. Schließen Sie dann die folgenden Abschnitte ab. Fahren Sie andernfalls mit dem nächsten Schritt fort.

- Network settings (Netzwerkeinstellungen)

1. Virtual Private Cloud (VPC) — Wählen Sie aus der Drop-down-Liste die VPC aus, die Sie für diesen Cluster verwenden möchten.
2. Subnetzgruppe — Wählen Sie aus der Drop-down-Liste die Subnetzgruppe für diesen Cluster aus.
3. VPC-Sicherheitsgruppen — Wählen Sie aus der Dropdownliste die VPC-Sicherheitsgruppen für diesen Cluster aus.

- Cluster options (Cluster-Optionen)
  1. Port — Akzeptieren Sie den Standardport (27017) oder verwenden Sie die Aufwärts- und Abwärtspfeile, um den Port für die Kommunikation mit diesem Cluster festzulegen.

- Protokollexporte
  1. Audit-Logs — Wählen Sie diese Option, um den Export von Audit-Logs nach Amazon CloudWatch Logs zu ermöglichen. Wenn Sie diese Option auswählen, müssen Sie `audit_logs` in der benutzerdefinierten Parametergruppe des Clusters aktivieren. Weitere Informationen finden Sie unter Amazon DocumentDB DocumentDB-Ereignisse prüfen.
  2. Profiler-Protokolle — Wählen Sie diese Option, um den Export von Operation-Profiler-Protokollen nach Amazon CloudWatch Logs zu ermöglichen. Wenn Sie diese Option auswählen, müssen Sie auch die folgenden Parameter in der benutzerdefinierten Parametergruppe des Clusters ändern:
     - `profiler`— Eingestellt auf. `enabled`
     - `profiler_threshold_ms`— Auf einen Wert setzen`[0-INT_MAX]`, um den Schwellenwert für Profilierungsvorgänge festzulegen.
     - `profiler_sampling_rate`— Geben Sie einen Wert ein, `[0.0-1.0]` um den Prozentsatz langsamer Operationen festzulegen, für den ein Profil erstellt werden soll.

     Weitere Informationen finden Sie unter Profilierung von Amazon DocumentDB DocumentDB-Vorgängen.
  3. Profiler-Protokolle — Exportieren Sie Profiler-Protokolle nach Amazon CloudWatch
  4. IAM-Rolle — Wählen Sie aus der Drop-down-Liste die Option RDS Service Linked Role aus.

- Tags

1. Tag hinzufügen — Geben Sie im Feld Schlüssel den Namen für das Tag für Ihren Cluster ein. Geben Sie optional im Feld Value (Wert) den Tag-Wert ein. Tags werden zusammen mit AWS Identity and Access Management (IAM-) Richtlinien verwendet, um den Zugriff auf Amazon DocumentDB DocumentDB-Ressourcen zu verwalten und zu kontrollieren, welche Aktionen auf die Ressourcen angewendet werden können.

- Löschschutz

1. Löschschutz aktivieren — Schützt den Cluster davor, versehentlich gelöscht zu werden. Wenn diese Option aktiviert ist, können Sie den Cluster nicht löschen.

8. Um den Cluster wiederherzustellen, wählen Sie Create cluster (Cluster erstellen). Alternativ können Sie Cancel (Abbrechen) auswählen, um den Vorgang abzubrechen.

Using the AWS CLI

Um einen Cluster zu einem bestimmten Zeitpunkt mit Hilfe der Aufbewahrungsdauer des Snapshots wiederherzustellen, verwenden Sie die Operation `restore-db-cluster-to-point-in-time` mit den folgenden Parametern.

- **`--db-cluster-identifier`**— Erforderlich. Der Name des neuen Clusters, der erstellt werden soll. Dieser Cluster darf vor der Operation nicht vorhanden sein. Der Parameterwert muss den folgenden Einschränkungen entsprechen.

  Einschränkungen bei der Benennung von Clustern:

  - Die Länge beträgt [1—63] Buchstaben, Zahlen oder Bindestriche.
  - Muss mit einem Buchstaben beginnen.
  - Darf nicht mit einem Bindestrich enden oder zwei aufeinanderfolgende Bindestriche enthalten.
  - Muss für alle Cluster in Amazon RDS, Neptune und Amazon DocumentDB pro AWS-Konto Region eindeutig sein.

- **`--restore-to-time`**— Das UTC-Datum und die Uhrzeit für die Wiederherstellung des Clusters. Beispiel, `2018-06-07T23:45:00Z`.

  Zeiteinschränkungen:

  - Muss vor dem letzten wiederherstellbaren Zeitpunkt für den Cluster liegen.
  - Muss angegeben werden, wenn der Parameter `--use-latest-restorable-time` nicht angegeben ist.

  - Kann nicht angegeben werden, wenn der Parameter `--use-latest-restorable-time` auf `true` festgelegt ist.
  - Kann nicht angegeben werden, wenn der Parameterwert `--restore-type copy-on-write` ist.
- **`--source-db-cluster-identifier`**— Der Name des Quell-Clusters, aus dem wiederhergestellt werden soll. Dieser Cluster muss vorhanden und verfügbar sein.
- **`--use-latest-restorable-time`**oder **`--no-use-latest-restorable-time`** — Ob die Wiederherstellung auf die letzte wiederherstellbare Backup-Zeit erfolgen soll. Darf nicht angegeben werden, wenn der Parameter `--restore-to-time` angegeben ist.
- **`--storage-type standard | iopt1`**— Fakultativ. Standard: `standard`.

Der AWS CLI Vorgang stellt `restore-db-cluster-to-point-in-time` nur den Cluster wieder her, nicht die Instanzen für diesen Cluster. Sie müssen die Operation `create-db-instance` aufrufen, um Instances für den wiederhergestellten Cluster zu erstellen, wobei Sie in `--db-cluster-identifier` die ID des wiederhergestellten Clusters angeben. Sie können Instances erst erstellen, nachdem die Operation `restore-db-cluster-to-point-in-time` abgeschlossen wurde und wenn der wiederhergestellte Cluster verfügbar ist.

Example

Das folgende Beispiel erstellt `sample-cluster-restored` aus Snapshot `sample-cluster-snapshot` für den letzten wiederherstellbaren Zeitpunkt.

Für Linux, macOS oder Unix:

```
aws docdb restore-db-cluster-to-point-in-time \
    --db-cluster-identifier sample-cluster-restored \
    --source-db-cluster-identifier sample-cluster-snapshot \
    --use-latest-restorable-time
```

Für Windows:

```
aws docdb restore-db-cluster-to-point-in-time ^
    --db-cluster-identifier sample-cluster-restored ^
    --source-db-cluster-identifier sample-cluster-snapshot ^
    --use-latest-restorable-time
```

Example

Das folgende Beispiel erstellt `sample-cluster-restored` aus Snapshot `sample-cluster-snapshot` für 03:15 Uhr am 11. Dezember 2018 (UTC) (liegt innerhalb des Aufbewahrungszeitraums für Backups von `sample-cluster`).

Für Linux, macOS oder Unix:

```
aws docdb restore-db-cluster-to-point-in-time \
    --db-cluster-identifier sample-cluster-restore \
    --source-db-cluster-identifier sample-cluster \
    --restore-to-time 2020-05-12T03:15:00Z
```

Für Windows:

```
aws docdb restore-db-cluster-to-point-in-time ^
    --db-cluster-identifier sample-cluster-restore ^
    --source-db-cluster-identifier sample-cluster ^
    --restore-to-time 2020-05-12T03:15:00Z
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus.

```
{
    "DBCluster": {
        "AvailabilityZones": [
            "us-east-1c",
            "us-west-2b",
            "us-west-2a"
        ],
        "BackupRetentionPeriod": 1,
        "DBClusterIdentifier": "sample-cluster-restored",
        "DBClusterParameterGroup": "sample-parameter-group",
        "DBSubnetGroup": "default",
        "Status": "creating",
        "Endpoint": "sample-cluster-restored.node.us-east-1.docdb.amazonaws.com",
        "ReaderEndpoint": "sample-cluster-restored.node.us-
east-1.docdb.amazonaws.com",
        "MultiAZ": false,
        "Engine": "docdb",
        "EngineVersion": "4.0.0",
        "Port": 27017,
```

```
        "MasterUsername": "master-user",
        "PreferredBackupWindow": "02:00-02:30",
        "PreferredMaintenanceWindow": "tue:09:50-tue:10:20",
        "DBClusterMembers": [],
        "VpcSecurityGroups": [
            {
                "VpcSecurityGroupId": "sg-abc0123",
                "Status": "active"
            }
        ],
        "HostedZoneId": "ABCDEFGHIJKLM",
        "StorageEncrypted": true,
        "KmsKeyId": "arn:aws:kms:us-east-1:<accountID^>:key/sample-key",
        "DbClusterResourceId": "cluster-ABCDEFGHIJKLMNOPQRSTUVWXYZ",
        "DBClusterArn": "arn:aws:rds:us-east-1:<accountID>:cluster:sample-cluster-
restored",
        "AssociatedRoles": [],
        "ClusterCreateTime": "2020-04-24T20:14:36.713Z",
        "DeletionProtection": false
    }
}
```

Löschen eines Cluster-Snapshots

Ein manueller Snapshot ist ein vollständiges Backup, das nur gelöscht wird, wenn Sie es manuell mit dem AWS-Managementkonsole oder AWS CLI löschen. Sie können einen automatischen Snapshot nicht manuell löschen, da automatische Snapshots nur gelöscht werden, wenn die Aufbewahrungsfrist des Snapshots abläuft oder Sie den Cluster des Snapshots löschen.

Using the AWS-Managementkonsole

Gehen Sie wie folgt vor AWS-Managementkonsole, um einen manuellen Cluster-Snapshot mithilfe von zu löschen.

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Wählen Sie im Navigationsbereich die Option Snapshots.

> **Tip**
>
> Wenn der Navigationsbereich auf der linken Seite des Bildschirms nicht angezeigt wird, wählen Sie links oben auf der Seite das Menüsymbol (≡) aus.

3. Wählen Sie in der Liste der Snapshots die Schaltfläche links neben dem Snapshot, den Sie löschen möchten. Der Typ des Snapshots muss manuell sein.

   1. Sie können überprüfen, ob der Snapshot-Typ manuell ist, indem Sie überprüfen, ob er als `manual` oder in der `automatic` Spalte Typ aufgeführt ist.

4. Wählen Sie im Menü Actions (Aktionen) die Option Delete (Löschen) aus. Wenn die Option Delete (Löschen) nicht verfügbar ist, haben Sie wahrscheinlich einen automatischen Snapshot auswählt.
5. Um den Snapshot zu löschen, wählen Sie auf der Bestätigungsseite des Löschvorgangs Delete (Löschen) aus. Um den Snapshot zu erhalten, wählen Sie Cancel (Abbrechen) aus.

Using the AWS CLI

Ein manueller Amazon DocumentDB-Cluster-Snapshot ist ein vollständiges Backup, das Sie manuell mit dem AWS CLI löschen können. Sie können einen automatischen Snapshot nicht manuell löschen.

Um einen manuellen Cluster-Snapshot mit dem zu löschen AWS CLI, verwenden Sie den `delete-db-cluster-snapshot` Vorgang mit den folgenden Parametern.

Parameters

- **`--db-cluster-snapshot-identifier`** – Erforderlich. Der Name des zu löschenden manuellen Snapshots.

Das folgende Beispiel löscht den Cluster-Snapshot `sample-cluster-snapshot`.

Für Linux, macOS oder Unix:

```
aws docdb delete-db-cluster-snapshot \
    --db-cluster-snapshot-identifier sample-cluster-snapshot
```

Für Windows:

```
aws docdb delete-db-cluster-snapshot ^
    --db-cluster-snapshot-identifier sample-cluster-snapshot
```

Die Ausgabe dieses Vorgangs führt die Einzelheiten des von Ihnen gelöschten Cluster-Snapshots auf.

Verwaltung von Amazon DocumentDB DocumentDB-Ressourcen

In diesen Abschnitten werden die verschiedenen Komponenten und die damit verbundenen Aufgaben für die Verwaltung Ihrer Amazon DocumentDB DocumentDB-Implementierung (mit MongoDB-Kompatibilität) behandelt.

Themen

- Überblick über die operativen Aufgaben von Amazon DocumentDB
- Überblick über die globalen Amazon DocumentDB-Cluster
- Verwaltung von Amazon DocumentDB-Clustern
- Verwaltung von Amazon DocumentDB DocumentDB-Instances
- Amazon DocumentDB-Subnetzgruppen verwalten
- Amazon DocumentDB Hochverfügbarkeit und Replikation
- Amazon DocumentDB DocumentDB-Indizes verwalten
- Verwaltung der Dokumentenkomprimierung auf Sammlungsebene
- Verwaltung der wörterbuchbasierten Komprimierung in Amazon DocumentDB 8.0
- Amazon DocumentDB DocumentDB-Ereignisse verwalten
- Auswahl von Regionen und Availability Zones
- Verwaltung von Amazon DocumentDB-Cluster-Parametergruppen
- Grundlegendes zu Amazon DocumentDB DocumentDB-Endpunkten
- Grundlegendes zu Amazon DocumentDB Amazon Resource Names (ARNs)
- Taggen von Amazon DocumentDB DocumentDB-Ressourcen
- Wartung von Amazon DocumentDB
- Grundlegendes zu Rollen im Zusammenhang mit Services
- Change-Streams mit Amazon DocumentDB verwenden
- Verwenden der Sortierung in Amazon DocumentDB 8.0
- Verwenden von Ansichten in Amazon DocumentDB 8.0
- Verwenden AWS Lambda mit Change-Streams

Überblick über die operativen Aufgaben von Amazon DocumentDB

Dieser Abschnitt behandelt betriebliche Aufgaben für Ihren Amazon DocumentDB-Cluster und wie Sie diese Aufgaben mit dem AWS CLI erledigen können.

Themen

- Hinzufügen eines Replikats zu einem Amazon DocumentDB-Cluster
- Beschreibung von Clustern und Instanzen
- Einen Cluster-Snapshot erstellen
- Wiederherstellung aus einem Snapshot
- Eine Instanz aus einem Cluster entfernen
- Löschen eines Clusters

Hinzufügen eines Replikats zu einem Amazon DocumentDB-Cluster

Nachdem Sie die primäre Instance für Ihren Amazon DocumentDB-Cluster erstellt haben, können Sie ein oder mehrere Replikate hinzufügen. Ein Replikat ist eine schreibgeschützte Instance, die zwei Zwecken dient:

- Skalierbarkeit — Wenn Sie über eine große Anzahl von Clients verfügen, die gleichzeitigen Zugriff benötigen, können Sie weitere Replikate für die Leseskalierung hinzufügen.
- Hochverfügbarkeit — Wenn die primäre Instance ausfällt, wechselt Amazon DocumentDB automatisch zu einer Replikat-Instance und bestimmt diese als neue primäre Instanz. Wenn ein Replikat ausfällt, können andere Instances im Cluster nach wie vor für die Bearbeitung von Anfragen verwendet werden, bis der ausgefallene Knoten wiederhergestellt werden kann.

Jeder Amazon DocumentDB-Cluster kann bis zu 15 Replikate unterstützen.

> **Note**
>
> Für maximale Fehlertoleranz sollten Sie Replikate in separaten Availability Zones bereitstellen. Dadurch wird sichergestellt, dass Ihr Amazon DocumentDB-Cluster auch dann weiter funktioniert, wenn eine gesamte Availability Zone nicht verfügbar ist.

Das folgende AWS CLI Beispiel zeigt, wie ein neues Replikat hinzugefügt wird. Der `--availability-zone`-Parameter platziert das Replikat in der angegebenen Availability Zone.

```
aws docdb create-db-instance \
    --db-instance-identifier sample-instance \
    --db-cluster-identifier sample-cluster \
    --engine docdb \
    --db-instance-class db.r5.large \
    --availability-zone us-east-1a
```

Beschreibung von Clustern und Instanzen

Das folgende AWS CLI Beispiel listet alle Amazon DocumentDB-Cluster in einer Region auf. Für bestimmte Verwaltungsfunktionen wie Cluster- und Instance-Lebenszyklusmanagement nutzt Amazon DocumentDB Betriebstechnologie, die mit Amazon RDS gemeinsam genutzt wird. Der `filterName=engine,Values=docdb` Filterparameter gibt nur Amazon DocumentDB-Cluster zurück.

Weitere Informationen zum Beschreiben und Ändern von Clustern finden Sie im Amazon DocumentDB-Cluster-Lebenszyklus.

```
aws docdb describe-db-clusters --filter Name=engine,Values=docdb
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus.

```
{
    "DBClusters": [
        {
            "AvailabilityZones": [
                "us-east-1c",
                "us-east-1b",
                "us-east-1a"
            ],
            "BackupRetentionPeriod": 1,
            "DBClusterIdentifier": "sample-cluster-1",
            "DBClusterParameterGroup": "sample-parameter-group",
            "DBSubnetGroup": "default",
            "Status": "available",
            ...
        },
```

```
        {
            "AvailabilityZones": [
                "us-east-1c",
                "us-east-1b",
                "us-east-1a"
            ],
            "BackupRetentionPeriod": 1,
            "DBClusterIdentifier": "sample-cluster-2",
            "DBClusterParameterGroup": "sample-parameter-group",
            "DBSubnetGroup": "default",
            "Status": "available",
            ...
        },
        {
            "AvailabilityZones": [
                "us-east-1c",
                "us-east-1b",
                "us-east-1a"
            ],
            "BackupRetentionPeriod": 1,
            "DBClusterIdentifier": "sample-cluster-3",
            "DBClusterParameterGroup": "sample-parameter-group",
            "DBSubnetGroup": "default",
            "Status": "available",
            ...
        }
    ]
}
```

Das folgende AWS CLI Beispiel listet die Instances in einem Amazon DocumentDB-Cluster auf. Weitere Informationen zum Beschreiben und Ändern von Clustern finden Sie im Lebenszyklus einer Amazon DocumentDB DocumentDB-Instanz.

```
aws docdb describe-db-clusters \
    --db-cluster-identifier sample-cluster \
    --query 'DBClusters[*].[DBClusterMembers]'
```

Die Ausgabe sieht wie unten aus. Diese Ausgabe enthält zwei Instances. Die Primär-Instance ist `sample-instance-1` (`"IsClusterWriter": true`). Es gibt auch eine Replikat-Instance, nämlich `sample-instance2` (`"IsClusterWriter: false"`).

```
[
```

```
    [
        [
            {
                "DBInstanceIdentifier": "sample-instance-1",
                "IsClusterWriter": true,
                "DBClusterParameterGroupStatus": "in-sync",
                "PromotionTier": 1
            },
            {
                "DBInstanceIdentifier": "sample-cluster-2",
                "IsClusterWriter": false,
                "DBClusterParameterGroupStatus": "in-sync",
                "PromotionTier": 1
            }
        ]
    ]
]
```

Einen Cluster-Snapshot erstellen

Ein Cluster-Snapshot ist eine vollständige Sicherung der Daten in Ihrem Amazon DocumentDB-Cluster. Wenn der Snapshot erstellt wird, liest Amazon DocumentDB Ihre Daten direkt aus dem Cluster-Volume. Aus diesem Grund können Sie einen Snapshot erstellen, auch wenn zum jeweiligen Zeitpunkt keine Instances in Ihrem Cluster ausgeführt werden. Die zum Erstellen eines Snapshots erforderliche Zeit hängt von der Größe Ihres Cluster-Volumes ab.

Amazon DocumentDB unterstützt automatische Backups, die täglich während des bevorzugten Backup-Fensters — einem Zeitraum von 30 Minuten am Tag — durchgeführt werden. Das folgende AWS CLI Beispiel zeigt, wie Sie das Backup-Fenster für Ihren Cluster anzeigen können:

```
aws docdb describe-db-clusters \
    --db-cluster-identifier sample-cluster \
    --query 'DBClusters[*].PreferredBackupWindow'
```

Die Ausgabe zeigt das Sicherungszeitfenster (in UTC):

```
[
    "00:18-00:48"
]
```

Sie können das Backup-Fenster definieren, wenn Sie Ihren Amazon DocumentDB-Cluster erstellen. Sie können das Sicherungszeitfenster auch ändern, wie im folgenden Beispiel gezeigt wird. Wenn Sie kein Backup-Fenster definieren, weist Amazon DocumentDB Ihrem Cluster automatisch eines zu.

```
aws docdb modify-db-cluster \
    --db-cluster-identifier sample-cluster \
    --preferred-backup-window "02:00-02:30"
```

Zusätzlich zu automatischen Sicherungen können Sie jederzeit manuell einen Cluster-Snapshot erstellen. Wenn Sie dies tun, müssen Sie das zu sichernde Cluster festlegen und dem Snapshot einen eindeutigen Namen geben, damit er später für Wiederherstellungszwecke verwendet werden kann.

Das folgende AWS CLI Beispiel zeigt, wie Sie einen Snapshot Ihrer Daten erstellen.

```
aws docdb create-db-cluster-snapshot \
    --db-cluster-identifier sample-cluster \
    --db-cluster-snapshot-identifier sample-cluster-snapshot
```

Wiederherstellung aus einem Snapshot

Sie können einen Cluster-Snapshot in einem neuen Amazon DocumentDB-Cluster wiederherstellen. Dazu geben Sie den Namen des Snapshots und den Namen eines neuen Clusters an. Sie können keine Wiederherstellung von einem Snapshot in einem vorhandenen Cluster durchführen. Stattdessen erstellt Amazon DocumentDB bei der Wiederherstellung einen neuen Cluster und füllt ihn dann mit Ihren Snapshot-Daten.

Das folgende Beispiel zeigt alle Snapshots für den Cluster `sample-cluster`.

```
aws docdb describe-db-cluster-snapshots \
    --db-cluster-identifier sample-cluster \
    --query 'DBClusterSnapshots[*].[DBClusterSnapshotIdentifier,SnapshotType,Status]'
```

Die Ausgabe sieht ungefähr wie folgt aus. Ein manueller Snapshot ist ein Snapshot, den Sie manuell erstellt haben, wohingegen ein automatisierter Snapshot von Amazon DocumentDB innerhalb des Cluster-Backup-Fensters erstellt wird.

```
[
```

```
        "sample-cluster-snapshot",
        "manual",
        "available"
    ],
    [
        "rds:sample-cluster",
        "automated",
        "available"
    ]
]
```

Das folgende Beispiel zeigt, wie ein Amazon DocumentDB-Cluster aus einem Snapshot wiederhergestellt wird.

```
aws docdb restore-db-cluster-from-snapshot \
    --engine docdb \
    --db-cluster-identifier new-sample-cluster \
    --snapshot-identifier sample-cluster-snapshot
```

Dem neuen Cluster sind keine Instances zugeordnet. Wenn Sie mit dem Cluster interagieren möchten, müssen Sie ihm also eine Instance hinzufügen.

```
aws docdb create-db-instance \
    --db-instance-identifier new-sample-instance \
    --db-instance-class db.r5.large \
    --engine docdb \
    --db-cluster-identifier new-sample-cluster
```

Sie können die folgenden AWS CLI Operationen verwenden, um den Fortschritt der Cluster- und Instance-Erstellung zu überwachen. Wenn die Cluster- und Instance-Status verfügbar sind, können Sie eine Verbindung zum neuen Endpunkt des Clusters herstellen und auf Ihre Daten zugreifen.

```
aws docdb describe-db-clusters \
    --db-cluster-identifier new-sample-cluster  \
    --query 'DBClusters[*].[Status,Endpoint]'
```

```
aws docdb describe-db-instances \
    --db-instance-identifier new-sample-instance \
    --query 'DBInstances[*].[DBInstanceStatus]'
```

Eine Instanz aus einem Cluster entfernen

Amazon DocumentDB speichert all Ihre Daten im Cluster-Volume. Die Daten bleiben in diesem Cluster-Volume erhalten. Dies gilt auch dann, wenn Sie alle Instances von Ihrem Cluster entfernen. Wenn Sie erneut auf die Daten zugreifen müssen, können Sie jederzeit dem Cluster eine Instance hinzufügen und da weitermachen, wo Sie aufgehört haben.

Das folgende Beispiel zeigt, wie Sie eine Instance aus Ihrem Amazon DocumentDB-Cluster entfernen.

```
aws docdb delete-db-instance \
    --db-instance-identifier sample-instance
```

Löschen eines Clusters

Bevor Sie einen Amazon DocumentDB-Cluster löschen können, müssen Sie zunächst alle zugehörigen Instances entfernen. Das folgende AWS CLI Beispiel gibt Informationen über die Instances in einem Cluster zurück. Wenn diese Operation Instance-Kennungen zurückgibt, müssen Sie die einzelnen Instances löschen. Weitere Informationen finden Sie unter Eine Instanz aus einem Cluster entfernen.

```
aws docdb describe-db-clusters \
    --db-cluster-identifier sample-cluster \
    --query 'DBClusters[*].DBClusterMembers[*].DBInstanceIdentifier'
```

Wenn keine Instances mehr vorhanden sind, können Sie das Cluster löschen. Sie müssen dann eine der folgenden Optionen wählen:

- Einen endgültigen Snapshot erstellen — Erfassen Sie alle Clusterdaten in einem Snapshot, sodass Sie später eine neue Instanz mit diesen Daten neu erstellen können. Das Verfahren wird im folgenden Beispiel beschrieben:

  ```
  aws docdb delete-db-cluster \
      --db-cluster-identifier sample-cluster \
      --final-db-snapshot-identifier sample-cluster-snapshot
  ```

- Den letzten Snapshot überspringen — Alle Clusterdaten werden dauerhaft gelöscht. Diese Aktion ist unwiderruflich. Das Verfahren wird im folgenden Beispiel beschrieben:

```
aws docdb delete-db-cluster \
    --db-cluster-identifier sample-cluster \
    --skip-final-snapshot
```

Überblick über die globalen Amazon DocumentDB-Cluster

Was ist ein globaler Cluster?

Ein globaler Cluster besteht aus einer primären Region und bis zu 10 schreibgeschützten sekundären Regionen. Sie führen Schreibvorgänge direkt in den primären Cluster in der primären Region durch und Amazon DocumentDB repliziert die Daten mithilfe einer dedizierten Infrastruktur automatisch in die sekundären Regionen. Die Latenz liegt in der Regel unter einer Sekunde.

Wie sind globale Cluster nützlich?

- Wiederherstellung nach regionalen Ausfällen — Im Falle eines regionsweiten Ausfalls können Sie einen der sekundären Cluster innerhalb von Minuten zu einem primären Cluster heraufstufen, wobei ein typisches Recovery Time Objective (RTO) unter einer Minute liegt. Das Recovery Point Objective (RPO) wird in der Regel in Sekunden gemessen. Dies hängt jedoch von der Verzögerung im Netzwerk zum Zeitpunkt des Ausfalls ab.
- Globale Lesevorgänge mit lokaler Latenz — Wenn Sie Niederlassungen auf der ganzen Welt haben, können Sie einen globalen Cluster verwenden, um Ihre wichtigsten Informationsquellen in der Primärregion auf dem neuesten Stand zu halten. Niederlassungen in Ihren anderen Regionen können mit lokaler Latenz auf die Informationen in ihrer eigenen Region zugreifen.
- Skalierbare sekundäre Cluster — Sie können Ihre sekundären Cluster skalieren, indem Sie einer sekundären Region weitere Nur-Lese-Instances hinzufügen. Der sekundäre Cluster ist schreibgeschützt, sodass er bis zu 16 schreibgeschützte Replikatinstanzen anstelle der üblichen Grenze von 15 für einen einzelnen Cluster unterstützen kann.
- Schnelle Replikation vom primären zum sekundären Cluster — Die von einem globalen Cluster durchgeführte Replikation hat nur geringe Auswirkungen auf die Leistung des primären Datenbank-Clusters. Die Ressourcen der DB-Instances werden ausschließlich für Lese- und Schreib-Workloads von Anwendungen genutzt.
- Streams ändern — Sie können Change-Streams aus einem sekundären Cluster in globalen Clustern lesen, wodurch die Belastung des primären Clusters reduziert wird und Sie Lese-Workloads von sekundären Regionen aus skalieren können.

Was sind die aktuellen Einschränkungen globaler Cluster?

- Globale Cluster werden in Amazon DocumentDB v3.6 nicht unterstützt.
- Globale Cluster werden auf allen Instance-Typen außer db.t3, db.t4g und db.r4 unterstützt.
- Globale Cluster sind in den folgenden Regionen nicht verfügbar: Südamerika (São Paulo), Europa (Mailand), China (Peking) und China (Ningxia).
- Switchover und globales Failover werden nicht unterstützt, wenn Regionen unterschiedliche Engine-Versionen verwenden. Manuelles Failover wird unterstützt, wenn die Engine-Versionen nicht übereinstimmen.
- Nur der primäre Cluster führt Schreibvorgänge aus. Clients, die Schreibvorgänge ausführen, stellen eine Verbindung zum Clusterendpunkt des primären Clusters her.
- Sie können maximal 10 sekundäre Regionen und eine primäre Region für Ihren Cluster einrichten.
- Ein sekundärer Cluster kann nicht gestoppt werden. Ein primärer Cluster kann nicht gestoppt werden, wenn ihm sekundäre Cluster zugeordnet sind. Nur ein regionaler Cluster ohne sekundäre Cluster kann gestoppt werden.
- An den sekundären Cluster angehängte Replikate können unter bestimmten Umständen neu gestartet werden. Wenn die Instanz der primären Region neu gestartet oder ein Failover durchgeführt wird, werden auch die Replikate in der sekundären Region neu gestartet. Der Cluster ist dann nicht verfügbar, bis alle Replikate wieder mit der Writer-Instance des primären Datenbankclusters synchronisiert sind. Dieses Verhalten wird erwartet. Stellen Sie sicher, dass Sie die Auswirkungen auf Ihren globalen Cluster verstehen, bevor Sie Änderungen an Ihrem primären Cluster vornehmen.

Themen

- Schnellstartanleitung: globale Cluster
- Verwaltung eines globalen Amazon DocumentDB-Clusters
- Stellen Sie eine Connect zu einem globalen Amazon DocumentDB-Cluster her
- Überwachung globaler Amazon DocumentDB-Cluster
- Disaster Recovery und globale Amazon DocumentDB-Cluster

Schnellstartanleitung: globale Cluster

Themen

- Konfiguration
- Einen globalen Amazon DocumentDB-Cluster erstellen
- Hinzufügen eines AWS-Region zu einem globalen Amazon DocumentDB-Cluster
- Verwenden eines Snapshots für Ihren globalen Amazon DocumentDB-Cluster

Konfiguration

Der globale Amazon DocumentDB-Cluster umfasst mindestens zwei. AWS-Regionen Die primäre Region unterstützt einen Cluster mit einer primären (Writer-) Instance und bis zu 15 Replikat-Instances, während in einer sekundären Region ein schreibgeschütztes Cluster läuft, das ausschließlich aus bis zu 16 Replikat-Instances besteht. Ein globaler Cluster kann bis zu 10 sekundäre Regionen haben. In der Tabelle sind die maximal zulässigen Cluster, Instances und Replikate in einem globalen Cluster aufgeführt.

Description	Primär AWS-Region	Sekundär AWS-Region
Cluster	1	10 (maximal)
Writer-Inst	1	0
Read-only Instanzen (Amazon DocumentDB DocumentDB-Replikate), pro Cluster	15 (Max.)	16 (Total)
Read-only Instanzen (maximal zulässig, bei gegebener Anzahl sekundärer Regionen)	15 - s	s = Gesamtzahl der sekundäre n AWS-Regionen

Für die Cluster gelten die folgenden spezifischen Anforderungen:

- Klassenanforderungen für Datenbank-Instances — Sie können nur die Klassen `db.r5` und `db.r6g` Instance verwenden.
- AWS-Region Anforderungen — Der primäre Cluster muss sich in einer Region befinden, und mindestens ein sekundärer Cluster muss sich in einer anderen Region desselben Kontos befinden. Sie können bis zu 10 sekundäre (schreibgeschützte) Cluster erstellen, und jeder muss sich in einer

anderen Region befinden. Mit anderen Worten, es können sich keine zwei Cluster in derselben Region befinden.

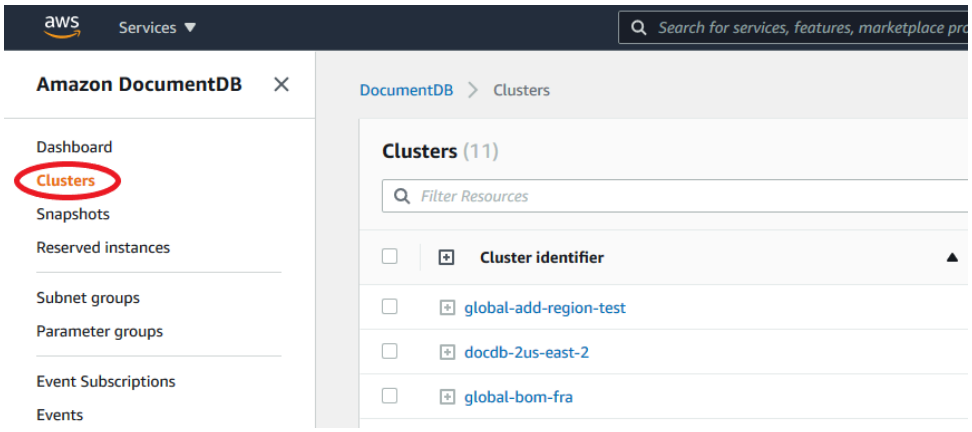
- Anforderungen an die Benennung — Die Namen, die Sie für jeden Ihrer Cluster wählen, müssen in allen Regionen eindeutig sein. Sie können nicht denselben Namen für verschiedene Cluster verwenden, auch wenn sie sich in verschiedenen Regionen befinden.

Einen globalen Amazon DocumentDB-Cluster erstellen

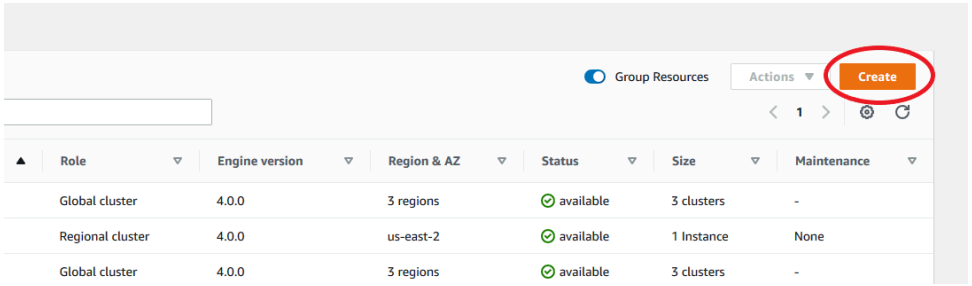
Sind Sie bereit, Ihren ersten globalen Cluster aufzubauen? In diesem Abschnitt erklären wir, wie Sie einen brandneuen globalen Cluster mit neuen Datenbankclustern und Instances erstellen, indem Sie entweder die AWS-Managementkonsole oder AWS CLI die folgenden Anweisungen verwenden.

Verwendung der AWS-Managementkonsole

1. Navigieren Sie in der AWS-Managementkonsole zu Amazon DocumentDB.
2. Wenn Sie zur Amazon DocumentDB DocumentDB-Konsole gelangen, wählen Sie Clusters.

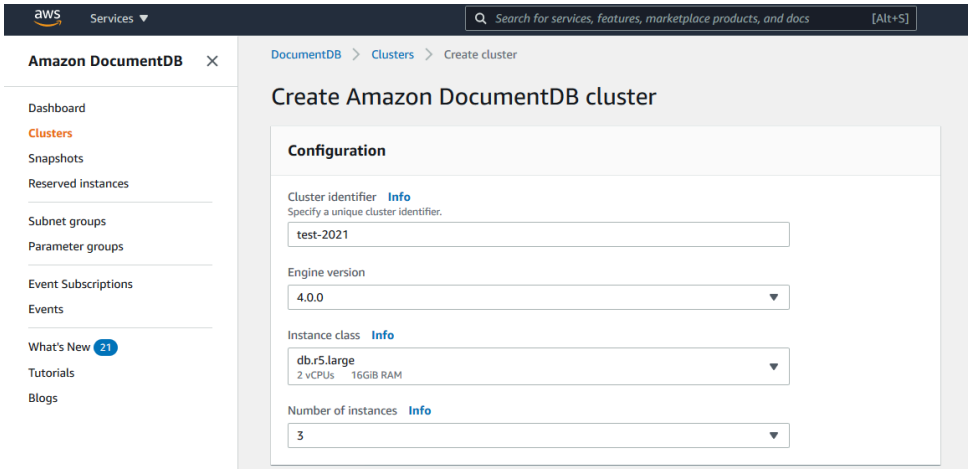


3. Wählen Sie Erstellen aus.

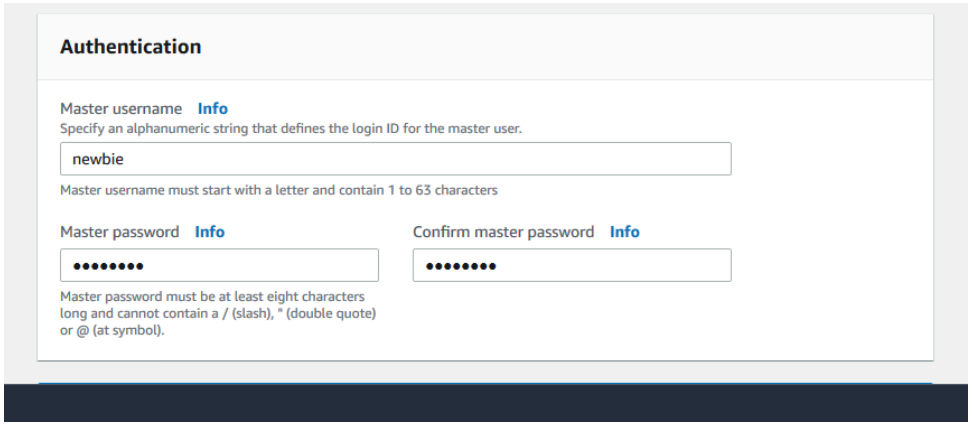


4. Füllen Sie den Abschnitt Konfiguration des Formulars Amazon DocumentDB-Cluster erstellen entsprechend aus:

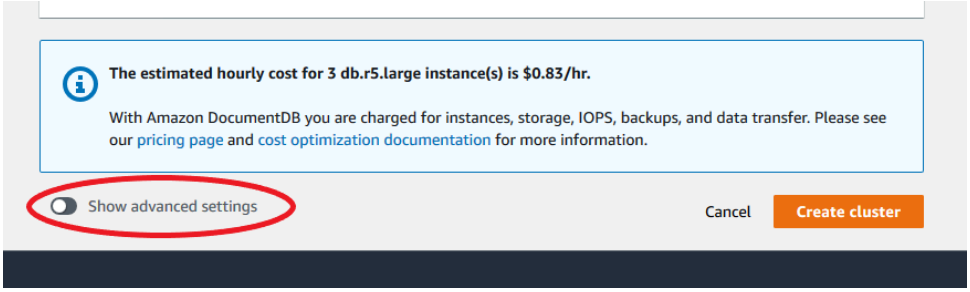
- Cluster-ID: Sie können entweder eine eindeutige Kennung für diese Instance eingeben oder Amazon DocumentDB erlauben, die Instance-ID auf der Grundlage der Cluster-ID bereitzustellen.
- Engine-Version: Wählen Sie 4.0.0
- Instanzklasse: Wählen Sie db.r5.large
- Anzahl der Instanzen: Wählen Sie 3.



5. Geben Sie im Abschnitt Authentifizierung einen Master-Benutzernamen und ein Master-Passwort ein.

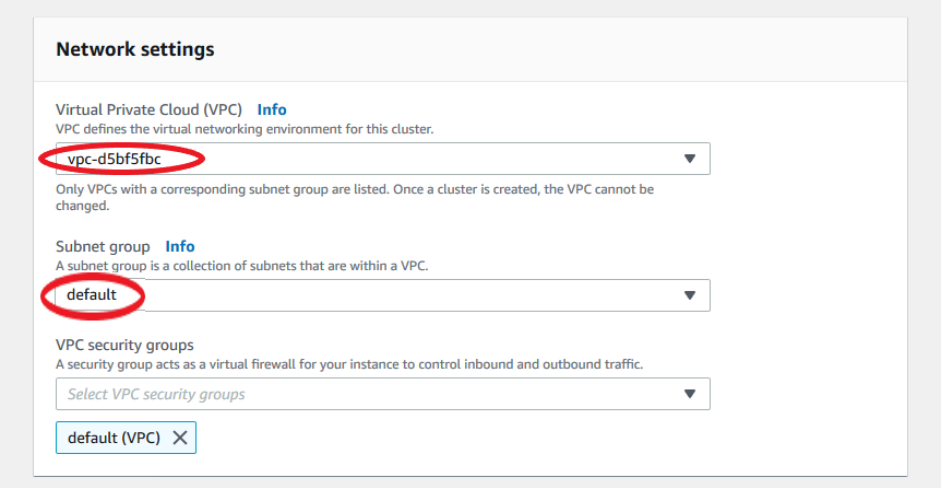


6. Wählen Sie Erweiterte Einstellungen anzeigen.

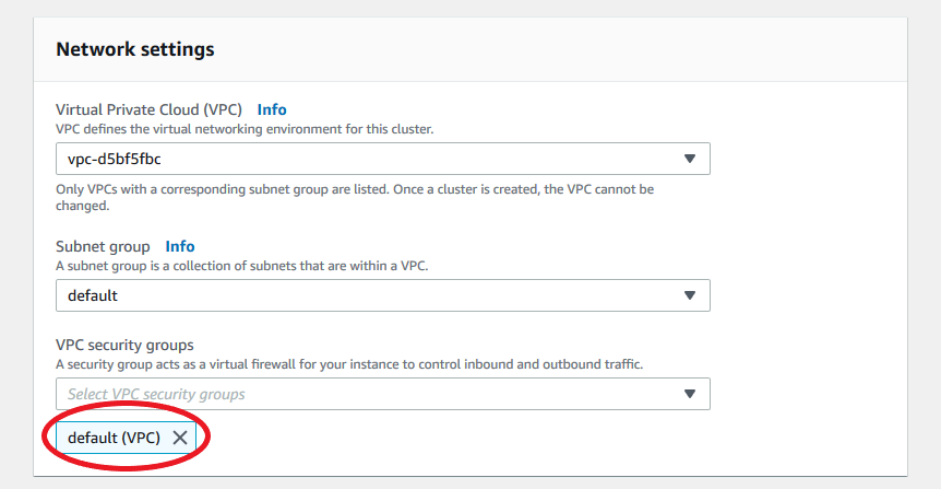


7. Gehen Sie im Bereich Netzwerkeinstellungen wie folgt vor:

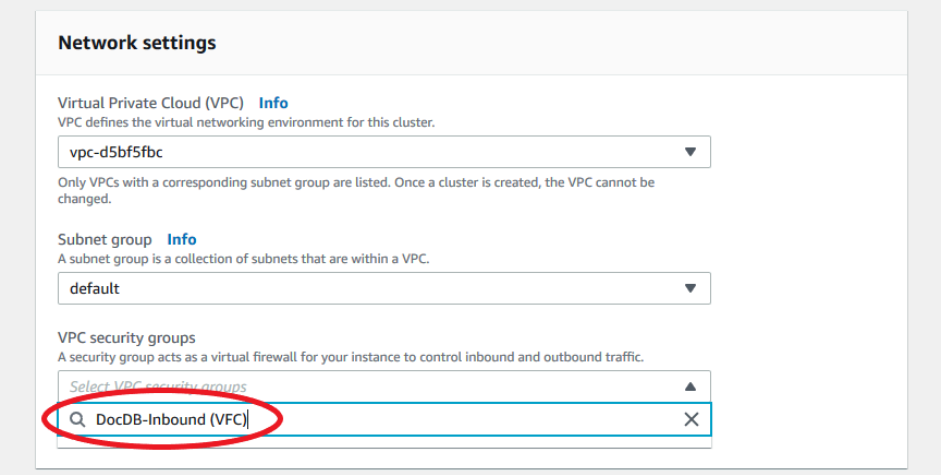
   - Behalten Sie die Standardoptionen für Virtual Private Cloud (VPC) und Subnetzgruppe bei.



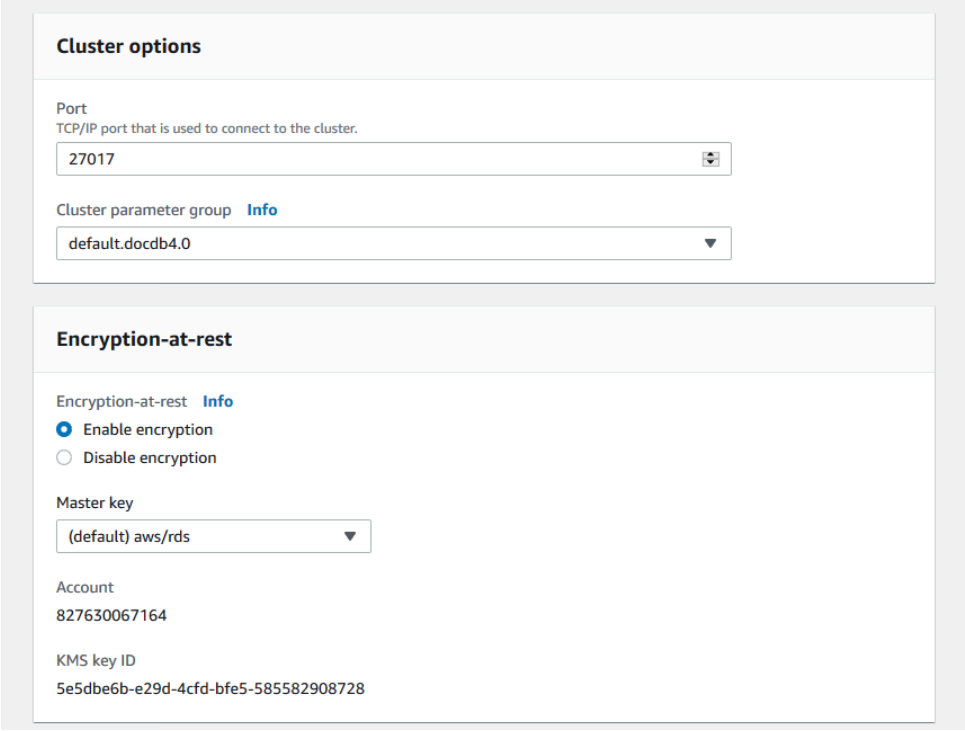
   - Für VPC-Sicherheitsgruppen sollte Standard (VPC) bereits hinzugefügt sein.



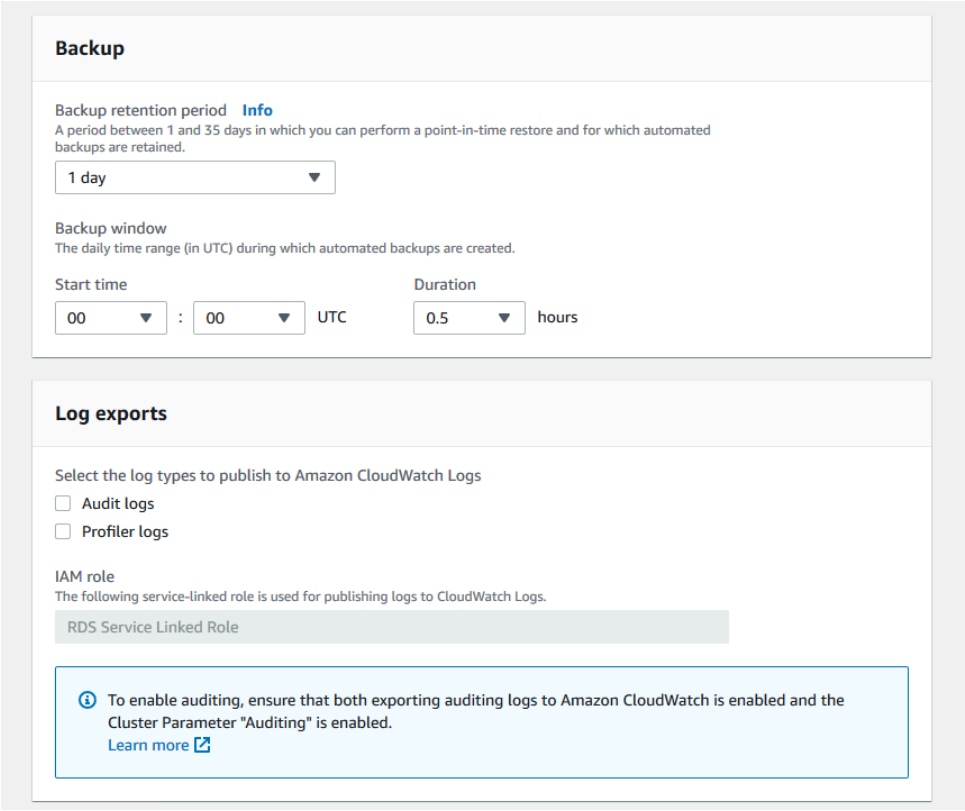
   - Geben Sie `DocDB` in das Feld VPC-Sicherheitsgruppen ein und wählen Sie DocDB-Inbound (VFC) aus.



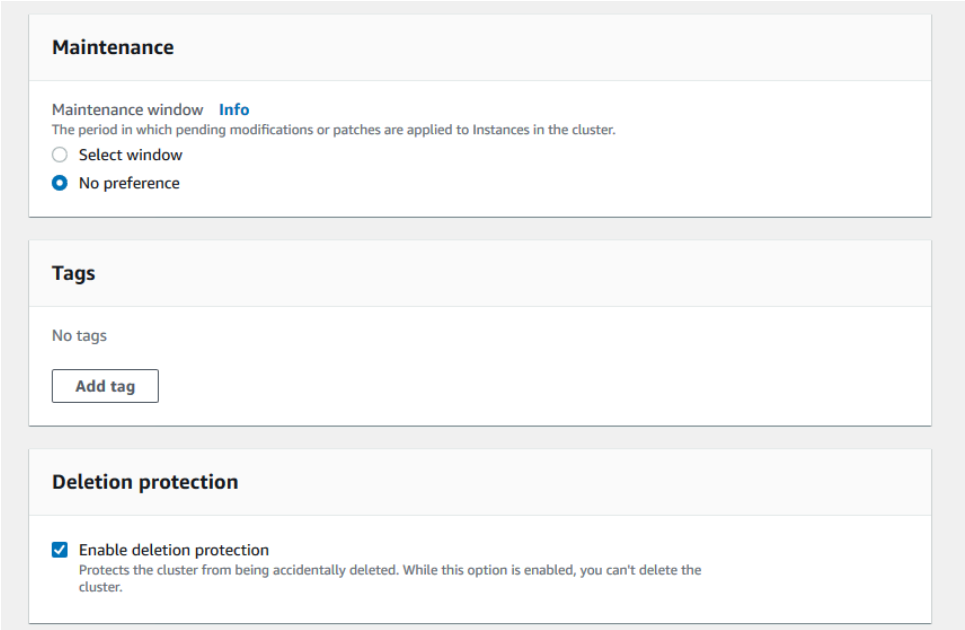
8. Behalten Sie für Cluster-Optionen und Encryption-at-restdie Standardauswahl bei.



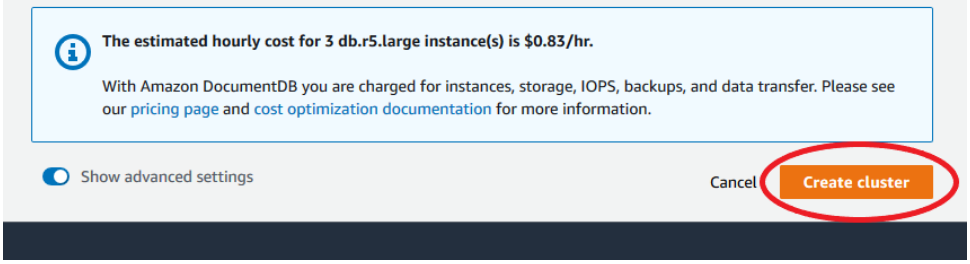
9. Behalten Sie für Backup - und Protokollexporte die Standardauswahl bei.



10. Behalten Sie für Wartung, Tags und Löschschutz die Standardauswahl bei.



11. Wählen Sie nun Cluster erstellen.



Verwendung der AWS CLI

Um einen regionalen Amazon DocumentDB-Cluster zu erstellen, rufen Sie den AWS CLI create-global-cluster auf. Der folgende AWS CLI Befehl erstellt einen Amazon DocumentDB-Cluster mit dem Namen`global-cluster-id`. Weitere Informationen zum Löschschutz finden Sie unterLöschen eines Amazon DocumentDB-Clusters.

Außerdem `--engine-version` ist dies ein optionaler Parameter, der standardmäßig die neueste Hauptversion der Engine verwendet. Die aktuelle Standard-Engine-Version ist `5.0.0` (Hinweis: Amazon DocumentDB 8.0 ist verfügbar, muss aber explizit als angegeben werden`8.0.0`). Wenn neue Hauptversionen der Engine veröffentlicht werden, `--engine-version` wird die Standard-Engine-Version für aktualisiert, sodass sie die letzte Hauptversion der Engine widerspiegelt. Daher empfehlen wir für Produktionsworkloads, insbesondere solche, die von Skripten, Automatisierung oder CloudFormation Vorlagen abhängig sind, die Angabe der `--engine-version` beabsichtigten Hauptversion ausdrücklich.

Wenn ein `db-subnet-group-name` oder nicht angegeben `vpc-security-group-id` ist, verwendet Amazon DocumentDB die Standard-Subnetzgruppe und die Amazon VPC-Sicherheitsgruppe für die angegebene Region.

Ersetzen Sie im folgenden Beispiel jede Information durch Ihre *`user input placeholder`* eigenen Informationen.

Für Linux, macOS oder Unix:

```
aws docdb create-db-cluster \
      --global-cluster-identifier global-cluster-id \
      --source-db-cluster-identifier arn:aws:rds:us-east-1:111122223333:cluster-id
```

Für Windows:

```
aws docdb create-db-cluster ^
      --global-cluster-identifier global-cluster-id ^
      --source-db-cluster-identifier arn:aws:rds:us-east-1:111122223333:cluster-id
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus (JSON-Format).

```
{
    "DBCluster": {
        "StorageEncrypted": false,
        "DBClusterMembers": [],
        "Engine": "docdb",
        "DeletionProtection" : "enabled",
        "ClusterCreateTime": "2018-11-26T17:15:19.885Z",
        "DBSubnetGroup": "default",
        "EngineVersion": "4.0.0",
        "MasterUsername": "masteruser",
        "BackupRetentionPeriod": 1,
        "DBClusterArn": "arn:aws:rds:us-east-1:123456789012:cluster:cluster-id",
        "DBClusterIdentifier": "cluster-id",
        "MultiAZ": false,
        "DBClusterParameterGroup": "default.docdb4.0",
        "PreferredBackupWindow": "09:12-09:42",
        "DbClusterResourceId": "cluster-KQSGI4MHU4NTDDRVNLNTU7XVAY",
        "PreferredMaintenanceWindow": "tue:04:17-tue:04:47",
        "Port": 27017,
        "Status": "creating",
        "ReaderEndpoint": "cluster-id.cluster-ro-sfcrlcjcoroz.us-
east-1.docdb.amazonaws.com",
        "AssociatedRoles": [],
        "HostedZoneId": "ZNKXTT8WH85VW",
        "VpcSecurityGroups": [
            {
                "VpcSecurityGroupId": "sg-77186e0d",
                "Status": "active"
            }
        ],
        "AvailabilityZones": [
            "us-east-1a",
            "us-east-1c",
            "us-east-1e"
        ],
        "Endpoint": "cluster-id.cluster-sfcrlcjcoroz.us-east-1.docdb.amazonaws.com"
```

```
    }
}
```

Die Erstellung des Clusters dauert mehrere Minuten. Sie können das AWS-Managementkonsole oder verwenden AWS CLI , um den Status Ihres Clusters zu überwachen. Weitere Informationen finden Sie unter Den Status eines Amazon DocumentDB-Clusters überwachen.

> **Important**
>
> Wenn Sie den verwenden AWS CLI , um einen regionalen Amazon DocumentDB-Cluster zu erstellen, werden keine Instances erstellt. Daher müssen Sie explizit eine primäre Instance und alle benötigten Replikat-Instances anlegen. Sie können entweder die Konsole oder AWS CLI zum Erstellen der Instances verwenden. Weitere Informationen finden Sie unter Hinzufügen einer Amazon DocumentDB DocumentDB-Instance zu einem Cluster und createDBCluster in der Amazon DocumentDB API-Referenz.

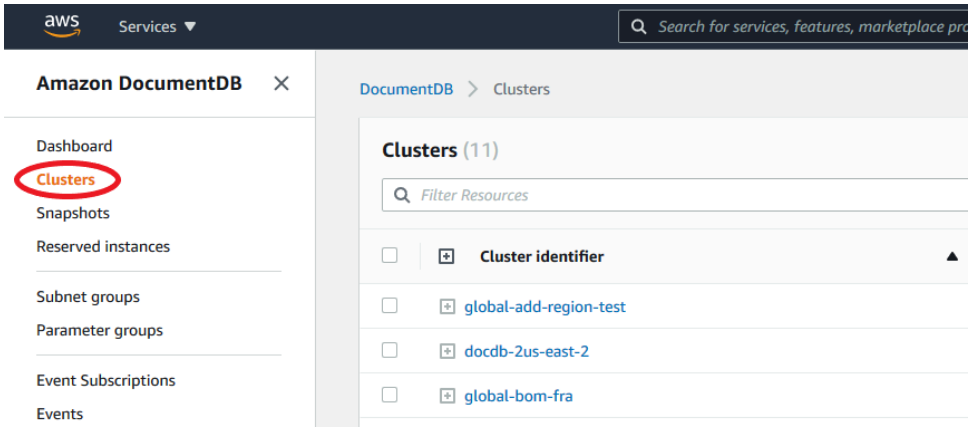
Sobald Ihr regionaler Cluster verfügbar ist, können Sie mit den folgenden Anweisungen einen sekundären Cluster in einer anderen Region hinzufügen:. Hinzufügen eines AWS-Region zu einem globalen Amazon DocumentDB-Cluster Wenn Sie eine Region hinzufügen, wird Ihr regionaler Cluster zu Ihrem primären Cluster, und Sie haben einen neuen sekundären Cluster in der von Ihnen ausgewählten Region.

Hinzufügen eines AWS-Region zu einem globalen Amazon DocumentDB-Cluster

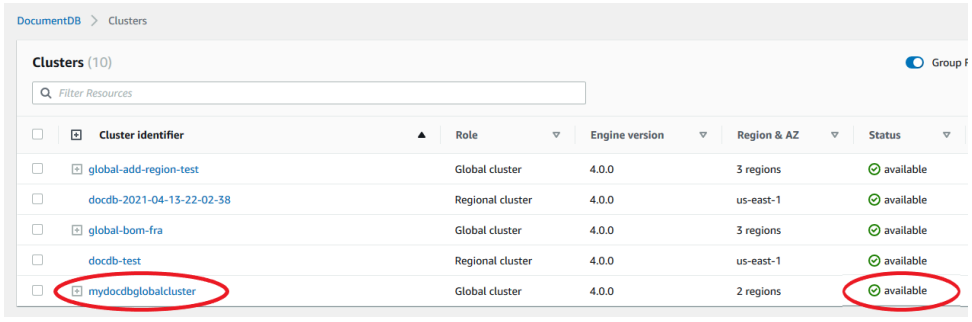
Ein globaler Cluster benötigt mindestens einen sekundären Cluster in einer anderen Region als der primäre Cluster, und Sie können bis zu 10 sekundäre Cluster hinzufügen. Beachten Sie, dass Sie für jeden sekundären Cluster, den Sie hinzufügen, die Anzahl der im primären Cluster zulässigen Replikate um eins reduzieren müssen. Wenn Ihr globaler Cluster beispielsweise 10 sekundäre Regionen hat, kann Ihr primärer Cluster nur 5 (statt 15) Replikate haben. Weitere Informationen finden Sie unter Konfigurationsanforderungen eines globalen Amazon DocumentDB-Clusters.

Verwendung der AWS-Managementkonsole

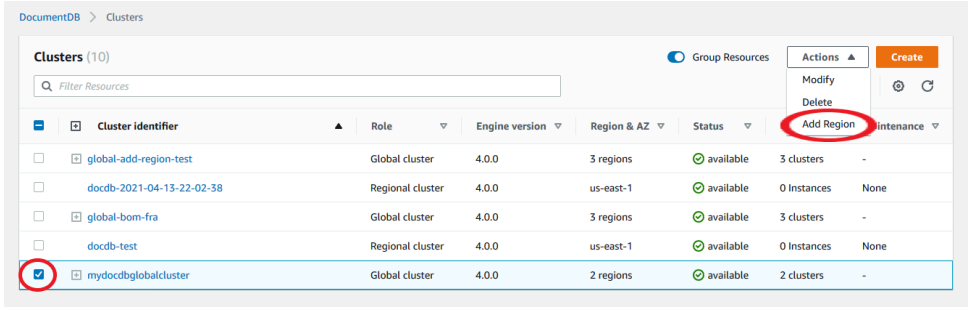
1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole.
2. Klicken Sie im Navigationsbereich auf Cluster.



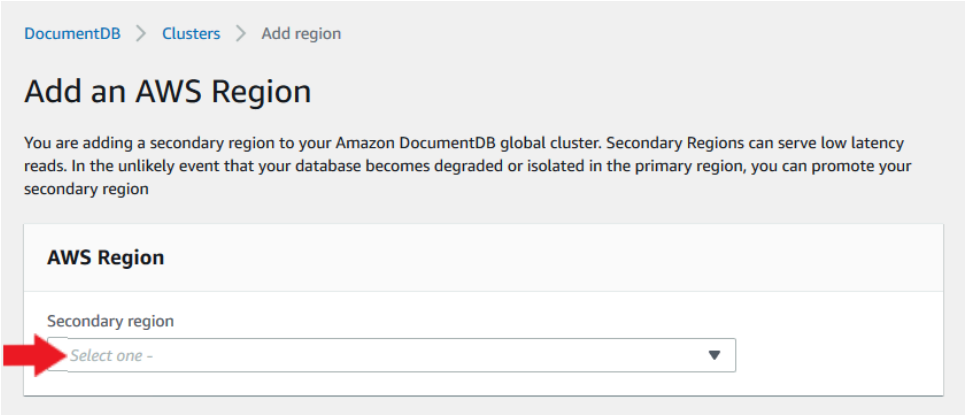
3. Wählen Sie den Cluster aus, dem Sie einen sekundären Cluster hinzufügen möchten. Stellen Sie sicher, dass der `Available` Cluster



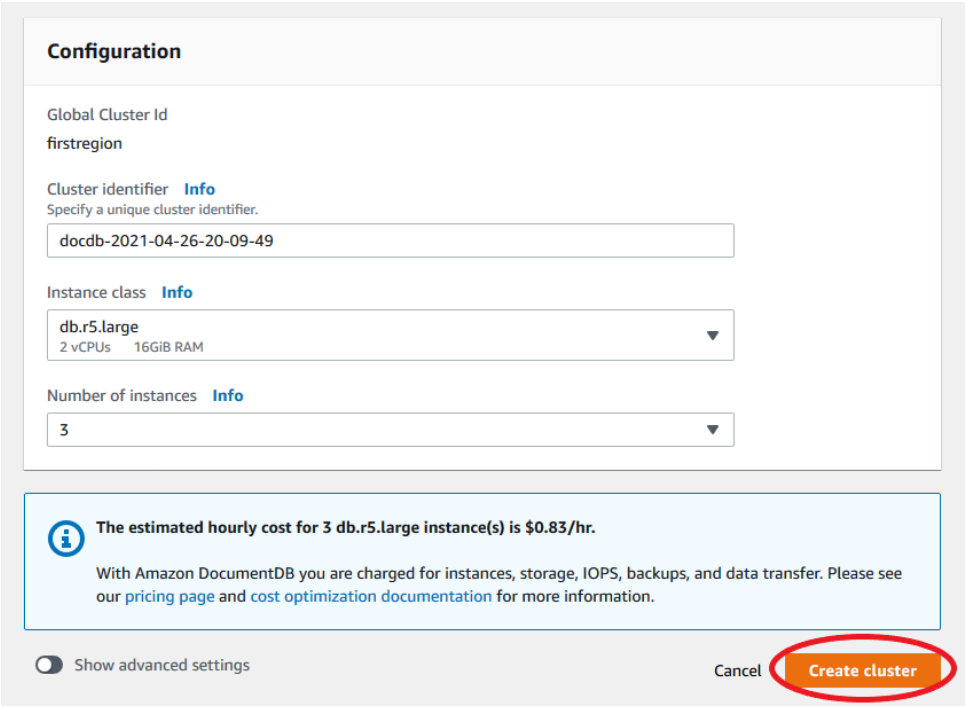
4. Wählen Sie die Dropdownliste für Aktionen aus und wählen Sie dann Region hinzufügen aus.



5. Wählen Sie auf der AWS-Region Seite Hinzufügen die sekundäre Region aus. Beachten Sie, dass Sie keine Region auswählen können, die bereits über einen sekundären Cluster für denselben globalen Cluster verfügt. Außerdem kann es sich nicht um dieselbe Region wie der primäre Cluster handeln. Wenn dies die erste Region ist, die Sie hinzufügen, müssen Sie auch eine globale Cluster-ID Ihrer Wahl angeben.



6. Füllen Sie die verbleibenden Felder für den sekundären Cluster in der neuen Region aus und wählen Sie dann Cluster erstellen aus. Nachdem Sie die Region hinzugefügt haben, können Sie sie in der Liste der Cluster in der sehen AWS-Managementkonsole.



Verwendung der AWS CLI

- Verwenden Sie den `create-db-cluster` CLI-Befehl mit dem Namen (`--global-cluster-identifier`) Ihres globalen Clusters. Für andere Parameter, führen Sie die folgenden Schritte aus:
  - Wählen Sie für `--region` eine andere Region AWS-Region als die Ihrer Hauptregion.
  - Wählen Sie bestimmte Werte für die Parameter `--engine-version` und `--engine` aus.

- Geben Sie für einen verschlüsselten Cluster Ihren primären Cluster AWS-Region als `--source-region` für die Verschlüsselung an.

Im folgenden Beispiel wird ein neuer Amazon DocumentDB-Cluster erstellt und als schreibgeschützter sekundärer Cluster an den globalen Cluster angehängt. Im letzten Schritt wird die Instance dem neuen Cluster hinzugefügt.

Ersetzen Sie im folgenden Beispiel jede *`user input placeholder`* durch Ihre eigenen Informationen.

Für Linux, macOS oder Unix:

```
aws docdb --region secondary-region-id \
  create-db-cluster \
    --db-cluster-identifier cluster-id \
    --global-cluster-identifier global-cluster-id \
    --engine-version version \
    --engine docdb

aws docdb --region secondary-region-id \
  create-db-instance \
    --db-cluster-identifier cluster-id \
    --global-cluster-identifier global-cluster-id \
    --engine-version version \
    --engine docdb
```

Für Windows:

```
aws docdb --region secondary-region-id ^
  create-db-cluster ^
    --db-cluster-identifier cluster-id ^
    --global-cluster-identifier global-cluster-id ^
    --engine-version version ^
    --engine docdb

aws docdb --region secondary-region-id ^
  create-db-instance ^
    --db-cluster-identifier cluster-id ^
    --global-cluster-identifier global-cluster-id ^
    --engine-version version ^
    --engine docdb
```

Verwenden eines Snapshots für Ihren globalen Amazon DocumentDB-Cluster

Sie können einen Snapshot eines Amazon DocumentDB-Clusters wiederherstellen, um ihn als Ausgangspunkt für Ihren globalen Cluster zu verwenden. Dazu müssen Sie den Snapshot wiederherstellen und einen neuen Cluster erstellen. Dieser wird als primärer Cluster Ihres globalen Clusters dienen. Anschließend können Sie dem wiederhergestellten Cluster eine weitere Region hinzufügen und ihn so in einen globalen Cluster konvertieren.

Verwaltung eines globalen Amazon DocumentDB-Clusters

Sie führen die meisten Verwaltungsvorgänge auf den einzelnen Clustern aus, aus denen ein globaler Cluster besteht. Wenn Sie auf der Seite Cluster in der Konsole die Option Gruppenverwandte Ressourcen auswählen, werden der primäre Cluster und die sekundären Cluster unter dem zugehörigen globalen Cluster gruppiert angezeigt.

Auf der Registerkarte Konfiguration für einen globalen Cluster werden der AWS-Regionen Ort, an dem die Cluster ausgeführt werden, die Version und die globale Cluster-ID angezeigt.

Themen

- Ändern eines globalen Amazon DocumentDB-Clusters
- Parameter eines globalen Amazon DocumentDB-Clusters ändern
- Einen Cluster aus einem globalen Amazon DocumentDB-Cluster entfernen
- Löschen eines Clusters aus einem globalen Amazon DocumentDB-Cluster
- Erstellen eines Headless-Amazon-DocumentDB-Clusters in einer sekundären Region

Ändern eines globalen Amazon DocumentDB-Clusters

Auf der Cluster-Seite AWS-Managementkonsole werden alle Ihre globalen Cluster aufgeführt, wobei der primäre Cluster und die sekundären Cluster für jeden Cluster angezeigt werden. Der globale Cluster hat seine eigenen Konfigurationseinstellungen. Insbesondere gibt es Regionen, die seinen primären und sekundären Clustern zugeordnet sind.

Wenn Sie Änderungen am globalen Cluster vornehmen, haben Sie die Möglichkeit, Änderungen rückgängig zu machen.

Wenn Sie Weiter wählen, bestätigen Sie die Änderungen.

Parameter eines globalen Amazon DocumentDB-Clusters ändern

Sie können die Cluster-Parametergruppen unabhängig für jeden Cluster innerhalb des globalen Clusters konfigurieren. Die meisten Parameter funktionieren genauso wie für andere Arten von Amazon DocumentDB-Clustern. Wir empfehlen, dass Sie die Einstellungen zwischen allen Clustern in einer globalen Datenbank konsistent halten. Dies hilft, unerwartete Verhaltensänderungen zu vermeiden, wenn Sie einen sekundären Cluster zum primären Cluster hochstufen.

Sie sollten z. B. die gleichen Einstellungen für Zeitzonen und Zeichensätze verwenden, um inkonsistentes Verhalten zu vermeiden, wenn ein anderer Cluster die Rolle des primären Clusters übernimmt.

Einen Cluster aus einem globalen Amazon DocumentDB-Cluster entfernen

Es gibt mehrere Situationen, in denen Sie möglicherweise Cluster aus Ihrem globalen Cluster entfernen möchten. Beispielsweise möchten Sie möglicherweise einen Cluster aus einem globalen Cluster entfernen, wenn der primäre Cluster heruntergestuft oder isoliert wird. Er wird dann zu einem eigenständigen bereitgestellten Cluster, der zur Erstellung eines neuen globalen Clusters verwendet werden kann. Weitere Informationen hierzu finden Sie unter Durchführen eines manuellen Failovers für einen globalen Amazon DocumentDB-Cluster.

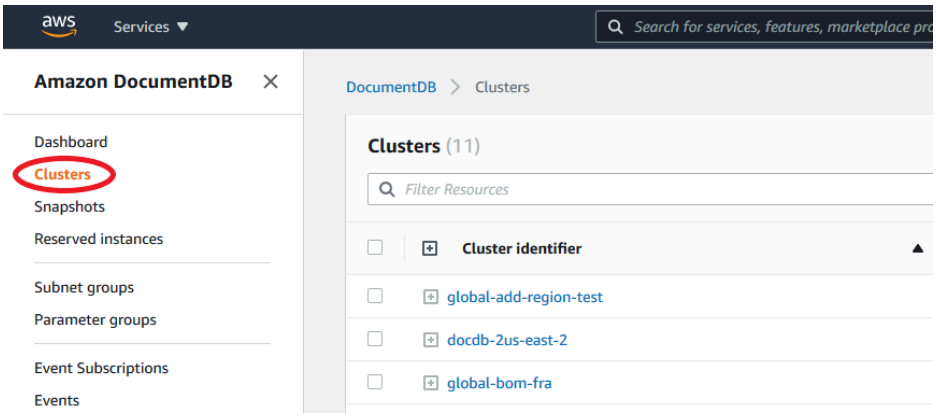
Möglicherweise möchten Sie auch Cluster entfernen, weil Sie einen globalen Cluster löschen möchten, den Sie nicht mehr benötigen. Sie können den globalen Cluster erst löschen, nachdem Sie alle zugehörigen Cluster getrennt haben und den primären Cluster als letzten übrig lassen. Weitere Informationen finden Sie unter Löschen eines Clusters aus einem globalen Amazon DocumentDB-Cluster.

> **Note**
>
> Wenn ein Cluster vom globalen Cluster getrennt wird, wird er nicht mehr mit dem primären Cluster synchronisiert. Er wird zu einem eigenständigen bereitgestellten Cluster mit vollem read/write Funktionsumfang. Außerdem ist es in der Amazon DocumentDB DocumentDB-Konsole nicht mehr sichtbar. Es ist nur sichtbar, wenn Sie die Region in der Konsole auswählen, in der sich der Cluster befand.

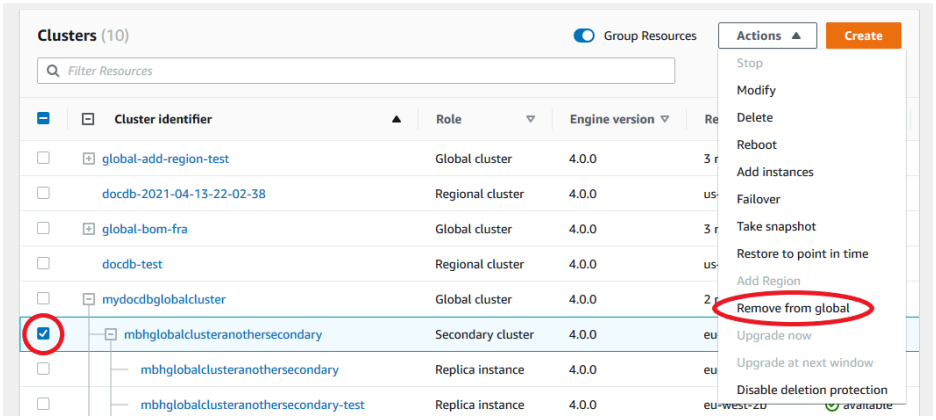
Sie können Cluster mithilfe der AWS-Managementkonsole, der oder der RDS-API aus Ihrem globalen Cluster entfernen. AWS CLI

Using the AWS-Managementkonsole

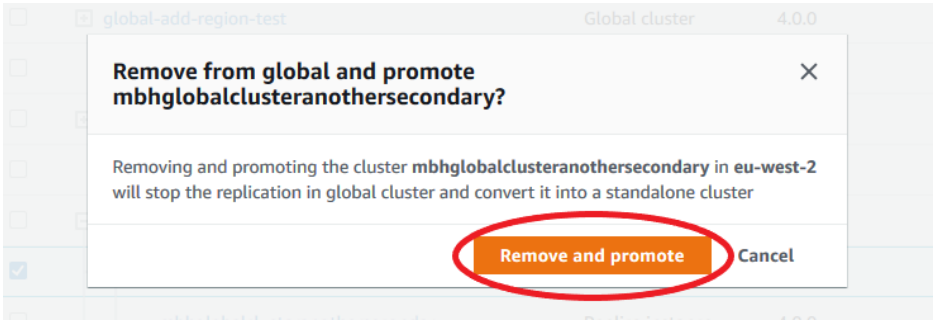
1. Melden Sie sich bei der an AWS-Managementkonsole und navigieren Sie zur Amazon DocumentDB DocumentDB-Konsole.
2. Wählen Sie in der linken Navigationsleiste Clusters aus.



3. Erweitern Sie den globalen Cluster, sodass Sie alle sekundären Cluster sehen können. Wählen Sie die sekundären Cluster aus, die Sie entfernen möchten. Wählen Sie Aktionen und wählen Sie im Dropdownmenü die Option Aus Global entfernen aus.



4. Es wird eine Aufforderung angezeigt, in der Sie aufgefordert werden, zu bestätigen, dass Sie den sekundären Cluster vom globalen Cluster trennen möchten. Wählen Sie Entfernen und heraufstufen, um den Cluster aus dem globalen Cluster zu entfernen.



Jetzt dient dieser Cluster nicht mehr als sekundärer Cluster und ist nicht mehr mit dem primären Cluster synchronisiert. Es handelt sich um einen eigenständigen Cluster mit voller read/write Kapazität.

Nachdem Sie alle sekundären Cluster entfernt oder gelöscht haben, können Sie den primären Cluster auf die gleiche Weise entfernen. Sie können den primären Cluster erst vom globalen Cluster trennen oder entfernen, nachdem Sie alle sekundären Cluster entfernt haben. Der globale Cluster verbleibt möglicherweise in der Clusterliste mit null Regionen und AZs. Sie können diesen globalen Cluster löschen, wenn Sie ihn nicht mehr verwenden möchten.

Using the AWS CLI

Um einen Cluster aus einem globalen Cluster zu entfernen, führen Sie den `remove-from-global-cluster` CLI-Befehl mit den folgenden Parametern aus:

- `--global-cluster-identifier`— Der Name (Bezeichner) Ihres globalen Clusters.
- `--db-cluster-identifier`— Der Name jedes Clusters, der aus dem globalen Cluster entfernt werden soll.

In den folgenden Beispielen wird zuerst ein sekundärer Cluster und dann der primäre Cluster aus einem globalen Cluster entfernt.

Für Linux, macOS oder Unix:

```
aws docdb --region secondary_region \
  remove-from-global-cluster \
    --db-cluster-identifier secondary_cluster_ARN \
    --global-cluster-identifier global_cluster_id

aws docdb --region primary_region \
  remove-from-global-cluster \
    --db-cluster-identifier primary_cluster_ARN \
    --global-cluster-identifier global_cluster_id
```

Wiederholen Sie den `remove-from-global-cluster --db-cluster-identifier secondary_cluster_ARN` Befehl für jede sekundäre Region in Ihrem globalen Cluster.

Für Windows:

```
aws docdb --region secondary_region ^
```

```
  remove-from-global-cluster ^
    --db-cluster-identifier secondary_cluster_ARN ^
    --global-cluster-identifier global_cluster_id

aws docdb --region primary_region ^
  remove-from-global-cluster ^
    --db-cluster-identifier primary_cluster_ARN ^
    --global-cluster-identifier global_cluster_id
```

Wiederholen Sie den `remove-from-global-cluster --db-cluster-identifier secondary_cluster_ARN` Befehl für jede sekundäre Region in Ihrem globalen Cluster.

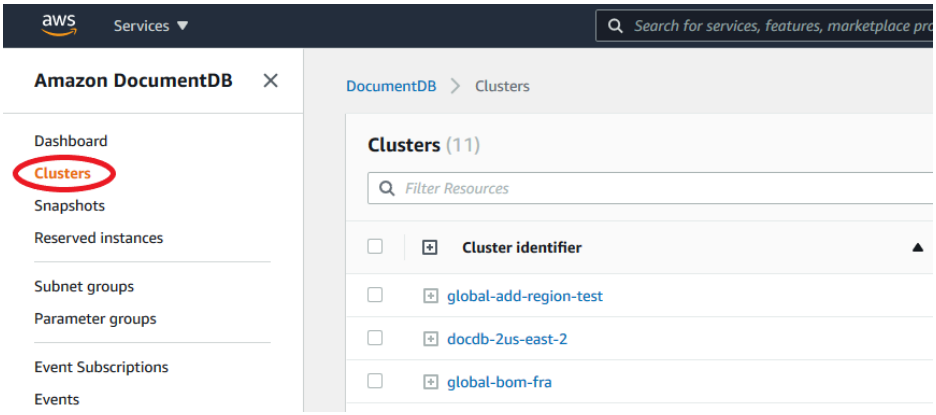
Löschen eines Clusters aus einem globalen Amazon DocumentDB-Cluster

Gehen Sie wie folgt vor, um einen globalen Cluster zu löschen:

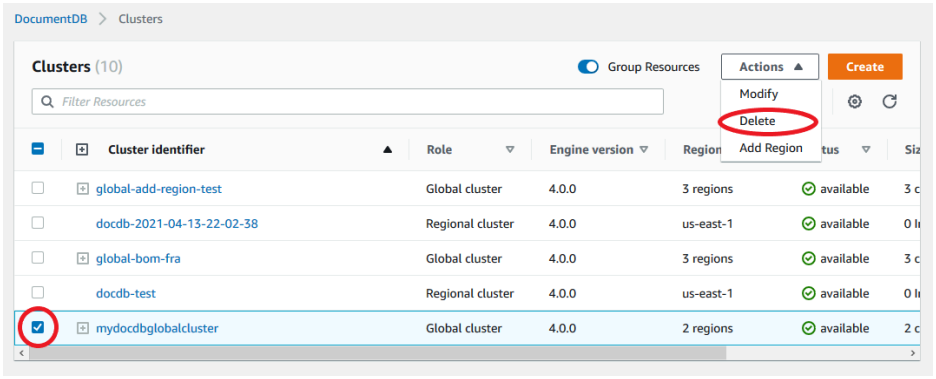
- Entfernen Sie alle sekundären Cluster aus dem globalen Cluster. Jeder Cluster wird zu einem eigenständigen Cluster. Siehe den vorherigen Abschnitt,Einen Cluster aus einem globalen Amazon DocumentDB-Cluster entfernen.
- Löschen Sie aus jedem eigenständigen Cluster alle Replikate.
- Entfernen Sie den primären Cluster aus dem globalen Cluster. Dies wird zu einem eigenständigen Cluster.
- Löschen Sie aus dem primären Cluster zuerst alle Replikate und dann die primäre Instanz. Wenn Sie die primäre Instanz aus dem neuen eigenständigen Cluster löschen, werden in der Regel auch der Cluster und der globale Cluster entfernt.

Using the AWS-Managementkonsole

1. Melden Sie sich bei der an AWS-Managementkonsole und navigieren Sie zur Amazon DocumentDB DocumentDB-Konsole.
2. Wählen Sie Clusters und suchen Sie den globalen Cluster, den Sie löschen möchten.



3. Wählen Sie Ihren globalen Cluster aus und wählen Sie im Menü Aktionen die Option Löschen aus.



Vergewissern Sie sich, dass alle Cluster aus dem globalen Cluster entfernt wurden. Der globale Cluster sollte keine Regionen und AZs und eine Größe von Null Clustern aufweisen. Wenn der globale Cluster Cluster enthält, können Sie ihn noch nicht löschen. Sie müssen zunächst den Anweisungen im vorherigen Schritt folgen, Einen Cluster aus einem globalen Amazon DocumentDB-Cluster entfernen.

Using the AWS CLI

Um einen globalen Cluster zu löschen, führen Sie den `delete-global-cluster` CLI-Befehl mit dem Namen des AWS-Region und der globalen Cluster-ID aus, wie im folgenden Beispiel gezeigt.

Für Linux, macOS oder Unix:

```
aws docdb --region primary_region delete-global-cluster \
   --global-cluster-identifier global_cluster_id
```

Für Windows:

```
aws docdb --region primary_region delete-global-cluster ^
   --global-cluster-identifier global_cluster_id
```

Erstellen eines Headless-Amazon-DocumentDB-Clusters in einer sekundären Region

Obwohl ein globaler Amazon DocumentDB-Cluster mindestens einen sekundären Cluster in einem anderen AWS-Region als dem primären Cluster benötigt, können Sie für den sekundären Cluster eine Headless-Konfiguration verwenden. Ein kopfloser sekundärer Amazon DocumentDB-Cluster ist ein Cluster ohne Instance. Diese Art der Konfiguration kann die Kosten für einen globalen Cluster senken. In einem Amazon DocumentDB-Cluster sind Rechenleistung und Speicher entkoppelt. Ohne die Instance werden Ihnen keine Rechenleistung, sondern nur Speicherplatz in Rechnung gestellt. Wenn es korrekt eingerichtet ist, wird das Speichervolumen eines sekundären Headless-Clusters mit dem des primären Clusters synchronisiert.

Sie fügen den sekundären Cluster wie gewohnt hinzu, wenn Sie einen globalen Amazon DocumentDB-Cluster erstellen. Nachdem der primäre Cluster jedoch mit der Replikation auf den sekundären Cluster begonnen hat, löschen Sie die schreibgeschützte Instance aus dem sekundären Cluster. Dieser sekundäre Cluster gilt nun als „kopflos“, da er keine Instanz mehr hat. Das Speichervolumen wird jedoch mit dem primären Amazon DocumentDB-Cluster synchronisiert.

> **Important**
>
> Wir empfehlen Headless-Cluster nur für Kunden, die regionsweite Ausfälle für mehr als 15 Minuten tolerieren können. Dies liegt daran, dass der Benutzer bei der Wiederherstellung nach einem regionsweiten Ausfall mit einem sekundären Headless-Cluster nach einem Failover eine neue Instanz erstellen muss. Es kann ~10-15 Minuten dauern, bis eine neue Instanz verfügbar ist.

So fügen Sie Ihrem globalen Cluster einen sekundären Headless-Cluster hinzu

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole.
2. Wählen Sie in der linken Navigationsleiste Clusters aus.
3. Wählen Sie den globalen Cluster aus, der einen sekundären Cluster benötigt. Stellen Sie sicher, dass der primäre `Available` Cluster
4. Wählen Sie unter Actions (Aktionen) die Option Add region (Region hinzufügen) aus.

5. Wählen Sie auf der Seite Region hinzufügen die sekundäre Region aus.

   > **Note**
   >
   > Sie können keine Region auswählen, die bereits über einen sekundären Cluster für denselben globalen Cluster verfügt. Außerdem kann es sich nicht um dieselbe Region wie der primäre Cluster handeln.

6. Füllen Sie die verbleibenden Felder für den sekundären Cluster in der neuen Region aus. Dies sind dieselben Konfigurationsoptionen wie für jede Clusterinstanz.
7. Fügen Sie eine Region hinzu. Nachdem Sie die Region zu Ihrem globalen Cluster hinzugefügt haben, wird sie in der Liste von `Clusters` angezeigt AWS-Managementkonsole.
8. Überprüfen Sie den Status des sekundären Clusters und seiner Reader-Instance, bevor Sie fortfahren, indem Sie den Befehl AWS-Managementkonsole oder den verwenden AWS CLI. Hier ist ein Beispielbefehl, wenn Sie den folgenden Befehl verwenden AWS CLI:

   ```
   $ aws docdb describe-db-clusters --db-cluster-identifier secondary-cluster-id --
   query '*[].[Status]' --output text
   ```

   Es kann mehrere Minuten dauern, bis der Status eines neu hinzugefügten sekundären Clusters von „Wird erstellt“ auf „Verfügbar“ geändert wird. Wenn der Cluster verfügbar ist, können Sie die Reader-Instanz löschen.
9. Wählen Sie die Reader-Instanz im sekundären Cluster aus und klicken Sie dann auf Löschen.
10. Nach dem Löschen der Reader-Instanz bleibt der sekundäre Cluster Teil des globalen Clusters. Ihm sollte keine Instanz zugeordnet sein.

> **Note**
>
> Sie können diesen kopflosen sekundären Amazon DocumentDB-Cluster verwenden, um Ihren globalen Amazon DocumentDB-Cluster manuell nach einem ungeplanten Ausfall in der primären Region wiederherzustellen, falls ein solcher Ausfall auftritt.

Stellen Sie eine Connect zu einem globalen Amazon DocumentDB-Cluster her

Wie Sie eine Verbindung zu einem globalen Cluster herstellen, hängt davon ab, ob Sie in den Cluster schreiben oder aus dem Cluster lesen müssen:

- Für schreibgeschützte Anfragen oder Abfragen stellen Sie eine Verbindung zum Reader-Endpunkt für den Cluster in Ihrem her. AWS-Region
- Stellen Sie zum Ausführen von Data Manipulation Language (DML)- und Data Definition Language (DDL)-Anweisungen eine Verbindung zum Cluster-Endpunkt des primären Clusters her. Dieser Endpunkt befindet sich möglicherweise in einer anderen Anwendung AWS-Region als Ihrer Anwendung.

Wenn Sie sich einen globalen Cluster in der Konsole ansehen, können Sie alle Allzweck-Endpunkte sehen, die mit all seinen Clustern verknüpft sind.

Wie Sie eine Verbindung zu einem globalen Cluster herstellen, hängt davon ab, ob Sie in die Datenbank schreiben oder aus der Datenbank lesen müssen. Für DDL-, DML- und Lesevorgänge, die Sie von der primären Region aus ausführen möchten, sollten Sie eine Verbindung zu Ihrem primären Cluster herstellen. Wir empfehlen, dass Sie eine Verbindung zu Ihrem primären Cluster herstellen, indem Sie den Cluster-Endpunkt im Replikatsatzmodus verwenden, mit der Lesepräferenz von. `secondaryPreferred=true` Dadurch wird der Schreibdatenverkehr an die Writer-Instance Ihres primären Clusters und der Lesetraffic an die Replikat-Instance Ihres primären Clusters weitergeleitet.

Für regionsübergreifenden, schreibgeschützten Datenverkehr sollten Sie eine Verbindung zu einem Ihrer sekundären Cluster herstellen. Wir empfehlen, dass Sie über den Cluster-Endpunkt im Replikatsatzmodus eine Verbindung zu Ihrem sekundären Cluster herstellen. Da es sich bei allen Instanzen um schreibgeschützte Replikatinstanzen handelt, sollten Sie eine andere Lesepräferenz als `primary` (z. B.`secondary`, `secondaryPreferred` oder) angeben. `nearest` Um die Latenz zu minimieren, wählen Sie den Reader-Endpunkt aus, der sich in Ihrer Region oder in der Region befindet, die Ihnen am nächsten ist.

Überwachung globaler Amazon DocumentDB-Cluster

Amazon DocumentDB (mit MongoDB-Kompatibilität) lässt sich integrieren, CloudWatch sodass Sie Betriebsmetriken für Ihre Cluster sammeln und analysieren können. Sie können diese Metriken mit

der CloudWatch Konsole, der Amazon DocumentDB DocumentDB-Konsole, der AWS Command Line Interface (AWS CLI) oder der CloudWatch API überwachen.

Verwenden Sie die folgenden CloudWatch Metriken, um einen globalen Cluster zu überwachen.

Metrik	Description
`GlobalClusterReplicatedWriteIO`	Die durchschnittliche Anzahl der fakturierten I/O Schreibvorgänge, die vom Cluster-Volume im primären AWS-Region auf das Cluster-Volume in einem sekundären Cluster-Volume replizier t wurden AWS-Region, wird in Intervallen von 5 Minuten gemeldet. Die Anzahl der Replikati onen in `ReplicatedWriteIOs` jede sekundäre Region entspricht der Anzahl der in der Region `VolumeWriteIOPs` durchgefü hrten Replikationen in der primären Region.
`GlobalClusterDataTransferBytes`	Die Datenmenge, die vom primären Cluster AWS-Region zu dem eines sekundären Clusters übertragen wird AWS-Region, gemessen in Byte.
`GlobalClusterReplicationLag`	Das Ausmaß der Verzögerung in Millisekunden bei der Replikation von Änderungsereignissen vom primären Cluster auf das eines sekundäre n Clusters AWS-Region AWS-Region

Weitere Informationen zum Anzeigen dieser Metriken finden Sie unter Daten anzeigen. CloudWatch

Disaster Recovery und globale Amazon DocumentDB-Cluster

Topics

- Durchführen eines verwalteten Failovers für einen globalen Amazon DocumentDB-Cluster
- Durchführen eines manuellen Failovers für einen globalen Amazon DocumentDB-Cluster
- Durchführen eines Switchovers für einen globalen Amazon DocumentDB-Cluster
- Entsperren eines globalen Cluster-Switchovers oder -Failovers

Durch die Verwendung eines globalen Clusters können Sie nach Katastrophen wie regionalen Ausfällen schnell Daten wiederherstellen. Die Wiederherstellung nach einem Notfall wird in der Regel anhand von RTO- und RPO-Werten gemessen.

- Recovery Time Objective (RTO) – Die Zeit, die ein System benötigt, um nach einem Notfall in einen arbeitsfähigen Zustand zurückzukehren. Mit anderen Worten: RTO misst die Ausfallzeit. Für einen globalen Cluster: RTO innerhalb von Minuten.
- Recovery Point Objective (RPO) – Die Datenmenge, die verloren gehen kann (gemessen in Zeit). Für einen globalen Cluster wird RPO in der Regel in Sekunden gemessen.
- Zur Wiederherstellung nach einem ungeplanten Ausfall können Sie ein regionsübergreifendes Failover zu einem der sekundären Cluster in Ihrem globalen Cluster durchführen. Wenn Ihr globaler Cluster über mehrere sekundäre Regionen verfügt, stellen Sie sicher, dass Sie alle sekundären Regionen, die Sie als primäre Regionen heraufstufen möchten, abtrennen. Anschließend stufen Sie eine dieser sekundären Regionen zur neuen Hauptregion herauf. AWS-Region Schließlich erstellen Sie in jeder der anderen sekundären Regionen neue Cluster und fügen diese Cluster Ihrem globalen Cluster hinzu.

Durchführen eines verwalteten Failovers für einen globalen Amazon DocumentDB-Cluster

Dieser Ansatz dient der Geschäftskontinuität im Falle einer echten regionalen Katastrophe oder eines kompletten Service-Level-Ausfalls.

Während eines verwalteten Failovers wird Ihr primärer Cluster auf die sekundäre Region Ihrer Wahl umgestellt, während die bestehende Replikationstopologie Ihres globalen Amazon DocumentDB-Clusters beibehalten wird. Der gewählte sekundäre Cluster stuft einen seiner schreibgeschützten Knoten auf vollen Writer-Status herauf. In diesem Schritt kann der Cluster die Rolle des primären Clusters übernehmen. Ihre Datenbank ist für kurze Zeit nicht verfügbar, während dieser Cluster seine neue Rolle annimmt. Daten, die nicht vom alten primären auf den ausgewählten sekundären Cluster repliziert wurden, fehlen möglicherweise, wenn dieser sekundäre zum neuen primären Cluster wird. Das alte primäre Volume versucht nach besten Kräften, vor der Synchronisierung mit dem neuen primären Volume einen Snapshot zu erstellen, sodass nicht replizierte Daten auf dem Snapshot erhalten bleiben.

> **Note**
>
> Sie können ein verwaltetes regionsübergreifendes Cluster-Failover auf einem globalen Amazon DocumentDB-Cluster nur durchführen, wenn der primäre und alle sekundären Cluster dieselben Engine-Versionen haben. Wenn Ihre Engine-Versionen nicht kompatibel sind, können Sie das Failover manuell durchführen, indem Sie die Schritte unter Durchführen eines manuellen Failovers für einen globalen Amazon DocumentDB-Cluster ausführen. Wenn die Engine-Versionen der Region nicht übereinstimmen, wird der Failover blockiert. Suchen Sie nach ausstehenden Upgrades und wenden Sie sie an, um sicherzustellen, dass die Engine-Versionen aller Regionen übereinstimmen und der globale Cluster-Failover entsperrt ist. Weitere Informationen finden Sie unter Entsperren eines globalen Cluster-Switchovers oder -Failovers.

Um Datenverlust zu minimieren, empfehlen wir Ihnen, vor der Verwendung dieser Funktion Folgendes zu tun:

- Schalten Sie Anwendungen offline, um zu verhindern, dass Schreibvorgänge an den primären Cluster des globalen Amazon DocumentDB-Clusters gesendet werden.
- Überprüfen Sie die Verzögerungszeiten für alle sekundären Amazon DocumentDB-Cluster. Durch die Auswahl der sekundären Region mit der geringsten Replikationsverzögerung kann der Datenverlust in der aktuell ausgefallenen primären Region minimiert werden. Überprüfen Sie die Verzögerungszeiten für alle sekundären Amazon DocumentDB-Cluster im globalen Cluster, indem Sie sich die `GlobalClusterReplicationLag` Metrik in Amazon CloudWatch ansehen. Diese Metriken zeigen Ihnen, wie weit (in Millisekunden) die Replikation auf einen sekundären Cluster auf den primären Cluster zurückliegt.

  Weitere Informationen zu CloudWatch Metriken für Amazon DocumentDB finden Sie unterAmazon DocumentDB-Metriken.

Während eines verwalteten Failovers wird dem ausgewählten sekundären Cluster seine neue Rolle als primärer Cluster zugewiesen. Er erbt jedoch nicht die verschiedenen Konfigurationsoptionen des primären Clusters. Wenn die Konfiguration nicht übereinstimmt, kann dies Leistungsprobleme, Workload-Inkompatibilitäten und anderes anomales Verhalten zur Folge haben. Um solche Probleme zu vermeiden, empfehlen wir Ihnen, die Unterschiede zwischen Ihren globalen Amazon DocumentDB-Clustern für Folgendes zu beheben:

- Konfigurieren Sie bei Bedarf eine Amazon DocumentDB-Cluster-Parametergruppe für den neuen Primärserver — Sie können Ihre Amazon DocumentDB-Cluster-Parametergruppen unabhängig für jeden Cluster in Ihrem globalen Amazon DocumentDB-Cluster konfigurieren. Wenn Sie also einen sekundären Cluster zur Übernahme der primären Rolle heraufstufen, wird die Parametergruppe aus dem sekundären Cluster möglicherweise anders konfiguriert als für den primären. Wenn ja, ändern Sie die Parametergruppe des hochgestuften sekundären Clusters so, dass sie den Einstellungen Ihres primären Clusters entspricht. Um zu erfahren wie dies geht, vgl. Amazon DocumentDB-Cluster-Parametergruppen ändern.
- Überwachungstools und -optionen wie CloudWatch Amazon-Ereignisse und -Alarme konfigurieren — Konfigurieren Sie den beworbenen Cluster mit denselben Protokollierungsfunktionen, Alarmen usw., wie es für den globalen Cluster erforderlich ist. Wie bei Parametergruppen wird die Konfiguration für diese Funktionen während des Failover-Prozesses nicht vom primären Cluster übernommen. Einige CloudWatch Metriken, wie z. B. die Verzögerung bei der Replikation, sind nur für sekundäre Regionen verfügbar. Daher ändert ein Failover die Art und Weise, wie diese Metriken angezeigt und Alarme für sie eingerichtet werden, und es können Änderungen an allen vordefinierten Dashboards erforderlich sein. Weitere Informationen zu Amazon DocumentDB-Clustern und deren Überwachung finden Sie unterAmazon DocumentDB überwachen.

In der Regel übernimmt der gewählte sekundäre Cluster innerhalb einer Minute die primäre Rolle. Sobald der Writer-Knoten der neuen primären Region verfügbar ist, können Sie Ihre Anwendungen mit diesem verbinden und Ihre Workloads fortsetzen. Nachdem Amazon DocumentDB den neuen primären Cluster hochgestuft hat, erstellt es automatisch alle zusätzlichen sekundären Regionscluster neu.

Da globale Amazon DocumentDB-Cluster asynchrone Replikation verwenden, kann die Replikationsverzögerung in jeder sekundären Region variieren. Amazon DocumentDB erstellt diese sekundären Regionen neu, sodass sie genau dieselben Point-in-Time-Daten wie der neue primäre Region-Cluster haben. Die Dauer der vollständigen Neuerstellungsaufgabe kann je nach Größe des Speichervolumens und der Entfernung zwischen den Regionen einige Minuten bis mehrere Stunden dauern. Wenn der Wiederaufbau der Cluster der sekundären Region aus der neuen primären Region abgeschlossen ist, stehen sie für den Lesezugriff zur Verfügung. Sobald der neue primäre Writer beworben und verfügbar ist, kann der Cluster der neuen primären Region Lese- und Schreibvorgänge für den globalen Amazon DocumentDB-Cluster abwickeln.

Um die ursprüngliche Topologie des globalen Clusters wiederherzustellen, überwacht Amazon DocumentDB die Verfügbarkeit der alten primären Region. Sobald diese Region fehlerfrei und wieder verfügbar ist, fügt Amazon DocumentDB sie automatisch wieder als sekundäre Region zum globalen

Cluster hinzu. Bevor das neue Speichervolume in der alten primären Region erstellt wird, versucht Amazon DocumentDB, zum Zeitpunkt des Fehlers einen Snapshot des alten Speichervolumes zu erstellen. Auf diese Weise können Sie alle fehlenden Daten wiederherstellen. Wenn dieser Vorgang erfolgreich ist, platziert Amazon DocumentDB diesen Snapshot mit dem Namen „rds:docdb-unplanned-global-failover-name-of-old-primary-“ im Snapshot-Abschnitt von. DB-cluster-timestamp AWS-Managementkonsole Sie können diesen Snapshot auch in `DescribeDBClusterSnapshots` den Informationen sehen, die von der API-Operation zurückgegeben werden.

> **Note**
>
> Der Snapshot des alten Speichervolumes ist ein System-Snapshot, der der auf dem alten primären Cluster konfigurierten Aufbewahrungsfrist für Backups unterliegt. Um diesen Snapshot außerhalb des Aufbewahrungszeitraums zu speichern, können Sie ihn kopieren, um ihn als manuellen Snapshot zu speichern. Weitere Informationen zum Kopieren von Snapshots, einschließlich der Preise, finden Sie unter Einen Cluster-Snapshot kopieren.

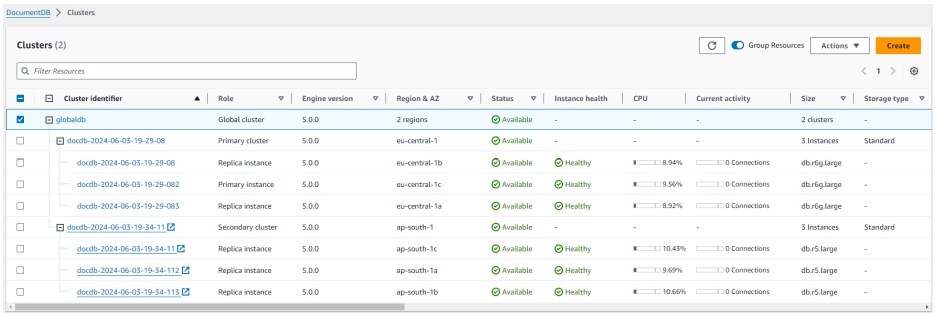
Nachdem die ursprüngliche Topologie wiederhergestellt ist, können Sie Ihr globales Cluster auf die ursprüngliche primäre Region zurückführen, indem Sie einen Switchover-Vorgang durchführen, wenn dies für Ihr Unternehmen und Ihre Arbeitslast am sinnvollsten ist. Eine Schritt-für-Schritt-Anleitung hierzu finden Sie unter Durchführen eines Switchovers für einen globalen Amazon DocumentDB-Cluster.

Sie können ein Failover Ihres globalen Amazon DocumentDB-Clusters mithilfe der AWS-Managementkonsole, der oder der Amazon DocumentDB DocumentDB-API durchführen. AWS CLI

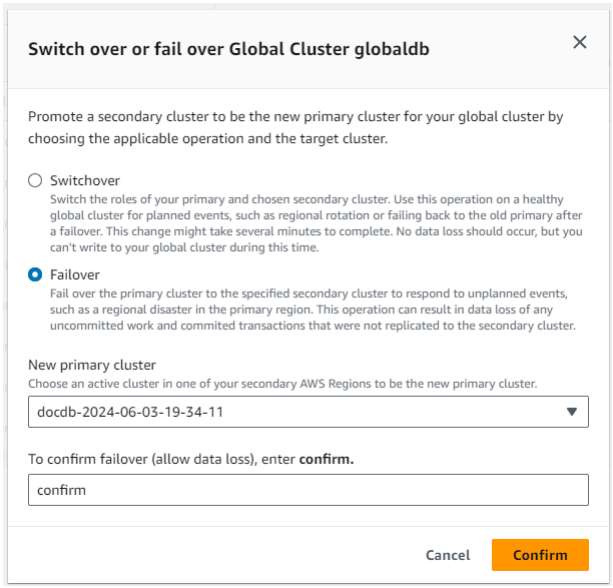
Using the AWS-Managementkonsole

Führen Sie ein verwaltetes Failover auf Ihrem globalen Amazon DocumentDB-Cluster durch

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Klicken Sie im Navigationsbereich auf Cluster.
3. Suchen Sie den globalen Amazon DocumentDB-Cluster, für den Sie ein Failover durchführen möchten, und wählen Sie ihn aus.

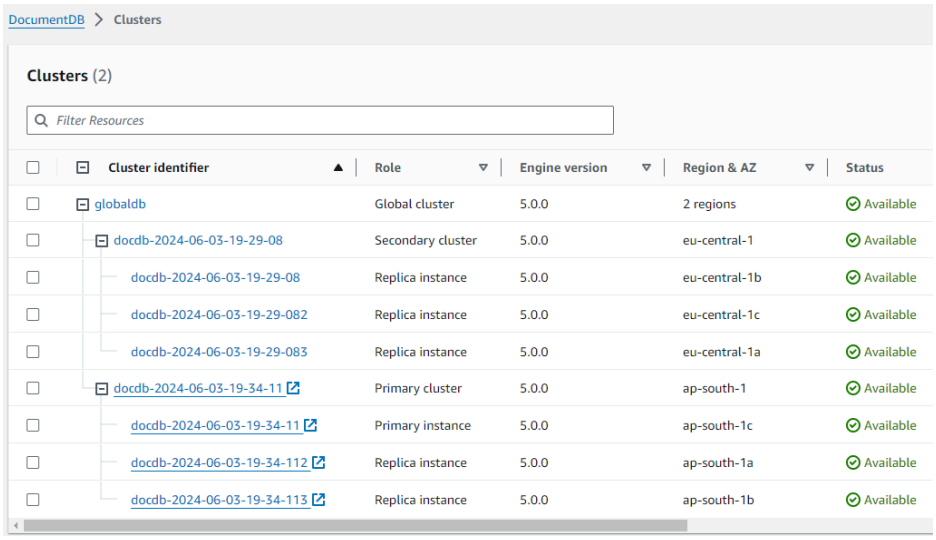


4. Wählen Sie im Aktionsmenü Switchover oder Failover aus.
5. Wählen Sie im daraufhin angezeigten Dialogfeld Failover und dann den sekundären Cluster aus der Dropdownliste Neues primäres Clusterfeld aus.



6. Geben Sie „Bestätigen“ in das letzte Feld ein. Wählen Sie dann Confirm (Bestätigen) aus.

   Der Status des primären Clusters ändert sich in "Failing-over“. Dieser Zustand sollte ungefähr eine Minute dauern. Während dieser Zeit zeigt der Status des neuen primären Clusters "Wird geändert... “. Sobald der neue Primärserver hochgestuft wurde, wird dort "Verfügbar" angezeigt und er kann Lese- und Schreibtransaktionen ausführen. In den sekundären Regionen, einschließlich der alten Primärregion, wird "Resyncing... angezeigt ", während es mit dem neuen primären System erneut synchronisiert wird. Ähnlich wie bei der neuen primären Version kann die Transaktion erst ausgeführt werden, wenn sich der Status auf "Verfügbar" ändert.
7. Wenn der Vorgang abgeschlossen ist, wird der ursprüngliche primäre Cluster zum sekundären Cluster. Der ausgewählte sekundäre Cluster wird zum primären Cluster.



Using the AWS CLI

Führen Sie ein verwaltetes Failover auf Ihrem globalen Amazon DocumentDB-Cluster durch

Führen Sie den `failover-global-cluster`CLI-Befehl aus, um ein Failover für Ihren globalen Amazon DocumentDB-Cluster durchzuführen. Übergeben Sie mit dem Befehl Werte für die folgenden Optionen:

- `--region`
- `--global-cluster-identifier`
- `--target-db-cluster-identifier`
- `--allow-data-loss`

Ersetzen Sie in den folgenden Beispielen jedes *`user input placeholder`* durch die Informationen Ihres Clusters.

Für Linux, macOS oder Unix:

```
aws docdb failover-global-cluster \
   --region region_of_selected_secondary \
   --global-cluster-identifier global_cluster_id \
   --target-db-cluster-identifier arn_of_secondary_to_promote \
   --allow-data-loss
```

Für Windows:

```
aws docdb failover-global-cluster ^
   --region region_of_selected_secondary ^
   --global-cluster-identifier global_cluster_id ^
   --target-db-cluster-identifier arn_of_secondary_to_promote ^
   --allow-data-loss
```

Durchführen eines manuellen Failovers für einen globalen Amazon DocumentDB-Cluster

Wenn ein ganzer Cluster in einem Cluster nicht AWS-Region mehr verfügbar ist, können Sie einen anderen Cluster im globalen Cluster so heraufstufen, dass er über read/write Kapazitäten verfügt.

Sie können den globalen Cluster-Failover-Mechanismus manuell aktivieren, wenn ein Cluster in einem anderen Cluster die bessere Wahl als primärer Cluster AWS-Region ist. Sie können beispielsweise die Kapazität eines sekundären Clusters erhöhen und diesen Cluster dann zum primären Cluster hochstufen. Oder das Gleichgewicht zwischen den Aktivitäten AWS-Regionen könnte sich ändern, sodass ein Wechsel des primären Clusters zu einem anderen zu einer geringeren Latenz bei Schreibvorgängen führen AWS-Region kann.

Das folgende Verfahren beschreibt, wie Sie einen der sekundären Cluster in einem globalen Amazon DocumentDB-Cluster bewerben können.

Um einen sekundären Cluster heraufzustufen:

1. Beenden Sie die Ausgabe von DML-Anweisungen und anderen Schreibvorgängen an den primären Cluster während des AWS-Region Ausfalls.
2. Identifizieren Sie einen Cluster aus einem sekundären Cluster AWS-Region , der als neuer primärer Cluster verwendet werden soll. Wenn Sie zwei (oder mehr) sekundäre Cluster AWS-Regionen in Ihrem globalen Cluster haben, wählen Sie den sekundären Cluster mit der geringsten Verzögerungszeit aus.
3. Trennen Sie den ausgewählten sekundären Cluster vom globalen Cluster.

   Wenn Sie einen sekundären Cluster aus einem globalen Cluster entfernen, wird die Replikation vom primären auf diesen sekundären Cluster sofort beendet und der Cluster wird zu einem eigenständigen, bereitgestellten Cluster mit vollem read/write Funktionsumfang heraufgestuft. Alle anderen sekundären Cluster, die dem primären Cluster in der Region zugeordnet sind, in der der Ausfall aufgetreten ist, sind weiterhin verfügbar und können Anrufe von Ihrer Anwendung annehmen. Sie verbrauchen auch Ressourcen. Da Sie den globalen Cluster neu erstellen,

sollten Sie zur Vermeidung von Split-Brain- und anderen Problemen die anderen sekundären Cluster entfernen, bevor Sie den neuen globalen Cluster in den folgenden Schritten erstellen.

Ausführliche Schritte zum Trennen finden Sie unter Einen Cluster aus einem globalen Amazon DocumentDB-Cluster entfernen.

4. Dieser Cluster wird zum primären Cluster eines neuen globalen Clusters, wenn Sie im nächsten Schritt damit beginnen, ihm Regionen hinzuzufügen.
5. Fügen Sie AWS-Region dem Cluster eine hinzu. Wenn Sie dies tun, beginnt der Replikationsprozess vom primären zum sekundären Cluster.
6. Fügen Sie nach AWS-Regionen Bedarf weitere hinzu, um die Topologie neu zu erstellen, die zur Unterstützung Ihrer Anwendung erforderlich ist. Stellen Sie sicher, dass Anwendungsschreibvorgänge vor, während und nach solchen Änderungen an den richtigen Cluster gesendet werden, um Dateninkonsistenzen zwischen den Clustern im globalen Cluster zu vermeiden (Split-Brain-Probleme).
7. Wenn der Ausfall behoben ist und Sie bereit sind, Ihren ursprünglichen Cluster wieder AWS-Region als primären Cluster zuzuweisen, führen Sie dieselben Schritte in umgekehrter Reihenfolge durch.
8. Entfernen Sie einen der sekundären Cluster aus dem globalen Cluster. Dadurch kann er read/write Datenverkehr bereitstellen.
9. Leiten Sie den gesamten Schreibverkehr auf den primären Cluster im Original um AWS-Region.
10. Fügen Sie einen hinzu AWS-Region , um einen oder mehrere sekundäre Cluster AWS-Region wie zuvor einzurichten.

Globale Amazon DocumentDB-Cluster können mithilfe von AWS SDKs verwaltet werden, sodass Sie Lösungen zur Automatisierung des globalen Cluster-Failover-Prozesses für Anwendungsfälle wie Disaster Recovery und Business Continuity Planning erstellen können. Eine solche Lösung wird unseren Kunden unter der Apache 2.0-Lizenz zur Verfügung gestellt und kann hier in unserem Tool-Repository abgerufen werden. Diese Lösung nutzt Amazon Route 53 für das Endpunktmanagement und bietet AWS Lambda Funktionen, die auf der Grundlage geeigneter Ereignisse ausgelöst werden können.

Durchführen eines Switchovers für einen globalen Amazon DocumentDB-Cluster

Mithilfe von Umstellungen können Sie die Region Ihres primären Clusters routinemäßig ändern. Dieser Ansatz ist für kontrollierte Szenarien gedacht, z. B. für betriebliche Wartungen und andere geplante Betriebsverfahren.

Es gibt drei gängige Anwendungsfälle für die Verwendung von Switchovers:

- Für Anforderungen an die „regionale Rotation“, die in bestimmten Branchen gelten. Beispielsweise könnten die Vorschriften für Finanzdienstleistungen vorschreiben, dass Tier-0-Systeme für mehrere Monate in eine andere Region wechseln müssen, um sicherzustellen, dass die Notfallwiederherstellungsverfahren regelmäßig geübt werden.
- Für regionsübergreifende „Follow-the-Sun“-Anwendungen. Beispielsweise möchte ein Unternehmen möglicherweise Schreibvorgänge mit niedrigerer Latenz in verschiedenen Regionen bereitstellen, basierend auf den Geschäftszeiten in verschiedenen Zeitzonen.
- Als Methode ohne Datenverlust, um nach einem Failover zur ursprünglichen Primärregion zurückzukehren.

> **Note**
>
> Switchover sind für die Verwendung in einem gesunden globalen Amazon DocumentDB-Cluster konzipiert. Folgen Sie zur Wiederherstellung nach einem ungeplanten Ausfall dem entsprechenden Verfahren unter Durchführen eines manuellen Failovers für einen globalen Amazon DocumentDB-Cluster.
> Um einen Switchover durchzuführen, müssen in allen sekundären Regionen exakt dieselbe Engine-Version wie in der primären Region ausgeführt werden. Wenn die Engine-Versionen der Region nicht übereinstimmen, wird der Switchover blockiert. Suchen Sie nach ausstehenden Upgrades und wenden Sie sie an, um sicherzustellen, dass die Engine-Versionen aller Regionen übereinstimmen und der globale Cluster-Switchover entsperrt ist. Weitere Informationen finden Sie unter Entsperren eines globalen Cluster-Switchovers oder -Failovers.

Während eines Switchovers wechselt Amazon DocumentDB Ihren primären Cluster in die von Ihnen gewählte sekundäre Region, während die bestehende Replikationstopologie Ihres globalen Clusters beibehalten wird. Bevor der Switchover-Prozess gestartet wird, wartet Amazon DocumentDB, bis alle Cluster der sekundären Region vollständig mit dem Cluster der primären Region synchronisiert sind. Dann wird der DB-Cluster in der primären Region schreibgeschützt, und der ausgewählte sekundäre Cluster stuft einen seiner schreibgeschützten Knoten auf vollen Writer-Status hoch. Durch die Heraufstufung dieses Knotens zu einem Writer kann dieser sekundäre Cluster die Rolle des primären Clusters übernehmen. Da alle sekundären Cluster zu Beginn des Prozesses mit dem primären synchronisiert wurden, setzt der neue primäre Cluster den Betrieb für den globalen Amazon

DocumentDB-Cluster fort, ohne Daten zu verlieren. Ihre Datenbank ist für kurze Zeit nicht verfügbar, während der primäre und der ausgewählte sekundäre Cluster ihre neuen Rollen übernehmen.

Um die Anwendungsverfügbarkeit zu optimieren, empfehlen wir Ihnen, vor der Verwendung dieser Funktion Folgendes zu tun:

- Führen Sie diesen Vorgang außerhalb der Spitzenzeiten oder zu einem anderen Zeitpunkt durch, zu dem die Schreibvorgänge auf den primären Cluster minimal sind.
- Schalten Sie Anwendungen offline, um zu verhindern, dass Schreibvorgänge an den primären Cluster des globalen Amazon DocumentDB-Clusters gesendet werden.
- Überprüfen Sie die Verzögerungszeiten für alle sekundären Amazon DocumentDB-Cluster im globalen Cluster, indem Sie sich die `GlobalClusterReplicationLag` Metrik in Amazon CloudWatch ansehen. Diese Metrik zeigt Ihnen, wie weit (in Millisekunden) die Replikation auf einen sekundären Cluster auf den primären Cluster zurückliegt. Dieser Wert ist direkt proportional zu der Zeit, die Amazon DocumentDB benötigt, um den Switchover abzuschließen. Je größer der Verzögerungswert, desto länger dauert die Umstellung.

  Weitere Informationen zu CloudWatch Metriken für Amazon DocumentDB finden Sie unterAmazon DocumentDB-Metriken.

Während einer Umstellung wird der ausgewählte sekundäre DB-Cluster in seine neue Rolle als primärer Cluster hochgestuft. Er übernimmt jedoch nicht die verschiedenen Konfigurationsoptionen des primären DB-Clusters. Wenn die Konfiguration nicht übereinstimmt, kann dies Leistungsprobleme, Workload-Inkompatibilitäten und anderes anomales Verhalten zur Folge haben. Um solche Probleme zu vermeiden, empfehlen wir Ihnen, die Unterschiede zwischen Ihren globalen Amazon DocumentDB-Clustern für Folgendes zu beheben:

- Konfigurieren Sie die Amazon DocumentDB-DB-Cluster-Parametergruppe für den neuen Primärserver, falls erforderlich — Sie können Ihre Amazon DocumentDB-Cluster-Parametergruppen unabhängig für jeden Cluster in Ihrem globalen Amazon DocumentDB-Cluster konfigurieren. Wenn Sie also einen sekundären DB-Cluster zur Übernahme der primären Rolle hochstufen, kann die Parametergruppe des sekundären Clusters im Vergleich zum primären Cluster möglicherweise anders konfiguriert werden. Ist dies der Fall, ändern Sie die Parametergruppe des hochgestuften sekundären DB-Clusters so, dass sie den Einstellungen des primären Clusters entspricht. Um zu erfahren wie, siehe Verwaltung von Amazon DocumentDB-Cluster-Parametergruppen.

- Überwachungstools und -optionen wie Amazon CloudWatch Events und Alarme konfigurieren — Konfigurieren Sie den beworbenen Cluster mit den gleichen Protokollierungsfunktionen, Alarmen usw., wie es für den globalen Cluster erforderlich ist. Wie bei Parametergruppen wird die Konfiguration für diese Funktionen während der Umstellung nicht vom primären Cluster übernommen. Einige CloudWatch Metriken, wie z. B. die Verzögerung bei der Replikation, sind nur für primäre Regionen verfügbar. Daher ändert sich bei einer Umstellung die Art und Weise, wie diese Metriken angezeigt und Alarme für sie eingerichtet werden, und es können Änderungen an allen vordefinierten Dashboards erforderlich sein. Weitere Informationen finden Sie unter Amazon DocumentDB überwachen.

> **Note**
>
> In der Regel kann der Rollenwechsel bis zu mehreren Minuten dauern.

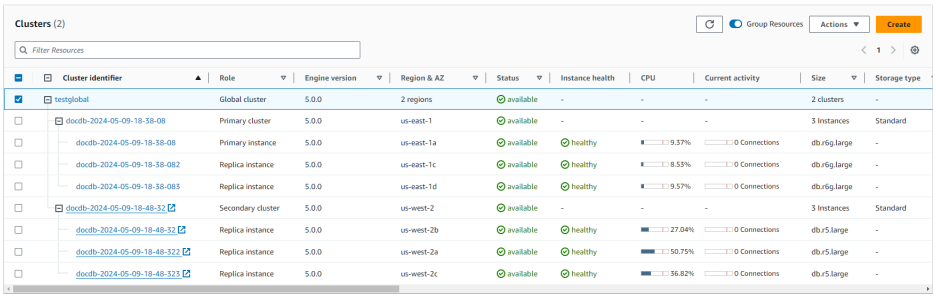
Wenn der Switchover-Prozess abgeschlossen ist, kann der beworbene Amazon DocumentDB-Cluster Schreibvorgänge für den globalen Cluster verarbeiten.

Sie können Ihren globalen Amazon DocumentDB-Cluster mit dem AWS-Managementkonsole oder dem AWS CLI folgenden Befehl umschalten:

Using the AWS-Managementkonsole

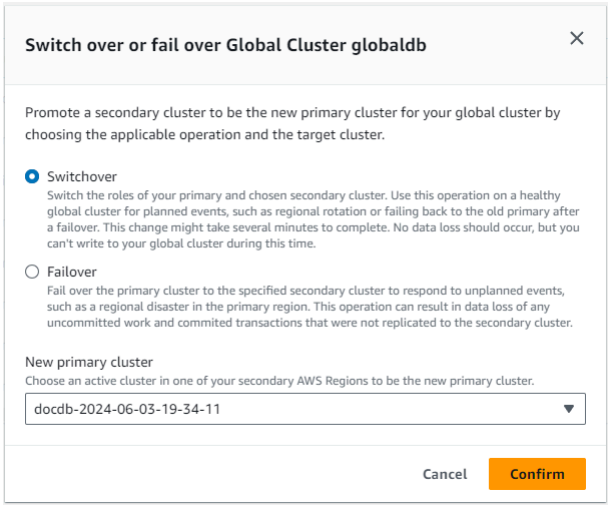
Führen Sie einen Switchover auf Ihrem globalen Amazon DocumentDB-Cluster durch

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Klicken Sie im Navigationsbereich auf Cluster.
3. Suchen Sie den globalen Amazon DocumentDB-Cluster, zu dem Sie wechseln möchten, und wählen Sie ihn aus.



4. Wählen Sie im Aktionsmenü Switchover oder Failover aus.

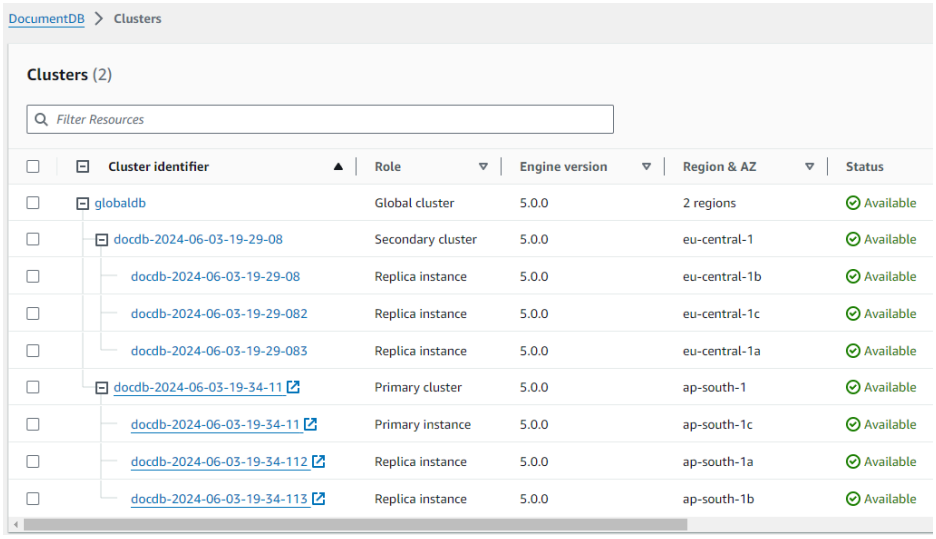
5. Wählen Sie im daraufhin angezeigten Dialogfeld Switchover und dann den sekundären Cluster aus der Dropdownliste Neues primäres Clusterfeld aus.



6. Wählen Sie Bestätigen aus.

   Der Status des primären Clusters ändert sich in "Switching-over“. Dieser Zustand sollte ungefähr drei Minuten dauern. Während dieser Zeit zeigt der Status aller regionalen Cluster "Wird geändert... “. Sobald die Regionen synchronisiert sind und die neue Primärregion beworben wurde, wird in allen Statusfeldern "Verfügbar" angezeigt und Transaktionen können bearbeitet werden.

7. Wenn der Vorgang abgeschlossen ist, wird der ursprüngliche primäre Cluster zum sekundären Cluster. Der ausgewählte sekundäre Cluster wird zum primären Cluster.



Using the AWS CLI

Führen Sie einen Switchover auf Ihrem globalen Amazon DocumentDB-Cluster durch

Führen Sie den `switchover-global-cluster`CLI-Befehl aus, um Ihren globalen Amazon DocumentDB-Cluster umzuschalten. Übergeben Sie mit dem Befehl Werte für die folgenden Optionen:

- `--region`
- `--global-cluster-identifier`
- `--target-db-cluster-identifier`

Ersetzen Sie in den folgenden Beispielen jedes *`user input placeholder`* durch die Informationen Ihres Clusters.

Für Linux, macOS oder Unix:

```
aws docdb switchover-global-cluster \
   --region region_of_primary \
   --global-cluster-identifier global_cluster_id \
   --target-db-cluster-identifier arn_of_secondary_to_promote
```

Für Windows:

```
aws docdb switchover-global-cluster ^
   --region region_of_primary ^
   --global-cluster-identifier global_cluster_id ^
   --target-db-cluster-identifier arn_of_secondary_to_promote
```

Entsperren eines globalen Cluster-Switchovers oder -Failovers

Globale Cluster-Switchover und -Failover werden blockiert, wenn sich nicht alle regionalen Cluster im globalen Cluster auf derselben Engine-Version befinden. Wenn die Versionen nicht übereinstimmen, wird beim Aufrufen eines Switchovers oder Failovers möglicherweise dieser Fehler angezeigt:
Auf dem angegebenen Ziel-DB-Cluster wird eine Engine-Version mit einem anderen Patch-Level ausgeführt als auf dem Quell-DB-Cluster. Wir empfehlen, regelmäßig die neuesten Engine-Versionen zu installieren, um sicherzustellen, dass Sie die neuesten Updates ausführen, damit Ihre globalen Cluster in einem fehlerfreien Zustand bleiben.

Um diesen Fehler zu beheben, aktualisieren Sie zuerst alle sekundären Regionen und dann die primäre Region auf dieselbe Engine-Version, indem Sie alle ausstehenden Wartungsmaßnahmen anwenden. Führen Sie die Anweisungen auf einer der folgenden Registerkarten aus, um ausstehende Wartungsmaßnahmen anzuzeigen und die zur Behebung des Problems erforderlichen Änderungen vorzunehmen:

Using the AWS-Managementkonsole

Um die Blockierung eines globalen Cluster-Switchovers oder -Failovers aufzuheben, müssen Sie feststellen, ob noch Wartungsaktionen für Ihre Cluster ausstehen, und diese anwenden. Gehen Sie wie folgt vor, um Wartungsaktionen anzuzeigen und anzuwenden:

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Klicken Sie im Navigationsbereich auf Cluster.
3. Suchen Sie in der Cluster-Tabelle in der Spalte Cluster-ID nach Ihrem globalen Cluster. Notieren Sie sich unter Ihrem globalen Cluster jeden sekundären Cluster und den primären Cluster für den jeweiligen globalen Cluster und führen Sie für jeden Cluster die folgenden Schritte aus.
4. Für jeden sekundären Cluster:
    a. Wenn ein Update für Ihren Cluster verfügbar ist, wird es in der Spalte Wartung als Verfügbar, Erforderlich oder Nächstes Fenster angezeigt.
    b. Um eine Aktion auszuführen, wählen Sie den Cluster aus, dessen Details angezeigt werden sollen, und wählen Sie dann Wartung und Backups aus. Die Einträge „Ausstehende Wartung“ werden angezeigt.
    c. Wenn unter Beschreibung angezeigt wird, dass ein „Neues Wartungsupdate verfügbar ist“, wählen Sie es aus und klicken Sie dann auf Jetzt anwenden.
5. Für Ihren primären Cluster:
    a. Wenn ein Update für Ihren Cluster verfügbar ist, wird es in der Spalte Wartung als Verfügbar, Erforderlich oder Nächstes Fenster angezeigt.
    b. Um eine Aktion auszuführen, wählen Sie den Cluster aus, dessen Details angezeigt werden sollen, und wählen Sie dann Wartung und Backups aus. Die Einträge „Ausstehende Wartung“ werden angezeigt.
    c. Wenn unter Beschreibung angezeigt wird, dass ein „Neues Wartungsupdate verfügbar ist“, wählen Sie es aus und klicken Sie dann auf Jetzt anwenden.

Using the AWS CLI

Um die Blockierung eines globalen Cluster-Switchovers oder -Failovers aufzuheben, müssen Sie feststellen, ob noch Wartungsaktionen für den Cluster ausstehen, und diese anwenden. Gehen Sie wie folgt vor, um Wartungsaktionen zunächst auf den sekundären Clustern und dann auf dem primären Cluster für Ihren globalen Cluster anzuzeigen und anzuwenden:

1. Führen Sie Folgendes zuerst für den regionalen Cluster jeder sekundären Region und dann für den regionalen Cluster der primären Regionen aus.
2. Führen Sie den `describe-pending-maintenance-actions`CLI-Befehl mit der `--resource-identifier` Option aus, um festzustellen, ob Wartungsaktionen für Ihren regionalen Amazon DocumentDB-Cluster verfügbar sind.

   Ersetzen Sie in den folgenden Beispielen jedes *`user input placeholder`* durch die Informationen Ihres Clusters.

   Für Linux, macOS oder Unix:

   ```
   aws docdb describe-pending-maintenance-action \
      --resource-identifier arn:aws:rds:us-
   east-1:001234567890:cluster:docdb-2025-03-27-19-21-15
   ```

   Für Windows:

   ```
   aws docdb describe-pending-maintenance-action ^
      --resource-identifier arn:aws:rds:us-
   east-1:001234567890:cluster:docdb-2025-03-27-19-21-15
   ```

   Das Ergebnis sieht in etwa so aus:

   ```
   {
       "PendingMaintenanceActions": [
           {
               "ResourceIdentifier": "arn:aws:rds:us-
   east-1:001234567890:cluster:docdb-2025-03-27-19-21-15",
               "PendingMaintenanceActionDetails": [
                   {
                       "Action": "system-update",
                       "CurrentApplyDate": "2025-04-11T03:01:00Z",
                       "Description": "db-version-upgrade",
   ```

```
                    "ForcedApplyDate": "2025-06-18T03:01:00Z",
                    "AutoAppliedAfterDate": "2025-05-11T03:01:00Z"
                    "OptInStatus": "pending"
                }
            ]
        }
    ]
}
```

3. Wenn eine Wartungsaktion erforderlich ist, führen Sie den [apply-pending-maintenance-action](#)CLI-Befehl mit den folgenden Optionen aus:

   - `--resource-identifier`
   - `--apply-action`
   - `--opt-in-type`
   - `--region`

   Ersetzen Sie in den folgenden Beispielen jedes Beispiel *`user input placeholder`* durch die Informationen Ihres Clusters.

   Für Linux, macOS oder Unix:

```
aws docdb apply-pending-maintenance-action \
   --resource-identifier arn:aws:rds:us-
east-1:001234567890:cluster:docdb-2025-03-27-19-21-15 \
   --apply-action system-update \
   --opt-in-type immediate \
   --region us-east-1
```

   Für Windows:

```
aws docdb apply-pending-maintenance-action ^
   --resource-identifier arn:aws:rds:us-
east-1:001234567890:cluster:docdb-2025-03-27-19-21-15 ^
   --apply-action system-update ^
   --opt-in-type immediate ^
   --region us-east-1
```

4. Sobald die Wartungsaktion abgeschlossen ist, führen Sie den `describe-pending-maintenance-actions`Befehl erneut aus, um sicherzustellen, dass keine weiteren Aktionen für Ihren Cluster ausstehen.

   Das gewünschte Ergebnis ist:

   ```
   {
       "PendingMaintenanceActions": []
   }
   ```

Using the Amazon DocumentDB API

Um die Blockierung eines globalen Cluster-Switchovers oder -Failovers aufzuheben, müssen Sie feststellen, ob noch Wartungsaktionen für den Cluster ausstehen, und diese anwenden. Verwenden Sie die folgenden APIs, um Wartungsaktionen anzuzeigen und anzuwenden:

1. Führen Sie den folgenden Befehl zuerst für den regionalen Cluster jeder sekundären Region und dann für den regionalen Cluster der primären Regionen aus.
2. Rufen Sie die `PendingMaintenanceAction`API auf, um festzustellen, ob Wartungsaktionen für Ihren globalen Amazon DocumentDB-Cluster verfügbar sind.
3. Wenden Sie alle Änderungen an, indem Sie die `ApplyPendingMaintenanceAction`API aufrufen.

Verwaltung von Amazon DocumentDB-Clustern

Um einen Amazon DocumentDB-Cluster zu verwalten, benötigen Sie eine IAM-Richtlinie mit den entsprechenden Berechtigungen für die Amazon DocumentDB-Steuerebene. Diese Berechtigungen ermöglichen das Erstellen, Ändern und Löschen von Clustern und Instances. Die `AmazonDocDBFullAccess` Richtlinie bietet alle erforderlichen Berechtigungen für die Verwaltung eines Amazon DocumentDB-Clusters.

Die folgenden Themen zeigen, wie Sie bei der Arbeit mit Amazon DocumentDB-Clustern verschiedene Aufgaben ausführen, darunter das Erstellen, Löschen, Ändern, Herstellen einer Verbindung zu und das Anzeigen von Clustern.

Themen

- Cluster verstehen

- Amazon DocumentDB-Cluster-Einstellungen
- Amazon DocumentDB-Cluster-Speicherkonfigurationen
- Den Status eines Clusters ermitteln
- Amazon DocumentDB-Cluster-Lebenszyklus
- Skalierung von Amazon DocumentDB-Clustern
- Klonen eines Volumes für einen Amazon DocumentDB-Cluster
- Grundlegendes zur Amazon DocumentDB-Cluster-Fehlertoleranz

Cluster verstehen

Amazon DocumentDB trennt Rechenleistung und Speicher und verlagert Datenreplikation und Backup auf das Cluster-Volume. Ein Cluster-Volume bietet eine dauerhafte, zuverlässige und hochverfügbare Speicherschicht, die Daten auf sechs Arten über drei Availability Zones repliziert. Replikate ermöglichen eine höhere Datenverfügbarkeit und Leseskalierung. Jeder Cluster kann auf bis zu 15 Replikate skaliert werden.

Substantiv	Description	API-Operationen (Verben)

Cluster	Besteht aus einer oder mehreren Instances und einem Cluster-Storage-Volume, das die Daten für diese Instances verwaltet.	`create-db-cluster`
		`delete-db-cluster`
		`describe-db-clusters`
		`modify-db-cluster`

Instance	Das Lesen und Schreiben von Daten auf das Cluster-Speichervolumen erfolgt über Instances. In einem gegebenen Cluster gibt es zwei Arten von Instances: Primär und Replikat. Ein Cluster hat immer eine primäre Instanz und kann 0—15 Replikate haben.	`create-db-instance`
		`delete-db-instance`
		`describe-db-instances`
		`modify-db-instance`
		`describe-orderable-db-instance-options`

Substantiv	Description	API-Operationen (Verben)
		`reboot-db-instance`
Cluster-Volumen	Ein virtuelles Datenbank speichervolumen, das sich über drei Availability Zones erstreckt, wobei jede Availabil ity Zone zwei Kopien der Cluster-Daten aufweist.	N/A
Primäre Instance	Unterstützt Lese- und Schreiboperationen und führt alle Datenänderungen im Cluster-Volume durch. Jeder Cluster verfügt über eine primäre Instance.	N/A
Replikat-Instance	Unterstützt nur Lesevorgänge. Jeder Amazon DocumentD B-Cluster kann zusätzlich zur primären Instance bis zu 15 Replikat-Instances haben. Mehrere Replikate verteilen den Lese-Workload. Durch die Platzierung von Replikaten in separaten Availability Zones können Sie außerdem die Verfügbarkeit der Datenbank erhöhen.	N/A

Substantiv	Description	API-Operationen (Verben)
Cluster-Endpunkt	Ein Endpunkt für einen Amazon DocumentDB-Cluster , der eine Verbindung zur aktuellen primären Instance für den Cluster herstellt. Jeder Amazon DocumentDB-Cluster hat einen Cluster-Endpunkt und eine primäre Instance.	N/A
Leser-Endpunkt	Ein Endpunkt für einen Amazon DocumentDB-Cluster, der eine Verbindung zu einem der verfügbaren Replikate für diesen Cluster herstellt. Jeder Amazon DocumentDB-Cluster hat einen Leser-Endpunkt. Wenn es mehr als ein Replikat gibt, leitet der Leser-Endpunkt jede Verbindungsanfrage an eines der Amazon DocumentDB DocumentDB-Replikate weiter.	N/A
Instance-Endpunkt	Ein Endpunkt für eine Instance in einem Amazon DocumentDB-Cluster, der eine Verbindung zu einer bestimmten Instance herstellt. Jede Instance in einem Cluster hat unabhängig vom Instance-Typ einen eigenen eindeutigen Instance-Endpunkt.	N/A

Amazon DocumentDB-Cluster-Einstellungen

Beim Erstellen oder Ändern eines Clusters müssen Sie wissen, welche Parameter unveränderlich und welche nach dem Anlegen des Clusters veränderbar sind. Die folgende Tabelle listet alle Einstellungen bzw. Parameter auf, die für einen Cluster spezifisch sind. Wie in der Tabelle angegeben, sind nur einige Parameter änderbar.

> **Note**
>
> Diese Einstellungen sollten nicht mit Amazon DocumentDB-Cluster-Parametergruppen und ihren Parametern verwechselt werden. Weitere Informationen zu Cluster-Parametergruppen finden Sie unter Verwaltung von Amazon DocumentDB-Cluster-Parametergruppen.

Parameter	Anpassbar	Hinweise
`DBClusterIdentifier`	Ja	Benennungseinschränkungen: • Die Länge beträgt [1—63] Buchstaben, Zahlen oder Bindestriche. • Muss mit einem Buchstaben beginnen. • Darf nicht mit einem Bindestrich enden oder zwei aufeinanderfolgende Bindestriche enthalten. • Muss für alle Cluster in Amazon RDS, Amazon Neptune und Amazon DocumentDB pro AWS-Konto Region eindeutig sein.
`Engine`	Nein	Der Wert muss `docdb` sein.
`BackupRetentionPeriod`	Ja	Muss zwischen 1 und 35 Tagen liegen.
`DBClusterParameterGroupName`	Ja	Benennungseinschränkungen: • Die Länge beträgt [1—255] alphanumerische Zeichen. • Muss mit einem Buchstaben beginnen.

Parameter	Anpassbar	Hinweise
		• Darf nicht mit einem Bindestrich enden oder zwei aufeinanderfolgende Bindestriche enthalten.
DBSubnetGroupName	Nein	Sie können das Subnetz des Clusters nach dem Anlegen eines Clusters nicht mehr ändern.
EngineVersion	Nein	Der Wert kann `5.0.0` (Standard), `4.0.0` oder sein. `3.6.0`
KmsKeyId	Nein	Wenn Sie Ihren Cluster verschlüsseln möchten, können Sie den AWS KMS Schlüssel, den Sie zur Verschlüsselung Ihres Clusters verwendet haben, nicht ändern.
MasterUsername	Nein	Sie können den `MasterUsername` nach dem Anlegen eines Clusters nicht mehr ändern. Benennungseinschränkungen: • Die Länge beträgt [1—63] alphanumerische Zeichen. • Muss mit einem Buchstaben beginnen. • Darf kein Wort sein, das von der Datenbank-Engine reserviert ist.

MasterUserPassword	Ja	Einschränkungen:
		
		• Die Länge beträgt [8—100] druckbare ASCII-Zeichen.
		• Es können alle druckbaren ASCII-Zeichen mit Ausnahme der folgenden verwendet werden:
		  • **/** (Schrägstrich)
		  • **"** (doppeltes Anführungszeichen)
		  • **@** ('At'-Symbol)

Parameter	Anpassbar	Hinweise
`Port`	Ja	Die Portnummer gilt für alle Instances im Cluster.
`PreferredBackupWindow`	Ja	
`PreferredMaintenanceWindow`	Ja	
`StorageEncrypted`	Nein	Wenn Sie Ihren Cluster verschlüsseln, kann er nicht unverschlüsselt sein.
`StorageType`	Ja	Der Speichertyp für den DB-Cluster: Standard (`standard`) oder (). I/O-Optimized `iopt1` Standard: `standard` Dieser Parameter kann mit `CreateDBCluster` und konfiguriert werden`ModifyDBCluster` . Weitere Informationen finden Sie unter Amazon DocumentDB-Cluster-Speicherkonfigurationen.
`Tags`	Ja	
`VpcSecurityGroupIds`	Nein	Nachdem ein Cluster erstellt wurde, können Sie die VPC nicht ändern, in der sich der Cluster befindet.

Amazon DocumentDB-Cluster-Speicherkonfigurationen

Ab Amazon DocumentDB 5.0 unterstützen instanzbasierte Cluster zwei Speicherkonfigurationstypen:

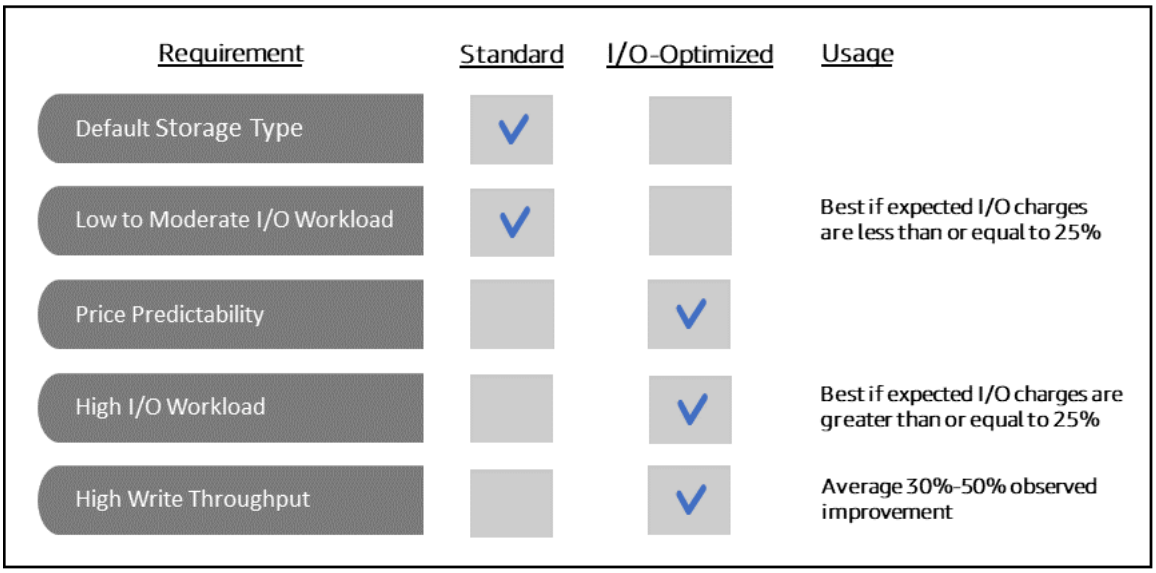
- Amazon DocumentDB DocumentDB-Standardspeicher: Konzipiert für Kunden mit geringem bis moderatem I/O Verbrauch. Wenn Sie davon ausgehen, dass Ihre I/O Kosten weniger als 25% Ihres gesamten Amazon DocumentDB-Clusters ausmachen werden, ist diese Wahl möglicherweise ideal

für Sie. Bei der Standardspeicherkonfiguration von Amazon DocumentDB wird Ihnen zusätzlich zu den Instance- und Speichergebühren eine I/O Pay-per-Request-Basis in Rechnung gestellt. Das bedeutet, dass Ihre Abrechnung je nach Nutzung von einem Zyklus zum anderen variieren kann. Die Konfiguration ist auf die schwankenden I/O Anforderungen Ihrer Anwendung zugeschnitten.

- Amazon DocumentDB I/O-optimized DocumentDB-Speicher: Konzipiert für Kunden, die Wert auf Preisvorhersehbarkeit legen oder umfangreiche Anwendungen haben I/O . Die I/O-optimized Konfiguration bietet eine verbesserte Leistung, einen höheren Durchsatz und eine geringere Latenz für Kunden mit I/O intensiven Workloads. Wenn Sie davon ausgehen, dass Ihre I/O Kosten 25% Ihrer gesamten Amazon DocumentDB-Clusterkosten übersteigen werden, bietet diese Option ein besseres Preis-Leistungs-Verhältnis. Mit der Amazon DocumentDB I/O-optimized DocumentDB-Speicherkonfiguration werden Ihnen keine Gebühren auf der Grundlage von I/O Vorgängen berechnet, sodass die Kosten in jedem Abrechnungszeitraum vorhersehbar sind. Die Konfiguration stabilisiert die Kosten und verbessert gleichzeitig die Leistung.

Sie können Ihre vorhandenen Datenbankcluster alle 30 Tage auf Amazon DocumentDB I/O-optimized DocumentDB-Speicher umstellen. Sie können jederzeit zum Amazon DocumentDB DocumentDB-Standardspeicher zurückkehren. Das nächste Datum, an dem die Speicherkonfiguration geändert werden soll, I/O-optimized kann mit dem `describe-db-clusters` Befehl über AWS CLI oder über die auf der AWS-Managementkonsole Konfigurationsseite des Clusters angegeben werden.

Sie können einen neuen Datenbank-Cluster einschließlich der Amazon DocumentDB I/O-optimized DocumentDB-Konfiguration erstellen oder Ihre vorhandenen Datenbank-Cluster mit ein paar Klicks AWS-Managementkonsole, einer einzigen Parameteränderung in der AWS Command Line Interface (AWS CLI) oder über AWS SDKs konvertieren. Während oder nach der Änderung der Speicherkonfiguration sind keine Ausfallzeiten oder Neustarts von Instances erforderlich.

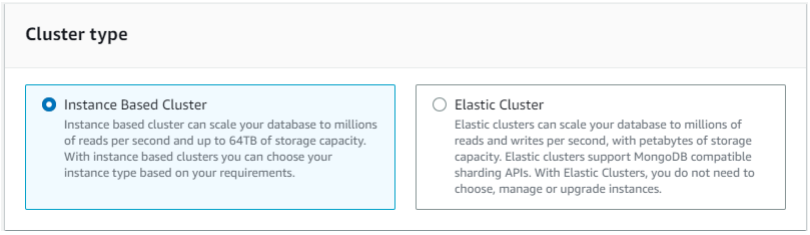


Einen Cluster erstellen I/O-optimized

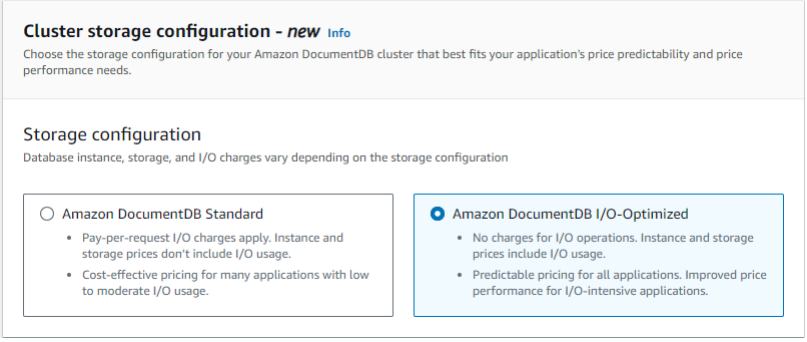
Using the AWS-Managementkonsole

Um einen I/O-optimized Cluster zu erstellen oder zu ändern, verwenden Sie AWS-Managementkonsole:

1. Wählen Sie in der Amazon DocumentDB-Managementkonsole unter Clusters entweder Create oder wählen Sie den Cluster aus und wählen Sie Actions und anschließend Modify aus.
2. Wenn Sie einen neuen Cluster erstellen, stellen Sie sicher, dass Sie im Abschnitt Clustertyp die Option Instance Based Cluster auswählen (dies ist die Standardoption).



3. Wählen Sie im Abschnitt Konfiguration unter Cluster-Speicherkonfiguration Amazon DocumentDB I/O-Optimized aus.



4. Schließen Sie die Erstellung oder Änderung Ihres Clusters ab und wählen Sie Cluster erstellen oder Cluster ändern aus.

   Den vollständigen Vorgang zum Erstellen eines Clusters finden Sie unterErstellen eines Clusters und einer primären Instance mit dem AWS-Managementkonsole.

   Den vollständigen Vorgang zum Ändern des Clusters finden Sie unterÄndern eines Amazon DocumentDB-Clusters.

Using the AWS CLI

Um einen I/O-optimized Cluster zu erstellen, verwenden Sie AWS CLI:

Ersetzen Sie in den folgenden Beispielen jedes *user input placeholder* durch Ihre eigenen Informationen.

Für Linux, macOS oder Unix:

```
aws docdb create-db-cluster \
      --db-cluster-identifier sample-cluster \
      --engine docdb \
      --engine-version 5.0.0 \
      --storage-type iopt1 \
      --deletion-protection \
      --master-username username \
      --master-user-password password
```

Für Windows:

```
aws docdb create-db-cluster ^
      --db-cluster-identifier sample-cluster ^
      --engine docdb ^
      --engine-version 5.0.0 ^
```

```
    --storage-type iopt1 ^
    --deletion-protection ^
    --master-username username ^
    --master-user-password password
```

Kostenanalyse zur Bestimmung der Speicherkonfiguration

Mit Amazon DocumentDB haben Sie die Flexibilität, Ihre Speicherkonfiguration für jeden vorhandenen Datenbank-Cluster auszuwählen. Um Ihre Cluster ordnungsgemäß zwischen Standard und zu verteilen I/O-optimized, können Sie Ihre Amazon DocumentDB DocumentDB-Kosten clusterweise verfolgen. Zu diesem Zweck können Sie Tags zu vorhandenen Clustern hinzufügen, die Kostenzuordnungskennzeichnung in Ihrem AWS Fakturierung und Kostenmanagement Dashboard aktivieren und Ihre Kosten für einen bestimmten Cluster im analysieren. AWS Cost Explorer Service Informationen zur Kostenanalyse finden Sie in unserem Blog Verwenden von Kostenzuordnungs-Tags.

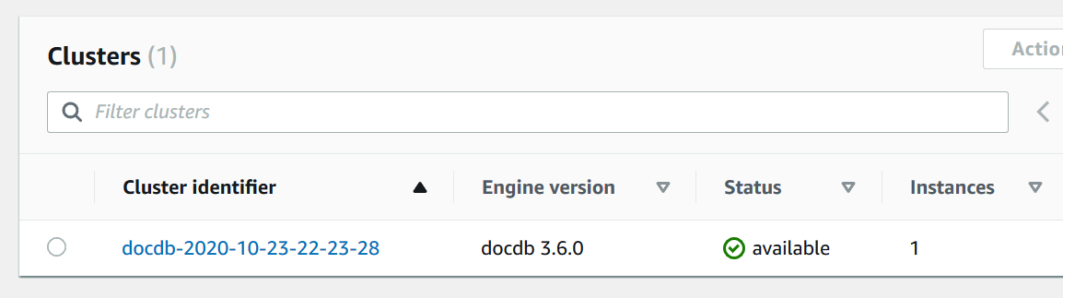
Den Status eines Clusters ermitteln

Sie können den Status eines Clusters mit dem AWS-Managementkonsole oder ermitteln AWS CLI.

Using the AWS-Managementkonsole

Gehen Sie wie folgt vor, um den Status Ihres Amazon DocumentDB-Clusters mithilfe der AWS-Managementkonsole

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Klicken Sie im Navigationsbereich auf Cluster.
3. Suchen Sie in der Spalte Cluster identifier (Cluster-ID) den Namen des Clusters, der Sie interessiert. Um dann den Status des Clusters zu ermitteln, lesen Sie diese Zeile in die Spalte Status, wie unten gezeigt.



Using the AWS CLI

Verwenden Sie den `describe-db-clusters` Vorgang, um den Status Ihres Amazon DocumentDB-Clusters mithilfe von zu überprüfen. AWS CLI

Der folgende Code ermittelt den Status des Clusters `sample-cluster`.

Für Linux, macOS oder Unix:

```
aws docdb describe-db-clusters \
    --db-cluster-identifier sample-cluster  \
    --query 'DBClusters[*].[DBClusterIdentifier,Status]'
```

Für Windows:

```
aws docdb describe-db-clusters ^
    --db-cluster-identifier sample-cluster  ^
    --query 'DBClusters[*].[DBClusterIdentifier,Status]'
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus (JSON-Format).

```
[
    [
        "sample-cluster",
        "available"
    ]
]
```

Amazon DocumentDB-Cluster-Lebenszyklus

Der Lebenszyklus eines Amazon DocumentDB-Clusters umfasst das Erstellen, Beschreiben, Ändern und Löschen des Clusters. Dieser Abschnitt enthält Informationen darüber, wie Sie diese Prozesse abschließen können.

Themen

- Einen Amazon DocumentDB-Cluster erstellen
- Beschreibung von Amazon DocumentDB-Clustern
- Ändern eines Amazon DocumentDB-Clusters

- Ermittlung ausstehender Wartungsarbeiten
- Durchführen eines Patch-Updates für die Engine-Version eines Clusters
- Einen Amazon DocumentDB-Cluster stoppen und starten
- Löschen eines Amazon DocumentDB-Clusters

Einen Amazon DocumentDB-Cluster erstellen

Ein Amazon DocumentDB-Cluster besteht aus Instances und einem Cluster-Volume, das die Daten für den Cluster darstellt. Das Cluster-Volumen wird auf sechs Arten über drei Availability Zones als ein einziges, virtuelles Volume repliziert. Der Cluster enthält eine primäre Instance und optional bis zu 15 Replikat-Instances.

In den folgenden Abschnitten wird gezeigt, wie Sie einen Amazon DocumentDB-Cluster mit dem AWS-Managementkonsole oder dem AWS CLI erstellen. Sie können dann weitere Replikat-Instances für diesen Cluster hinzufügen. Wenn Sie die Konsole verwenden, um Ihren Amazon DocumentDB-Cluster zu erstellen, wird gleichzeitig automatisch eine primäre Instance für Sie erstellt. Wenn Sie den verwenden, AWS CLI um Ihren Amazon DocumentDB-Cluster zu erstellen, müssen Sie, nachdem der Status des Clusters verfügbar ist, die primäre Instance für diesen Cluster erstellen.

Voraussetzungen

Im Folgenden sind die Voraussetzungen für die Erstellung eines Amazon DocumentDB-Clusters aufgeführt.

Wenn Sie noch keinen haben AWS-Konto, führen Sie die folgenden Schritte aus, um einen zu erstellen.

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie https://portal.aws.amazon.com/billing/signup.
2. Folgen Sie den Online-Anweisungen.

   Während der Anmeldung erhalten Sie einen Telefonanruf oder eine Textnachricht und müssen einen Verifizierungscode über die Telefontasten eingeben.

   Wenn Sie sich für eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontoswird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Als bewährte Sicherheitsmethode weisen Sie einem Benutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um Aufgaben auszuführen, die Root-Benutzerzugriff erfordern.

VPC-Voraussetzungen

Sie können einen Amazon DocumentDB-Cluster nur in einer Amazon Virtual Private Cloud (Amazon VPC) erstellen. Ihre Amazon VPC muss mindestens ein Subnetz in jeder von mindestens zwei Availability Zones haben, damit Sie sie mit einem Amazon DocumentDB-Cluster verwenden können. Durch die Verteilung Ihrer Cluster-Instances auf Availability Zones stellen Sie sicher, dass Instances in Ihrem Cluster für den unwahrscheinlichen Fall eines Ausfalls der Availability Zone verfügbar sind.

Voraussetzungen für das Subnetz

Wenn Sie einen Amazon DocumentDB-Cluster erstellen, müssen Sie eine VPC und die entsprechende Subnetzgruppe innerhalb dieser VPC auswählen, um Ihren Cluster zu starten. Subnetze bestimmen die Availability Zone und den IP-Bereich innerhalb dieser Availability Zone, die Sie zum Starten einer Instance verwenden möchten. Im Rahmen dieser Ausführungen werden die Begriffe Subnetz und Availability Zone synonym verwendet. Eine Subnetzgruppe ist ein benannter Satz von Subnetzen (oder Availability Zones). Mit einer Subnetzgruppe können Sie die Availability Zones angeben, die Sie zum Starten von Amazon DocumentDB DocumentDB-Instances verwenden möchten. So wird beispielsweise in einem Cluster mit drei Instances für eine hohe Verfügbarkeit empfohlen, dass jede dieser Instances in separaten Availability Zones bereitgestellt wird. Wenn eine einzelne Availability Zones ausfällt, wirkt sich dies nur auf eine einzelne Instance aus.

Amazon DocumentDB DocumentDB-Instances können derzeit in bis zu drei Availability Zones bereitgestellt werden. Selbst wenn eine Subnetzgruppe mehr als drei Subnetze hat, können Sie nur drei dieser Subnetze verwenden, um einen Amazon DocumentDB-Cluster zu erstellen. Daher wird empfohlen, dass Sie beim Anlegen einer Subnetzgruppe nur die drei Subnetze auswählen, in denen Sie Ihre Instances bereitstellen möchten. In USA Ost (Nord-Virginia) kann Ihre Subnetzgruppe sechs Subnetze (oder Availability Zones) haben. Wenn jedoch ein Amazon DocumentDB-Cluster bereitgestellt wird, wählt Amazon DocumentDB drei der Availability Zones aus, die es für die Bereitstellung von Instances verwendet.

Nehmen wir beispielsweise an, dass Amazon DocumentDB beim Erstellen eines Clusters die Availability Zones {1A, 1B und 1C} auswählt. Wenn Sie nun versuchen, eine Instance in Availability Zone {1D} zu erstellen, schlägt der API-Aufruf fehl. Wenn Sie sich jedoch dafür entscheiden, eine Instance zu erstellen, ohne eine bestimmte Availability Zone anzugeben, wählt Amazon DocumentDB in Ihrem Namen eine Availability Zone aus. Amazon DocumentDB verwendet einen Algorithmus für den Lastenausgleich der Instances in den Availability Zones, um Ihnen zu helfen, eine hohe Verfügbarkeit zu erreichen. Wenn beispielsweise drei Instances bereitgestellt werden, werden diese standardmäßig über drei Availability Zones verteilt und nicht alle in einer einzigen Availability Zone bereitgestellt.

Empfehlungen:

- Wenn Sie keinen speziellen Grund haben, legen Sie immer eine Subnetzgruppe mit drei Subnetzen an. Auf diese Weise wird sichergestellt, dass Cluster mit drei oder mehr Instances eine höhere Verfügbarkeit erreichen können, da Instances über drei Availability Zones bereitgestellt werden.
- Verteilen Sie Instances immer über mehrere Availability Zones, um eine hohe Verfügbarkeit zu erreichen. Platzieren Sie niemals alle Instances für einen Cluster in einer einzigen Availability Zone.
- Da Failover-Ereignisse jederzeit auftreten können, sollten Sie nicht davon ausgehen, dass sich eine primäre Instance oder Replikat-Instance immer in einer bestimmten Availability Zone befinden.

Zusätzliche Voraussetzungen

Im Folgenden sind einige zusätzliche Voraussetzungen für die Erstellung eines Amazon DocumentDB-Clusters aufgeführt:

- Wenn Sie eine Verbindung AWS mit AWS Identity and Access Management (IAM-) Anmeldeinformationen herstellen, muss Ihr IAM-Konto über IAM-Richtlinien verfügen, die die Berechtigungen gewähren, die für die Ausführung von Amazon DocumentDB DocumentDB-Vorgängen erforderlich sind.

  Wenn Sie ein IAM-Konto für den Zugriff auf die Amazon DocumentDB DocumentDB-Konsole verwenden, müssen Sie sich zunächst AWS-Managementkonsole mit Ihrem IAM-Konto bei der anmelden. Gehen Sie dann zur Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
- Wenn Sie die Konfigurationsparameter für Ihren Cluster anpassen möchten, müssen Sie eine Cluster-Parametergruppe und eine Parametergruppe mit den erforderlichen Parametereinstellungen festlegen. Informationen zum Erstellen oder Ändern einer Cluster-Parametergruppe oder Parametergruppe finden Sie unter Verwaltung von Amazon DocumentDB-Cluster-Parametergruppen.
- Sie müssen die TCP/IP Portnummer ermitteln, die Sie für Ihren Cluster angeben möchten. Die Firewalls einiger Unternehmen blockieren Verbindungen zu den Standardports für Amazon DocumentDB. Wenn die Firewall Ihres Unternehmens den Standard-Port blockiert, wählen Sie einen anderen Port für Ihr Cluster aus. Alle Instances in einem Cluster verwenden denselben Port.

Erstellen eines Clusters und einer primären Instance mit dem AWS-Managementkonsole

Die folgenden Verfahren beschreiben, wie Sie die Konsole verwenden, um einen Amazon DocumentDB-Cluster mit einer oder mehreren Instances zu starten.

Erstellen Sie einen Cluster: Verwenden Sie die Standardeinstellungen

Um einen Cluster mit Instanzen zu erstellen, verwenden Sie die Standardeinstellungen AWS-Managementkonsole

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Wenn Sie Ihren Cluster in einer AWS-Region anderen Region als der Region USA Ost (Nord-Virginia) erstellen möchten, wählen Sie die Region aus der Liste im oberen rechten Bereich der Konsole aus.
3. Wählen Sie im Navigationsbereich Clusters (Cluster) und dann Create (Erstellen).

   > **Tip**
   >
   > Wenn der Navigationsbereich auf der linken Seite des Bildschirms nicht angezeigt wird, wählen Sie links oben auf der Seite das Menüsymbol (≡) aus.

4. Füllen Sie auf der Seite Amazon DocumentDB-Cluster erstellen den Bereich Konfiguration aus.

   a. Cluster-ID — Akzeptieren Sie den von Amazon DocumentDB angegebenen Namen, oder geben Sie einen Namen für Ihren Cluster ein, z. B. **`sample-cluster`**

      Einschränkungen bei der Benennung von Clustern:

      - Die Länge beträgt [1—63] Buchstaben, Zahlen oder Bindestriche.
      - Muss mit einem Buchstaben beginnen.
      - Darf nicht mit einem Bindestrich enden oder zwei aufeinanderfolgende Bindestriche enthalten.
      - Muss für alle Cluster in Amazon RDS, Neptune und Amazon DocumentDB pro AWS-Konto Region eindeutig sein.

   b. Engine-Version — Akzeptieren Sie die Standard-Engine-Version 5.0.0 oder wählen Sie optional 8.0.0, 4.0.0 oder 3.6.0.

c. Instanzklasse — Akzeptieren Sie die Standardklasse`db.r5.large`, oder wählen Sie die gewünschte Instanzklasse aus der Liste aus.

d. Anzahl der Instanzen — Wählen Sie in der Liste die Anzahl der Instances aus, die Sie mit diesem Cluster erstellen möchten. Die erste Instance ist die primäre Instance. Alle anderen Instances sind schreibgeschützte Replikat-Instances. Sie können später Instances hinzufügen und löschen. Standardmäßig wird ein Amazon DocumentDB-Cluster mit drei Instances (einer primären und zwei Replikaten) gestartet.

5. Füllen Sie den Abschnitt Cluster-Speicherkonfiguration aus.

   Wählen Sie entweder Amazon DocumentDB Standard (Standard) oder Amazon I/O-Optimized DocumentDB. Weitere Informationen finden Sie unter Amazon DocumentDB-Cluster-Speicherkonfigurationen.

6. Vervollständigen Sie den Bereich Authentication (Authentifizierung).

   a. Benutzername — Geben Sie einen Namen für den Hauptbenutzer ein. Um sich bei Ihrem Cluster anzumelden, müssen Sie den primären Benutzernamen verwenden.

      Einschränkungen bei der Benennung primärer Benutzer:

      - Die Länge beträgt [1—63] alphanumerische Zeichen.
      - Muss mit einem Buchstaben beginnen.
      - Darf kein Wort sein, das von der Datenbank-Engine reserviert ist.

   b. Wählen Sie eine der folgenden Passwortoptionen:

      - Verwaltet in AWS Secrets Manager — Wählen Sie diese Option, wenn Sie Ihr primäres Benutzerkennwort automatisch verwalten möchten AWS Secrets Manager .

        Wenn Sie diese Option wählen, konfigurieren Sie den KMS-Schlüssel, indem Sie entweder Ihren eigenen Schlüssel erstellen oder einen Schlüssel verwenden, den Secrets Manager erstellt.

      - Selbstverwaltet — Wählen Sie diese Option, wenn Sie Ihr primäres Benutzerkennwort selbst verwalten möchten. Wenn Sie diese Option wählen, geben Sie ein Passwort für den Hauptbenutzer ein und bestätigen Sie es dann. Um sich bei Ihrem Cluster anzumelden, müssen Sie das Passwort für den Hauptbenutzer verwenden.

        Passwortbeschränkungen:

        - Länge beträgt [8–100] druckbare ASCII-Zeichen.

- Es können alle druckbaren ASCII-Zeichen mit Ausnahme der folgenden verwendet werden:
  - **/** (Schrägstrich)
  - **"** (doppeltes Anführungszeichen)
  - **@** ('At'-Symbol)

7. Wählen Sie am unteren Rand der Seite eine der folgenden Optionen:
   - Um den Cluster jetzt zu erstellen, wählen Sie Create Cluster (Cluster erstellen) aus.
   - Wenn der Cluster nicht neu erstellt werden soll, wählen Sie Cancel (Abbrechen) aus.
   - Um den Cluster vor der Erstellung weiter zu konfigurieren, wählen Sie Show additional configurations (Weitere Konfigurationen anzeigen) aus und fahren dann mit Einen Cluster erstellen: zusätzliche Konfigurationen fort.

     Im Bereich Additional Configurations (Zusätzliche Konfigurationen) sind die folgenden Konfigurationen zu finden:

     - Netzwerkeinstellungen — Standardmäßig wird die `default` VPC-Sicherheitsgruppe verwendet.
     - Clusteroptionen — Standardmäßig wird der Port 27017 und die Standardparametergruppe verwendet.
     - Verschlüsselung — Standardmäßig wird die Verschlüsselung mithilfe des `(default) aws/rds` Schlüssels aktiviert.

       > **Important**
       >
       > Die Verschlüsselung eines einmal verschlüsselten Clusters kann nicht wieder aufgehoben werden.

     - Backup — Standardmäßig werden Backups für einen Tag aufbewahrt und Amazon DocumentDB das Backup-Fenster wählen lassen.
     - Protokollexporte — Standardmäßig werden Audit-Logs nicht in Logs exportiert CloudWatch .
     - Wartung — Standardmäßig lässt Amazon DocumentDB das Wartungsfenster wählen.
     - Löschschutz — Schützt Ihren Cluster vor versehentlichem Löschen. Cluster, die mit der Konsole erstellt wurden, sind standardmäßig aktiviert.

Wenn Sie die Standardeinstellungen jetzt übernehmen, können Sie die meisten davon später durch Bearbeitung des Clusters wieder ändern.

8. Aktivieren Sie eingehende Verbindungen für die Sicherheitsgruppe Ihres Clusters.

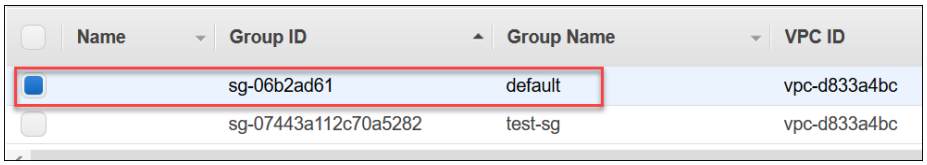
   Wenn Sie die Standardeinstellungen für Ihr Cluster nicht geändert haben, wurde mithilfe der Standard-Sicherheitsgruppe ein Cluster für die Standard-VPC in der angegebenen Region erstellt. Um eine Verbindung zu Amazon DocumentDB herzustellen, müssen Sie eingehende Verbindungen auf Port 27017 (oder dem Port Ihrer Wahl) für die Sicherheitsgruppe Ihres Clusters aktivieren.

   So fügen Sie eine eingehende Verbindung zur SicherheitsgruppeIhres Clusters hinzu:

   a. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon EC2 EC2-Konsole unter https://console.aws.amazon.com/ec2/.

   b. Wählen Sie im Abschnitt Resources (Ressourcen) des Hauptfensters die Option Security groups (Sicherheitsgruppen).

   c. Wählen Sie in der Liste der Sicherheitsgruppen die Sicherheitsgruppe aus, die Sie bei der Erstellung Ihres Cluster verwendet haben (höchstwahrscheinlich handelt es sich dabei um die Standard-Sicherheitsgruppe), und wählen Sie das Feld links neben dem Name der Sicherheitsgruppe aus.



   d. Wählen Sie im Menü Aktionen die Option Eingangsregeln bearbeiten aus. Wählen Sie dann die Regeleinschränkungen aus oder geben Sie diese ein.

      i. Typ — Wählen Sie aus der Liste das Protokoll aus, das für den Netzwerkverkehr geöffnet werden soll.

ii. Protokoll — Wählen Sie aus der Liste den Protokolltyp aus.

iii. Portbereich — Geben Sie für eine benutzerdefinierte Regel eine Portnummer oder einen Portbereich ein. Stellen Sie sicher, dass die Portnummer bzw. der Portbereich den Port enthält, den Sie beim Erstellen des Clusters angegeben haben (Standard: 27017).

iv. Quelle — Gibt den Datenverkehr an, der Ihre Instance erreichen kann. Wählen Sie die Datenverkehrquelle aus der Liste aus. Wenn Sie Benutzerdefiniert wählen, geben Sie eine einzelne IP-Adresse oder einen IP-Adressbereich in CIDR-Notation an (z. B. 203.0.113). 5/32).

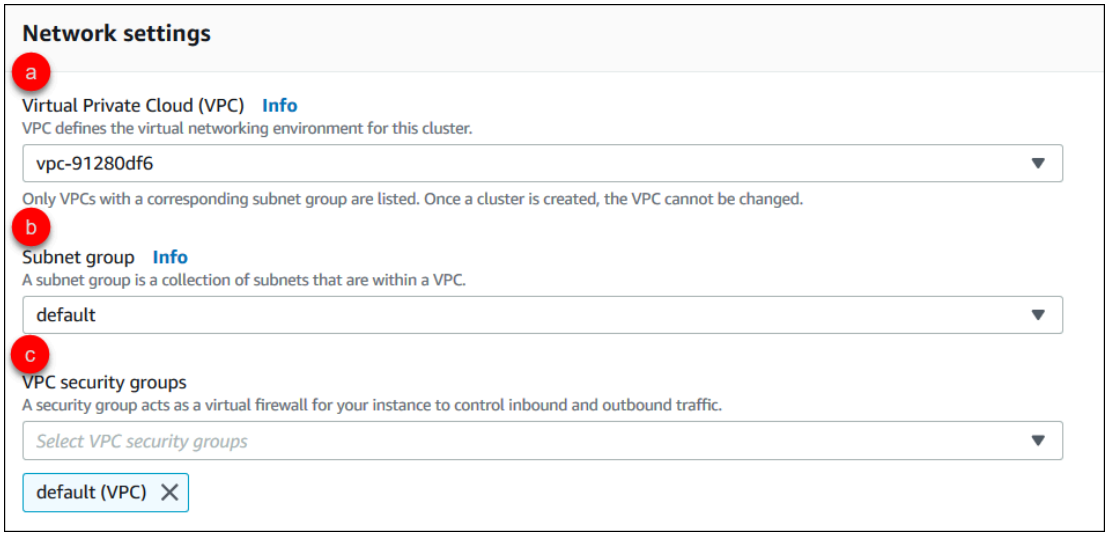
v. Beschreibung — Geben Sie eine Beschreibung für diese Regel ein.

vi. Wenn Sie die Regel fertig erstellt haben, wählen Sie Save (Speichern).

Einen Cluster erstellen: zusätzliche Konfigurationen

Wenn Sie die Standardeinstellungen für Ihren Cluster übernehmen möchten, können Sie die folgenden Schritte überspringen und Create cluster (Cluster erstellen) auswählen.

1. Vervollständigen Sie den Bereich Network settings (Netzwerkeinstellungen).

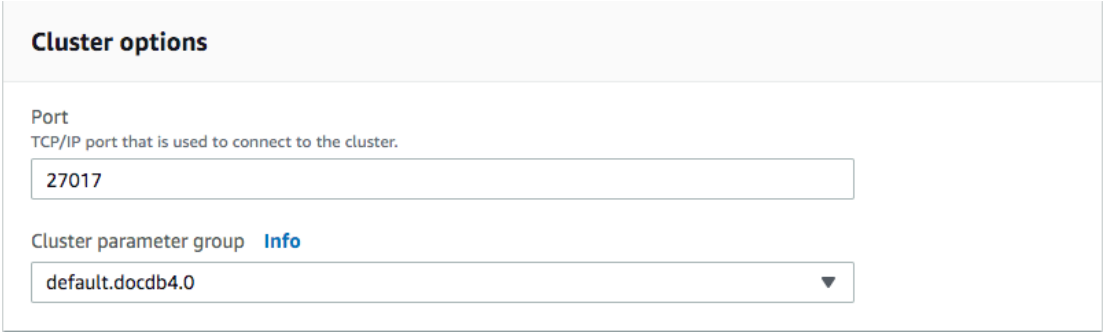


a. Virtual Private Cloud (VPC) — Wählen Sie in der Liste die Amazon-VPC aus, in der Sie diesen Cluster starten möchten.

b. Subnetzgruppe — Wählen Sie in der Liste die Subnetzgruppe aus, die Sie für diesen Cluster verwenden möchten.

c. VPC-Sicherheitsgruppen — Wählen Sie in der Liste die VPC-Sicherheitsgruppe für diesen Cluster aus.

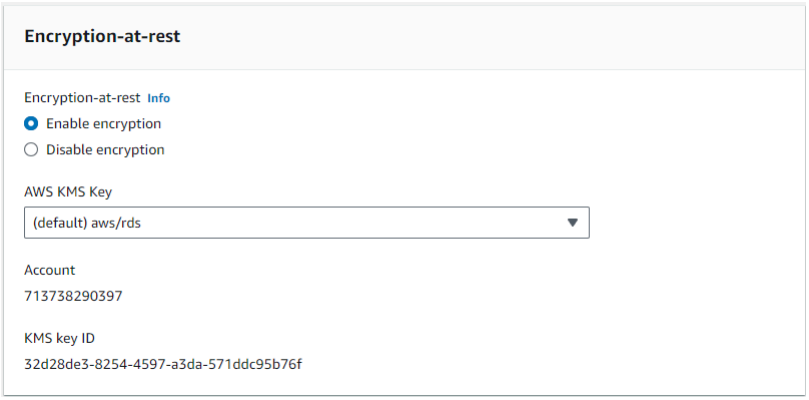
2. Vervollständigen Sie den Bereich Cluster options (Cluster-Optionen).



a. Datenbankport — Verwenden Sie die Aufwärts- und Abwärtspfeile, um den TCP/IP Port festzulegen, über den Anwendungen eine Verbindung zu Ihrer Instance herstellen.

b. Cluster-Parametergruppe — Wählen Sie in der Liste der Parametergruppen die Cluster-Parametergruppe für diesen Cluster aus.

3. Vervollständigen Sie den Bereich Encryption (Verschlüsselung).



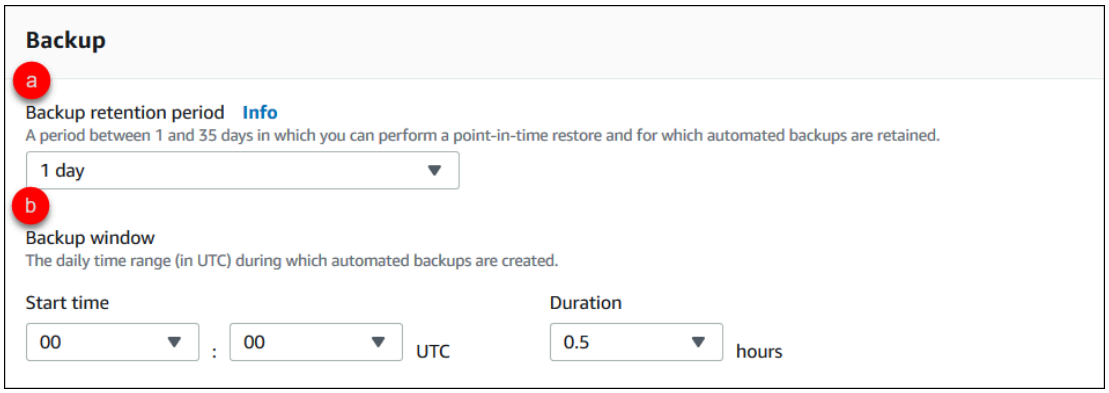
a. Encryption-at-rest— Wählen Sie eine der folgenden Optionen:

- Verschlüsselung aktivieren — Standard. Alle Daten im Ruhezustand werden verschlüsselt. Wenn Sie sich für die Verschlüsselung Ihrer Daten entscheiden, können Sie diese Aktion nicht rückgängig machen.
- Verschlüsselung deaktivieren — Ihre Daten sind nicht verschlüsselt.

b. AWS KMS-Schlüssel — Dieser ist nur verfügbar, wenn Sie Ihre Daten verschlüsseln. Wählen Sie aus der Liste den Schlüssel aus, den Sie für die Verschlüsselung der Daten in diesem Cluster verwenden möchten. Der Standardwert ist `(default) aws/rds`.

Wenn Sie Enter a key ARN (Einen Schlüssel-ARN eingeben) auswählen, müssen Sie einen Amazon-Ressourcenname (ARN) für den Schlüssel eingeben.

4. Vervollständigen Sie den Bereich Backup.



   a. Aufbewahrungszeitraum für Backup — Wählen Sie in der Liste die Anzahl der Tage aus, für die automatische Backups dieses Clusters aufbewahrt werden sollen, bevor sie gelöscht werden.

   b. Backup-Fenster — Legen Sie die tägliche Uhrzeit und Dauer fest, während der Amazon DocumentDB Backups dieses Clusters erstellen soll.

      i. Startzeit — Wählen Sie in der ersten Liste die Startzeit (UTC) für den Start Ihrer automatischen Backups aus. Wählen Sie in der zweiten Liste die Minute für den Beginn der automatischen Backups aus.

      ii. Dauer — Wählen Sie in der Liste die Anzahl der Stunden aus, die für die Erstellung automatischer Backups reserviert werden sollen.

5. Füllen Sie den Bereich Protokollexporte aus, indem Sie die Protokolltypen auswählen, die Sie in CloudWatch Protokolle exportieren möchten.

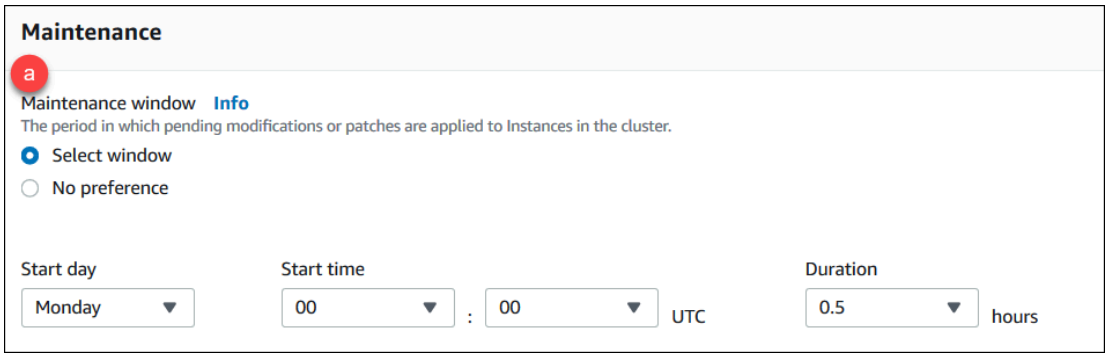
   - Audit-Logs — Wählen Sie diese Option, um den Export von Audit-Logs nach Amazon CloudWatch Logs zu ermöglichen. Wenn Sie Audit logs (Auditprotokolle), auswählen, müssen Sie `audit_logs` in der benutzerdefinierten Parametergruppe des Clusters aktivieren. Weitere Informationen finden Sie unter Amazon DocumentDB DocumentDB-Ereignisse prüfen.

- Profiler-Protokolle — Wählen Sie diese Option, um den Export von Operation-Profiler-Protokollen nach Amazon Logs zu aktivieren. CloudWatch Wenn Sie Profiler logs (Profiler-Protokolle) auswählen, müssen Sie auch die folgenden Parameter in der benutzerdefinierten Parametergruppe des Clusters ändern:

  - `profiler`— Eingestellt auf. `enabled`
  - `profiler_threshold_ms`— Auf einen Wert setzen, `[0-INT_MAX]` um den Schwellenwert für Profilerstellungsvorgänge festzulegen.
  - `profiler_sampling_rate`— Legen Sie einen Wert fest, um den Prozentsatz langsamer Vorgänge festzulegen`[0.0-1.0]`, für den ein Profil erstellt werden soll.

  Weitere Informationen finden Sie unter Profilierung von Amazon DocumentDB DocumentDB-Vorgängen.

6. Schließen Sie den Bereich Maintenance (Wartung) ab.



- Wählen Sie eine der folgenden Optionen aus:

  - Fenster auswählen — Sie können den Wochentag, die UTC-Startzeit und die Dauer angeben, für die Amazon DocumentDB Wartungsarbeiten an Ihrem Cluster durchführt.

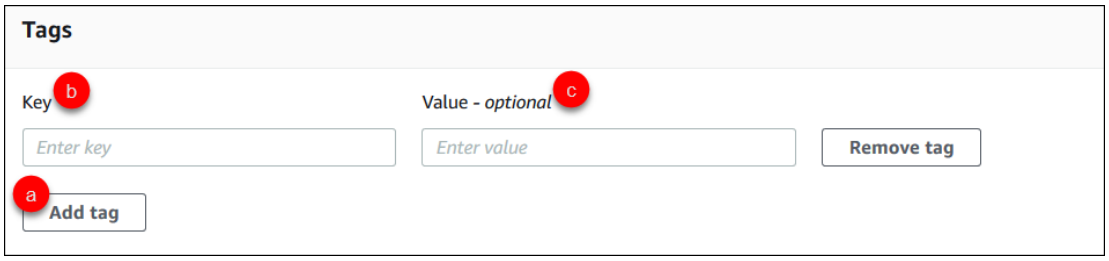
    a. Starttag — Wählen Sie in der Liste den Wochentag aus, an dem die Cluster-Wartung gestartet werden soll.

    b. Startzeit — Wählen Sie in den Listen die Stunde und Minute (UTC) aus, um mit der Wartung zu beginnen.

    c. Dauer — Wählen Sie in der Liste aus, wie viel Zeit für die Cluster-Wartung reserviert werden soll. Wenn die Wartung nicht innerhalb der angegebenen Zeit abgeschlossen werden kann, wird der Wartungsprozess über die angegebene Zeit hinaus bis zum Abschluss fortgesetzt.

- Keine Präferenz — Amazon DocumentDB wählt den Wochentag, die Startzeit und die Dauer für die Durchführung von Wartungsarbeiten.

7. Wenn Sie diesem Cluster ein oder mehrere Tags hinzufügen möchten, stellen Sie den Bereich Tags fertig.



Wiederholen Sie die folgenden Schritte für alle Tags, die Sie dem Cluster hinzufügen möchten. Sie können bis zu 10 in einem Cluster haben.

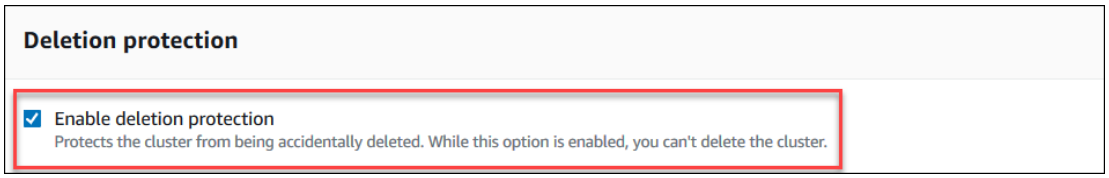
a. Wählen Sie Tags hinzufügen aus.

b. Geben Sie den Schlüssel des Tags ein.

c. Optional können Sie auch den Wert des Tags eingeben.

Klicken Sie zum Entfernen eines Tags auf Tag entfernen.

8. Der Löschschutz ist standardmäßig aktiviert, wenn Sie ein Cluster mit der Konsole erstellen. Deaktivieren Sie zum Ausschalten des Löschschutzes die Option Löschschutz aktivieren. Wenn diese Option aktiviert ist, verhindert der Löschschutz das Löschen eines Clusters. Wenn Sie einen löschgeschützten Cluster löschen möchten, müssen Sie zuerst den Cluster-Löschschutz deaktivieren.



Weitere Informationen über den Löschschutz finden Sie unter Löschen eines Amazon DocumentDB-Clusters.

9. Wählen Sie zum Erstellen des Clusters Cluster erstellen aus. Wählen Sie andernfalls Abbrechen.

Erstellen eines Clusters mit dem AWS CLI

Die folgenden Verfahren beschreiben, wie Sie den verwenden, um einen Amazon DocumentDB-Cluster AWS CLI zu starten und ein Amazon DocumentDB DocumentDB-Replikat zu erstellen.

Parameters

- **`--db-cluster-identifier`**—Erforderlich. Eine Zeichenfolge in Kleinbuchstaben, die diesen Cluster identifiziert.

  Einschränkungen bei der Benennung von Clustern:

  - Die Länge beträgt [1—63] Buchstaben, Zahlen oder Bindestriche.
  - Muss mit einem Buchstaben beginnen.
  - Darf nicht mit einem Bindestrich enden oder zwei aufeinanderfolgende Bindestriche enthalten.
  - Muss für alle Cluster (in Amazon RDS, Amazon Neptune und Amazon DocumentDB) pro AWS Konto und Region eindeutig sein.

- **`--engine`**—Erforderlich. Der Wert muss **`docdb`** sein.
- **`--deletion-protection | --no-deletion-protection`**— Fakultativ. Der aktivierte Löschschutz verhindert, dass ein Cluster gelöscht wird. Wenn Sie die verwenden AWS CLI, ist der Löschschutz standardmäßig deaktiviert.

  Weitere Informationen über den Löschschutz finden Sie unter Löschen eines Amazon DocumentDB-Clusters.
- **`--storage-type standard | iopt1`**— Fakultativ. Standard: **`standard`**. Die Speicherkonfiguration des Clusters. Gültige Werte sind `standard` (Standard) oder `iopt1` (I/O-optimized).
- **`--master-username`**—Erforderlich. Der Benutzername für die Authentifizierung des Benutzers.

  Namenseinschränkungen für Benutzer:

  - Die Länge beträgt [1 bis 63] alphanumerische Zeichen.
  - Muss mit einem Buchstaben beginnen.
  - Darf kein Wort sein, das von der Datenbank-Engine reserviert ist.

- **`--master-user-password`**— Fakultativ. Das Passwort für die Authentifizierung des Benutzers.

Einschränkungen für Hauptpasswort:

- Länge beträgt [8–100] druckbare ASCII-Zeichen.
- Es können alle druckbaren ASCII-Zeichen mit Ausnahme der folgenden verwendet werden:
  - **/** (Schrägstrich)
  - **"** (doppeltes Anführungszeichen)
  - **@** ('At'-Symbol)

- **`--manage-master-user-password`**—Fakultativ. Amazon DocumentDB generiert das Masterbenutzerkennwort und verwaltet es während seines gesamten Lebenszyklus in Secrets Manager.

Weitere Parameter finden Sie unter CreateDBCluster.

Um einen Amazon DocumentDB-Cluster mit dem zu starten AWS CLI

Um einen Amazon DocumentDB-Cluster zu erstellen, rufen Sie den auf `create-db-cluster` AWS CLI. Der folgende AWS CLI Befehl erstellt einen Amazon DocumentDB-Cluster `sample-cluster` mit dem Namen und aktiviertem Löschschutz. Weitere Informationen zum Löschschutz finden Sie unterLöschen eines Amazon DocumentDB-Clusters.

Außerdem `--engine-version` ist dies ein optionaler Parameter, der standardmäßig die neueste Hauptversion der Engine verwendet. Die aktuelle Standard-Engine-Version ist 5.0.0 (Hinweis: Amazon DocumentDB 8.0 ist verfügbar, muss aber explizit angegeben werden). Wenn neue Hauptversionen der Engine veröffentlicht werden, `--engine-version` wird die Standard-Engine-Version für aktualisiert, sodass sie die letzte Hauptversion der Engine widerspiegelt. Daher empfehlen wir für Produktionsworkloads, insbesondere solche, die von Skripten, Automatisierung oder CloudFormation Vorlagen abhängig sind, die Angabe der `--engine-version` beabsichtigten Hauptversion ausdrücklich.

> **Note**
>
> Wenn ein `db-subnet-group-name` oder nicht angegeben `vpc-security-group-id` ist, verwendet Amazon DocumentDB die Standard-Subnetzgruppe und die Amazon VPC-Sicherheitsgruppe für die angegebene Region.

Für Linux, macOS oder Unix:

```
aws docdb create-db-cluster \
      --db-cluster-identifier sample-cluster \
      --engine docdb \
      --engine-version 5.0.0 \
      --deletion-protection \
      --master-username masteruser \
      --master-user-password password
```

Für Windows:

```
aws docdb create-db-cluster ^
      --db-cluster-identifier sample-cluster ^
      --engine docdb ^
      --engine-version 5.0.0 ^
      --deletion-protection ^
      --master-username masteruser ^
      --master-user-password password
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus (JSON-Format).

```
{
    "DBCluster": {
        "StorageEncrypted": false,
        "DBClusterMembers": [],
        "Engine": "docdb",
        "DeletionProtection" : "enabled",
        "ClusterCreateTime": "2018-11-26T17:15:19.885Z",
        "DBSubnetGroup": "default",
        "EngineVersion": "5.0.0",
        "MasterUsername": "masteruser",
        "BackupRetentionPeriod": 1,
        "DBClusterArn": "arn:aws:rds:us-east-1:123456789012:cluster:sample-cluster",
        "DBClusterIdentifier": "sample-cluster",
        "MultiAZ": false,
        "DBClusterParameterGroup": "default.docdb5.0",
        "PreferredBackupWindow": "09:12-09:42",
        "DbClusterResourceId": "cluster-KQSGI4MHU4NTDDRVNLNTU7XVAY",
        "PreferredMaintenanceWindow": "tue:04:17-tue:04:47",
        "Port": 27017,
        "Status": "creating",
```

```
        "ReaderEndpoint": "sample-cluster.cluster-ro-sfcrlcjcoroz.us-
east-1.docdb.amazonaws.com",
        "AssociatedRoles": [],
        "HostedZoneId": "ZNKXTT8WH85VW",
        "VpcSecurityGroups": [
            {
                "VpcSecurityGroupId": "sg-77186e0d",
                "Status": "active"
            }
        ],
        "AvailabilityZones": [
            "us-east-1a",
            "us-east-1c",
            "us-east-1e"
        ],
        "Endpoint": "sample-cluster.cluster-sfcrlcjcoroz.us-east-1.docdb.amazonaws.com"
    }
}
```

Die Erstellung des Clusters dauert mehrere Minuten. Sie können das AWS-Managementkonsole oder verwenden AWS CLI , um den Status Ihres Clusters zu überwachen. Weitere Informationen finden Sie unter Den Status eines Amazon DocumentDB-Clusters überwachen.

> **Important**
>
> Wenn Sie den verwenden AWS CLI , um einen Amazon DocumentDB-Cluster zu erstellen, werden keine Instances erstellt. Daher müssen Sie explizit eine primäre Instance und alle benötigten Replikat-Instances anlegen. Sie können entweder die Konsole oder AWS CLI zum Erstellen der Instances verwenden. Weitere Informationen finden Sie unter Hinzufügen einer Amazon DocumentDB DocumentDB-Instance zu einem Cluster.

Weitere Informationen finden Sie `CreateDBCluster`in der Amazon DocumentDB DocumentDB-API-Referenz.

Beschreibung von Amazon DocumentDB-Clustern

Sie können entweder die Amazon DocumentDB Management Console oder die verwenden, AWS CLI um Details wie Verbindungsendpunkte, Sicherheitsgruppen, VPCs und Parametergruppen zu Ihren Amazon DocumentDB-Clustern anzuzeigen.

Weitere Informationen finden Sie hier:

- Den Status eines Amazon DocumentDB-Clusters überwachen
- Die Endpunkte eines Clusters finden

Using the AWS-Managementkonsole

Gehen Sie wie folgt vor, um die Details eines bestimmten Amazon DocumentDB-Clusters mithilfe der Konsole anzuzeigen.

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Klicken Sie im Navigationsbereich auf Cluster.

   > **Tip**
   >
   > Wenn der Navigationsbereich auf der linken Seite des Bildschirms nicht angezeigt wird, wählen Sie links oben auf der Seite das Menüsymbol (≡) aus.

3. Wählen Sie in der Liste der Cluster den Namen des Clusters aus, dessen Details Sie sehen möchten. Die Informationen über den Cluster sind in die folgenden Gruppierungen unterteilt:

   - Zusammenfassung — Allgemeine Informationen über den Cluster, einschließlich der Engine-Version, des Cluster-Status, ausstehender Wartungsarbeiten und des Status der zugehörigen Parametergruppe.
   - Konnektivität und Sicherheit — Der Abschnitt Connect listet Verbindungsendpunkte auf, um mit der Mongo-Shell oder mit einer Anwendung eine Verbindung zu diesem Cluster herzustellen. Im Abschnitt Sicherheitsgruppen werden die Sicherheitsgruppen aufgeführt, die diesem Cluster zugeordnet sind, sowie ihre VPC-ID und Beschreibungen.
   - Konfiguration — Im Abschnitt Cluster-Details werden Details zum Cluster aufgeführt, einschließlich des Amazon-Ressourcennamens (ARN), des Endpunkts und der Parametergruppe des Clusters. Außerdem werden die Sicherungsinformationen, Wartungsdetails sowie Sicherheits- und Netzwerkeinstellungen des Clusters aufgelistet. Im Abschnitt Cluster-Instances werden die Instances aufgeführt, die zu diesem Cluster gehören, mit dem Status der einzelnen Instance-Rollen und Cluster-Parametergruppen.

- Überwachung — Die Amazon CloudWatch Logs-Metriken für diesen Cluster. Weitere Informationen finden Sie unter Überwachen von Amazon DocumentDB mit CloudWatch.
- Ereignisse und Tags — Im Abschnitt Aktuelle Ereignisse werden die jüngsten Ereignisse für diesen Cluster aufgeführt. Amazon DocumentDB zeichnet Ereignisse auf, die sich auf Ihre Cluster, Instances, Snapshots, Sicherheitsgruppen und Cluster-Parametergruppen beziehen. Zu diesen Informationen gehören Datum, Uhrzeit und Nachricht, die jedem Ereignis zugeordnet sind. Der Abschnitt Tags listet die an diesen Cluster angehängten Tags auf.

Using the AWS CLI

Um die Details Ihrer Amazon DocumentDB-Cluster mithilfe von anzuzeigen AWS CLI, verwenden Sie den `describe-db-clusters` Befehl, wie in den folgenden Beispielen gezeigt. Weitere Informationen finden Sie `DescribeDBClusters`in der Amazon DocumentDB Resource Management API-Referenz.

> **Note**
>
> Für bestimmte Verwaltungsfunktionen wie Cluster- und Instance-Lebenszyklusmanagement nutzt Amazon DocumentDB Betriebstechnologie, die mit Amazon RDS gemeinsam genutzt wird. Der `filterName=engine,Values=docdb` Filterparameter gibt nur Amazon DocumentDB-Cluster zurück.

Example

Beispiel 1: Alle Amazon DocumentDB-Cluster auflisten

Der folgende AWS CLI Code listet die Details für alle Amazon DocumentDB-Cluster in einer Region auf.

```
aws docdb describe-db-clusters --filter Name=engine,Values=docdb
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus.

```
{
    "DBClusters": [
        {
```

```
            "AvailabilityZones": [
                "us-east-1c",
                "us-east-1b",
                "us-east-1a"
            ],
            "BackupRetentionPeriod": 1,
            "DBClusterIdentifier": "sample-cluster-1",
            "DBClusterParameterGroup": "sample-parameter-group",
            "DBSubnetGroup": "default",
            "Status": "available",
            ...
        },
        {
            "AvailabilityZones": [
                "us-east-1c",
                "us-east-1b",
                "us-east-1a"
            ],
            "BackupRetentionPeriod": 1,
            "DBClusterIdentifier": "sample-cluster-2",
            "DBClusterParameterGroup": "sample-parameter-group",
            "DBSubnetGroup": "default",
            "Status": "available",
            ...
        },
        {
            "AvailabilityZones": [
                "us-east-1c",
                "us-east-1b",
                "us-east-1a"
            ],
            "BackupRetentionPeriod": 1,
            "DBClusterIdentifier": "sample-cluster-3",
            "DBClusterParameterGroup": "sample-parameter-group",
            "DBSubnetGroup": "default",
            "Status": "available",
            ...
        }
    ]
}
```

Example

Beispiel 2: Alle Details für einen bestimmten Amazon DocumentDB-Cluster auflisten

Der folgende AWS CLI Code listet die Details für den Cluster `sample-cluster` auf.

Für Linux, macOS oder Unix:

```
aws docdb describe-db-clusters \
   --filter Name=engine,Values=docdb \
   --db-cluster-identifier sample-cluster
```

Für Windows:

```
aws docdb describe-db-clusters ^
   --filter Name=engine,Values=docdb ^
   --db-cluster-identifier sample-cluster
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus.

```
{
    "DBClusters": [
        {
            "AllocatedStorage": 1,
            "AvailabilityZones": [
                "us-east-1c",
                "us-east-1a",
                "us-east-1d"
            ],
            "BackupRetentionPeriod": 2,
            "DBClusterIdentifier": "sample-cluster",
            "DBClusterParameterGroup": "sample-parameter-group",
            "DBSubnetGroup": "default",
            "Status": "available",
            "EarliestRestorableTime": "2023-11-07T22:34:08.148000+00:00",
            "Endpoint": "sample-cluster.node.us-east-1.amazon.com",
            "ReaderEndpoint": "sample-cluster.node.us-east-1.amazon.com",
            "MultiAZ": false,
            "Engine": "docdb",
            "EngineVersion": "5.0.0",
            "LatestRestorableTime": "2023-11-10T07:21:16.772000+00:00",
            "Port": 27017,
            "MasterUsername": "chimeraAdmin",
            "PreferredBackupWindow": "22:22-22:52",
            "PreferredMaintenanceWindow": "sun:03:01-sun:03:31",
            "ReadReplicaIdentifiers": [],
            "DBClusterMembers": [
```

```
                {
                    "DBInstanceIdentifier": "sample-instance-1",
                    "IsClusterWriter": true,
                    "DBClusterParameterGroupStatus": "in-sync",
                    "PromotionTier": 1
                },
                {
                    "DBInstanceIdentifier": "sample-instance-2",
                    "IsClusterWriter": true,
                    "DBClusterParameterGroupStatus": "in-sync",
                    "PromotionTier": 1
                },

            ],
            "VpcSecurityGroups": [
                {
                    "VpcSecurityGroupId": "sg-9084c2ec",
                    "Status": "active"
                }
            ],
            "HostedZoneId": "Z06853723JYKYBXTJ49RB",
            "StorageEncrypted": false,
            "DbClusterResourceId": "cluster-T4LGLANHVAPGQYYULWUDKLVQL4",
            "DBClusterArn": "arn:aws:rds:us-east-1:123456789012:cluster:sample-
cluster",
            "AssociatedRoles": [],
            "IAMDatabaseAuthenticationEnabled": false,
            "ClusterCreateTime": "2023-11-06T18:05:41.568000+00:00",
            "EngineMode": "provisioned",
            "DeletionProtection": false,
            "HttpEndpointEnabled": false,
            "CopyTagsToSnapshot": false,
            "CrossAccountClone": false,
            "DomainMemberships": [],
            "TagList": [],
            "StorageType": "iopt1",
            "AutoMinorVersionUpgrade": false,
            "NetworkType": "IPV4",
            "IOOptimizedNextAllowedModificationTime":
 "2023-12-07T18:05:41.580000+00:00"
        }
    ]
}
```

Example

Beispiel 3: Spezifische Details für einen Amazon DocumentDB-Cluster auflisten

Um eine Teilmenge der Cluster-Details mithilfe von aufzulisten AWS CLI, fügen Sie eine hinzu, die `--query` angibt, welche Cluster-Mitglieder der `describe-db-clusters` Vorgang auflisten soll. Der `--db-cluster-identifier`-Parameter ist der Bezeichner für den jeweiligen Cluster, dessen Details Sie anzeigen möchten. Weitere Informationen zu Abfragen finden Sie unter So filtern Sie die Ausgabe mit der *`--query`* Option im AWS Command Line Interface Benutzerhandbuch.

Das folgende Beispiel listet die Instances in einem Amazon DocumentDB-Cluster auf.

Für Linux, macOS oder Unix:

```
aws docdb describe-db-clusters \
    --filter Name=engine,Values=docdb \
    --db-cluster-identifier sample-cluster \
    --query 'DBClusters[*].[DBClusterMembers]'
```

Für Windows:

```
aws docdb describe-db-clusters ^
    --filter Name=engine,Values=docdb ^
    --db-cluster-identifier sample-cluster ^
    --query 'DBClusters[*].[DBClusterMembers]'
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus.

```
[
    [
        [
            {
                "DBInstanceIdentifier": "sample-instance-1",
                "IsClusterWriter": true,
                "DBClusterParameterGroupStatus": "in-sync",
                "PromotionTier": 1
            },
            {
                "DBInstanceIdentifier": "sample-instance-2",
                "IsClusterWriter": false,
```

```
                "DBClusterParameterGroupStatus": "in-sync",
                "PromotionTier": 1
            }
        ]
    ]
]
```

Ändern eines Amazon DocumentDB-Clusters

Nur Cluster, die sich im Status available befinden, können geändert werden. Ein angehaltener Cluster kann nicht geändert werden. Wenn der Cluster angehalten ist, starten Sie zuerst den Cluster, warten Sie, bis der Cluster verfügbar wird, und nehmen Sie dann die gewünschten Änderungen vor. Weitere Informationen finden Sie unter Einen Amazon DocumentDB-Cluster stoppen und starten.

Using the AWS-Managementkonsole

Gehen Sie wie folgt vor, um einen bestimmten Amazon DocumentDB-Cluster mithilfe der Konsole zu ändern.

So ändern Sie einen Amazon-DocumentDB-Cluster

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Klicken Sie im Navigationsbereich auf Cluster.

   > **Tip**
   >
   > Wenn der Navigationsbereich auf der linken Seite des Bildschirms nicht angezeigt wird, wählen Sie links oben auf der Seite das Menüsymbol (≡) aus.

3. Geben Sie den Cluster an, den Sie ändern möchten, indem Sie die Schaltfläche links neben dem Namen des Clusters auswählen.
4. Wählen Sie Actions (Aktionen) und dann Modify (Ändern) aus.
5. Nehmen Sie im Bereich Modify Cluster: <cluster-name> (Cluster ändern: <cluster-name>) die gewünschten Änderungen vor. Sie können in den folgenden Bereichen Änderungen durchführen:

- Clusterspezifikationen — Der Name des Clusters, die Sicherheitsgruppen und die Verwaltung der Anmeldeinformationen.
- Cluster-Speicherkonfiguration — Der Datenspeichermodus des Clusters. Wählen Sie zwischen Standard und I/O-Optimized Konfiguration.
- Clusteroptionen — Der Port und die Parametergruppe des Clusters.
- Backup — Der Aufbewahrungszeitraum und das Backup-Fenster des Clusters.
- Protokollexporte — Aktiviert oder deaktiviert den Export von Audit- oder Profiler-Protokollen.
- Wartung — Legt das Wartungsfenster des Clusters fest.
- Löschschutz — Aktiviert oder deaktiviert den Löschschutz auf dem Cluster. Der Löschschutz ist standardmäßig aktiviert.

6. Wenn Sie fertig sind, wählen Sie Continue (Weiter) aus, um eine Zusammenfassung Ihrer Änderungen anzuzeigen.
7. Wenn Sie mit den Änderungen zufrieden sind, können Sie Modify cluster (Cluster ändern) auswählen, um den Cluster zu ändern. Alternativ können Sie Back (Zurück) oder Cancel (Abbrechen) wählen, um die Änderungen zu bearbeiten oder abzubrechen.

Es dauert einige Minuten, bis Ihre Änderungen übernommen werden. Sie können den Cluster nur verwenden, wenn sein Status available ist. Sie können den Status des Clusters über die Konsole oder AWS CLIüberwachen. Weitere Informationen finden Sie unter Den Status eines Amazon DocumentDB-Clusters überwachen.

Using the AWS CLI

Verwenden Sie die `modify-db-cluster`-Operation, um den angegebenen Cluster mit der AWS CLI zu ändern. Weitere Informationen finden Sie `ModifyDBCluster`in der Amazon DocumentDB DocumentDB-API-Referenz.

Parameters

- **`--db-cluster-identifier`**—Erforderlich. Die ID des Amazon DocumentDB-Clusters, den Sie ändern werden.
- **`--backup-retention-period`**— Fakultativ. Die Anzahl von Tagen, über die automatische Backups aufbewahrt werden. Gültige Werte sind 1—35.

- **`--storage-type`**— Fakultativ. Die Speicherkonfiguration des Clusters. Gültige Werte sind `standard` (Standard) oder `iopt1` (I/O-optimized).
- **`--db-cluster-parameter-group-name`**— Fakultativ. Der Name der Cluster-Parametergruppe, die für den Cluster verwendet werden soll.
- **`--manage-master-user-password`**—Fakultativ. Amazon DocumentDB generiert das Masterbenutzerkennwort und verwaltet es während seines gesamten Lebenszyklus in Secrets Manager.
- **`--rotate-master-user-password`**— Fakultativ. Secrets Manager generiert eine neue geheime Version für das bestehende Geheimnis. Die neue Version des Secrets enthält das neue primäre Benutzerkennwort. Amazon DocumentDB ändert das primäre Benutzerkennwort für den Cluster so, dass es mit dem Passwort für die neue geheime Version übereinstimmt.

  Sie müssen die **`--apply-immediately`** Option angeben, wenn Sie das primäre Passwort ändern.
- **`--master-user-password`**— Fakultativ. Das neue Passwort für den primären Datenbankbenutzer.

  Passwortbeschränkungen:

  - Die Länge beträgt [8—100] druckbare ASCII-Zeichen.
  - Es können alle druckbaren ASCII-Zeichen mit Ausnahme der folgenden verwendet werden:
    - **`/`** (Schrägstrich)
    - **`"`** (doppeltes Anführungszeichen)
    - **`@`** ('At'-Symbol)
- **`--new-db-cluster-identifier`**— Fakultativ. Die neue Cluster-ID für den Cluster beim Umbenennen eines Clusters. Dieser Wert wird als Zeichenfolge in Kleinbuchstaben gespeichert.

  Benennungseinschränkungen:

  - Die Länge beträgt [1—63] Buchstaben, Zahlen oder Bindestriche.
  - Muss mit einem Buchstaben beginnen.
  - Darf nicht mit einem Bindestrich enden oder zwei aufeinanderfolgende Bindestriche enthalten.
  - Muss für alle Cluster in Amazon RDS, Amazon Neptune und Amazon DocumentDB pro AWS-Konto Region eindeutig sein.

- **`--preferred-backup-window`**— Fakultativ. Der tägliche Zeitbereich, in dem automatisierte Backups erstellt werden, in Universal Coordinated Time (UTC).
  - Format: `hh24:mm-hh24:mm`
- **`--preferred-maintenance-window`**—Fakultativ. Der wöchentliche Zeitbereich, in dem Systemwartungen stattfinden können, in UTC.
  - Format: `ddd:hh24:mm-ddd:hh24:mm`
  - Gültige Tage: `Sun`, `Mon`, `Tue`, `Wed`, `Thu`, `Fri` und `Sat`.
- **`--deletion-protection`**oder **`--no-deletion-protection`** — Optional. Gibt an, ob der Löschschutz für diesen Cluster aktiviert werden soll. Der Löschschutz verhindert, dass ein Cluster versehentlich gelöscht wird, solange der Cluster-Löschschutz nicht deaktiviert wurde. Weitere Informationen finden Sie unter Löschen eines Amazon DocumentDB-Clusters.
- **`--apply-immediately`**oder **`--no-apply-immediately`** — Verwenden Sie diese Option`--apply-immediately`, um die Änderung sofort vorzunehmen. Verwenden Sie `--no-apply-immediately`, um die Änderung während des nächsten Wartungsfensters Ihres Clusters vorzunehmen.

Example

Der folgende Code ändert die Aufbewahrungsfrist für das Backup für den Cluster `sample-cluster`.

Für Linux, macOS oder Unix:

```
aws docdb modify-db-cluster \
       --db-cluster-identifier sample-cluster \
       --apply-immediately \
       --backup-retention-period 7
```

Für Windows:

```
aws docdb modify-db-cluster ^
       --db-cluster-identifier sample-cluster ^
       --apply-immediately ^
       --backup-retention-period 7
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus.

```
{
```

```
    "DBCluster": {
        "BackupRetentionPeriod": 7,
        "DbClusterResourceId": "cluster-VDP53QEWST7YHM36TTXOPJT5YE",
        "Status": "available",
        "DBClusterMembers": [
            {
                "PromotionTier": 1,
                "DBClusterParameterGroupStatus": "in-sync",
                "DBInstanceIdentifier": "sample-cluster-instance",
                "IsClusterWriter": true
            }
        ],
        "ReadReplicaIdentifiers": [],
        "AvailabilityZones": [
            "us-east-1b",
            "us-east-1c",
            "us-east-1a"
        ],
        "ReaderEndpoint": "sample-cluster.cluster-ro-ctevjxdlur57.us-
east-1.rds.amazonaws.com",
        "DBClusterArn": "arn:aws:rds:us-east-1:123456789012:cluster:sample-cluster",
        "PreferredMaintenanceWindow": "sat:09:51-sat:10:21",
        "EarliestRestorableTime": "2018-06-17T00:06:19.374Z",
        "StorageEncrypted": false,
        "MultiAZ": false,
        "AssociatedRoles": [],
        "MasterUsername": "<your-master-user-name>",
        "DBClusterIdentifier": "sample-cluster",
        "VpcSecurityGroups": [
            {
                "Status": "active",
                "VpcSecurityGroupId": "sg-77186e0d"
            }
        ],
        "HostedZoneId": "Z2SUY0A1719RZT",
        "LatestRestorableTime": "2018-06-18T21:17:05.737Z",
        "AllocatedStorage": 1,
        "Port": 27017,
        "Engine": "docdb",
        "DBClusterParameterGroup": "default.docdb3.4",
        "Endpoint": "sample-cluster.cluster-ctevjxdlur57.us-
east-1.rds.amazonaws.com",
        "DBSubnetGroup": "default",
        "PreferredBackupWindow": "00:00-00:30",
```

```
        "EngineVersion": "3.4",
        "ClusterCreateTime": "2018-06-06T19:25:47.991Z",
        "IAMDatabaseAuthenticationEnabled": false
    }
}
```

Es dauert einige Minuten, bis Ihre Änderungen übernommen werden. Sie können den Cluster nur verwenden, wenn sein Status available ist. Sie können den Status des Clusters über die Konsole oder AWS CLIüberwachen. Weitere Informationen finden Sie unter Den Status eines Amazon DocumentDB-Clusters überwachen.

Ermittlung ausstehender Wartungsarbeiten

Sie können feststellen, ob Sie über die neueste Version der Amazon DocumentDB DocumentDB-Engine verfügen, indem Sie feststellen, ob die Cluster-Wartung noch aussteht.

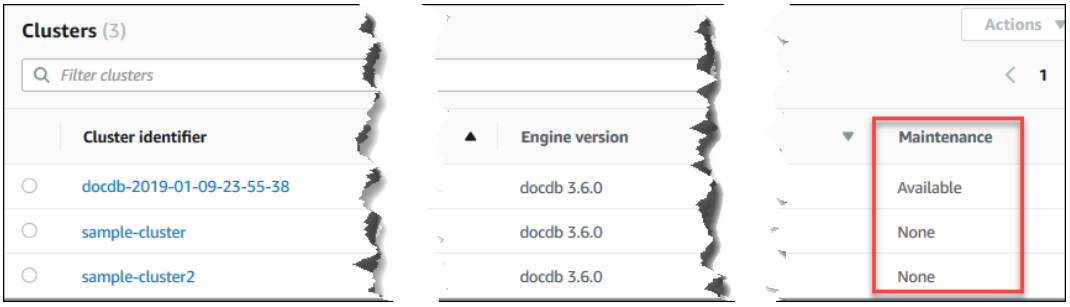
Using the AWS-Managementkonsole

Sie können den verwenden AWS-Managementkonsole , um festzustellen, ob für einen Cluster noch Wartungsarbeiten anstehen.

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Klicken Sie im Navigationsbereich auf Cluster.

   > **Tip**
   >
   > Wenn der Navigationsbereich auf der linken Seite des Bildschirms nicht angezeigt wird, wählen Sie links oben auf der Seite das Menüsymbol (≡) aus.

3. Überprüfen Sie die Spalte Maintenance (Wartung), um festzustellen, ob ein Cluster eine ausstehende Wartung hat.



None (Keine) bedeutet, dass auf dem Cluster die neueste Engine-Version ausgeführt wird. Available (Verfügbar) bedeutet, dass der Cluster noch nicht gewartet wurde. Somit ist ein Engine-Upgrade erforderlich.

4. Wenn Ihr Cluster noch nicht gewartet wurde, fahren Sie mit den Schritten unter Durchführen eines Patch-Updates für die Engine-Version eines Clusters fort.

Using the AWS CLI

Sie können den verwenden AWS CLI , um festzustellen, ob ein Cluster über die neueste Engine-Version verfügt, indem Sie den `describe-pending-maintenance-actions` Vorgang mit den folgenden Parametern verwenden.

Parameters

- **`--resource-identifier`**— Optional. Der ARN der Ressource (Cluster). Wenn dieser Parameter weggelassen wird, werden ausstehende Wartungsaktionen für alle Cluster aufgelistet.
- **`--region`**—Fakultativ. Die AWS-Region, in der Sie diese Operation durchführen möchten (z. B. `us-east-1`).

Example

Für Linux, macOS oder Unix:

```
aws docdb describe-pending-maintenance-actions \
   --resource-identifier arn:aws:rds:us-east-1:123456789012:cluster:sample-cluster \
   --region us-east-1
```

Für Windows:

```
aws docdb describe-pending-maintenance-actions ^
   --resource-identifier arn:aws:rds:us-east-1:123456789012:cluster:sample-cluster ^
   --region us-east-1
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus.

```
{
    "PendingMaintenanceActions": [
        {
            "ResourceIdentifier": "arn:aws:rds:us-
east-1:123456789012:cluster:sample-cluster",
            "PendingMaintenanceActionDetails": [
                {
                    "Description": "New feature",
                    "Action": "db-upgrade",
                    "ForcedApplyDate": "2019-02-25T21:46:00Z",
                    "AutoAppliedAfterDate": "2019-02-25T07:41:00Z",
                    "CurrentApplyDate": "2019-02-25T07:41:00Z"
                }
            ]
        }
    ]
}
```

Wenn Ihr Cluster noch nicht gewartet wurde, fahren Sie mit den Schritten unter Durchführen eines Patch-Updates für die Engine-Version eines Clusters fort.

Durchführen eines Patch-Updates für die Engine-Version eines Clusters

In diesem Abschnitt erklären wir, wie Sie ein Patch-Update mit dem AWS-Managementkonsole oder dem bereitstellen AWS CLI. Ein Patch-Update ist ein Update innerhalb derselben Engine-Version (z. B. die Aktualisierung einer 3.6-Engine-Version auf eine neuere 3.6-Engine-Version). Sie können es sofort oder während des nächsten Wartungsfensters Ihres Clusters aktualisieren. Informationen darüber, ob Ihre Engine aktualisiert werden muss, finden Sie unterErmittlung ausstehender Wartungsarbeiten. Beachten Sie, dass es bei der Installation des Updates zu einigen Ausfallzeiten auf Ihrem Cluster kommen kann.

> **Note**
>
> Wenn Sie versuchen, ein Upgrade von einer Hauptversion der Engine auf eine andere durchzuführen, z. B. 3.6 auf 5.0 oder 5.0 auf 8.0, finden Sie entweder Direktes Upgrade der Hauptversion von Amazon DocumentDB oderAktualisieren Ihres Amazon DocumentDB-Clusters mit AWS Database Migration Service.

Es gibt zwei Konfigurationsanforderungen, um die neuesten Patch-Updates für die Engine-Version eines Clusters zu erhalten:

- Der Cluster-Status muss available (verfügbar) lauten.
- Der Cluster muss eine ältere Engine-Version ausführen.

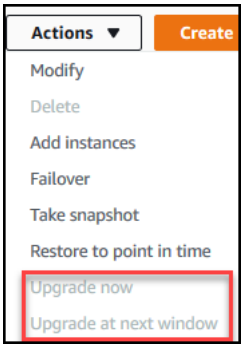
Using the AWS-Managementkonsole

Das folgende Verfahren wendet mithilfe der Konsole Patch-Updates auf die Engine-Version Ihres Clusters an. Sie haben die Möglichkeit, das Update sofort oder während des nächsten Wartungsfensters Ihres Clusters durchzuführen.

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Klicken Sie im Navigationsbereich auf Cluster. Wählen Sie in der Liste der Cluster die Schaltfläche links neben dem Cluster aus, den Sie upgraden möchten. Der Cluster-Status muss available (verfügbar) lauten.

   > **Tip**
   >
   > Wenn der Navigationsbereich auf der linken Seite des Bildschirms nicht angezeigt wird, wählen Sie links oben auf der Seite das Menüsymbol (≡) aus.

3. Wählen Sie im Menü Actions (Aktionen) eine der folgenden Optionen aus. Diese Menüoptionen sind nur auswählbar, wenn der ausgewählte Cluster nicht die neueste Engine-Version ausführt.



- Jetzt aktualisieren — Startet sofort den Upgrade-Vorgang. Ihr Cluster ist eine zeitlang offline, während er auf die neueste Engine-Version aktualisiert wird.
- Upgrade im nächsten Fenster — Initiiert den Upgrade-Vorgang während des nächsten Wartungsfensters des Clusters. Ihr Cluster ist eine zeitlang offline, während er auf die neueste Engine-Version aktualisiert wird.

4. Wenn sich das Bestätigungsfenster öffnet, wählen Sie eine der folgenden Optionen aus:
   - Upgrade — Um Ihren Cluster gemäß dem im vorherigen Schritt ausgewählten Zeitplan auf die neueste Engine-Version zu aktualisieren.
   - Abbrechen — Um das Engine-Upgrade des Clusters abzubrechen und mit der aktuellen Engine-Version des Clusters fortzufahren.

Using the AWS CLI

Sie können Patch-Updates auf Ihren Cluster anwenden, indem Sie den `apply-pending-maintenance-action` Vorgang AWS CLI und mit den folgenden Parametern verwenden.

Parameters

- **`--resource-identifier`**—Erforderlich. Der ARN des Amazon DocumentDB-Clusters, den Sie aktualisieren möchten.
- **`--apply-action`**—Erforderlich. Die folgenden Werte sind zulässig. Verwenden Sie `db-upgrade`, um Ihre Cluster-Engine-Version upzugraden.
  - **`db-upgrade`**
  - **`system-update`**
- **`--opt-in-type`**—Erforderlich. Die folgenden Werte sind zulässig.
  - `immediate`— Wenden Sie die Wartungsmaßnahme sofort an.
  - `next-maintenance`— Wendet die Wartungsaktion im nächsten Wartungsfenster an.

- `undo-opt-in`— Stornieren Sie alle bestehenden `next-maintenance` Opt-In-Anfragen.

Example

Mit dem folgenden Beispiel-Patch wird die Engine-Version von `sample-cluster` auf Version 4.0.0 aktualisiert.

Für Linux, macOS oder Unix:

```
aws docdb apply-pending-maintenance-action \
   --resource-identifier arn:aws:rds:us-east-1:123456789012\:cluster:sample-cluster
 \
   --apply-action db-upgrade \
   --opt-in-type immediate
```

Für Windows:

```
aws docdb apply-pending-maintenance-action ^
   --resource-identifier arn:aws:rds:us-east-1:123456789012:cluster:sample-cluster ^
   --apply-action db-upgrade ^
   --opt-in-type immediate
```

Die Ausgabe dieser Operation sieht folgendermaßen aus.

```
{
    "ResourcePendingMaintenanceActions": {
        "ResourceIdentifier": "arn:aws:rds:us-
east-1:444455556666:cluster:docdb-2019-01-09-23-55-38",
        "PendingMaintenanceActionDetails": [
            {
                "CurrentApplyDate": "2019-02-20T20:57:06.904Z",
                "Description": "Bug fixes",
                "ForcedApplyDate": "2019-02-25T21:46:00Z",
                "OptInStatus": "immediate",
                "Action": "db-upgrade",
                "AutoAppliedAfterDate": "2019-02-25T07:41:00Z"
            }
        ]
    }
}
```

Einen Amazon DocumentDB-Cluster stoppen und starten

Das Stoppen und Starten von Amazon DocumentDB-Clustern kann Ihnen helfen, die Kosten für Entwicklungs- und Testumgebungen zu verwalten. Anstatt jedes Mal, wenn Sie Amazon DocumentDB verwenden, Cluster und Instances zu erstellen und zu löschen, können Sie alle Instances in Ihrem Cluster vorübergehend beenden, wenn sie nicht benötigt werden. Sie können sie neu starten, wenn Sie Ihre Tests fortsetzen.

Themen

- Übersicht über das Stoppen und Starten eines Clusters
- Operationen, die Sie auf einem gestoppten Cluster ausführen können

Übersicht über das Stoppen und Starten eines Clusters

In Zeiten, in denen Sie keinen Amazon DocumentDB-Cluster benötigen, können Sie alle Instances in diesem Cluster gleichzeitig stoppen. Bei Bedarf können Sie den Cluster jederzeit erneut starten. Durch das Starten und Stoppen werden die Einrichtungs- und Entfernungsvorgänge für Cluster erleichtert, die in der Entwicklung, für Tests oder ähnliche Aktivitäten verwendet werden und keine kontinuierliche Verfügbarkeit erfordern. Sie können einen Cluster mithilfe von AWS-Managementkonsole oder AWS CLI mit einer einzigen Aktion beenden und starten, unabhängig davon, wie viele Instances sich im Cluster befinden.

Während Ihr Cluster gestoppt ist, bleibt des Cluster-Speichervolumen unverändert. Sie zahlen nur für Speicherung, manuelle Snapshots und automatischen Sicherungsspeicher innerhalb des angegebenen Aufbewahrungsfensters. Ihnen werden keine Instance-Stunden in Rechnung gestellt. Amazon DocumentDB startet Ihren Cluster automatisch nach sieben Tagen, sodass er nicht hinter den erforderlichen Wartungsupdates zurückbleibt. Wenn Ihr Cluster nach sieben Tagen wieder startet, werden Ihnen die Instances im Cluster wieder in Rechnung gestellt. Während Ihr Cluster gestoppt ist, können Sie Ihr Speichervolumen nicht abfragen, da die Abfrage erfordert, dass sich Instances im Status „available (verfügbar)“ befinden.

Wenn ein Amazon DocumentDB-Cluster gestoppt wird, können weder der Cluster noch seine Instances in irgendeiner Weise geändert werden. Dies umfasst das Hinzufügen oder Entfernen von Instances oder das Löschen des Clusters.

Using the AWS-Managementkonsole

Das folgende Verfahren zeigt, wie Sie einen Cluster mit einer oder mehreren Instances im Status „verfügbar“ stoppen oder einen gestoppten Cluster wieder starten.

So beenden oder starten Sie einen Amazon DocumentDB-Cluster

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Klicken Sie im Navigationsbereich auf Cluster.

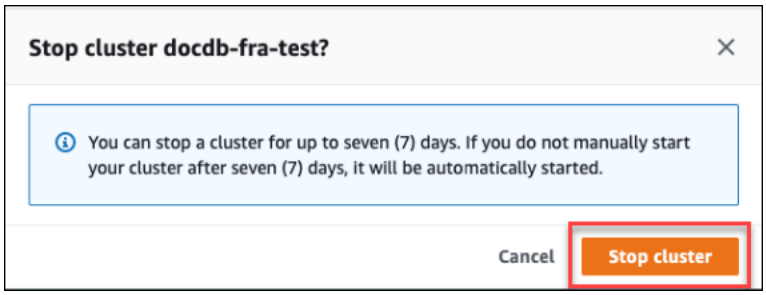
> **Tip**
>
> Wenn der Navigationsbereich auf der linken Seite des Bildschirms nicht angezeigt wird, wählen Sie links oben auf der Seite das Menüsymbol (≡) aus.

3. Wählen Sie in der Liste der Cluster die Schaltfläche links neben dem Namen des Clusters aus, den Sie stoppen oder starten möchten.
4. Wählen Sie Aktionen aus und dann die Aktion, die Sie auf dem Cluster ausführen möchten.
   - Wenn Sie den Cluster stoppen möchten und der Cluster verfügbar ist:

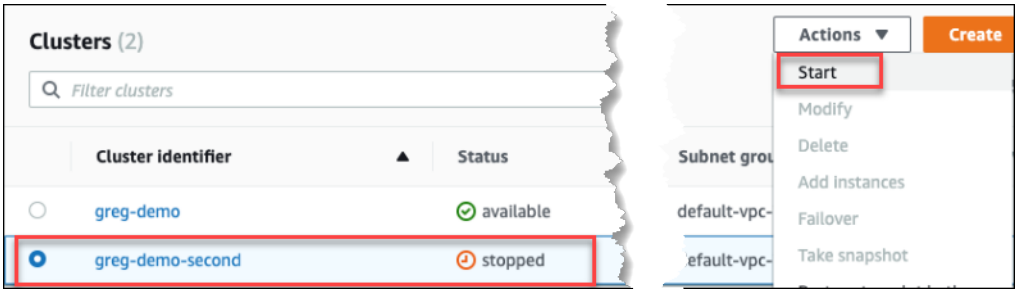
     a. Wählen Sie Beenden aus.

     Damit der Failover-Mechanismus nicht aktiviert wird, werden beim Stoppvorgang zuerst die Replikat-Instances und dann die primäre Instance gestoppt.

     b. Wenn Sie den Cluster stoppen möchten, wählen Sie im Bestätigungsdialogfeld Cluster stoppen aus und wenn der Cluster weiter ausgeführt werden soll, wählen Sie Abbrechen aus.



   - Wenn Sie einen gestoppten Cluster starten möchten, wählen Sie Starten aus.



5. Überwachen Sie den Status des Clusters und seiner Instances. Wenn Sie den Cluster gestartet haben, können Sie die Ausführung des Clusters fortsetzen, wenn der Cluster und dessen Instances verfügbar sind. Weitere Informationen finden Sie unter Den Status eines Clusters ermitteln.

Using the AWS CLI

Die folgenden Codebeispiele zeigen, wie Sie einen Cluster mit einer oder mehreren Instances im Status „verfügbar“ stoppen oder einen gestoppten Cluster starten.

Um einen Cluster mit einer oder mehreren verfügbaren Instances mithilfe von zu beenden AWS CLI, verwenden Sie den `stop-db-cluster` Vorgang. Verwenden Sie die `start-db-cluster`-Operation, um einen gestoppten Cluster zu starten. Beide Operationen verwenden den `--db-cluster-identifier`-Parameter.

Parameter:

- **`--db-cluster-identifier`**—Erforderlich. Der Name des Clusters, der gestoppt oder gestartet werden soll.

Example— Um einen Cluster mit dem zu beenden AWS CLI

Der folgende Code stoppt den Cluster `sample-cluster`. Der Cluster muss eine oder mehrere Instances im verfügbaren Zustand haben.

Für Linux, macOS oder Unix:

```
aws docdb stop-db-cluster \
   --db-cluster-identifier sample-cluster
```

Für Windows:

```
aws docdb stop-db-cluster ^
   --db-cluster-identifier sample-cluster
```

Example— Um einen Cluster mit dem zu starten AWS CLI

Der folgende Code startet den Cluster `sample-cluster`. Der Cluster muss jetzt gestoppt werden.

Für Linux, macOS oder Unix:

```
aws docdb start-db-cluster \
   --db-cluster-identifier sample-cluster
```

Für Windows:

```
aws docdb start-db-cluster ^
   --db-cluster-identifier sample-cluster
```

Operationen, die Sie auf einem gestoppten Cluster ausführen können

Während ein Amazon DocumentDB-Cluster gestoppt ist, können Sie eine Point-in-Time-Wiederherstellung zu einem beliebigen Zeitpunkt innerhalb Ihres angegebenen Zeitfensters für die automatische Aufbewahrung von Backups durchführen. Weitere Informationen zur Durchführung einer zeitpunktbezogenen Wiederherstellung finden Sie unter Zu einem bestimmten Zeitpunkt wiederherstellen.

Sie können die Konfiguration eines Amazon DocumentDB-Clusters oder einer seiner Instances nicht ändern, solange der Cluster gestoppt ist. Es ist auch nicht möglich, Instances zum Cluster hinzuzufügen oder daraus zu entfernen oder den Cluster zu löschen, wenn ihm noch Instances zugeordnet sind. Vor solchen administrativen Aktionen müssen Sie den Cluster starten.

Amazon DocumentDB wendet alle geplanten Wartungsarbeiten auf Ihren gestoppten Cluster erst an, nachdem er erneut gestartet wurde. Nach sieben Tagen startet Amazon DocumentDB automatisch

einen gestoppten Cluster, sodass er in seinem Wartungsstatus nicht zu weit zurückfällt. Sobald Ihr Cluster neu gestartet wird, werden Ihnen die Instances im Cluster wieder in Rechnung gestellt.

Solange ein Cluster gestoppt ist, führt Amazon DocumentDB keine automatisierten Backups durch und verlängert auch nicht den Aufbewahrungszeitraum für Backups.

Löschen eines Amazon DocumentDB-Clusters

Sie können einen Amazon DocumentDB-Cluster mit dem AWS-Managementkonsole oder dem AWS CLI löschen. Um einen Cluster zu löschen, muss sich der Cluster im Status available (verfügbar) befinden und es dürfen keine Instances mit ihm verknüpft sein. Wenn der Cluster angehalten ist, starten Sie zuerst den Cluster, warten Sie, bis der Cluster verfügbar wird, und löschen Sie dann den Cluster. Weitere Informationen finden Sie unter Einen Amazon DocumentDB-Cluster stoppen und starten.

Löschschutz

Zum Schutz Ihrer Cluster vor versehentlichem Löschen, können Sie den Löschschutz aktivieren. Wenn Sie mithilfe der Konsole einen Cluster erstellen, ist der Löschschutz standardmäßig aktiviert. Der Löschschutz ist jedoch standardmäßig deaktiviert, wenn Sie einen Cluster über die AWS CLI erstellen.

Amazon DocumentDB erzwingt den Löschschutz für einen Cluster, unabhängig davon, ob Sie den Löschvorgang über die Konsole oder die ausführen. AWS CLI Sie können einen Cluster nicht löschen, solange der Löschschutz aktiviert ist. Um einen Cluster mit aktiviertem Löschschutz zu löschen, müssen Sie zuerst den Cluster ändern und den Löschschutz deaktivieren.

Wenn Sie die Konsole mit aktiviertem Löschschutz für einen Cluster verwenden, können Sie die letzte Instance des Clusters nicht löschen, da dadurch auch der Cluster gelöscht werden würde. Sie können die letzte Instance eines mit Löschschutz geschützten Clusters mit der AWS CLI löschen. In diesen Fall bleibt der Cluster selbst bestehen und die Daten werden beibehalten. Sie können zum Zugriff auf die Daten neue Instances für den Cluster erstellen. Weitere Informationen zum Aktivieren und Deaktivieren des Löschschutzes siehe:

- Einen Amazon DocumentDB-Cluster erstellen
- Ändern eines Amazon DocumentDB-Clusters

Using the AWS-Managementkonsole

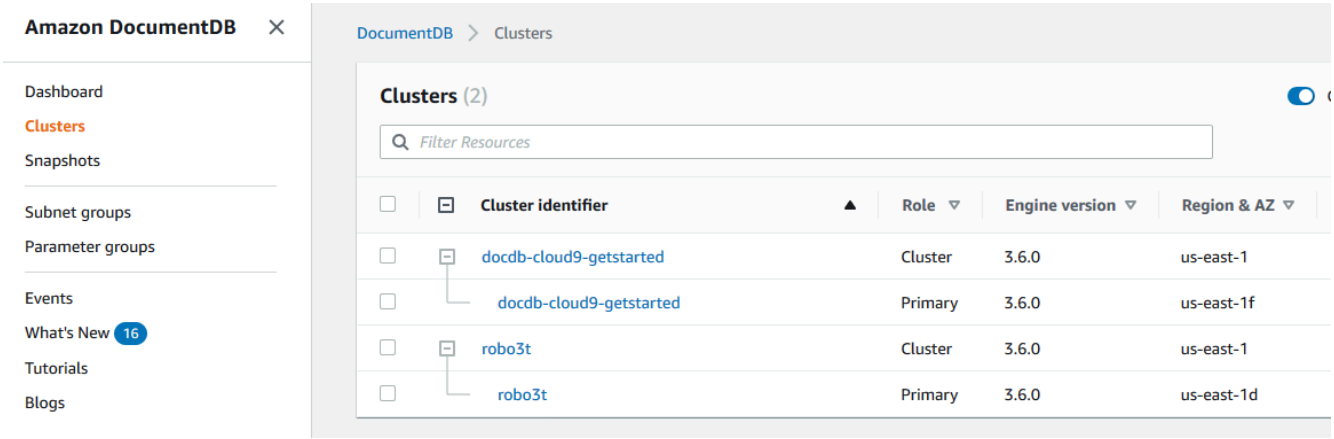
Um einen Cluster mit dem zu löschen AWS-Managementkonsole, muss der Löschschutz deaktiviert sein.

So finden Sie heraus, ob der Löschschutz für einen Cluster aktiviert ist:

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Klicken Sie im Navigationsbereich auf Cluster.

   > **Tip**
   >
   > Wenn der Navigationsbereich auf der linken Seite des Bildschirms nicht angezeigt wird, wählen Sie links oben auf der Seite das Menüsymbol (≡) aus.

3. Beachten Sie, dass im Cluster-Navigationsfeld in der Spalte Cluster-ID sowohl Cluster als auch Instances angezeigt werden. Instances werden unter Clustern aufgeführt, ähnlich wie im folgenden Screenshot.



4. Wählen Sie den Namen des Clusters und die Registerkarte Configuration (Konfiguration) aus. Suchen Sie im Abschnitt Cluster-Details die Option Deletion protection (Löschschutz). Wenn der Löschschutz aktiviert ist, bearbeiten Sie den Cluster, um den Löschschutz zu deaktivieren. Informationen über das Ändern eines Clusters finden Sie unter Ändern eines Amazon DocumentDB-Clusters.

   Nachdem Sie den Löschschutz deaktiviert haben, können Sie den Cluster löschen.

So löschen Sie einen Cluster:

1. Klicken Sie im Navigationsbereich auf Cluster.
2. Ermitteln Sie, ob der Cluster über Instances verfügt, indem Sie in der Spalte Cluster-ID nach den darunter aufgelisteten Instances suchen. Bevor Sie einen Cluster löschen können, müssen Sie alle seine Instances löschen. Weitere Informationen finden Sie unter Löschen einer Amazon DocumentDB DocumentDB-Instance.
3. Abhängig davon, ob Ihr Cluster Instances hat oder nicht, führen Sie einen der folgenden Schritte aus:
   - Wenn der Cluster über keine Instances verfügt, wählen Sie die Schaltfläche links neben dem Cluster-Namen und dann Actions (Aktionen) aus. Wählen Sie im Dropdown-Menü Löschen aus. Füllen Sie das Dialogfeld <cluster-name> löschen aus und klicken Sie dann auf Löschen.
   - Wenn der Cluster eine oder mehrere Instances hat, gehen Sie wie folgt vor:
     a. Klicken Sie im Navigationsbereich auf Cluster.
     b. Löschen Sie alle Instanzen des Clusters, indem Sie das Kontrollkästchen links neben dem Namen des Clusters aktivieren. Wählen Sie Actions (Aktionen) und anschließend Delete (Löschen) aus. Füllen Sie das Dialogfeld <cluster-name> löschen aus und klicken Sie dann auf Löschen.

        Wenn Sie die letzte Instanz löschen, wird auch der Cluster gelöscht. Weitere Informationen zum Löschen von Instanzen finden Sie unterLöschen einer Amazon DocumentDB DocumentDB-Instance.

Es dauert einige Minuten, bis der Cluster gelöscht ist. Informationen zur Überwachung des Status des Clusters finden Sie unter Den Status eines Amazon DocumentDB-Clusters überwachen.

Using the AWS CLI

Sie können einen Cluster, dem Instances zugeordnet sind, nicht löschen. Um festzustellen, welche Instances mit dem Cluster verknüpft sind, führen Sie den Befehl `describe-db-clusters` aus und löschen Sie alle Instances des Clusters. Deaktivieren Sie dann bei Bedarf den Löschschutz auf Ihrem Cluster und löschen Sie schließlich den Cluster.

1. Löschen Sie zuerst alle Instances des Clusters.

Um festzustellen, welche Instances Sie löschen müssen, führen Sie den folgenden Befehl aus.

```
aws docdb describe-db-clusters \
    --db-cluster-identifier sample-cluster \
    --query 'DBClusters[*].
[DBClusterIdentifier,DBClusterMembers[*].DBInstanceIdentifier]'
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus (JSON-Format).

```
[
    [
        "sample-cluster",
        [
            "sample-instance-1",
            "sample-instance-2"
        ]
    ]
]
```

Wenn der Cluster, den Sie löschen möchten, Instances enthält, löschen Sie diese wie unten dargestellt.

```
aws docdb delete-db-instance \
    --db-instance-identifier sample-instance
```

2. Zweitens deaktivieren Sie den Löschschutz.

   Wenn AWS CLI Sie alle Instanzen eines Clusters löschen, wird der Cluster nicht gelöscht. Sie müssen auch den Cluster löschen, aber dies ist nur möglich, wenn der Löschschutz deaktiviert ist.

   Um festzustellen, ob der Löschschutz für den Cluster aktiviert ist, führen Sie den folgenden Befehl aus.

> **Tip**
>
> Um den Löschschutzstatus all Ihrer Amazon DocumentDB-Cluster zu sehen, lassen Sie den `--db-cluster-identifier` Parameter weg.

```
aws docdb describe-db-clusters \
    --db-cluster-identifier sample-cluster \
    --query 'DBClusters[*].[DBClusterIdentifier,DeletionProtection]'
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus.

```
[
    [
        "sample-cluster",
        "true"
    ]
]
```

Wenn für einen Cluster der Löschschutz aktiviert ist, bearbeiten Sie den Cluster, um den Löschschutz zu deaktivieren. Führen Sie den folgenden Befehl aus, um den Löschschutz des Clusters zu deaktivieren.

```
aws docdb modify-db-cluster \
    --db-cluster-identifier sample-cluster \
    --no-deletion-protection \
    --apply-immediately
```

3. Löschen Sie schließlich den Cluster.

   Nachdem Sie den Löschschutz deaktiviert haben, können Sie den Cluster löschen. Um einen Cluster zu löschen, verwenden Sie die `delete-db-cluster`-Operation mit den folgenden Parametern.

   - **`--db-cluster-identifier`**—Erforderlich. Die ID des Clusters, den Sie löschen möchten.

- **`--final-db-snapshot-identifier`**— Fakultativ. Wenn Sie einen endgültigen Snapshot wünschen, müssen Sie diesen Parameter mit einem Namen für den endgültigen Snapshot angeben. Sie müssen entweder `--final-db-snapshot-identifier` oder `--skip-final-snapshot` angeben.

  Benennungseinschränkungen:

  - Die Länge beträgt [1—63] Buchstaben, Zahlen oder Bindestriche.
  - Muss mit einem Buchstaben beginnen.
  - Darf nicht mit einem Bindestrich enden oder zwei aufeinanderfolgende Bindestriche enthalten.
  - Muss für alle Cluster in Amazon RDS, Amazon Neptune und Amazon DocumentDB pro AWS-Konto Region eindeutig sein.
- **`--skip-final-snapshot`**— Fakultativ. Verwenden Sie diesen Parameter nur, wenn Sie vor dem Löschen Ihres Clusters keinen letzten Snapshot machen möchten. Standardmäßig wird ein letzter Snapshot erstellt. Sie müssen entweder `--final-db-snapshot-identifier` oder `--skip-final-snapshot` angeben.

Der folgende AWS CLI Code löscht den Cluster `sample-cluster` mit einem endgültigen Snapshot. Die Operation schlägt fehl, wenn Instances vorhanden sind, die mit dem Cluster verknüpft sind, oder wenn der Löschschutz aktiviert ist.

Example

Für Linux, macOS oder Unix:

```
aws docdb delete-db-cluster \
    --db-cluster-identifier sample-cluster \
    --final-db-snapshot-identifier sample-cluster-final-snapshot
```

Für Windows:

```
aws docdb delete-db-cluster ^
    --db-cluster-identifier sample-cluster ^
    --final-db-snapshot-identifier sample-cluster-final-snapshot
```

Example

Der folgende AWS CLI Code löscht den Cluster, `sample-cluster` ohne einen endgültigen Snapshot zu erstellen.

Für Linux, macOS oder Unix:

```
aws docdb delete-db-cluster \
    --db-cluster-identifier sample-cluster \
    --skip-final-snapshot
```

Für Windows:

```
aws docdb delete-db-cluster ^
    --db-cluster-identifier sample-cluster ^
    --skip-final-snapshot
```

Die Ausgabe der `delete-db-cluster`-Operation ist der Cluster, den Sie löschen.

Es dauert einige Minuten, bis der Cluster gelöscht ist. Informationen zur Überwachung des Status des Clusters finden Sie unter Den Status eines Clusters überwachen.

Skalierung von Amazon DocumentDB-Clustern

Mit Amazon DocumentDB können Sie den Speicher und die Rechenleistung in Ihren Clustern nach Ihren Bedürfnissen skalieren. In diesem Abschnitt wird beschrieben, wie Sie Speicherskalierung, Instanzskalierung und Leseskalierung verwenden können, um die Leistung und Skalierung für Ihre Amazon DocumentDB-Cluster und -Instances zu verwalten.

Themen

- Speicherskalierung
- Skalierung von Instances
- Skalierung von Lesevorgängen
- Skalierung schreiben

Speicherskalierung

Der Amazon DocumentDB DocumentDB-Speicher wird automatisch mit den Daten in Ihrem Cluster-Volume skaliert. Wenn Ihre Daten wachsen, wächst Ihr Cluster-Volumenspeicher in Schritten von 10 GiB auf bis zu 128 TiB.

Skalierung von Instances

Sie können Ihren Amazon DocumentDB-Cluster nach Bedarf skalieren, indem Sie die Instance-Klasse für jede Instance im Cluster ändern. Amazon DocumentDB unterstützt mehrere Instance-Klassen, die für Amazon DocumentDB optimiert sind.

Weitere Informationen finden Sie unter Ändern einer Amazon DocumentDB DocumentDB-Instance.

Skalierung von Lesevorgängen

Sie können die Leseskalierung für Ihren Amazon DocumentDB-Cluster erreichen, indem Sie bis zu 15 Amazon DocumentDB DocumentDB-Replikate im Cluster erstellen. Jedes Amazon DocumentDB DocumentDB-Replikat gibt dieselben Daten aus dem Cluster-Volume mit minimaler Replikatverzögerung zurück — normalerweise weniger als 100 Millisekunden, nachdem die primäre Instance ein Update geschrieben hat. Wenn Ihr Lesedatenverkehr zunimmt, können Sie zusätzliche Amazon DocumentDB DocumentDB-Replikate erstellen und sich direkt mit ihnen verbinden, um die Leselast für Ihren Cluster zu verteilen. Amazon DocumentDB DocumentDB-Replikate müssen nicht derselben Instance-Klasse angehören wie die primäre Instance.

Weitere Informationen finden Sie unter Hinzufügen einer Amazon DocumentDB DocumentDB-Instance zu einem Cluster.

Um den Lesesatz mit Amazon DocumentDB zu nutzen, empfehlen wir, dass Sie eine Verbindung zu Ihrem Cluster als Replikatsatz herstellen und Lesevorgänge mithilfe der integrierten Leseeinstellungen Ihres Treibers an Replikatinstanzen verteilen. Weitere Informationen finden Sie unter Als Replikatsatz eine Verbindung zu Amazon DocumentDB herstellen.

Skalierung schreiben

Sie können die Schreibkapazität in Ihrem Amazon DocumentDB-Cluster skalieren, indem Sie die Größe der primären Instance Ihres Clusters erhöhen. In diesem Abschnitt werden zwei Methoden für die Skalierung der primären Instance Ihres Clusters abhängig von Ihren Anforderungen beschrieben. Die erste Option zielt darauf ab, die Auswirkungen auf die Anwendung so gering wie möglich

zu halten, erfordert jedoch mehr Schritte. Die zweite Option ermöglicht Ihnen die Optimierung in Bezug auf die Einfachheit, da sie weniger Schritte erfordert. Die potenziellen Auswirkungen auf Anwendungen sind jedoch größer.

Abhängig von Ihrer Anwendung können Sie wählen, welcher Ansatz für Sie am besten geeignet ist. Weitere Informationen zu verfügbaren Instance-Größen und Kosten finden Sie auf der Seite mit den Amazon DocumentDB DocumentDB-Preisen.

1. Optimieren Sie für hohe Verfügbarkeit und Leistung — Wenn Sie im Replica-Set-Modus (empfohlen) eine Verbindung zu Ihrem Cluster herstellen, können Sie den folgenden Prozess verwenden, um die Auswirkungen auf Ihre Anwendung bei der Skalierung Ihrer primären Instance zu minimieren. Diese Methode minimiert die Auswirkungen, da Ihr Cluster den von Ihnen festgelegten Wert für Hochverfügbarkeit weiter einhält oder überschreitet. Darüber hinaus werden Leseskalierungsziele dem Cluster als Instances hinzugefügt, anstatt an Ort und Stelle aktualisiert zu werden.

   a. Fügen Sie ein oder mehrere Replikate des größeren Instance-Typs zu Ihrem Cluster hinzu (siehe ???). Alle Replikate sollten einen Instance-Typ besitzen, der größer oder gleich dem Typ der primären Instance ist. Dies vermeidet eine unbeabsichtigte Reduzierung der Schreibleistung aufgrund eines Failovers zu einem kleineren Instance-Typ. Für die meisten Kunden bedeutet dies, dass die Anzahl der Instances in ihrem Cluster vorübergehend verdoppelt wird und die kleineren Replikate nach Abschluss der Skalierung entfernt werden.

   b. Legen Sie die Failover-Stufe für alle neuen Replikate auf die Priorität Null fest. Dies stellt sicher, dass ein Replikat des kleineren Instance-Typs die höchste Failover-Priorität besitzt. Weitere Informationen finden Sie unter ???.

   c. Initiieren Sie einen manuellen Failover. Hierdurch wird eines der neuen Replikate zur primären Instance hochgestuft. Weitere Informationen finden Sie unter ???.

      > **Note**
      >
      > Dies führt zu einer Ausfallzeit von ca. 30 Sekunden für Ihren Cluster. Planen Sie diese Ausfallzeit ein.

   d. Entfernen Sie aus dem Cluster alle Replikate von Instance-Typen, die kleiner als der neue primäre Instance-Typ sind.

   e. Setzen Sie die Failover-Stufe aller Instances auf dieselbe Priorität zurück. (In der Regel bedeutet dies, dass sie auf 1 zurückgesetzt werden.)

Angenommen, Sie führen einen Cluster aus, der zurzeit drei `r5.large`-Instances enthält (eine primäre Instance und zwei Replikate). Sie möchten diese Instances auf den Instance-Typ `r5.xlarge` skalieren. Hierzu fügen Sie dem Cluster zunächst drei `r5.xlarge`-Replikat-Instances hinzu und legen anschließend die Failover-Stufe der neuen `r5.xlarge`-Replikate auf null fest. Als Nächstes leiten Sie einen manuellen Failover ein. (Ihnen ist bekannt, dass dies zu einer Ausfallzeit von ca. 30 Sekunden für Ihre Anwendung führt.) Nach Abschluss des Failovers entfernen Sie alle drei `r5.large`-Instances aus dem Cluster. Der Cluster ist nun auf `r5.xlarge`-Instances skaliert.

Um die Kosten zu optimieren, werden Amazon DocumentDB DocumentDB-Instances in Sekundenschritten abgerechnet, wobei eine Mindestgebühr von zehn Minuten nach einer Änderung des fakturierbaren Status, z. B. beim Erstellen, Ändern oder Löschen einer Instance, anfällt. Weitere Informationen finden Sie unter Kostenoptimierung in der Dokumentation zu bewährten Methoden.

2. Aus Gründen der Einfachheit optimieren — Dieser Ansatz ist aus Gründen der Einfachheit optimiert. Dadurch wird der Cluster nicht erweitert und verkleinert, aber es kann Ihre Lesekapazität vorübergehend reduzieren.

   Es ist möglich, dass das Ändern der Instanzklasse eines Replikats dazu führt, dass diese Instanz für einen kurzen Zeitraum, von einigen Sekunden bis weniger als 30 Sekunden, keine Anfragen bearbeitet. Wenn Sie im Replikat-Set-Modus (empfohlen) eine Verbindung zu Ihrem Cluster herstellen, würde dies Ihre Lesekapazität während des Skalierungsvorgangs um ein Replikat reduzieren (z. B. auf 66% Kapazität in einem 3-Knoten-Cluster oder 75% Kapazität in einem 4-Knoten-Cluster usw.).

   a. Skalieren Sie eine der Replikatinstanzen in Ihrem Cluster. Weitere Informationen finden Sie unter Instanzklassen verwalten.

   b. Warten Sie, bis die Instanz verfügbar ist (siheDen Status einer Amazon DocumentDB DocumentDB-Instance überwachen).

      > **Note**
      >
      > Dies führt zu einer Ausfallzeit von ca. 30 Sekunden für Ihren Cluster. Planen Sie diese Ausfallzeit ein.

c. Fahren Sie mit der Ausführung der Schritte 1 und 2 fort, bis alle Replikatinstanzen nacheinander skaliert wurden.

d. Initiieren Sie ein manuelles Failover. Dadurch wird eines der Replikate zur primären Instanz heraufgestuft. Weitere Informationen finden Sie unter Amazon DocumentDB-Failover.

> **Note**
>
> Dies führt zu Ausfallzeiten von bis zu 30 Sekunden für Ihren Cluster, dauert aber oft weniger Zeit. Planen Sie diese Ausfallzeit ein.

e. Skalieren Sie die frühere primäre Instanz (jetzt ein Replikat).

Klonen eines Volumes für einen Amazon DocumentDB-Cluster

Durch das Klonen von Amazon DocumentDB können Sie einen neuen Cluster erstellen, der dasselbe Amazon DocumentDB-Cluster-Volume verwendet und dieselben Daten wie das Original hat. Der Prozess ist so konzipiert, dass er schnell und kostengünstig ist. Der neue Cluster mit dem zugehörigen Datenvolume wird als clone (Klon) bezeichnet. Das Erstellen eines Klons ist schneller und platzsparender als das physische Kopieren der Daten mit anderen Techniken, wie z. B. das Wiederherstellen eines Snapshots.

Amazon DocumentDB unterstützt die Erstellung eines von Amazon DocumentDB bereitgestellten Klons aus einem bereitgestellten Amazon DocumentDB-Cluster. Wenn Sie einen Clone mit einer anderen Bereitstellungskonfiguration als der Quelle erstellen, wird der Clone mit der neuesten Version der Amazon DocumentDB DocumentDB-Engine der Quelle erstellt.

Wenn Sie Klone aus Ihren Amazon DocumentDB-Clustern erstellen, werden die Klone in Ihrem Konto erstellt AWS — demselben Konto, dem der Amazon DocumentDB DocumentDB-Quellcluster gehört.

Themen

- Überblick über das Klonen von Amazon DocumentDB
- Einschränkungen beim Klonen von Amazon DocumentDB
- So funktioniert das Klonen von Amazon DocumentDB
- Einen Amazon DocumentDB-Klon erstellen

Überblick über das Klonen von Amazon DocumentDB

Amazon DocumentDB verwendet ein Copy-on-Write-Protokoll, um einen Klon zu erstellen. Dieser Mechanismus verwendet minimalen zusätzlichen Speicherplatz, um einen ersten Klon zu erstellen. Wenn der Klon zum ersten Mal erstellt wird, behält Amazon DocumentDB eine einzige Kopie der Daten, die vom Quell-DB-Cluster und dem neuen (geklonten) Amazon DocumentDB-Cluster verwendet werden. Zusätzlicher Speicherplatz wird nur zugewiesen, wenn Änderungen an Daten (auf dem Amazon DocumentDB-Speichervolume) durch den Amazon DocumentDB-Quellcluster oder den Amazon DocumentDB-Cluster-Klon vorgenommen werden. Weitere Informationen zum Copy-on-Write-Protokoll finden Sie unter So funktioniert das Klonen von Amazon DocumentDB.

Das Klonen von Amazon DocumentDB ist besonders nützlich, um schnell Testumgebungen mit Ihren Produktionsdaten einzurichten, ohne das Risiko einer Datenbeschädigung einzugehen. Sie können Klone für viele Arten von Anwendungen verwenden, z. B. für Folgende:

- Experimentieren Sie mit möglichen Änderungen (z. B. Schemaänderungen und Parametergruppenänderungen), um alle Auswirkungen zu bewerten.
- Führen Sie Workload-intensive Vorgänge aus, z. B. das Exportieren von Daten oder das Ausführen analytischer Abfragen auf dem Klon.
- Erstellen Sie eine Kopie Ihres Produktions-DB-Clusters zu Entwicklungs-, Test- oder anderen Zwecken.

Sie können mehr als einen Klon aus demselben Amazon DocumentDB-Cluster erstellen. Sie können auch mehrere Klone aus einem anderen Klon erstellen.

Nachdem Sie einen Amazon DocumentDB-Klon erstellt haben, können Sie die Amazon DocumentDB DocumentDB-Instances anders konfigurieren als der Amazon DocumentDB DocumentDB-Quellcluster. Beispielsweise benötigen Sie möglicherweise keinen Klon für Entwicklungszwecke, um dieselben Hochverfügbarkeitsanforderungen wie der Amazon DocumentDB DocumentDB-Quellproduktionscluster zu erfüllen. In diesem Fall können Sie den Clone mit einer einzigen Amazon DocumentDB-Instance statt mit mehreren DB-Instances konfigurieren, die vom Amazon DocumentDB-Cluster verwendet werden.

Wenn Sie den Klon für Test-, Entwicklungs- oder andere Zwecke nicht mehr verwenden, können Sie ihn löschen.

Einschränkungen beim Klonen von Amazon DocumentDB

Amazon DocumentDB; das Klonen hat derzeit die folgenden Einschränkungen:

- Sie können so viele Klone erstellen, wie Sie möchten, bis zur maximalen Anzahl von DB-Clustern, die in der AWS-Region zulässig sind. Nachdem Sie jedoch 15 Klone erstellt haben, ist der nächste Klon eine vollständige Kopie. Der Klonvorgang funktioniert wie eine zeitpunktbezogene Wiederherstellung.
- Sie können keinen Clone in einer anderen AWS Region als dem Amazon DocumentDB DocumentDB-Quellcluster erstellen.
- Sie können keinen Clone aus einem Amazon DocumentDB-Cluster erstellen, der keine DB-Instances hat. Sie können nur Amazon DocumentDB-Cluster klonen, die über mindestens eine DB-Instance verfügen.
- Sie können einen Clone in einer anderen Virtual Private Cloud (VPC) als der des Amazon DocumentDB-Clusters erstellen. In diesem Fall müssen die Subnetze der VPCs denselben Availability Zones zugeordnet sein.

So funktioniert das Klonen von Amazon DocumentDB

Das Klonen von Amazon DocumentDB funktioniert auf der Speicherebene eines Amazon DocumentDB-Clusters. Es verwendet ein Copy-on-Write-Protokoll, das sowohl schnell als auch platzsparend ist, was die zugrunde liegenden dauerhaften Medien angeht, die das Amazon DocumentDB DocumentDB-Speichervolumen unterstützen. Weitere Informationen zu Amazon DocumentDB-Cluster-Volumes finden Sie unterVerwaltung von Amazon DocumentDB-Clustern.

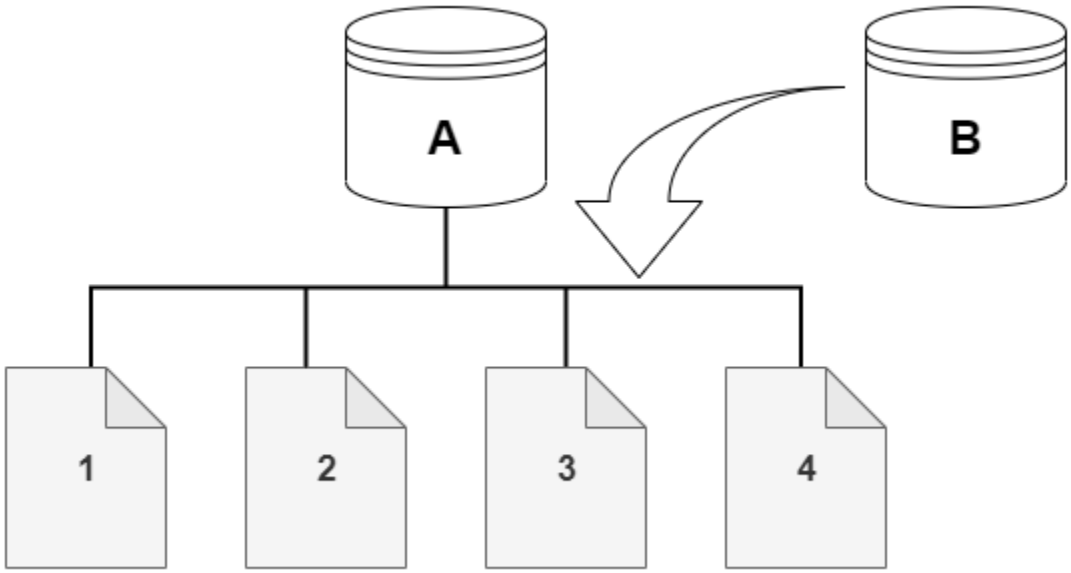
Themen

- Copy-On-Write-Protokoll verstehen
- Löschen eines Quell-Cluster-Volumes

Copy-On-Write-Protokoll verstehen

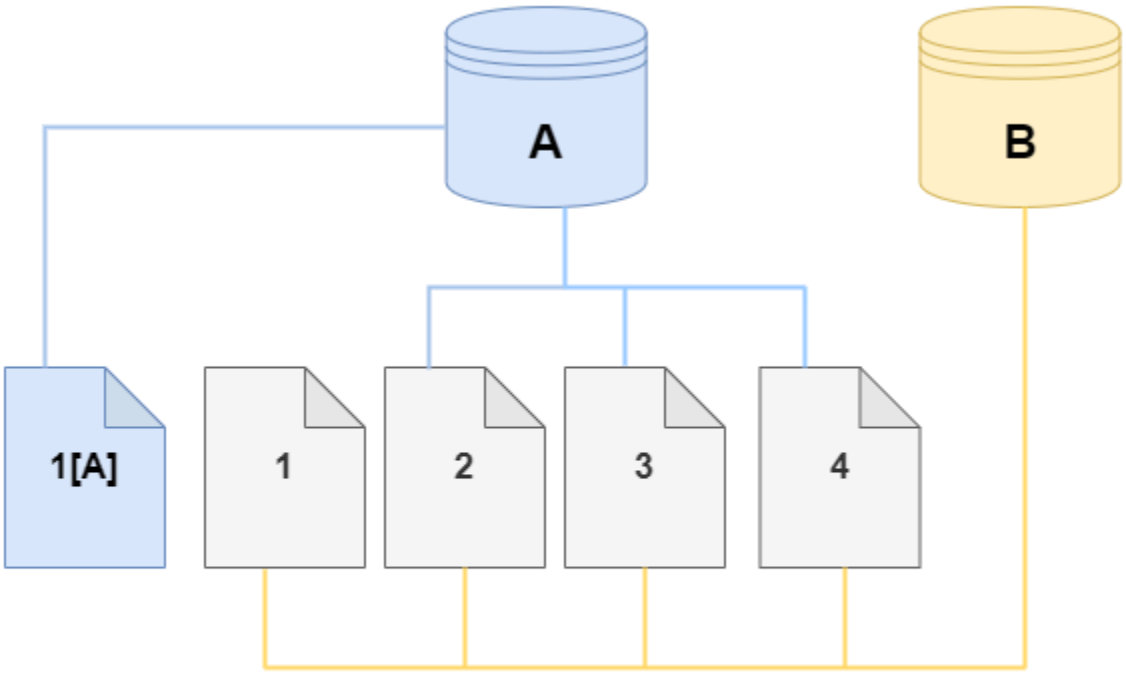
Ein Amazon DocumentDB-Cluster speichert Daten in Seiten auf dem zugrunde liegenden Amazon DocumentDB DocumentDB-Speichervolume.

Im folgenden Diagramm finden Sie beispielsweise einen Amazon DocumentDB-Cluster (A) mit vier Datenseiten, 1, 2, 3 und 4. Stellen Sie sich vor, dass ein Klon, B, aus dem Amazon DocumentDB-Cluster erstellt wird. Wenn der Klon erstellt wird, werden keine Daten kopiert. Vielmehr verweist der Klon auf denselben Seitensatz wie der Amazon DocumentDB DocumentDB-Quellcluster.

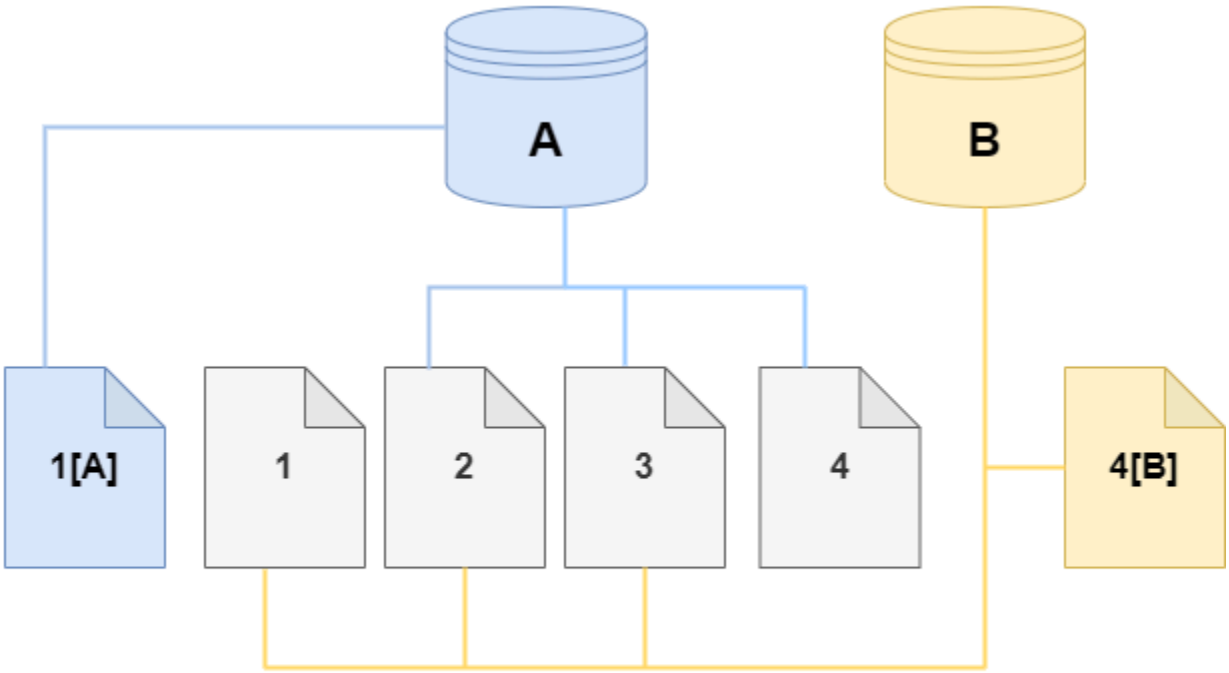


Wenn der Klon erstellt wird, ist normalerweise kein zusätzlicher Speicher erforderlich. Das Copy-on-Write-Protokoll verwendet dasselbe Segment auf dem physischen Speichermedium wie das Quellsegment. Zusätzlicher Speicher ist nur erforderlich, wenn die Kapazität des Quellsegments für das gesamte Klonsegment nicht ausreicht. Wenn dies der Fall ist, wird das Quellsegment auf ein anderes physisches Gerät kopiert.

In den folgenden Diagrammen finden Sie ein Beispiel für das Copy-on-Write-Protokoll in Aktion mit demselben Cluster A und dessen Klon, B, wie oben gezeigt. Nehmen wir an, Sie nehmen eine Änderung an Ihrem Amazon DocumentDB-Cluster (A) vor, die zu einer Änderung der auf Seite 1 gespeicherten Daten führt. Anstatt auf die ursprüngliche Seite 1 zu schreiben, erstellt Amazon DocumentDB eine neue Seite 1 [A]. Das Amazon DocumentDB-Cluster-Volume für Cluster (A) verweist jetzt auf die Seiten 1 [A], 2, 3 und 4, während der Klon (B) immer noch auf die Originalseiten verweist.



Auf dem Klon wird eine Änderung an Seite 4 auf dem Speichervolume vorgenommen. Anstatt auf die ursprüngliche Seite 4 zu schreiben, erstellt Amazon DocumentDB eine neue Seite, 4 [B]. Der Klon verweist nun auf die Seiten 1, 2, 3 und auf Seite 4[B], während der Cluster (A) weiterhin auf 1[A], 2, 3 und 4 verweist.



Da im Laufe der Zeit immer mehr Änderungen sowohl im Amazon DocumentDB DocumentDB-Quell-Cluster-Volume als auch im Clone vorgenommen werden, wird mehr Speicherplatz benötigt, um die Änderungen zu erfassen und zu speichern.

Löschen eines Quell-Cluster-Volumes

Wenn Sie ein Quell-Cluster-Volume löschen, dem ein oder mehrere Klone zugeordnet sind, sind die Klone nicht betroffen. Die Klone verweisen weiter auf die Seiten, die zuvor im Besitz des Quell-Cluster-Volumes waren.

Einen Amazon DocumentDB-Klon erstellen

Sie können einen Clone in demselben AWS Konto wie der Amazon DocumentDB DocumentDB-Quellcluster erstellen. Dazu können Sie das AWS-Managementkonsole oder das AWS CLI und die folgenden Verfahren verwenden.

Mithilfe von Amazon DocumentDB-Cloning können Sie einen bereitgestellten Amazon DocumentDB-Cluster-Klon aus einem bereitgestellten Amazon DocumentDB-Cluster erstellen.

Using the AWS-Managementkonsole

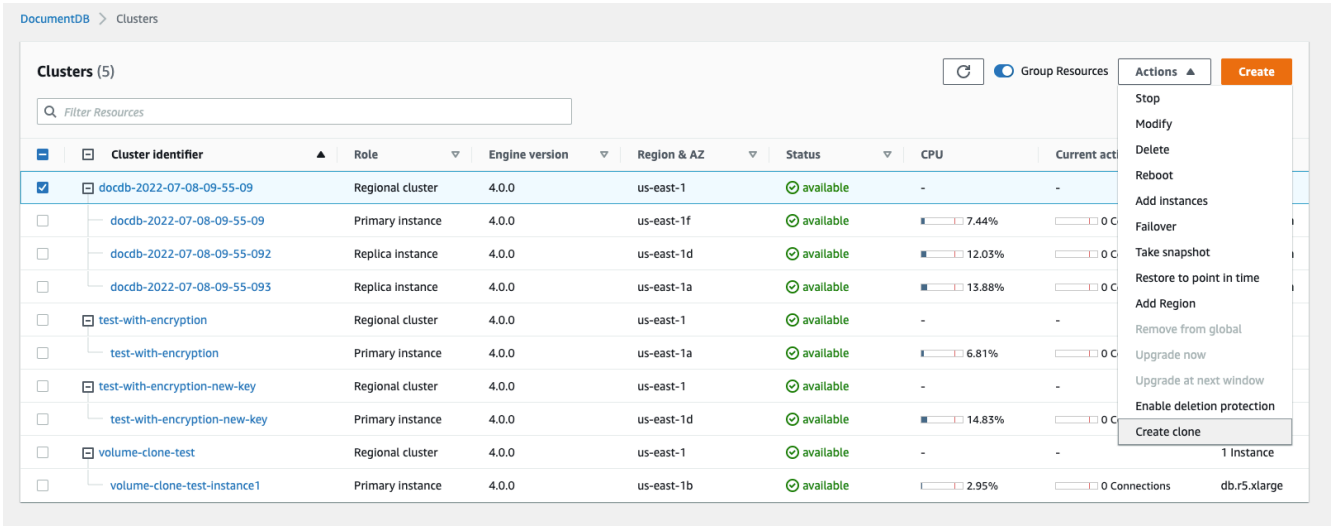
Das folgende Verfahren beschreibt, wie Sie einen Amazon DocumentDB-Cluster mit dem AWS-Managementkonsole klonen.

Erstellen eines Klons anhand der AWS-Managementkonsole Ergebnisse in einem Amazon DocumentDB-Cluster mit einer Amazon DocumentDB DocumentDB-Instance.

Diese Anweisungen gelten für DB-Cluster, die demselben AWS Konto gehören, das den Klon erstellt. Der DB-Cluster muss demselben AWS Konto gehören, da kontoübergreifendes Klonen in Amazon DocumentDB nicht unterstützt wird.

Um einen Klon eines DB-Clusters zu erstellen, der Ihrem gehört AWS Konto mit dem AWS-Managementkonsole

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Klicken Sie im Navigationsbereich auf Cluster.
3. Wählen Sie Ihren Amazon DocumentDB-Cluster aus der Liste aus und wählen Sie für Aktionen die Option Create clone aus.

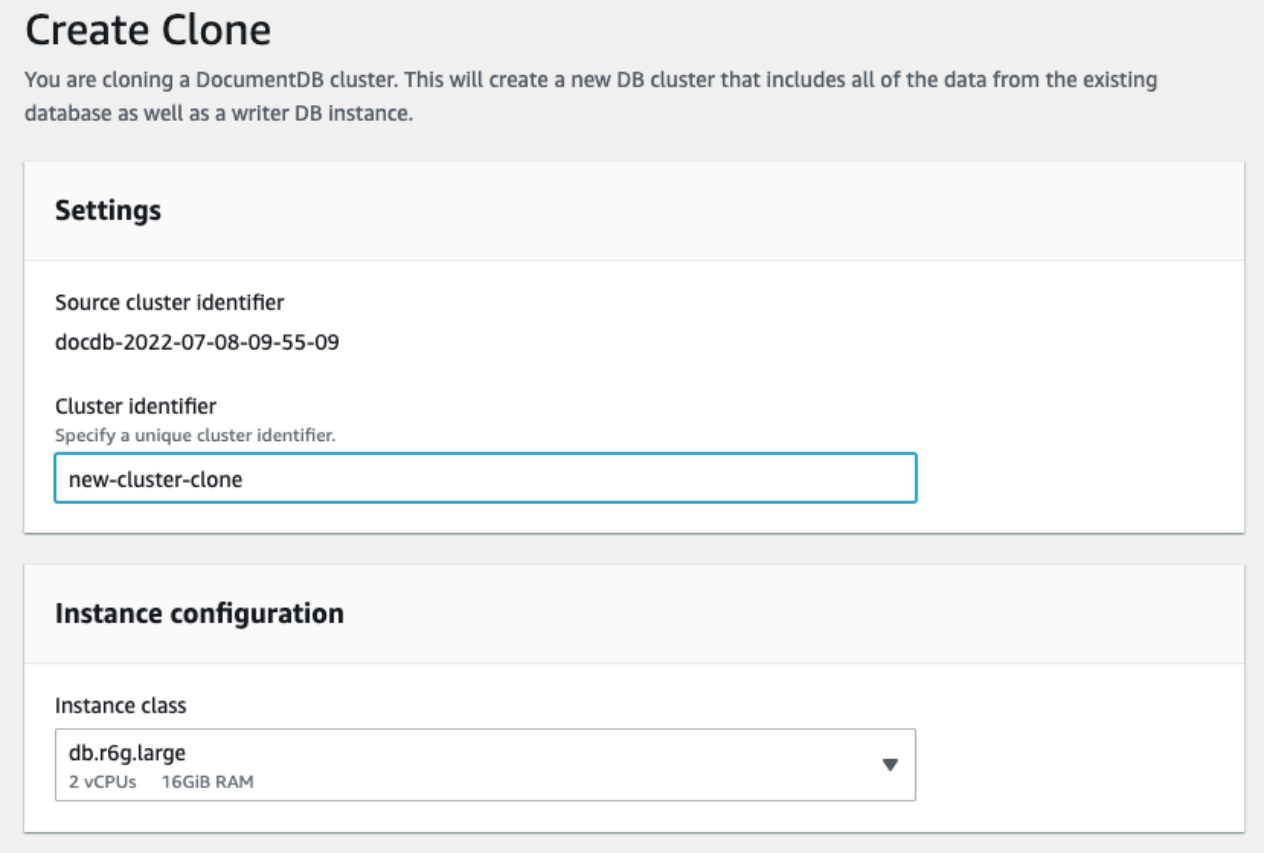


Die Seite „Clone erstellen“ wird geöffnet, auf der Sie eine Cluster-ID und eine Instance-Klasse sowie andere Optionen für den Amazon DocumentDB-Cluster-Klon konfigurieren können.

4. Gehen Sie im Abschnitt Settings (Einstellungen) wie folgt vor:

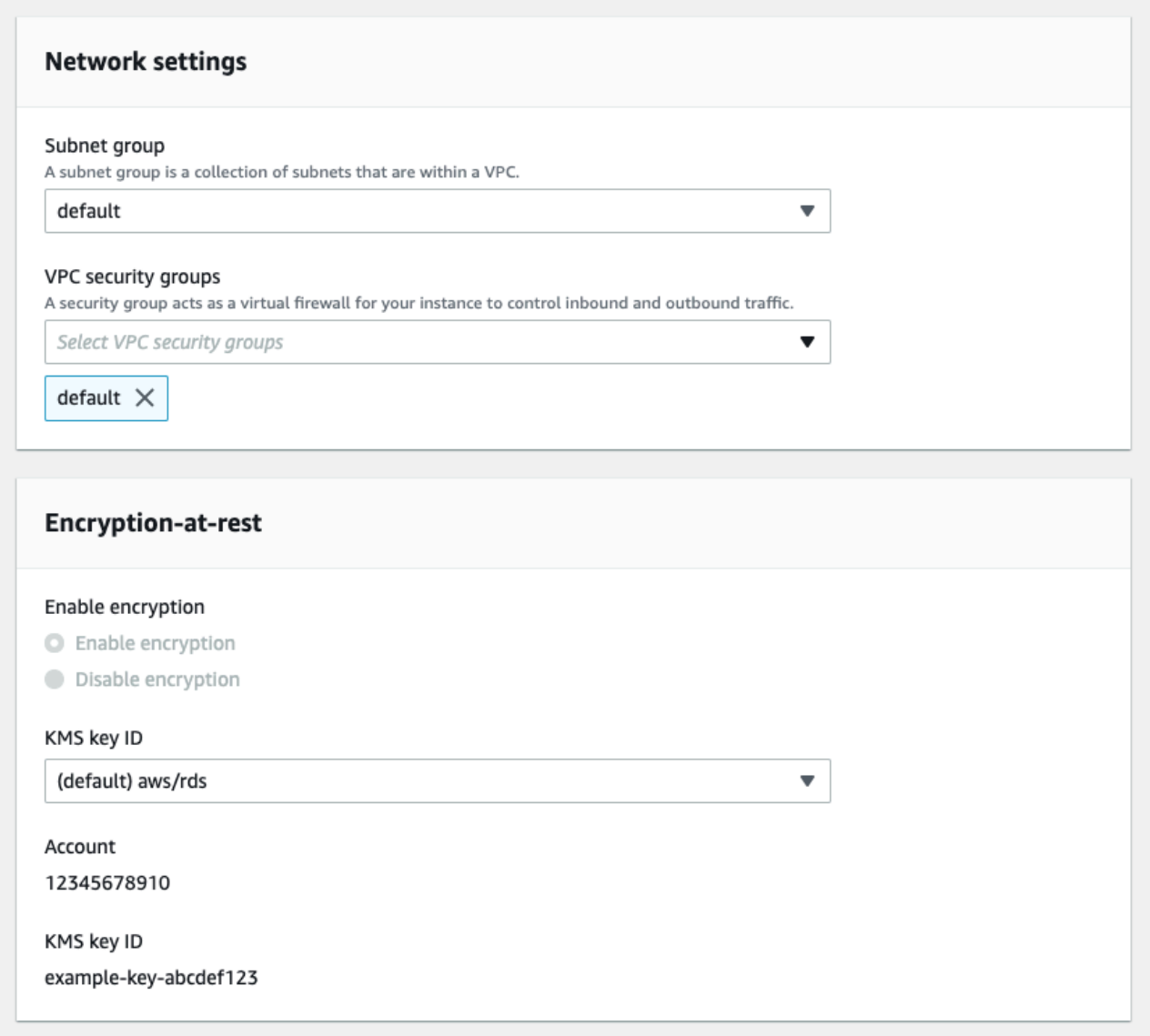
   a. Geben Sie unter Cluster-ID den Namen ein, den Sie Ihrem geklonten Amazon DocumentDB-Cluster geben möchten.

b. Wählen Sie für die Instance-Konfiguration eine geeignete Instance-Klasse für Ihren geklonten Amazon DocumentDB-Cluster aus.

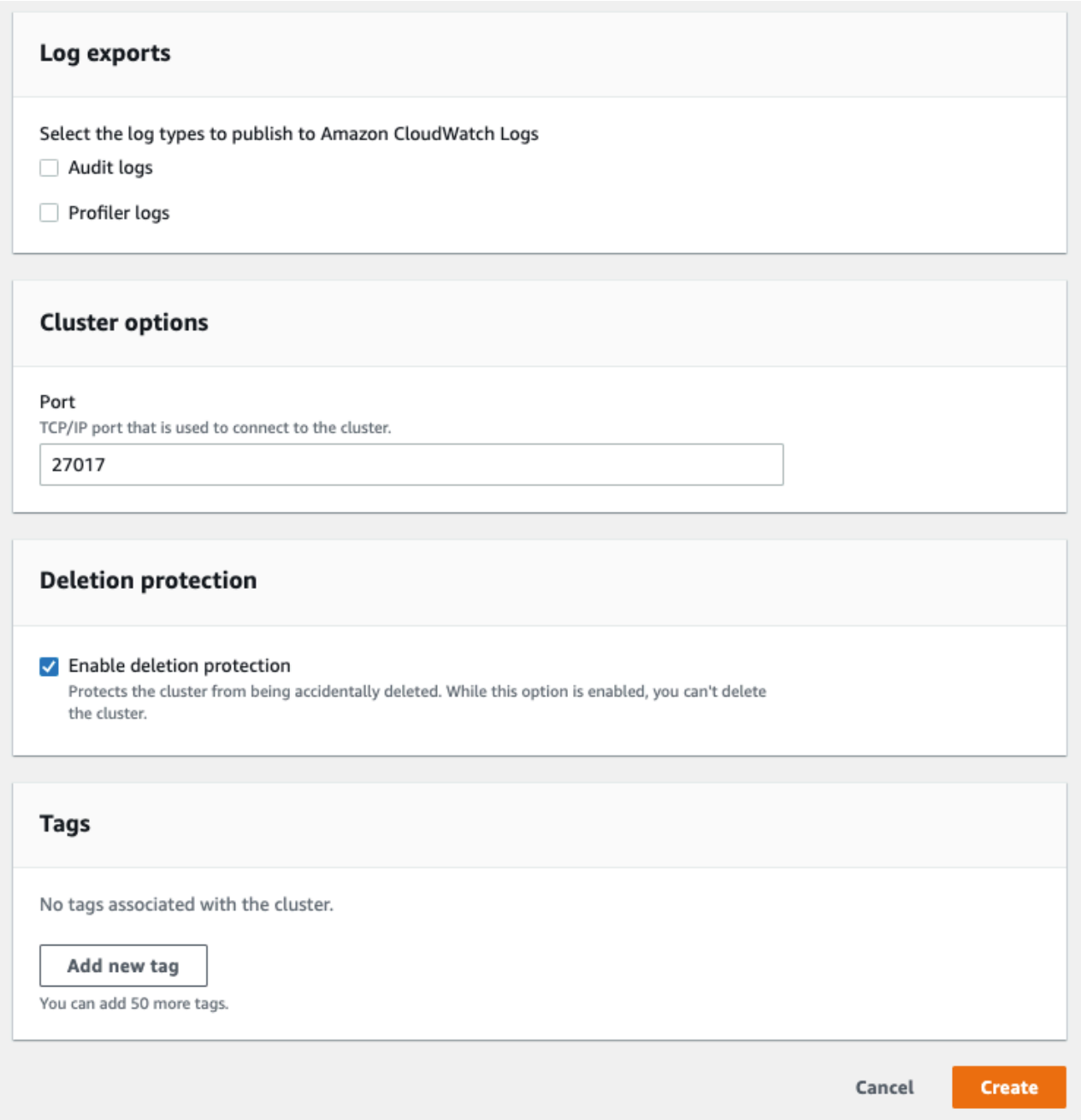


c. Wählen Sie für Netzwerkeinstellungen eine Subnetzgruppe für Ihren Anwendungsfall und die zugehörigen VPC-Sicherheitsgruppen aus.

d. Denn wenn für den Quellcluster (der Cluster Encryption-at-rest, der geklont wird) die Verschlüsselung aktiviert ist, muss auch für den geklonten Cluster die Verschlüsselung aktiviert sein. Wenn dieses Szenario zutrifft, sind die Optionen Verschlüsselung aktivieren ausgegraut (deaktiviert), aber die Option Verschlüsselung aktivieren ist ausgewählt. Umgekehrt, wenn für den Quellcluster keine Verschlüsselung aktiviert ist, sind die Optionen Verschlüsselung aktivieren verfügbar und Sie können wählen, ob die Verschlüsselung aktiviert oder deaktiviert werden soll.



e. Vervollständigen Sie die neue Cluster-Clone-Konfiguration, indem Sie den Typ der zu exportierenden Protokolle auswählen (optional), einen bestimmten Port eingeben, der für die Verbindung mit dem Cluster verwendet wird, und den Schutz vor versehentlichem Löschen des Clusters aktivieren (standardmäßig aktiviert).



f. Beenden Sie die Eingabe aller Einstellungen für Ihren Amazon DocumentDB-Cluster-Klon. Weitere Informationen zu den Cluster- und Instance-Einstellungen von Amazon DocumentDB finden Sie unter[Verwaltung von Amazon DocumentDB-Clustern](#).

5. Wählen Sie Create clone, um den Amazon DocumentDB-Klon Ihres ausgewählten Amazon DocumentDB-Clusters zu starten.

Wenn der Klon erstellt wurde, wird er zusammen mit Ihren anderen Amazon DocumentDB-Clustern im Bereich Datenbanken der Konsole aufgeführt und zeigt seinen aktuellen Status an. Ihr Klon ist einsatzbereit, wenn sein Status Verfügbar ist.

Using the AWS CLI

Die Verwendung des AWS CLI zum Klonen Ihres Amazon DocumentDB-Clusters umfasst einige Schritte.

Der `restore-db-cluster-to-point-in-time` AWS CLI Befehl, den Sie verwenden, führt zu einem leeren Amazon DocumentDB-Cluster mit 0 Amazon DocumentDB DocumentDB-Instances. Das heißt, der Befehl stellt nur den Amazon DocumentDB-Cluster wieder her, nicht die DB-Instances für diesen Cluster. Sie tun dies separat, nachdem der Klon verfügbar ist. Die zwei Schritte im Prozess sind wie folgt:

1. Erstellen Sie den Klon mit dem CLI-Befehl restore-db-cluster-to-point-in-time. Die Parameter, die Sie mit diesem Befehl verwenden, steuern den Kapazitätstyp und andere Details des leeren Amazon DocumentDB-Clusters (Klons), der erstellt wird.
2. Erstellen Sie die Amazon DocumentDB-Instance für den Clone, indem Sie den CLI-Befehl create-db-instance verwenden, um die Amazon DocumentDB-Instance im wiederhergestellten Amazon DocumentDB-Cluster neu zu erstellen.

Bei den folgenden Befehlen wird davon ausgegangen, dass der standardmäßig mit Ihrer AWS CLI Region eingerichtet ist. AWS Dieser Ansatz erspart Ihnen die Übergabe des `--region`-Namens in jedem der Befehle. Weitere Informationen finden Sie unter Konfigurieren der AWS CLI. Sie können die `--region` auch in jedem der folgenden CLI-Befehle angeben.

Der Klon wird erstellt

Die spezifischen Parameter, die Sie an den `restore-db-cluster-to-point-in-time`-CLI-Befehl übergeben, variieren. Was Sie übergeben, hängt von der Art des Klons ab, den Sie erstellen möchten.

Gehen Sie wie folgt vor, um einen bereitgestellten Amazon DocumentDB-Klon aus einem bereitgestellten Amazon DocumentDB-Cluster zu erstellen.

Um einen Klon desselben Engine-Modus wie der Amazon DocumentDB DocumentDB-Quellcluster zu erstellen

- Verwenden Sie den `restore-db-cluster-to-point-in-time`-CLI-Befehl und geben Sie Werte für die folgenden Parameter an:

  - `--db-cluster-identifier` – Wählen Sie einen aussagekräftigen Namen für Ihren Klon. Sie benennen den Klon, wenn Sie den CLI-Befehl restore-db-cluster-to-point-in-time verwenden.
  - `--restore-type` – Verwenden Sie `copy-on-write`, um einen Klon des Quell-DB-Clusters zu erstellen. Ohne diesen Parameter `restore-db-cluster-to-point-in-time` stellt der den Amazon DocumentDB-Cluster wieder her, anstatt einen Klon zu erstellen. Die Standardeinstellung für `restore-type` ist`full-copy`.
  - `--source-db-cluster-identifier`— Verwenden Sie den Namen des Amazon DocumentDB DocumentDB-Quellclusters, den Sie klonen möchten.
  - `--use-latest-restorable-time` – Dieser Wert verweist auf die neuesten wiederherstellbaren Volume-Daten für den Klon. Dieser Parameter ist erforderlich für`restore-type copy-on-write`, Sie können den jedoch nicht `restore-to-time parameter` zusammen verwenden.

Im folgenden Beispiel wird ein Klon namens `my-clone` aus einem Cluster namens `my-source-cluster` erstellt.

Für Linux, macOS oder Unix:

```
aws docdb restore-db-cluster-to-point-in-time \
    --source-db-cluster-identifier my-source-cluster \
    --db-cluster-identifier my-clone \
    --restore-type copy-on-write \
    --use-latest-restorable-time
```

Für Windows:

```
aws docdb restore-db-cluster-to-point-in-time ^
    --source-db-cluster-identifier my-source-cluster ^
    --db-cluster-identifier my-clone ^
    --restore-type copy-on-write ^
    --use-latest-restorable-time
```

Der Befehl gibt das JSON-Objekt zurück, das Details des Klons enthält. Stellen Sie sicher, dass Ihr geklonter DB-Cluster verfügbar ist, bevor Sie versuchen, die DB-Instance für Ihren Klon zu erstellen. Weitere Informationen finden Sie weiter unten unter Status überprüfen und Details zum Klonen abrufen:

Status überprüfen und Details zum Klonen abrufen

Mit dem folgenden Befehl können Sie den Status Ihres neu erstellten leeren DB-Clusters überprüfen.

```
$ aws docdb describe-db-clusters --db-cluster-identifier my-clone --query '*[].
[Status]' --output text
```

Oder Sie können den Status und die anderen Werte, die Sie zum Erstellen der DB-Instance für Ihren Clone benötigen, mithilfe der folgenden AWS CLI Abfrage abrufen:

Für Linux, macOS oder Unix:

```
aws docdb describe-db-clusters --db-cluster-identifier my-clone \
  --query '*[].{Status:Status,Engine:Engine,EngineVersion:EngineVersion}'
```

Für Windows:

```
aws docdb describe-db-clusters --db-cluster-identifier my-clone ^
  --query "*[].{Status:Status,Engine:Engine,EngineVersion:EngineVersion}"
```

Diese Abfrage gibt eine Ausgabe ähnlich der folgenden zurück.

```
[
  {
        "Status": "available",
        "Engine": "docdb",
        "EngineVersion": "4.0.0",
    }
]
```

Erstellen der Amazon DocumentDB DocumentDB-Instance für Ihren Clone

Verwenden Sie den CLI-Befehl create-db-instance, um die DB-Instance für Ihren Klon zu erstellen.

Der `--db-instance-class` Parameter wird nur für bereitgestellte Amazon DocumentDB-Cluster verwendet.

Für Linux, macOS oder Unix:

```
aws docdb create-db-instance \
    --db-instance-identifier my-new-db \
    --db-cluster-identifier my-clone \
    --db-instance-class  db.r5.4xlarge \
    --engine docdb
```

Für Windows:

```
aws docdb create-db-instance ^
    --db-instance-identifier my-new-db ^
    --db-cluster-identifier my-clone ^
    --db-instance-class  db.r5.4xlarge ^
    --engine docdb
```

Parameter, die für das Klonen verwendet werden sollen

In der folgenden Tabelle sind die verschiedenen Parameter zusammengefasst, die zum Klonen von Amazon DocumentDB-Clustern verwendet werden. `restore-db-cluster-to-point-in-time`

Parameter	Beschreibung
--source-db-cluster-identifier	Verwenden Sie den Namen des Amazon DocumentDB DocumentDB-Quellclusters, den Sie klonen möchten.
--db-cluster-identifier	Wählen Sie einen aussagekräftigen Namen für Ihren Klon. Sie benennen Ihren Klon mit dem `restore-db-cluster-to-point-in-time` -Befehl. Dann übergeben Sie diesen Namen an den `create-db-instance` -Befehl.
--restore-type	Geben Sie `copy-on-write` als an`--restore-type` , um einen Klon des Quell-DB-Clusters zu erstellen, anstatt den Amazon DocumentDB DocumentDB-Quellcluster wiederherzustellen.

Parameter	Beschreibung
--use-latest-restorable-time	ieser Wert verweist auf die neuesten wiederherstellbaren Volume-Daten für den Klon.

Grundlegendes zur Amazon DocumentDB-Cluster-Fehlertoleranz

Amazon DocumentDB-Cluster sind von Natur aus fehlertolerant. Das Volume jedes Clusters erstreckt sich über mehrere Availability Zones in einem einzigen AWS-Region, und jede Availability Zone enthält eine Kopie der Volume-Daten des Clusters. Diese Funktionalität bedeutet, dass Ihr Cluster einen Ausfall der Availability Zone ohne Datenverlust und nur eine kurze Unterbrechung des Services tolerieren kann.

Wenn die primäre Instance in einem Cluster ausfällt, führt Amazon DocumentDB auf zwei Arten automatisch einen Failover zu einer neuen primären Instance durch:

- Indem Sie ein vorhandenes Amazon DocumentDB DocumentDB-Replikat auf die neue primäre Instance heraufstufen, die auf der Grundlage der Promotion-Kontingent-Einstellung für jedes Replikat ausgewählt wurde, und dann einen Ersatz für die frühere primäre Instance erstellen. Ein Failover zur Replikat-Instance dauert in der Regel weniger als 30 Sekunden. Während dieses Zeitraums kann es bei Lese- und Schreibvorgängen zu kurzen Unterbrechungen kommen. Um die Verfügbarkeit Ihres Clusters zu erhöhen, empfehlen wir Ihnen, mindestens ein oder mehrere Amazon DocumentDB DocumentDB-Replikate in zwei oder mehr verschiedenen Availability Zones zu erstellen.
- Über das Anlegen einer neuen primären Instance. Dies passiert nur, wenn Sie keine Replikatinstanz in Ihrem Cluster haben und es kann einige Minuten dauern, bis der Vorgang abgeschlossen ist.

Wenn der Cluster über ein oder mehrere Amazon DocumentDB DocumentDB-Replikate verfügt, wird ein Amazon DocumentDB DocumentDB-Replikat bei einem Ausfall zur primären Instance heraufgestuft. Ein Fehlerereignis hat eine kurze Unterbrechung zufolge, während die Lese- und Schreibvorgänge mit einer Ausnahme fehlschlagen. Jedoch wird der Service im Normalfall in weniger als 120 Sekunden und oft sogar schon nach 60 Sekunden wiederhergestellt. Um die Verfügbarkeit Ihres Clusters zu erhöhen, empfehlen wir Ihnen, mindestens ein oder mehrere Amazon DocumentDB DocumentDB-Replikate in zwei oder mehr verschiedenen Availability Zones zu erstellen.

Sie können die Reihenfolge anpassen, in der Ihre Amazon DocumentDB DocumentDB-Replikate nach einem Ausfall zur primären Instance heraufgestuft werden, indem Sie jedem Replikat eine Priorität zuweisen. Prioritäten liegen im Bereich zwischen 0 als höchste Priorität und 15 als niedrigste Priorität. Wenn die primäre Instance ausfällt, wird das Amazon DocumentDB DocumentDB-Replikat mit der höchsten Priorität zur neuen primären Instance heraufgestuft. Sie können die Priorität eines Amazon DocumentDB DocumentDB-Replikats jederzeit ändern. Das Ändern der Priorität löst kein Failover aus. Sie können die `modify-db-instance`-Operation mit dem `--promotion-tier`-Parameter verwenden. Weitere Informationen zum Anpassen der Failover-Priorität einer Instance finden Sie unter Amazon DocumentDB-Failover.

Mehr als ein Amazon DocumentDB DocumentDB-Replikat kann dieselbe Priorität haben, was zu Aktionsstufen führt. Wenn zwei oder mehr Amazon DocumentDB DocumentDB-Replikate dieselbe Priorität haben, wird das Replikat mit der größten Größe zum primären Replikat heraufgestuft. Wenn zwei oder mehr Amazon DocumentDB DocumentDB-Replikate dieselbe Priorität und Größe haben, wird ein beliebiges Replikat in derselben Promotion-Stufe heraufgestuft.

Wenn der Cluster keine Amazon DocumentDB DocumentDB-Replikate enthält, wird die primäre Instance bei einem Ausfall neu erstellt. Ein Fehlerereignis hat eine Unterbrechung zufolge, während die Lese- und Schreibvorgänge mit einer Ausnahme fehlschlagen. Der Service wird wiederhergestellt, wenn die primäre Instance erstellt wird. Dies dauert im Normalfall weniger als 10 Minuten. Das Heraufstufen eines Amazon DocumentDB-Replikats zur primären Instance ist viel schneller als das Erstellen einer neuen primären Instance.

Verwaltung von Amazon DocumentDB DocumentDB-Instances

Die folgenden Themen enthalten Informationen, die Ihnen bei der Verwaltung Ihrer Amazon DocumentDB DocumentDB-Instances helfen sollen. Sie umfassen Details über Instance-Klassen und Statusarten und das Erstellen, Löschen und Ändern einer Instance.

Themen

- Den Status einer Instance ermitteln
- Lebenszyklus einer Amazon DocumentDB DocumentDB-Instanz
- Instanzklassen verwalten
- NVMe-backed Instanzen

Den Status einer Instance ermitteln

Mehr zu den gültigen Instance-Zuständen, ihre Bedeutung und die Bestimmung des Status Ihrer Instances finden Sie unter Den Status einer Amazon DocumentDB DocumentDB-Instance überwachen.

Lebenszyklus einer Amazon DocumentDB DocumentDB-Instanz

Der Lebenszyklus einer Amazon DocumentDB DocumentDB-Instance umfasst das Erstellen, Ändern, Verwalten und Aktualisieren, das Durchführen von Backups und Wiederherstellungen, das Neustarten und Löschen der Instance. Dieser Abschnitt enthält Informationen darüber, wie Sie diese Prozesse abschließen können.

Themen

- Hinzufügen einer Amazon DocumentDB DocumentDB-Instance zu einem Cluster
- Beschreibung von Amazon DocumentDB DocumentDB-Instances
- Ändern einer Amazon DocumentDB DocumentDB-Instance
- Eine Amazon DocumentDB DocumentDB-Instance neu starten
- Löschen einer Amazon DocumentDB DocumentDB-Instance

Sie können eine neue Amazon DocumentDB DocumentDB-Instance mit dem AWS-Managementkonsole oder dem AWS CLI erstellen. Um eine Instance zu einem Cluster hinzuzufügen, muss sich der Cluster im Zustand available befinden. Zu einem angehaltenen Cluster können keine Instances hinzugefügt werden. Wenn der Cluster angehalten ist, starten Sie zuerst den Cluster, warten Sie, bis der Cluster verfügbar wird, und fügen Sie dann eine Instance hinzu. Weitere Informationen finden Sie unter Einen Amazon DocumentDB-Cluster stoppen und starten.

> **Note**
>
> Wenn Sie mit der Konsole einen Amazon DocumentDB-Cluster erstellen, wird gleichzeitig automatisch eine Instance für Sie erstellt. Wenn Sie zusätzliche Instances erstellen möchten, verwenden Sie eines der folgenden Verfahren.

Hinzufügen einer Amazon DocumentDB DocumentDB-Instance zu einem Cluster

Using the AWS-Managementkonsole

Gehen Sie wie folgt vor, um mithilfe der Amazon DocumentDB DocumentDB-Konsole eine Instance für Ihren Cluster zu erstellen.

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Klicken Sie im Navigationsbereich auf Cluster.

   > **Tip**
   >
   > Wenn der Navigationsbereich auf der linken Seite des Bildschirms nicht angezeigt wird, wählen Sie links oben auf der Seite das Menüsymbol (≡) aus.

3. Um den Cluster zu wählen, dem Sie eine Instance hinzufügen möchten, wählen Sie die Schaltfläche links vom Namen des Clusters aus.
4. Wählen Sie Actions (Aktionen) und dann Add instances (Instances hinzufügen) aus.
5. Wiederholen Sie die folgenden Schritte für jede Instance, die Sie dem Cluster hinzufügen möchten, auf der Seite Add instance to: (Instance hinzufügen zu:)<cluster-name>. Sie können bis zu 15 haben.

   a. Instance-ID — Sie können entweder eine eindeutige Kennung für diese Instance eingeben oder Amazon DocumentDB erlauben, die Instance-ID auf der Grundlage der Cluster-ID bereitzustellen.

      Einschränkungen für Instance-Benennungen:

      - Die Länge beträgt [1—63] Buchstaben, Zahlen oder Bindestriche.
      - Muss mit einem Buchstaben beginnen.
      - Darf nicht mit einem Bindestrich enden oder zwei aufeinanderfolgende Bindestriche enthalten.
      - Muss für alle Instances in Amazon RDS, Neptune und Amazon DocumentDB pro AWS-Konto Region eindeutig sein.

   b. Instance-Klasse — Wählen Sie aus der Drop-down-Liste den Instance-Typ aus, den Sie für diese Instance benötigen.

c. Promotion-Stufe — Wählen Sie aus der Drop-down-Liste die Promotion-Stufe für Ihre Instance oder wählen Sie Keine Präferenz, damit Amazon DocumentDB die Promotion-Stufe für Ihre Instance festlegen kann. Niedrigere Nummern bedeuten eine höhere Priorität. Weitere Informationen finden Sie unter Steuerung des Failover-Ziels.

d. Zum Hinzufügen weiterer Instances wählen Sie die Option Add additional instances (Weitere Instances hinzufügen) und wiederholen Sie die Schritte a, b und c.

6. Schließen Sie den Vorgang ab.

   - Wenn Sie die Instances zu Ihrem Cluster hinzufügen möchten, klicken Sie auf Create (Erstellen).
   - Um die Operation abzubrechen, wählen Sie Abbrechen aus.

Es dauert einige Minuten, bis eine Instance erstellt ist. Sie können die Konsole verwenden oder AWS CLI den Status der Instance einsehen. Weitere Informationen finden Sie unter Den Status einer Instance überwachen.

Using the AWS CLI

Verwenden Sie den `create-db-instance` AWS CLI Vorgang mit den folgenden Parametern, um die primäre Instance für Ihren Cluster zu erstellen.

- **`--db-instance-class`** – Erforderlich. Die Rechen- und Speicherkapazität der Instance, beispielsweise `db.m4.large`. Nicht alle Instanzklassen sind in allen verfügbar AWS-Regionen.
- **`--db-instance-identifier`** – Erforderlich. Eine -Zeichenfolge in Kleinbuchstaben, die die Instance bezeichnet.

  Instance-Benennungseinschränkungen:

  - Die Länge beträgt [1—63] Buchstaben, Zahlen oder Bindestriche.
  - Muss mit einem Buchstaben beginnen.
  - Darf nicht mit einem Bindestrich enden oder zwei aufeinanderfolgende Bindestriche enthalten.
  - Muss für alle Instances in Amazon RDS, Neptune und Amazon DocumentDB pro AWS-Konto Region eindeutig sein.
- **`--engine`** – Erforderlich. Der Wert muss `docdb` sein.
- **`--availability-zone`**— Fakultativ. Die Availability Zone, in der diese Instance erstellt werden soll. Verwenden Sie diesen Parameter, um Ihre Instances in verschiedenen Availability

Zones zur Erhöhung der Fehlertoleranz zu finden. Weitere Informationen finden Sie unter Amazon DocumentDB Hochverfügbarkeit und Replikation.

- **`--promotion-tier`**— Fakultativ. Die Failover-Prioritätsstufe für diese Instance. Muss zwischen 0 und 15 liegen, wobei niedrigere Nummern eine höhere Priorität bedeuten. Weitere Informationen finden Sie unter Steuerung des Failover-Ziels.

1. Bestimmen Sie zunächst, in welchen Availability Zones Sie Ihre Instance erstellen können.

   Wenn Sie die Availability Zone angeben möchten, bevor Sie Ihre Instance erstellen, führen Sie den folgenden Befehl aus, um zu ermitteln, welche Availability Zones für Ihren Amazon DocumentDB-Cluster verfügbar sind.

   Für Linux, macOS oder Unix:

   ```
   aws docdb describe-db-clusters \
         --query 'DBClusters[*].[DBClusterIdentifier,AvailabilityZones[*]]'
   ```

   Für Windows:

   ```
   aws docdb describe-db-clusters ^
         --query 'DBClusters[*].[DBClusterIdentifier,AvailabilityZones[*]]'
   ```

   Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus.

   ```
   [
       [
           "sample-cluster",
           [
               "us-east-1c",
               "us-east-1b",
               "us-east-1a"
           ]
       ]
   ]
   ```

2. Bestimmen Sie dann, welche Instance-Klassen Sie in Ihrer Region erstellen können.

Führen Sie den folgenden Befehl aus, um festzustellen, welche Instance-Klassen Ihnen in Ihrer Region zur Verfügung stehen. Wählen Sie aus der Ausgabe eine Instance-Klasse für die Instance aus, die Sie Ihrem Amazon DocumentDB-Cluster hinzufügen möchten.

Für Linux, macOS oder Unix:

```
aws docdb describe-orderable-db-instance-options \
        --engine docdb \
        --query 'OrderableDBInstanceOptions[*].DBInstanceClass'
```

Für Windows:

```
aws docdb describe-orderable-db-instance-options ^
        --engine docdb ^
        --query 'OrderableDBInstanceOptions[*].DBInstanceClass'
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus.

```
[
    "db.r5.16xlarge",
    "db.r5.2xlarge",
    "db.r5.4xlarge",
    "db.r5.8xlarge",
    "db.r5.large",
    "db.r5.xlarge"
]
```

3. Fügen Sie abschließend eine Instance zu Ihrem Amazon DocumentDB-Cluster hinzu.

   Um Ihrem Amazon DocumentDB-Cluster eine Instance hinzuzufügen, führen Sie den folgenden Befehl aus.

   Für Linux, macOS oder Unix:

```
aws docdb create-db-instance \
       --db-cluster-identifier sample-cluster \
       --db-instance-identifier sample-instance-2 \
       --availability-zone us-east-1b \
       --promotion-tier 2 \
       --db-instance-class db.r5.xlarge \
```

```
        --engine docdb
```

Für Windows:

```
aws docdb create-db-instance ^
       --db-cluster-identifier sample-cluster ^
       --db-instance-identifier sample-instance-2 ^
       --availability-zone us-east-1b ^
       --promotion-tier 2 ^
       --db-instance-class db.r5.xlarge ^
       --engine docdb
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus.

```
{
    "DBInstance": {
        "DBInstanceIdentifier": "sample-instance-2",
        "DBInstanceClass": "db.r5.xlarge",
        "Engine": "docdb",
        "DBInstanceStatus": "creating",
        "PreferredBackupWindow": "02:00-02:30",
        "BackupRetentionPeriod": 1,
        "VpcSecurityGroups": [
            {
                "VpcSecurityGroupId": "sg-abcd0123",
                "Status": "active"
            }
        ],
        "AvailabilityZone": "us-east-1b",
        "DBSubnetGroup": {
            "DBSubnetGroupName": "default",
            "DBSubnetGroupDescription": "default",
            "VpcId": "vpc-6242c31a",
            "SubnetGroupStatus": "Complete",
            "Subnets": [
                {
                    "SubnetIdentifier": "subnet-abcd0123",
                    "SubnetAvailabilityZone": {
                        "Name": "us-west-2a"
                    },
                    "SubnetStatus": "Active"
                },
```

```
                {
                    "SubnetIdentifier": "subnet-wxyz0123",
                    "SubnetAvailabilityZone": {
                        "Name": "us-west-2b"
                    },
                    "SubnetStatus": "Active"
                }
            ]
        },
        "PreferredMaintenanceWindow": "sun:11:35-sun:12:05",
        "PendingModifiedValues": {},
        "EngineVersion": "3.6.0",
        "AutoMinorVersionUpgrade": true,
        "PubliclyAccessible": false,
        "DBClusterIdentifier": "sample-cluster",
        "StorageEncrypted": true,
        "KmsKeyId": "arn:aws:kms:us-east-1:<accountID>:key/sample-key",
        "DbiResourceId": "db-ABCDEFGHIJKLMNOPQRSTUVWXYZ",
        "CACertificateIdentifier": "rds-ca-2019",
        "PromotionTier": 2,
        "DBInstanceArn": "arn:aws:rds:us-east-1:<accountID>:db:sample-instance-2"
    }
}
```

Es dauert einige Minuten, bis die Instance erstellt ist. Sie können die Konsole verwenden oder AWS CLI den Status der Instance einsehen. Weitere Informationen finden Sie unter Den Status einer Amazon DocumentDB DocumentDB-Instance überwachen.

Beschreibung von Amazon DocumentDB DocumentDB-Instances

Sie können entweder die Amazon DocumentDB-Managementkonsole oder die verwenden, AWS CLI um Details wie Verbindungsendpunkte, Sicherheitsgruppen, VPCs, Zertifizierungsstellen und Parametergruppen zu Ihren Amazon DocumentDB DocumentDB-Instances anzuzeigen.

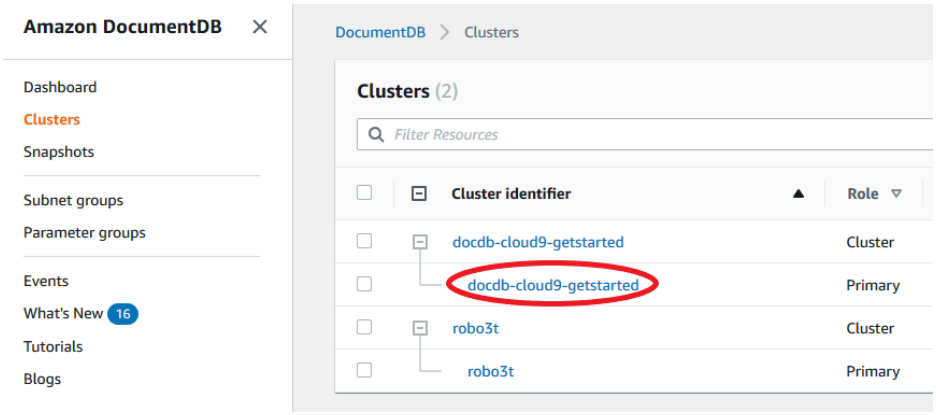
Using the AWS-Managementkonsole

Gehen Sie folgendermaßen vor, um die Details Ihrer Instances mithilfe der AWS-Managementkonsole anzuzeigen.

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Klicken Sie im Navigationsbereich auf Cluster.

> **Tip**
>
> Wenn der Navigationsbereich auf der linken Seite des Bildschirms nicht angezeigt wird, wählen Sie links oben auf der Seite das Menüsymbol (≡) aus.

3. Im Cluster-Navigationsfeld sehen Sie die Spalte Cluster-ID. Ihre Instances werden unter Clustern aufgeführt, ähnlich wie im folgenden Screenshot.



4. Wählen Sie in der Liste der Instances den Namen der Instanz aus, deren Details Sie sehen möchten. Die Informationen über die Instance sind in die folgenden Gruppierungen unterteilt:

   - Zusammenfassung — Allgemeine Informationen über die Instanz, einschließlich der Engine-Version, der Klasse, des Status und aller ausstehenden Wartungsarbeiten.
   - Konnektivität und Sicherheit — Der Abschnitt Connect listet die Verbindungsendpunkte auf, um mit der Mongo-Shell oder mit einer Anwendung eine Verbindung zu dieser Instanz herzustellen. Im Abschnitt Sicherheitsgruppen werden die Sicherheitsgruppen aufgeführt, die dieser Instance zugeordnet sind, sowie ihre VPC-ID und Beschreibungen.
   - Konfiguration — Der Abschnitt „Details“ listet die Konfigurationen und den Status der Instance auf, einschließlich des Amazon-Ressourcennamens (ARN), des Endpunkts, der Rolle, der Klasse und der Zertifizierungsstelle der Instance. Außerdem werden die Sicherheits- und Netzwerkeinstellungen der Instance sowie die Sicherungsinformationen aufgelistet. Im Abschnitt Cluster-Details werden die Details des Clusters aufgeführt, zu dem diese Instance gehört. Im Abschnitt Cluster-Instances werden alle Instances aufgeführt,

die zu Ihrem Cluster gehören, mit dem Status der einzelnen Instance-Rollen und Cluster-Parametergruppen.

> **Note**
>
> Sie können den mit Ihrer Instance verknüpften Cluster ändern, indem Sie neben der Überschrift Cluster-Details auf Ändern klicken. Weitere Informationen finden Sie unter Ändern eines Amazon DocumentDB-Clusters.

- Überwachung — Die CloudWatch Log-Metriken für diese Instance. Weitere Informationen finden Sie unter Überwachen von Amazon DocumentDB mit CloudWatch.
- Ereignisse und Tags — Der Abschnitt Aktuelle Ereignisse listet die jüngsten Ereignisse für diese Instance auf. Amazon DocumentDB zeichnet Ereignisse auf, die sich auf Ihre Cluster, Instances, Snapshots, Sicherheitsgruppen und Cluster-Parametergruppen beziehen. Zu diesen Informationen gehören Datum, Uhrzeit und Nachricht, die jedem Ereignis zugeordnet sind. Der Abschnitt Tags listet die an diesen Cluster angehängten Tags auf. Weitere Informationen finden Sie unter Taggen von Amazon DocumentDB DocumentDB-Ressourcen.

Using the AWS CLI

Um die Details Ihrer Amazon DocumentDB DocumentDB-Instances mithilfe von anzuzeigen AWS CLI, verwenden Sie den `describe-db-clusters` Befehl, wie in den folgenden Beispielen gezeigt. Weitere Informationen finden Sie `DescribeDBInstances`in der Amazon DocumentDB Resource Management API-Referenz.

> **Note**
>
> Für bestimmte Verwaltungsfunktionen wie Cluster- und Instance-Lebenszyklusmanagement nutzt Amazon DocumentDB Betriebstechnologie, die mit Amazon RDS gemeinsam genutzt wird. Der `filterName=engine,Values=docdb` Filterparameter gibt nur Amazon DocumentDB-Cluster zurück.

1. Listet alle Amazon DocumentDB DocumentDB-Instances auf.

   Der folgende AWS CLI Code listet die Details für alle Amazon DocumentDB DocumentDB-Instances in einer Region auf.

Für Linux, macOS oder Unix:

```
aws docdb describe-db-instances \
    --filter Name=engine,Values=docdb
```

Für Windows:

```
aws docdb describe-db-instances \
    --filter Name=engine,Values=docdb
```

2. Alle Details für eine angegebene Amazon DocumentDB DocumentDB-Instance auflisten

Der folgende Code listet die Details für `sample-cluster-instance` auf. Das Einschließen des Parameters `--db-instance-identifier` mit dem Namen einer Instance beschränkt die Ausgabe auf Informationen zu dieser bestimmten Instance.

Für Linux, macOS oder Unix:

```
aws docdb describe-db-instances \
    --db-instance-identifier sample-cluster-instance
```

Für Windows:

```
aws docdb describe-db-instances \
    --db-instance-identifier sample-cluster-instance
```

Die Ausgabe dieser Operation sieht folgendermaßen aus.

```
{
    "DBInstances": [
        {
            "DbiResourceId": "db-BJKKB54PIDV5QFKGVRX5T3S6GM",
            "DBInstanceArn": "arn:aws:rds:us-east-1:012345678901:db:sample-
cluster-instance-00",
            "VpcSecurityGroups": [
                {
                    "VpcSecurityGroupId": "sg-77186e0d",
                    "Status": "active"
                }
            ],
```

```
            "DBInstanceClass": "db.r5.large",
            "DBInstanceStatus": "creating",
            "AutoMinorVersionUpgrade": true,
            "PreferredMaintenanceWindow": "fri:09:32-fri:10:02",
            "BackupRetentionPeriod": 1,
            "StorageEncrypted": true,
            "DBClusterIdentifier": "sample-cluster",
            "EngineVersion": "3.6.0",
            "AvailabilityZone": "us-east-1a",
            "Engine": "docdb",
            "PromotionTier": 2,
            "DBInstanceIdentifier": "sample-cluster-instance",
            "PreferredBackupWindow": "00:00-00:30",
            "PubliclyAccessible": false,
            "DBSubnetGroup": {
                "DBSubnetGroupName": "default",
                "Subnets": [
                    {
                        "SubnetIdentifier": "subnet-4e26d263",
                        "SubnetAvailabilityZone": {
                            "Name": "us-east-1a"
                        },
                        "SubnetStatus": "Active"
                    },
                    {
                        "SubnetIdentifier": "subnet-afc329f4",
                        "SubnetAvailabilityZone": {
                            "Name": "us-east-1c"
                        },
                        "SubnetStatus": "Active"
                    },
                    {
                        "SubnetIdentifier": "subnet-b3806e8f",
                        "SubnetAvailabilityZone": {
                            "Name": "us-east-1e"
                        },
                        "SubnetStatus": "Active"
                    },
                    {
                        "SubnetIdentifier": "subnet-53ab3636",
                        "SubnetAvailabilityZone": {
                            "Name": "us-east-1d"
                        },
                        "SubnetStatus": "Active"
```

```
                    },
                    {
                        "SubnetIdentifier": "subnet-991cb8d0",
                        "SubnetAvailabilityZone": {
                            "Name": "us-east-1b"
                        },
                        "SubnetStatus": "Active"
                    },
                    {
                        "SubnetIdentifier": "subnet-29ab1025",
                        "SubnetAvailabilityZone": {
                            "Name": "us-east-1f"
                        },
                        "SubnetStatus": "Active"
                    }
                ],
                "VpcId": "vpc-91280df6",
                "DBSubnetGroupDescription": "default",
                "SubnetGroupStatus": "Complete"
            },
            "PendingModifiedValues": {},
            "KmsKeyId": "arn:aws:kms:us-east-1:012345678901:key/0961325d-
a50b-44d4-b6a0-a177d5ff730b"
        }
    ]
}
```

Ändern einer Amazon DocumentDB DocumentDB-Instance

Sie können Ihre Amazon DocumentDB DocumentDB-Instance entweder mit dem AWS-Managementkonsole oder dem AWS CLIändern. Nur Instances im Status available können geändert werden. Eine angehaltene Instance kann nicht geändert werden. Wenn der Cluster angehalten ist, starten Sie zuerst den Cluster, warten Sie, bis die Instance verfügbar wird, und nehmen Sie dann die gewünschten Änderungen vor. Weitere Informationen finden Sie unter Einen Amazon DocumentDB-Cluster stoppen und starten.

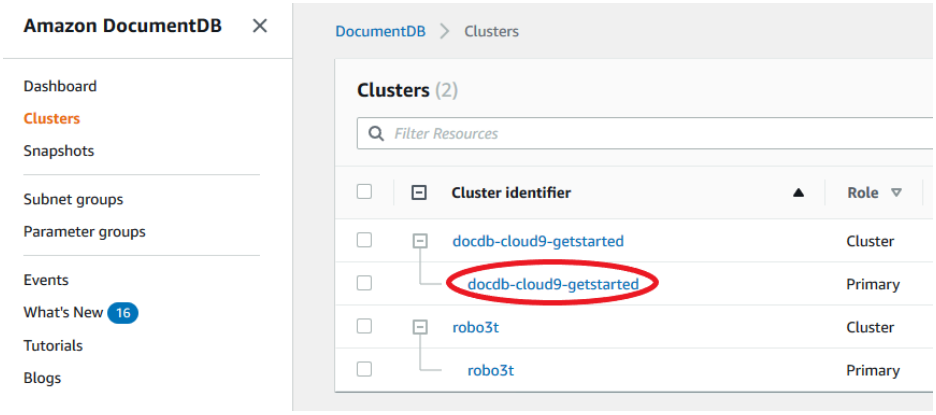
Using the AWS-Managementkonsole

Gehen Sie wie folgt vor, um eine bestimmte Amazon DocumentDB DocumentDB-Instance mithilfe der Konsole zu ändern.

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Klicken Sie im Navigationsbereich auf Cluster.

> **Tip**
>
> Wenn der Navigationsbereich auf der linken Seite des Bildschirms nicht angezeigt wird, wählen Sie links oben auf der Seite das Menüsymbol (≡) aus.

3. Im Cluster-Navigationsfeld sehen Sie die Spalte Cluster-ID. Ihre Instances werden unter Clustern aufgeführt, ähnlich wie im folgenden Screenshot.



4. Markieren Sie das Kästchen links neben der Instanz, die Sie ändern möchten.
5. Wählen Sie Actions (Aktionen) und dann Modify (Ändern) aus.
6. Nehmen Sie im Bereich Modify instance: <instance-name> (Instance ändern: <instance-name>) die gewünschten Änderungen vor. Sie können die folgenden Änderungen ausführen:

   - Instanzspezifikationen — Die Instanz-ID und Klasse. Benennungseinschränkungen für Instance-IDs:
     - Instanz-ID — Geben Sie einen Namen ein, der für alle Instances, die Ihnen gehören, AWS-Konto in der aktuellen Region eindeutig ist. Die Instance-ID muss [1—63] alphanumerische Zeichen oder Bindestriche enthalten, einen Buchstaben als erstes Zeichen haben und darf nicht mit einem Bindestrich enden oder zwei aufeinanderfolgende Bindestriche enthalten.
     - Instance-Klasse — Wählen Sie im Drop-down-Menü eine Instance-Klasse für Ihre Amazon DocumentDB DocumentDB-Instance aus. Weitere Informationen finden Sie unter Instanzklassen verwalten.

- Zertifizierungsstelle — Serverzertifikat für diese Instance. Weitere Informationen finden Sie unter Aktualisierung Ihrer Amazon DocumentDB-TLS-Zertifikate.
- Failover — Während des Failovers wird die Instanz mit der höchsten Heraufstufungsstufe zur primären Instanz heraufgestuft. Weitere Informationen finden Sie unter Amazon DocumentDB-Failover.
- Wartung — Das Wartungsfenster, in dem ausstehende Änderungen oder Patches auf Instanzen im Cluster angewendet werden.

7. Wenn Sie fertig sind, wählen Sie Continue (Weiter) aus, um eine Zusammenfassung Ihrer Änderungen anzuzeigen.
8. Nachdem Sie Ihre Änderungen überprüft haben, können Sie diese sofort oder während des nächsten Wartungsfensters unter Scheduling of modifications (Planen von Änderungen) anwenden. Klicken Sie auf Modify instance (Instance ändern), um Ihre Änderungen zu speichern. Alternativ können Sie auf Cancel (Abbrechen) klicken, um Ihre Änderungen zu verwerfen.

Es dauert einige Minuten, bis Ihre Änderungen übernommen werden. Sie können die Instance nur verwenden, wenn ihr Status available ist. Sie können mit der Konsole oder der AWS CLI den Status der Instance überwachen. Weitere Informationen finden Sie unter Den Status einer Amazon DocumentDB DocumentDB-Instance überwachen.

Using the AWS CLI

Um eine bestimmte Amazon DocumentDB DocumentDB-Instance mithilfe von zu ändern AWS CLI, verwenden Sie die `modify-db-instance` mit den folgenden Parametern. Weitere Informationen finden Sie unter ModifyDBInstance. Der folgende Code ändert die Instance-Klasse für die Instance `sample-instance` in `db.r5.large`.

Parameters

- **`--db-instance-identifier`** – Erforderlich. Die Kennung der zu ändernden Instance.
- **`--db-instance-class`**— Fakultativ. Die neue Rechen- und Speicherkapazität der Instanz; zum Beispiel`db.r5.large`. Nicht alle Instanzklassen sind in allen verfügbar AWS-Regionen. Wenn Sie die Instanzklasse ändern, kommt es während der Änderung zu einem Ausfall. Die Änderung wird im nächsten Wartungsfenster übernommen, sofern sie `ApplyImmediately` für diese Anfrage nicht als wahr angegeben wurde.
- **`--apply-immediately`**oder **`--no-apply-immediately`** — Optional. Gibt an, ob diese Änderung sofort angewandt oder bis zum nächsten Wartungszeitraum verschoben

werden sollte. Wenn dieser Parameter weggelassen wird, wird die Änderung im nächsten Wartungszeitraum ausgeführt.

Example

Für Linux, macOS oder Unix:

```
aws docdb modify-db-instance \
       --db-instance-identifier sample-instance \
       --db-instance-class db.r5.large \
       --apply-immediately
```

Für Windows:

```
aws docdb modify-db-instance ^
       --db-instance-identifier sample-instance ^
       --db-instance-class db.r5.large ^
       --apply-immediately
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus.

```
{
    "DBInstances": [
        {
            "DBInstanceIdentifier": "sample-instance-1",
            "DBInstanceClass": "db.r5.large",
            "Engine": "docdb",
            "DBInstanceStatus": "modifying",
            "Endpoint": {
                "Address": "sample-instance-1.node.us-east-1.docdb.amazonaws.com",
                "Port": 27017,
                "HostedZoneId": "ABCDEFGHIJKLM"
            },
            "InstanceCreateTime": "2020-01-10T22:18:55.921Z",
            "PreferredBackupWindow": "02:00-02:30",
            "BackupRetentionPeriod": 1,
            "VpcSecurityGroups": [
                {
                    "VpcSecurityGroupId": "sg-abcd0123",
                    "Status": "active"
                }
            ],
```

```
            "AvailabilityZone": "us-east-1a",
            "DBSubnetGroup": {
                "DBSubnetGroupName": "default",
                "DBSubnetGroupDescription": "default",
                "VpcId": "vpc-abcd0123",
                "SubnetGroupStatus": "Complete",
                "Subnets": [
                    {
                        "SubnetIdentifier": "subnet-abcd0123",
                        "SubnetAvailabilityZone": {
                            "Name": "us-east-1a"
                        },
                        "SubnetStatus": "Active"
                    },
                    {
                        "SubnetIdentifier": "subnet-abcd0123",
                        "SubnetAvailabilityZone": {
                            "Name": "us-east-1b"
                        },
                        "SubnetStatus": "Active"
                    }
                ]
            },
            "PreferredMaintenanceWindow": "sun:10:57-sun:11:27",
            "PendingModifiedValues": {
                "DBInstanceClass": "db.r5.large"
            },
            "EngineVersion": "3.6.0",
            "AutoMinorVersionUpgrade": true,
            "PubliclyAccessible": false,
            "DBClusterIdentifier": "sample-cluster",
            "StorageEncrypted": true,
            "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/wJalrXUtnFEMI/
K7MDENG/bPxRfiCYEXAMPLEKEY",
            "DbiResourceId": "db-ABCDEFGHIJKLMNOPQRSTUVWXYZ",
            "CACertificateIdentifier": "rds-ca-2019",
            "PromotionTier": 1,
            "DBInstanceArn": "arn:aws:rds:us-east-1:123456789012:db:sample-
instance-1",
            "EnabledCloudwatchLogsExports": [
                "profiler"
            ]
        }
    ]
```

```
}
```

Es dauert einige Minuten, bis Ihre Änderungen angewendet werden. Sie können die Instance nur verwenden, wenn ihr Status available ist. Sie können den Status der Instanz mit dem AWS-Managementkonsole oder überwachen AWS CLI. Weitere Informationen finden Sie unter Den Status einer Amazon DocumentDB DocumentDB-Instance überwachen.

Eine Amazon DocumentDB DocumentDB-Instance neu starten

Gelegentlich müssen Sie Ihre Amazon DocumentDB DocumentDB-Instance möglicherweise neu starten, normalerweise aus Wartungsgründen. Wenn Sie bestimmte Änderungen vornehmen, z. B. die Clusterparametergruppe, die einem Cluster zugeordnet ist, müssen Sie die Instances im Cluster neu starten, damit die Änderungen wirksam werden. Sie können eine angegebene Instance mit dem AWS-Managementkonsole oder dem AWS CLI neu starten.

Durch den Neustart einer Instance wird der Datenbank-Engine-Service neu gestartet. Das Neustarten bewirkt einen vorübergehenden Nutzungsausfall, wobei der Status für die Instance währenddessen auf `rebooting` gesetzt wird. Ein Amazon DocumentDB DocumentDB-Ereignis wird erstellt, wenn der Neustart abgeschlossen ist.

Ein Neustart einer Instance führt nicht zu einem Failover. Verwenden Sie die Operation AWS-Managementkonsole oder, um ein Failover für einen Amazon DocumentDB-Cluster durchzuführen. AWS CLI `failover-db-cluster` Weitere Informationen finden Sie unter Amazon DocumentDB-Failover.

Sie können Ihre Instance nicht neu starten, wenn sie sich nicht im verfügbaren Zustand befindet. Ihre Datenbank kann aus mehreren Gründen nicht verfügbar sein, zum Beispiel aufgrund einer zuvor angeforderten Änderung oder einer Aktion im Wartungsfenster. Weitere Informationen zu Instance-Status finden Sie unter Den Status einer Amazon DocumentDB DocumentDB-Instance überwachen.

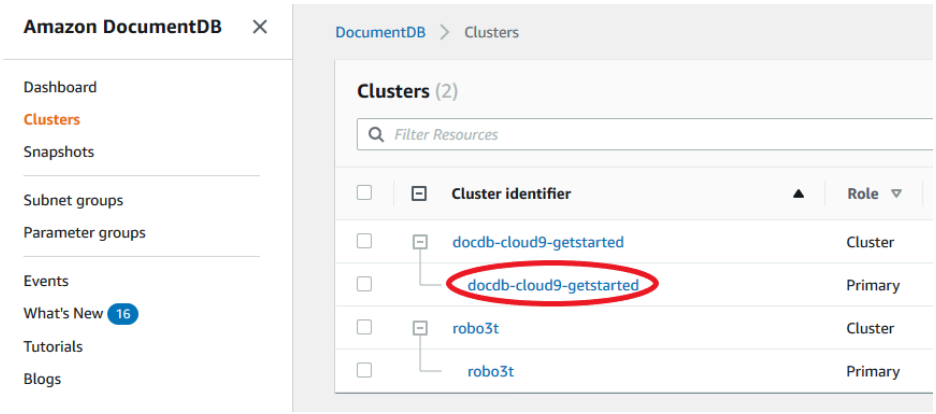
Using the AWS-Managementkonsole

Das folgende Verfahren startet eine Instance neu, die Sie unter Verwendung der Konsole angeben.

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Klicken Sie im Navigationsbereich auf Cluster.

> **Tip**
>
> Wenn der Navigationsbereich auf der linken Seite des Bildschirms nicht angezeigt wird, wählen Sie links oben auf der Seite das Menüsymbol (≡) aus.

3. Im Cluster-Navigationsfeld sehen Sie die Spalte Cluster-ID. Ihre Instances werden unter Clustern aufgeführt, ähnlich wie im folgenden Screenshot.



4. Markieren Sie das Kästchen links neben der Instance, die Sie neu starten möchten.
5. Wählen Sie Actions (Aktionen), Reboot (Neustart) und dann Reboot (Neustart)aus, um den Neustart zu bestätigen.

Es dauert einige Minuten, bis Ihre Instance neu gestartet wird. Sie können die Instance nur verwenden, wenn ihr Status available ist. Sie können mit der Konsole oder der AWS CLI den Status der Instance überwachen. Weitere Informationen finden Sie unter Den Status einer Amazon DocumentDB DocumentDB-Instance überwachen.

Using the AWS CLI

Um eine Amazon DocumentDB DocumentDB-Instance neu zu starten, verwenden Sie den `reboot-db-instance` Vorgang mit dem `--db-instance-identifier` Parameter. Dieser Parameter gibt den Bezeichner für die Instance an, die neu gestartet werden soll.

Der folgende Code startet die Instance `sample-instance` neu.

Example

Für Linux, macOS oder Unix:

```
aws docdb reboot-db-instance \
       --db-instance-identifier sample-instance
```

Für Windows:

```
aws docdb reboot-db-instance ^
       --db-instance-identifier sample-instance
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus.

```
{
    "DBInstance": {
        "DBInstanceIdentifier": "sample-instance",
        "DBInstanceClass": "db.r5.large",
        "Engine": "docdb",
        "DBInstanceStatus": "rebooting",
        "Endpoint": {
            "Address": "sample-instance.node.us-east-1.docdb.amazonaws.com",
            "Port": 27017,
            "HostedZoneId": "ABCDEFGHIJKLM"
        },
        "InstanceCreateTime": "2020-03-27T08:05:56.314Z",
        "PreferredBackupWindow": "02:00-02:30",
        "BackupRetentionPeriod": 1,
        "VpcSecurityGroups": [
            {
                "VpcSecurityGroupId": "sg-abcd0123",
                "Status": "active"
            }
        ],
        "AvailabilityZone": "us-east-1c",
        "DBSubnetGroup": {
            "DBSubnetGroupName": "default",
            "DBSubnetGroupDescription": "default",
            "VpcId": "vpc-abcd0123",
            "SubnetGroupStatus": "Complete",
            "Subnets": [
                {
                    "SubnetIdentifier": "subnet-abcd0123",
                    "SubnetAvailabilityZone": {
                        "Name": "us-east-1a"
                    },
```

```
                    "SubnetStatus": "Active"
                },
                {
                    "SubnetIdentifier": "subnet-wxyz0123",
                    "SubnetAvailabilityZone": {
                        "Name": "us-east-1b"
                    },
                    "SubnetStatus": "Active"
                }
            ]
        },
        "PreferredMaintenanceWindow": "sun:06:53-sun:07:23",
        "PendingModifiedValues": {},
        "EngineVersion": "3.6.0",
        "AutoMinorVersionUpgrade": true,
        "PubliclyAccessible": false,
        "DBClusterIdentifier": "sample-cluster",
        "StorageEncrypted": true,
        "KmsKeyId": "arn:aws:kms:us-east-1:<accountID>:key/sample-key",
        "DbiResourceId": "db-ABCDEFGHIJKLMNOPQRSTUVWXYZ",
        "CACertificateIdentifier": "rds-ca-2019",
        "PromotionTier": 1,
        "DBInstanceArn": "arn:aws:rds:us-east-1:<accountID>:db:sample-instance",
        "EnabledCloudwatchLogsExports": [
            "profiler"
        ]
    }
}
```

Es dauert einige Minuten, bis Ihre Instance neu gestartet wird. Sie können die Instance nur verwenden, wenn ihr Status available ist. Sie können mit der Konsole oder der AWS CLI den Status der Instance überwachen. Weitere Informationen finden Sie unter Den Status einer Amazon DocumentDB DocumentDB-Instance überwachen.

Löschen einer Amazon DocumentDB DocumentDB-Instance

Sie können Ihre Amazon DocumentDB DocumentDB-Instance entweder mit dem AWS-Managementkonsole oder dem AWS CLI löschen. Nur Instances im Status available können gelöscht werden. Eine angehaltene Instance kann nicht gelöscht werden. Wenn der Amazon DocumentDB-Cluster, der Ihre Instance enthält, gestoppt ist, starten Sie zuerst den Cluster, warten Sie, bis die

Instance verfügbar ist, und löschen Sie dann die Instance. Weitere Informationen finden Sie unter Einen Amazon DocumentDB-Cluster stoppen und starten.

> **Note**
>
> Amazon DocumentDB speichert all Ihre Daten im Cluster-Volume. Die Daten bleiben in diesem Cluster-Volume erhalten. Dies gilt auch dann, wenn Sie alle Instances von Ihrem Cluster entfernen. Wenn Sie erneut auf die Daten zugreifen müssen, können Sie jederzeit dem Cluster eine Instance hinzufügen und da fortfahren, wo Sie aufgehört haben.

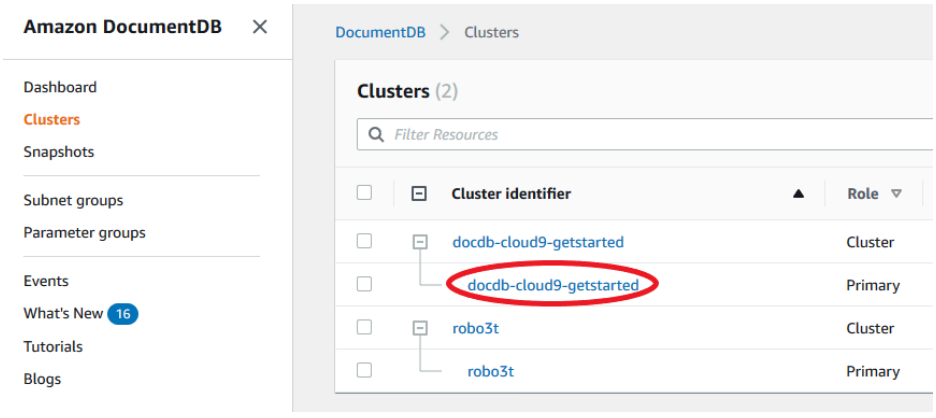
Using the AWS-Managementkonsole

Das folgende Verfahren löscht eine angegebene Amazon DocumentDB DocumentDB-Instance mithilfe der Konsole.

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Klicken Sie im Navigationsbereich auf Cluster.

   > **Tip**
   >
   > Wenn der Navigationsbereich auf der linken Seite des Bildschirms nicht angezeigt wird, wählen Sie links oben auf der Seite das Menüsymbol (≡) aus.

3. Im Cluster-Navigationsfeld sehen Sie die Spalte Cluster-ID. Ihre Instances werden unter Clustern aufgeführt, ähnlich wie im folgenden Screenshot.



4. Markieren Sie das Kästchen links neben der Instance, die Sie löschen möchten.

5. Wählen Sie Actions (Aktionen) und anschließend Delete (Löschen) aus.

    1. Wenn Sie die letzte Instance in Ihrem Cluster löschen:

        - Create final cluster snapshot? (Endgültigen Cluster-Snapshot erstellen?) — Wählen Sie Ja, wenn Sie einen endgültigen Snapshot erstellen möchten, bevor der Cluster gelöscht wird. Wählen Sie andernfalls No (Nein) aus.
        - Name des endgültigen Snapshots — Wenn Sie einen endgültigen Snapshot erstellen möchten, geben Sie die Cluster-Snapshot-ID des neu erstellten Cluster-Snapshots ein.
        - Delete <instance-name> instance? (Instance <instance-name> löschen?) — Geben Sie den Ausdruck Gesamten Cluster löschen in das Feld ein, um das Löschen zu bestätigen.

    2. Wenn Sie nicht die letzte Instance in Ihrem Cluster löschen:

        - Delete <instance-name> instance? (Instance <instance-name> löschen?) — Geben Sie den Ausdruck delete me in das Feld ein, um das Löschen zu bestätigen.

6. Wählen Sie Delete (Löschen), um die Instance zu löschen.

Es dauert einige Minuten, bis die Instance gelöscht ist. Informationen zum Überwachen des Status einer Instance finden Sie unter Den Status einer Amazon DocumentDB DocumentDB-Instance überwachen.

Using the AWS CLI

Das folgende Verfahren löscht eine Amazon DocumentDB DocumentDB-Instance mithilfe von. AWS CLI

1. Stellen Sie zunächst fest, wie viele Instances sich in Ihrem Amazon DocumentDB-Cluster befinden:

    Führen Sie den `describe-db-clusters`-Befehl wie folgt aus, um festzustellen, wie viele Instances sich in Ihrem Cluster befinden.

    ```
    aws docdb describe-db-clusters \
        --db-cluster-identifier sample-cluster \
        --query 'DBClusters[*].
    [DBClusterIdentifier,DBClusterMembers[*].DBInstanceIdentifier]'
    ```

    Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus.

```
[
    [
        "sample-cluster",
        [
            "sample-instance-1",
            "sample-instance-2"
        ]
    ]
]
```

2. Wenn es mehr als eine Instance in Ihrem Amazon DocumentDB-Cluster gibt:

   Um eine angegebene Amazon DocumentDB DocumentDB-Instance zu löschen, verwenden Sie den `delete-db-instance` Befehl mit dem `--db-instance-identifier` Parameter, wie unten gezeigt. Es dauert einige Minuten, bis die Instance gelöscht ist. Informationen zum Überwachen des Status einer Instance finden Sie unter Den Status einer Amazon DocumentDB DocumentDB-Instance überwachen.

   ```
   aws docdb delete-db-instance \
          --db-instance-identifier sample-instance-2
   ```

   Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus.

   ```
   {
       "DBInstance": {
           "DBInstanceIdentifier": "sample-instance-2",
           "DBInstanceClass": "db.r5.large",
           "Engine": "docdb",
           "DBInstanceStatus": "deleting",
           "Endpoint": {
               "Address": "sample-instance-2.node.us-east-1.docdb.amazonaws.com",
               "Port": 27017,
               "HostedZoneId": "ABCDEFGHIJKLM"
           },
           "InstanceCreateTime": "2020-03-27T08:05:56.314Z",
           "PreferredBackupWindow": "02:00-02:30",
           "BackupRetentionPeriod": 1,
           "VpcSecurityGroups": [
               {
                   "VpcSecurityGroupId": "sg-abcd0123",
                   "Status": "active"
   ```

```
            }
        ],
        "AvailabilityZone": "us-east-1c",
        "DBSubnetGroup": {
            "DBSubnetGroupName": "default",
            "DBSubnetGroupDescription": "default",
            "VpcId": "vpc-6242c31a",
            "SubnetGroupStatus": "Complete",
            "Subnets": [
                {
                    "SubnetIdentifier": "subnet-abcd0123",
                    "SubnetAvailabilityZone": {
                        "Name": "us-east-1a"
                    },
                    "SubnetStatus": "Active"
                },
                {
                    "SubnetIdentifier": "subnet-wxyz0123",
                    "SubnetAvailabilityZone": {
                        "Name": "us-east-1b"
                    },
                    "SubnetStatus": "Active"
                }
            ]
        },
        "PreferredMaintenanceWindow": "sun:06:53-sun:07:23",
        "PendingModifiedValues": {},
        "EngineVersion": "3.6.0",
        "AutoMinorVersionUpgrade": true,
        "PubliclyAccessible": false,
        "DBClusterIdentifier": "sample-cluster",
        "StorageEncrypted": true,
        "KmsKeyId": "arn:aws:kms:us-east-1:<accountID>:key/sample-key",
        "DbiResourceId": "db-ABCDEFGHIJKLMNOPQRSTUVWXYZ",
        "CACertificateIdentifier": "rds-ca-2019",
        "PromotionTier": 1,
        "DBInstanceArn": "arn:aws:rds:us-east-1:<accountID>:db:sample-instance-2",
        "EnabledCloudwatchLogsExports": [
            "profiler"
        ]
    }
}
```

3. Wenn die Instance, die Sie löschen möchten, die letzte Instance in Ihrem Amazon DocumentDB-Cluster ist:

   Wenn Sie die letzte Instance in einem Amazon DocumentDB-Cluster löschen, löschen Sie auch diesen Cluster und die mit diesem Cluster verknüpften automatischen Snapshots und kontinuierlichen Backups.

   Um die letzte Instance in Ihrem Cluster zu löschen, können Sie den Cluster löschen und optional einen endgültigen Snapshot erstellen. Weitere Informationen finden Sie unter Löschen eines Amazon DocumentDB-Clusters.

Löschschutz

Wenn Sie die letzte Instanz eines Amazon DocumentDB-Clusters löschen, werden auch der Cluster sowie die mit diesem Cluster verknüpften automatischen Snapshots und kontinuierlichen Backups gelöscht. Amazon DocumentDB erzwingt den Löschschutz für einen Cluster, unabhängig davon, ob Sie den Löschvorgang mit AWS-Managementkonsole oder dem ausführen. AWS CLI Sie können einen Cluster nicht löschen, solange der Löschschutz aktiviert ist.

Um einen Cluster mit aktiviertem Löschschutz zu löschen, müssen Sie zuerst den Cluster ändern und den Löschschutz deaktivieren. Weitere Informationen finden Sie unter Löschen eines Amazon DocumentDB-Clusters.

Instanzklassen verwalten

Die Instance-Klasse bestimmt die Rechenleistung und Speicherkapazität einer Amazon DocumentDB DocumentDB-Instance (mit MongoDB-Kompatibilität). Welche Instance-Klasse Sie benötigen, hängt von der benötigten Rechenleistung und dem Speicherbedarf ab.

Amazon DocumentDB unterstützt die Instance-Klassen R4, R5, R6G, R8G, T3 und T4G. Diese Klassen sind Instance-Klassen der aktuellen Generation, die für speicherintensive Anwendungen optimiert sind. Die Spezifikationen dieser Klassen finden Sie unter Spezifikationen der Instanzklasse.

Themen

- Bestimmung einer Instance-Klasse
- Die Klasse einer Instance ändern
- Unterstützte Instance-Klassen nach Region
- Spezifikationen der Instanzklasse

Bestimmung einer Instance-Klasse

Um die Klasse einer Instanz zu ermitteln, können Sie die `describe-db-instances` AWS CLI Operation AWS-Managementkonsole oder verwenden.

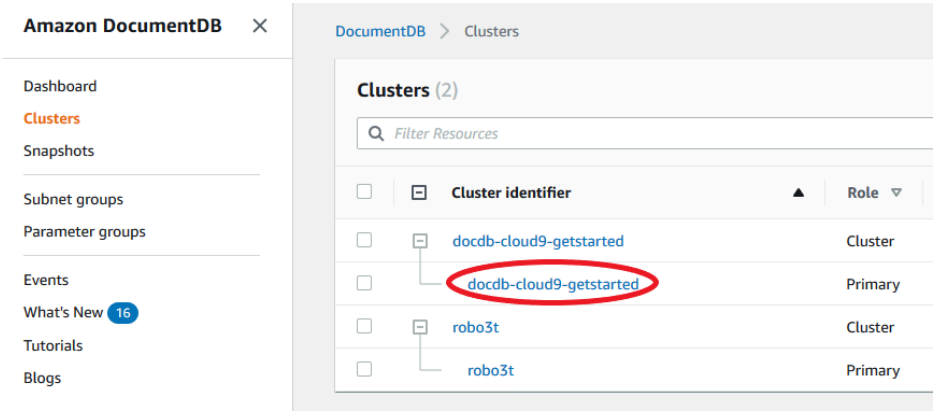
Using the AWS-Managementkonsole

Führen Sie die folgenden Schritte in der Konsole aus, um die Instanzklasse für die Instances Ihres Clusters zu ermitteln.

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Wählen Sie im Navigationsbereich Clusters aus, um die Instance zu finden, an der Sie interessiert sind.

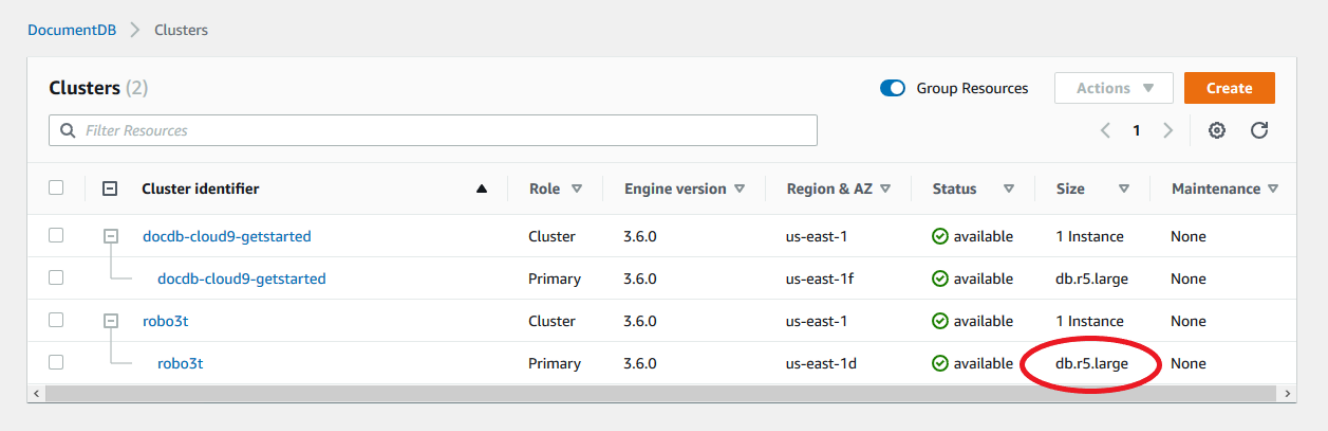
   > **Tip**
   >
   > Wenn der Navigationsbereich auf der linken Seite des Bildschirms nicht angezeigt wird, wählen Sie links oben auf der Seite das Menüsymbol (≡) aus.

3. Im Navigationsfeld „Cluster“ sehen Sie die Spalte Cluster-ID. Ihre Instances werden unter Clustern aufgeführt, ähnlich wie im folgenden Screenshot.



4. Erweitern Sie in der Liste der Instances den Cluster, um die Instances zu finden, an denen Sie interessiert sind. Suchen Sie die gewünschte Instanz. Sehen Sie sich dann die Spalte Größe in der Zeile der Instanz an, um deren Instanzklasse zu sehen.

   In der folgenden Abbildung ist die Instance-Klasse für die Instance `robo3t` `db.r5.4xlarge`.



Using the AWS CLI

Verwenden Sie die `describe-db-instances` Operation mit den folgenden Parametern AWS CLI, um die Klasse einer Instance mithilfe von zu ermitteln.

- **`--db-instance-identifier`**— Fakultativ. Gibt die Instance an, für die Sie die Instance-Klasse suchen möchten. Wenn dieser Parameter ausgelassen wird, gibt `describe-db-instances` eine Beschreibung für bis zu 100 Ihrer Instances zurück.
- **`--query`**— Fakultativ. Gibt die Mitglieder der Instance an, die in die Ergebnisse einbezogen werden sollen. Wenn dieser Parameter ausgelassen wird, werden alle Instance-Mitglieder zurückgegeben.

Example

Im folgenden Beispiel werden der Instanzname und die Klasse für die Instanz ermitteltsample-instance-1.

Für Linux, macOS oder Unix:

```
aws docdb describe-db-instances \
    --query 'DBInstances[*].[DBInstanceIdentifier,DBInstanceClass]' \
    --db-instance-identifier sample-instance-1
```

Für Windows:

```
aws docdb describe-db-instances ^
    --query 'DBInstances[*].[DBInstanceIdentifier,DBInstanceClass]' ^
```

```
    --db-instance-identifier sample-instance-1
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus.

```
[
    [
        "sample-instance-1",
        "db.r5.large"
    ]
```

Example

Das folgende Beispiel ermittelt den Instanznamen und die Klasse für bis zu 100 Amazon DocumentDB DocumentDB-Instances.

Für Linux, macOS oder Unix:

```
aws docdb describe-db-instances \
    --query 'DBInstances[*].[DBInstanceIdentifier,DBInstanceClass]' \
    --filter Name=engine,Values=docdb
```

Für Windows:

```
aws docdb describe-db-instances ^
    --query 'DBInstances[*].[DBInstanceIdentifier,DBInstanceClass]' ^
    --filter Name=engine,Values=docdb
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus.

```
[
    [
        "sample-instance-1",
        "db.r5.large"
    ],
    [
        "sample-instance-2",
        "db.r5.large"
    ],
    [
        "sample-instance-3",
        "db.r5.4xlarge"
    ],
```

```
    [
        "sample-instance-4",
        "db.r5.4xlarge"
    ]
]
```

Weitere Informationen finden Sie unter Beschreibung von Amazon DocumentDB DocumentDB-Instances.

Die Klasse einer Instance ändern

Sie können die Instanzklasse Ihrer Instanz mit dem AWS-Managementkonsole oder dem ändern AWS CLI. Weitere Informationen finden Sie unter Ändern einer Amazon DocumentDB DocumentDB-Instance.

Unterstützte Instance-Klassen nach Region

Amazon DocumentDB unterstützt die folgenden Instance-Klassen:

- R8G—Speicheroptimierte Instances der neuesten Generation mit Arm-based AWS Graviton4-Prozessoren, die im Vergleich zu R6G-Instances eine um bis zu 30% bessere Leistung bieten.
- R6G— Memory-optimized Instances mit Arm-based AWS Graviton2-Prozessoren, die eine um bis zu 30% bessere Leistung als R5-Instances bei 5% geringeren Kosten bieten.
- R6GD— Memory-optimized R6G-Instances mit lokalem Solid-State Festplattenspeicher (NVMe) auf NVMe-Basis (Non-Volatile Memory Express) für kurzlebige Daten.
- R5— Memory-optimized Instances, die bei gleichen Instance-Kosten eine bis zu 100% bessere Leistung als R4-Instances bieten.
- R4— Frühere Generation speicheroptimierter Instances.
- T4G— Latest-generation kostengünstiger Burstable-Instance-Typ für allgemeine Zwecke mit Arm-based AWS Graviton2-Prozessoren, der eine grundlegende CPU-Leistung bietet, ein bis zu 35% besseres Preis-Leistungs-Verhältnis als T3-Instances bietet und sich ideal für die Ausführung von Anwendungen mit moderater CPU-Auslastung eignet, bei denen es zu vorübergehenden Auslastungsspitzen kommt.
- T3— Kostengünstiger Burstable-Allzweck-Instance-Typ, der eine grundlegende CPU-Leistung bietet und die Möglichkeit bietet, die CPU-Auslastung jederzeit und so lange wie nötig zu erhöhen.

Detaillierte Angaben zu den Instance-Klassen finden Sie unter Spezifikationen der Instanzklasse.

> **Note**
>
> I/O-Optimized Speicher ist nur in den Engine-Versionen 5.0 und 8.0 (instanzbasierte Cluster) verfügbar.

Eine bestimmte Instanzklasse kann in einer bestimmten Region unterstützt werden oder auch nicht. Die folgende Tabelle gibt an, welche Instance-Klassen von Amazon DocumentDB in jeder Region unterstützt werden.

Unterstützte Instance-Klassen nach Region

Region	R8G	R6GD	R6G	R5	R4	T4 G	T3	Serverless
USA Ost (Ohio)	Unterstützt	Unterstützt	Unterstützt	Unterstützt	Unterstützt	Unterstützt	Unterstützt	Unterstützt
USA Ost (Nord-Virginia)	Unterstützt	Unterstützt	Unterstützt	Unterstützt	Unterstützt	Unterstützt	Unterstützt	Unterstützt
USA West (Oregon)	Unterstützt	Unterstützt	Unterstützt	Unterstützt	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Afrika (Kapstadt)			Unterstützt	Unterstützt		Unterstützt	Unterstützt	Unterstützt
Südamerika (São Paulo)		Unterstützt	Unterstützt	Unterstützt		Unterstützt	Unterstützt	Unterstützt
Asien-Pazifik (Hongkong)			Unterstützt	Unterstützt		Unterstützt	Unterstützt	Unterstützt
Asien-Pazifik (Hyderabad)			Unterstützt	Unterstützt		Unterstützt	Unterstützt	Unterstützt
Asien-Pazifik (Malaysia)			Unterstützt			Unterstützt	Unterstützt	

Region	R8G	R6GD	R6G	R5	R4	T4 G	T3	Serverless
Asien-Pazifik (Mumbai)	Unterstützt	Unterstützt	Unterstützt	Unterstützt		Unterstützt	Unterstützt	Unterstützt
Asien-Pazifik (Osaka)		Unterstützt	Unterstützt	Unterstützt		Unterstützt	Unterstützt	
Asien-Pazifik (Seoul)	Unterstützt	Unterstützt	Unterstützt	Unterstützt		Unterstützt	Unterstützt	Unterstützt
Asien-Pazifik (Sydney)	Unterstützt	Unterstützt	Unterstützt	Unterstützt		Unterstützt	Unterstützt	Unterstützt
Asien-Pazifik (Jakarta)	Unterstützt	Unterstützt	Unterstützt	Unterstützt		Unterstützt	Unterstützt	
Asien-Pazifik (Melbourne)			Unterstützt	Unterstützt		Unterstützt	Unterstützt	
Asien-Pazifik (Singapur)	Unterstützt	Unterstützt	Unterstützt	Unterstützt		Unterstützt	Unterstützt	Unterstützt
Asien-Pazifik (Thailand)			Unterstützt			Unterstützt	Unterstützt	
Asien-Pazifik (Tokio)	Unterstützt	Unterstützt	Unterstützt	Unterstützt		Unterstützt	Unterstützt	Unterstützt
Kanada (Zentral)	Unterstützt	Unterstützt	Unterstützt	Unterstützt		Unterstützt	Unterstützt	Unterstützt
Kanada West (Calgary)			Unterstützt	Unterstützt		Unterstützt	Unterstützt	
Europa (Frankfurt)	Unterstützt	Unterstützt	Unterstützt	Unterstützt		Unterstützt	Unterstützt	Unterstützt

Region	R8G	R6GD	R6G	R5	R4	T4 G	T3	Serverless
Europa (Zürich)		Unterstützt	Unterstützt	Unterstützt		Unterstützt	Unterstützt	
Europa (Irland)	Unterstützt	Unterstützt	Unterstützt	Unterstützt	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Europa (London)		Unterstützt	Unterstützt	Unterstützt		Unterstützt	Unterstützt	Unterstützt
Europa (Milan)			Unterstützt	Unterstützt		Unterstützt	Unterstützt	Unterstützt
Europa (Paris)		Unterstützt	Unterstützt	Unterstützt		Unterstützt	Unterstützt	Unterstützt
Europa (Spain)	Unterstützt	Unterstützt	Unterstützt	Unterstützt		Unterstützt	Unterstützt	Unterstützt
Europa (Stockholm)	Unterstützt	Unterstützt	Unterstützt	Unterstützt		Unterstützt	Unterstützt	
Mexiko (Zentral)			Unterstützt			Unterstützt	Unterstützt	
Naher Osten (VAE)			Unterstützt	Unterstützt		Unterstützt	Unterstützt	Unterstützt
China (Peking)		Unterstützt	Unterstützt	Unterstützt		Unterstützt	Unterstützt	Unterstützt
China (Ningxia)			Unterstützt	Unterstützt		Unterstützt	Unterstützt	Unterstützt
Israel (Tel Aviv)			Unterstützt	Unterstützt		Unterstützt	Unterstützt	

Region	R8G	R6GD	R6G	R5	R4	T4 G	T3	Serverless
AWS GovCloud (US-West)	Unterstützt	Unterstützt	Unterstützt	Unterstützt			Unterstützt	Unterstützt
AWS GovCloud (US-East)		Unterstützt	Unterstützt	Unterstützt		Unterstützt	Unterstützt	Unterstützt

Spezifikationen der Instanzklasse

Die folgende Tabelle enthält Einzelheiten zu den Amazon DocumentDB DocumentDB-Instance-Klassen, einschließlich der Instance-Typen, die in den einzelnen Klassen unterstützt werden. Erläuterungen zu den einzelnen Tabellenspalten finden Sie unterhalb der Tabelle.

Instance-Klasse	vCPU[1]	Speicher (GiB) [2]	Tierierter NVMe SSD-Cache (GiB) 3	Max. Speichertemperatur (GiB) 4	Basis-/Burst-Bandbreite (Gbit/s) 5	Unterstützende Engines 6
R8G — Memory-Optimized Instance-Klasse der aktuellen Generation, basierend auf Graviton4 R8G ist die neueste Instance-Familie (Graviton4), die nur in den Engine-Versionen 5.0 und 8.0 verfügbar ist. Die Größe db.r8g.48xlarge ist noch nicht verfügbar.						
`db.r8g.large`	2	16	-	30	0,937 / 12,5	5.0.0 und 8.0.0
`db.r8g.xlarge`	4	32	-	60	1,875 / 12,5	5.0.0 und 8.0.0
`db.r8g.2xlarge`	8	64	-	121	3,75 / 15,0	5.0.0 und 8.0.0
`db.r8g.4xlarge`	16	128	-	243	7,5 / 15,0	5.0.0 und 8.0.0
`db.r8g.8xlarge`	32	256	-	488	15	5.0.0 und 8.0.0

Instance-Klasse	vCPU[1]	Speicher (GiB) [2]	Tierierter NVMe SSD-Cache (GiB) 3	Max. Speichert emperatur (GiB) 4	Basis-/Burst-Bandbreite (Gbit/s) 5	Unterstützende Engines 6
db.r8g.12xlarge	48	384	-	732	22	5.0.0 und 8.0.0
db.r8g.16xlarge	64	512	-	987	30	5.0.0 und 8.0.0
db.r8g.24xlarge	96	768	-	1484	40	5.0.0 und 8.0.0
R6G — Memory-Optimized Instance-Klasse der aktuellen Generation, basierend auf Graviton2						
db.r6g.large	2	16	-	32	0,75/10	4.0.0, 5.0.0 und 8.0.0
db.r6g.xlarge	4	32	-	63	1,25/10	4.0.0, 5.0.0 und 8.0.0
db.r6g.2xlarge	8	64	-	126	2.5/10	4.0.0, 5.0.0 und 8.0.0
db.r6g.4xlarge	16	128	-	252	5.0/10	4.0.0, 5.0.0 und 8.0.0
db.r6g.8xlarge	32	256	-	504	12	4.0.0, 5.0.0 und 8.0.0
db.r6g.12xlarge	48	384	-	756	20	4.0.0, 5.0.0 und 8.0.0
db.r6g.16xlarge	64	512	-	1008	25	4.0.0, 5.0.0 und 8.0.0
R6GD — Instance-Klasse der aktuellen Generation NVMe-backed , basierend auf Graviton2						
db.r6gd.xlarge	4	32	173	64	1,25/10	5.0.0 und 8.0.0

Instance-Klasse	vCPU[1]	Speicher (GiB) [2]	Tierierter NVMe SSD-Cache (GiB) 3	Max. Speichert emperatur (GiB) 4	Basis-/Burst-Bandbreite (Gbit/s) 5	Unterstützende Engines 6
db.r6gd.2xlarge	8	64	346	128	2,5/10	5.0.0 und 8.0.0
db.r6gd.4xlarge	16	128	694	256	5,0/10	5.0.0 und 8.0.0
db.r6gd.8xlarge	32	256	1388	512	12	5.0.0 und 8.0.0
db.r6gd.12xlarge	48	384	2082	768	20	5.0.0 und 8.0.0
db.r6gd.16xlarge	64	512	2776	1024	25	5.0.0 und 8.0.0
R5 — Instance-Klasse der vorherigen Generation Memory-Optimized						
db.r5.large	2	16	-	31	0,75/10	3.6.0, 4.0.0, 5.0.0 und 8.0.0
db.r5.xlarge	4	32	-	62	1,25/10	3.6.0, 4.0.0, 5.0.0 und 8.0.0
db.r5.2xlarge	8	64	-	124	2,5/10	3.6.0, 4.0.0, 5.0.0 und 8.0.0
db.r5.4xlarge	16	128	-	249	5,0/10	3.6.0, 4.0.0, 5.0.0 und 8.0.0

Instance-Klasse	vCPU[1]	Speicher (GiB) [2]	Tierierter NVMe SSD-Cache (GiB) 3	Max. Speichert emperatur (GiB) 4	Basis-/Burst-Bandbreite (Gbit/s) 5	Unterstützende Engines 6
db.r5.8xlarge	32	256	-	504	10	3.6.0, 4.0.0, 5.0.0 und 8.0.0
db.r5.12xlarge	48	384	-	748	12	3.6.0, 4.0.0, 5.0.0 und 8.0.0
db.r5.16xlarge	64	512	-	1008	20	3.6.0, 4.0.0, 5.0.0 und 8.0.0
db.r5.24xlarge	96	768	-	1500	25	3.6.0, 4.0.0, 5.0.0 und 8.0.0
R4 — Instance-Klasse der vorherigen Generation Memory-Optimized R4-Instances werden nur in der Engine-Version 3.6 unterstützt. Beachten Sie, dass der Standards upport für Amazon DocumentDB 3.6 am 30. März 2026 endet. Extended Support (kostenpflichtig) ist bis März 2029 verfügbar.						
db.r4.large	2	15,25	-	30	0,75/10	nur 3.6.0
db.r4.xlarge	4	30,5	-	60	1,25/10	nur 3.6.0
db.r4.2xlarge	8	61	-	120	2,5/10	nur 3.6.0
db.r4.4xlarge	16	122	-	240	5,0 /10	nur 3.6.0

Instance-Klasse	vCPU[1]	Speicher (GiB) [2]	Tierierter NVMe SSD-Cache (GiB) 3	Max. Speichert emperatur (GiB) 4	Basis-/Burst-Bandbreite (Gbit/s) 5	Unterstützende Engines 6
`db.r4.8xlarge`	32	244	-	480	10	nur 3.6.0
`db.r4.16xlarge`	64	488	-	960	25	nur 3.6.0
T4G — Instance-Klassen mit Burstable Performance der neuesten Generation, die auf Graviton2 basieren T-series Instances werden im Burst-Modus „Unlimited CPU“ ausgeführt. Eine Burst-Nutzung, die über den Basiswert hinausgeht, wird zusätzlich in Rechnung gestellt. Wird für globale Cluster nicht unterstützt.						
`db.t4g.medium`	2	4	-	8.13	0,256/5	4.0.0, 5.0.0 und 8.0.0
T3 — Instance-Klassen mit Burstable Performance der vorherigen Generation						
`db.t3.medium`	2	4	-	7,5	0,256/5	3.6.0, 4.0.0, 5.0.0 und 8.0.0

Instance-Klasse	vCPU[1]	Speicher (GiB) [2]	Tierierter NVMe SSD-Cache (GiB) 3	Max. Speichert emperatur (GiB) 4	Basis-/Burst-Bandbreite (Gbit/s) 5	Unterstützende Engines 6

1. vCPU — Die Anzahl der virtuellen Zentraleinheiten (CPUs). Eine virtuelle CPU ist eine Kapazitätseinheit, mit der Sie Instance-Klassen vergleichen können. Anstatt einen bestimmte n Prozessor für mehrere Monate oder Jahre zu erwerben oder zu leasen, wird jetzt Kapazität stundenweise gemietet. Unser Ziel besteht darin, unabhängig von der tatsächlich zu Grunde liegenden Hardware eine gleichbleibende Menge an CPU-Kapazität zu bieten.
2. Arbeitsspeicher (GiB) — Der RAM in Gigabyte, der der Instance zugewiesen ist. Häufig ist das Verhältnis zwischen Arbeitsspeicher- und vCPU konsistent.
3. Tiered Cache für NVMe SSD — Der Speicherplatz auf dem SSD-Volume, gemessen in Gigabyte, der als erweiterter Cache zum Speichern flüchtiger Daten zugewiesen wird. Dieser Cache ist nur in Instanzen verfügbar. NVMe-backed
4. Max. Temp. Storage (GiB) — Der Speicherplatz, gemessen in Gigabyte, der der Instanz für nicht persistenten temporären Dateispeicher zugewiesen wurde. Bei NVMe-backed Instanzen wird dieser Speicher auf einem SSD-Volume gehostet. NVMe-based In allen anderen Fällen wird es im Amazon Elastic Block Store (EBS) gehostet.
5. Baseline-/Burst-Bandbreite (Gbit/s) — Die Burst-Bandbreite stellt die maximale Bandbreite in Gigabit pro Sekunde dar. Teilen Sie durch 8, um den erwarteten Durchsatz in Gigabyte pro Sekunde zu erhalten. Instanzen der Größe 4xlarge und kleiner haben eine Basisbandbreite. Um den zusätzlichen Bedarf zu decken, können sie einen I/O Netzwerk-Kreditmechanismus verwenden, um ihre Basisbandbreite zu überschreiten. Instances können Aufteilungsbandbreite für einen begrenzten Zeitraum verwenden, in der Regel zwischen 5 und 60 Minuten, abhängig von der Instancegröße.
6. Unterstützende Engines — Die Amazon DocumentDB DocumentDB-Engines, die die Instance-Klasse unterstützen.

NVMe-backed Instanzen

NVMe-backed Instances bieten eine bis zu 7-mal schnellere Abfrageleistung für Anwendungen mit großen Datensätzen, die den Arbeitsspeicher einer regulären Instanz überschreiten. Diese Instances nutzen den lokalen NVMe (NVMe) -basierten Solid-State Drive-Speicher (SSD), der auf r6gd-Instances verfügbar ist, um kurzlebige Daten zu speichern, den netzwerkbasierten Speicherzugriff zu reduzieren und die Leselatenz und den Durchsatz zu verbessern.

Der lokale SSD-Speicherplatz ist in zwei Abschnitte unterteilt:

- Mehrstufiger Cache — Ungefähr 73% der lokalen SSD sind als Datenbank-Cache zugewiesen, sodass das System bis zu fünfmal mehr Datenbankseiten speichern kann als der Hauptspeicher allein. Die lokale SSD fungiert als Cache der zweiten Ebene, während der vorhandene In-Memory-Buffer-Cache der Cache der ersten Ebene bleibt. Die Abfrage greift nur dann auf externen Speicher zu, wenn sowohl im Puffer-Cache als auch im SSD-Cache ein Fehler auftritt.
- Temporärer Speicher — Die restlichen 27% sind für nicht persistenten temporären Dateispeicher reserviert, der für komplexe Abfragen mit Sortieroperationen oder ressourcenintensiven Vorgängen wie Indexerstellungen verwendet wird. Bei regulären Instances befindet sich der temporäre Speicherplatz auf einem Amazon Elastic Block Store (EBS) -Volume. Der lokal gehostete temporäre Speicher auf der SSD reduziert die Abfragelatenz bei Sortierungen um das bis zu Zweifache und beschleunigt ressourcenintensive Operationen wie Indexerstellungen.

Einzelheiten zu den unterstützten NVMe-backed Instanztypen und deren Spezifikationen finden Sie unter. Spezifikationen der Instanzklasse

Topics

- Empfohlene Anwendungsfälle für NVMe-backed Instanzen
- NVMe-backed Instances mit Amazon DocumentDB verwenden
- Instanzen überwachen NVMe-backed

Empfohlene Anwendungsfälle für NVMe-backed Instanzen

Wir empfehlen Ihnen, NVMe-backed Instances in den folgenden Szenarien zu verwenden:

- Read-heavy Workloads — Wenn Ihre Arbeitslast leseintensiv ist und Ihr Datensatz größer als der Puffer-Cache ist, was durch niedrige `BufferCacheHitRatio` und hohe `ReadIOPS` Messwerte angezeigt wird, können NVMe-backed Instances Leistungsvorteile bieten.
- Update-heavy Workloads — Wenn Ihr Workload aktualisierungsintensiv ist und die Garbage-Collection aufgrund der Leselatenz im Netzwerkspeicher nicht Schritt halten kann, können NVMe-backed Instances helfen, das Problem zu beheben.

NVMe-backed Instanzen können für verschiedene Anwendungsfälle von Vorteil sein, darunter:

- Internet-scale Anwendungen — Anwendungen wie Zahlungsabwicklung, Rechnungsstellung und E-Commerce mit strengen Leistungsvereinbarungen (Service Level Agreements, SLAs) können die Leistungsvorteile von NVMe-backed Instances nutzen.
- Real-time Berichts-Dashboards — Dashboards, die Hunderte von Abfragen zur metrics/data Erfassung ausführen, können von der geringen Latenz und dem hohen Durchsatz der Instanzen profitieren. NVMe-backed
- Generative KI-Anwendungen — Anwendungen, die die Vektorsuche verwenden, um anhand von Millionen von Vektoreinbettungen exakte oder nächstgelegene Nachbarn zu finden, können die hohe Leistung von Instanzen nutzen. NVMe-backed

NVMe-backed Instances mit Amazon DocumentDB verwenden

So verwenden Sie NVMe-backed Instances von Amazon DocumentDB:

- Erstellen Sie einen Amazon DocumentDB-Cluster und fügen Sie eine der NVMe-backed Instance-Klassen hinzu. Weitere Informationen finden Sie unter Einen Amazon DocumentDB-Cluster erstellen.
- Sie können auch einen vorhandenen Amazon DocumentDB-Cluster so ändern, dass er eine der NVMe-backed Instance-Klassen verwendet. Weitere Informationen finden Sie unter Ändern eines Amazon DocumentDB-Clusters.

Informationen zur Verfügbarkeit von NVMe-backed Instances in verschiedenen AWS Regionen finden Sie unterUnterstützte Instance-Klassen nach Region.

Wenn Sie von einer NVMe-backed Instance zu einer regulären Instance zurückkehren möchten, ändern Sie die Datenbank-Instance-Klasse Ihrer Amazon DocumentDB DocumentDB-Instance in eine ähnliche Instance-Klasse ohne NVMe-Speicher. Wenn Ihre aktuelle Instance-Klasse beispielsweise 'db.r6gd.4xlarge' ist, wählen Sie 'db.r6g.4xlarge', um zurückzuschalten. Weitere Informationen finden Sie unter Ändern eines Amazon DocumentDB-Clusters.

Instanzen überwachen NVMe-backed

Zusätzlich zu den regulären Instance-Metriken, die bei Amazon verfügbar sind CloudWatch, geben NVMe-backed Instances zusätzliche Metriken aus, die sich auf NVMe-based SSD-Speicher, IOPS und Durchsatz beziehen.

```
NVMeStorageCacheHitRatio
```

```
FreeNVMeStorage
ReadIOPSNVMeStorage
ReadLatencyNVMeStorage
ReadThroughputNVMeStorage
WriteIOPSNVMeStorage
WriteLatencyNVMeStorage
WriteThroughputNVMeStorage
```

Weitere Informationen zu diesen Metriken finden Sie unter NVMe-backed Instanz-Metriken

Amazon DocumentDB-Subnetzgruppen verwalten

Eine Virtual Private Cloud (VPC) ist ein virtuelles Netzwerk, das Ihrem AWS-Konto gewidmet ist. Es ist logisch von anderen virtuellen Netzwerken in der AWS Cloud isoliert. Sie können Ihre AWS Ressourcen, wie Amazon DocumentDB-Cluster, in Ihrer Amazon VPC starten. Sie können einen IP-Adressbereich für die VPC angeben, Subnetze hinzufügen, Sicherheitsgruppen zuordnen und Routing-Tabellen konfigurieren.

Ein Subnetz ist ein Bereich von IP-Adressen in Ihrer Amazon VPC. Sie können AWS Ressourcen in einem bestimmten Subnetz starten. Verwenden Sie öffentliche Subnetze für Ressourcen, die mit dem Internet verbunden sein müssen. Verwenden Sie private Subnetze für Ressourcen, die nicht mit dem Internet verbunden sein werden. Weitere Informationen zu öffentlichen und privaten Subnetzen finden Sie unter VPC and Subnet Basics im Amazon Virtual Private Cloud Cloud-Benutzerhandbuch.

Eine DB-Subnetzgruppe ist eine Sammlung von Subnetzen, die Sie in einer VPC erstellen, welche Sie dann für Ihre Cluster festlegen. Mithilfe einer Subnetzgruppe können Sie beim Erstellen von Clustern eine bestimmte VPC festlegen. Wenn Sie die `default` Subnetzgruppe verwenden, umfasst diese alle Subnetze in der VPC.

Jede DB-Subnetzgruppe sollte über Subnetze in mindestens zwei Availability Zones in einer bestimmten -Region verfügen. Wenn Sie einen DB-Cluster in einer VPC erstellen, müssen Sie eine DB-Subnetzgruppe auswählen. Amazon DocumentDB verwendet diese DB-Subnetzgruppe und Ihre bevorzugte Availability Zone, um ein Subnetz und eine IP-Adresse innerhalb dieses Subnetzes auszuwählen, die mit Ihrem Cluster verknüpft werden sollen. Wenn die primäre Instance ausfällt, kann Amazon DocumentDB eine entsprechende Replikat-Instance zur neuen primären Instance heraufstufen. Anschließend kann mithilfe einer IP-Adresse aus dem Subnetz, in dem sich der vorherige primäre Cluster befand, eine neue Replikat-Instance erstellt werden.

Wenn Amazon DocumentDB eine Instance in einer VPC erstellt, weist es Ihrem Cluster mithilfe einer IP-Adresse, die Sie aus Ihrer DB-Subnetzgruppe ausgewählt haben, eine Netzwerkschnittstelle zu.

Es wird ausdrücklich empfohlen, den DNS-Namen zu verwenden, da sich die zugrunde liegende IP-Adresse ändern kann (z. B während eines Failovers). Weitere Informationen finden Sie unter Amazon DocumentDB DocumentDB-Endpunkte.

Informationen zum Erstellen Ihrer eigenen VPC und Subnetze finden Sie unter Arbeiten mit VPCs und Subnetzen im Amazon Virtual Private Cloud Cloud-Benutzerhandbuch.

Themen

- Eine Amazon DocumentDB-Subnetzgruppe erstellen
- Beschreibung einer Amazon DocumentDB-Subnetzgruppe
- Ändern einer Amazon DocumentDB-Subnetzgruppe
- Löschen einer Amazon DocumentDB-Subnetzgruppe

Eine Amazon DocumentDB-Subnetzgruppe erstellen

Wenn Sie einen Amazon DocumentDB-Cluster erstellen, müssen Sie eine Amazon VPC und die entsprechende Subnetzgruppe innerhalb dieser Amazon VPC auswählen, um Ihren Cluster zu starten. Subnetze bestimmen die Availability Zone und den IP-Bereich innerhalb der Availability Zone, die Sie zum Starten einer Instance verwenden möchten.

Eine Subnetzgruppe ist eine benannte Gruppe von Subnetzen (oder AZs), mit der Sie die Availability Zones angeben können, die Sie für den Start von Amazon DocumentDB DocumentDB-Instances verwenden möchten. In einem Cluster mit drei Instances wird beispielsweise empfohlen, dass jede dieser Instances in separaten AZs bereitgestellt wird. Dadurch wird die Hochverfügbarkeit optimiert. Wenn also eine einzelne AZ ausfällt, wirkt sich dies nur auf eine einzelne Instanz aus.

Derzeit können Amazon DocumentDB DocumentDB-Instances in bis zu drei AZs bereitgestellt werden. Selbst wenn eine Subnetzgruppe mehr als drei Subnetze hat, können Sie nur drei dieser Subnetze verwenden, um einen Amazon DocumentDB-Cluster zu erstellen. Daher empfehlen wir, bei der Erstellung einer Subnetzgruppe nur die drei Subnetze auszuwählen, für die Sie Ihre Instances bereitstellen möchten.

Beispiel: Ein Cluster wird erstellt und Amazon DocumentDB wählt AZs {1A, 1B und 1C} aus. Wenn Sie versuchen, eine Instance in AZ {1D} zu erstellen, schlägt der API-Aufruf fehl. Wenn Sie sich jedoch dafür entscheiden, eine Instance zu erstellen, ohne die jeweilige AZ anzugeben, wählt Amazon DocumentDB in Ihrem Namen eine AZ aus. Amazon DocumentDB verwendet einen Algorithmus für den Lastenausgleich der Instances zwischen AZs, um Ihnen zu helfen, eine hohe

Verfügbarkeit zu erreichen. Wenn drei Instances bereitgestellt werden, werden sie standardmäßig über drei AZs bereitgestellt und nicht alle in einer einzigen AZ bereitgestellt.

Bewährte Methoden

- Wenn Sie keinen speziellen Grund haben, legen Sie immer eine Subnetzgruppe mit drei Subnetzen an. Dadurch wird sichergestellt, dass Cluster mit drei oder mehr Instances eine höhere Verfügbarkeit erreichen können, da Instances über drei AZs bereitgestellt werden.
- Verteilen Sie Instances immer über mehrere AZs, um eine hohe Verfügbarkeit zu erreichen. Platzieren Sie niemals alle Instances für einen Cluster in einer einzigen AZ.
- Da Failover-Ereignisse jederzeit auftreten können, sollten Sie nicht davon ausgehen, dass sich eine primäre Instance oder Replikat-Instance immer in einer bestimmten AZ befinden.

Wie erstellt man eine Subnetzgruppe

Sie können das AWS-Managementkonsole oder verwenden AWS CLI , um eine Amazon DocumentDB-Subnetzgruppe zu erstellen:

Using the AWS-Managementkonsole

Gehen Sie wie folgt vor, um eine Amazon DocumentDB-Subnetzgruppe zu erstellen.

So erstellen Sie eine Amazon-DocumentDB-Subnetzgruppe

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Wählen Sie im Navigationsbereich Subnet groups (Subnetzgruppen) und anschließend Create (Erstellen) aus.

   > **Tip**
   >
   > Wenn der Navigationsbereich auf der linken Seite des Bildschirms nicht angezeigt wird, wählen Sie links oben auf der Seite das Menüsymbol (≡) aus.

3. Auf der Seite Create subnet group (Subnetzgruppe erstellen):

   a. Im Abschnitt Subnet group details (Subnetzgruppen-Details:

i. Name — Geben Sie einen aussagekräftigen Namen für die Subnetzgruppe ein.

ii. Beschreibung – Geben Sie eine Beschreibung für die Subnetzgruppe ein.

b. Im Abschnitt Add subnets (Subnetze hinzufügen):

i. VPC — Wählen Sie in der Liste eine VPC für diese Subnetzgruppe aus.

ii. Führen Sie eine der folgenden Aktionen aus:

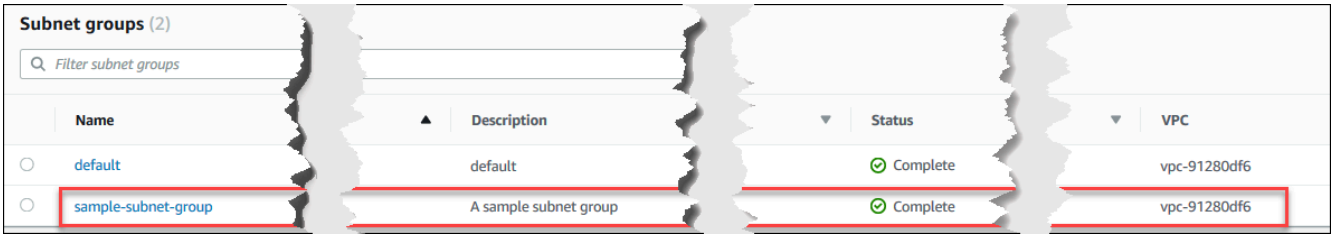
- Um alle Subnetze in der ausgewählten VPC miteinzuschließen, wählen Sie Add all the subnets related to this VPC (Alle zu dieser VPC gehörenden Subnetze hinzufügen).
- Um Subnetze für diese Subnetzgruppe festzulegen, führen Sie folgende Aufgaben für jede Availability Zone aus, für die Sie Subnetze miteinschließen möchten. Sie müssen mindestens zwei Availability Zones einschließen.

A. Availability Zone — Wählen Sie in der Liste eine Availability Zone aus.

B. Subnetz — Wählen Sie in der Liste ein Subnetz aus der ausgewählten Availability Zone für diese Subnetzgruppe aus.

C. Wählen Sie Add subnet (Subnetz hinzufügen) aus.

4. Wählen Sie Erstellen aus. Wenn die Subnetzgruppe erstellt wurde, wird sie mit Ihren anderen Subnetzgruppen aufgeführt.



Using the AWS CLI

Bevor Sie mithilfe von eine Subnetzgruppe erstellen können, müssen Sie zunächst ermitteln AWS CLI, welche Subnetze verfügbar sind. Führen Sie den folgenden AWS CLI Vorgang aus, um die Availability Zones und ihre Subnetze aufzulisten.

Parameter:

- **`--db-subnet-group`**— Fakultativ. Bei Angabe einer bestimmten Subnetzgruppe werden die Availability Zones und Subnetze für diese Gruppe aufgelistet. Durch Auslassen dieses

Parameters werden Availability Zones und Subnetze für alle Ihre Subnetzgruppen aufgelistet. Bei Angabe der `default`-Subnetzgruppe werden alle Subnetze der VPC aufgelistet.

Example

Für Linux, macOS oder Unix:

```
aws docdb describe-db-subnet-groups \
    --db-subnet-group-name default \
    --query 'DBSubnetGroups[*].[DBSubnetGroupName,Subnets[*].
[SubnetAvailabilityZone.Name,SubnetIdentifier]]'
```

Für Windows:

```
aws docdb describe-db-subnet-groups ^
    --db-subnet-group-name default ^
    --query 'DBSubnetGroups[*].[DBSubnetGroupName,Subnets[*].
[SubnetAvailabilityZone.Name,SubnetIdentifier]]'
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus (JSON-Format).

```
[
    [
        "default",
        [
            [
                "us-east-1a",
                "subnet-4e26d263"
            ],
            [
                "us-east-1c",
                "subnet-afc329f4"
            ],
            [
                "us-east-1e",
                "subnet-b3806e8f"
            ],
            [
                "us-east-1d",
                "subnet-53ab3636"
            ],
```

```
            [
                "us-east-1b",
                "subnet-991cb8d0"
            ],
            [
                "us-east-1f",
                "subnet-29ab1025"
            ]
        ]
    ]
]
```

Sie können eine neue Subnetzgruppe erstellen, indem Sie die Ausgabe des vorherigen Vorgangs verwenden. Die neue Subnetzgruppe muss über Subnetze aus mindestens zwei Availability Zones verfügen.

Parameter:

- **`--db-subnet-group-name`**—Erforderlich. Der Name für diese Subnetzgruppe.
- **`--db-subnet-group-description`**—Erforderlich. Beschreibung dieser Subnetzgruppe.
- **`--subnet-ids`**—Erforderlich. Eine Liste der Subnetze in dieser Subnetzgruppe. Beispiel: `subnet-53ab3636`.
- --Schlagworte — Optional. Eine Liste der Tags (Schlüssel-Wert-Paare) zum Anfügen an diese Subnetzgruppe.

Der folgende Code erstellt die Subnetzgruppe `sample-subnet-group` mit drei Subnetzen, `subnet-4e26d263`, `subnet-afc329f4` und `subnet-b3806e8f`.

Für Linux, macOS oder Unix:

```
aws docdb create-db-subnet-group \
    --db-subnet-group-name sample-subnet-group \
    --db-subnet-group-description "A sample subnet group" \
    --subnet-ids subnet-4e26d263 subnet-afc329f4 subnet-b3806e8f \
    --tags Key=tag1,Value=One Key=tag2,Value=2
```

Für Windows:

```
aws docdb create-db-subnet-group ^
```

```
    --db-subnet-group-name sample-subnet-group ^
    --db-subnet-group-description "A sample subnet group" ^
    --subnet-ids subnet-4e26d263 subnet-afc329f4 subnet-b3806e8f ^
    --tags Key=tag1,Value=One Key=tag2,Value=2
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus (JSON-Format).

```
{
    "DBSubnetGroup": {
        "DBSubnetGroupDescription": "A sample subnet group",
        "DBSubnetGroupName": "sample-subnet-group",
        "Subnets": [
            {
                "SubnetAvailabilityZone": {
                    "Name": "us-east-1a"
                },
                "SubnetIdentifier": "subnet-4e26d263",
                "SubnetStatus": "Active"
            },
            {
                "SubnetAvailabilityZone": {
                    "Name": "us-east-1c"
                },
                "SubnetIdentifier": "subnet-afc329f4",
                "SubnetStatus": "Active"
            },
            {
                "SubnetAvailabilityZone": {
                    "Name": "us-east-1e"
                },
                "SubnetIdentifier": "subnet-b3806e8f",
                "SubnetStatus": "Active"
            }
        ],
        "VpcId": "vpc-91280df6",
        "DBSubnetGroupArn": "arn:aws:rds:us-east-1:123SAMPLE012:subgrp:sample-
subnet-group",
        "SubnetGroupStatus": "Complete"
    }
}
```

Beschreibung einer Amazon DocumentDB-Subnetzgruppe

Sie können das AWS-Managementkonsole oder das verwenden AWS CLI , um die Details einer Amazon DocumentDB-Subnetzgruppe abzurufen.

Using the AWS-Managementkonsole

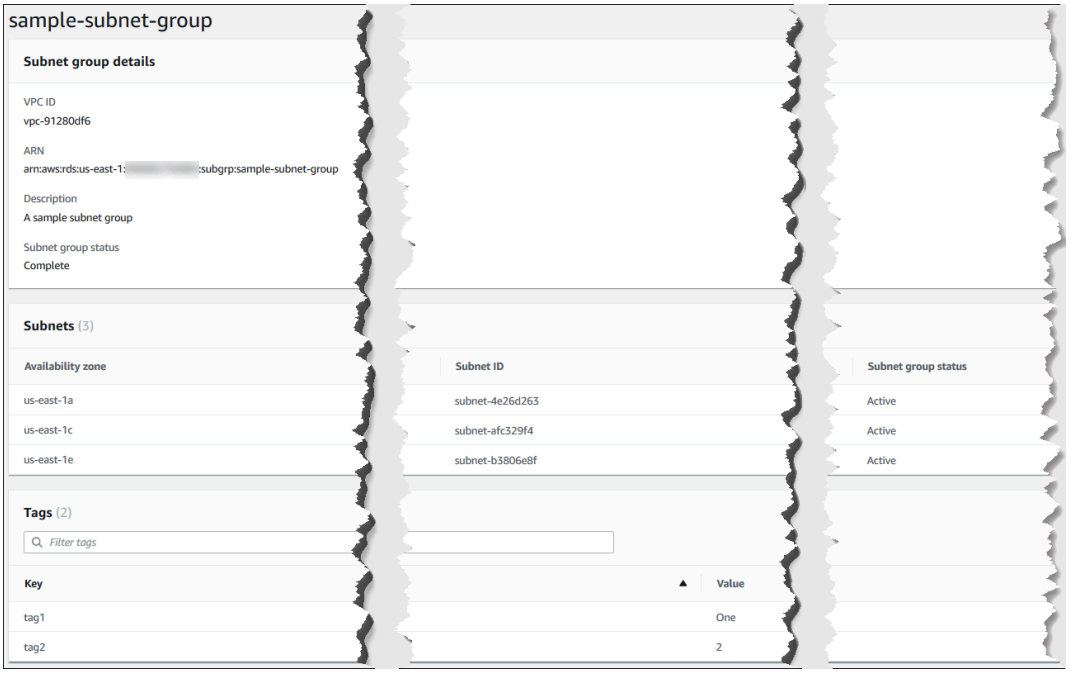
Das folgende Verfahren zeigt Ihnen, wie Sie die Details einer Amazon DocumentDB-Subnetzgruppe abrufen können.

So suchen Sie die Details einer Subnetzgruppe

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Wählen Sie im Navigationsbereich Subnetzgruppe aus.

> **Tip**
>
> Wenn der Navigationsbereich auf der linken Seite des Bildschirms nicht angezeigt wird, wählen Sie links oben auf der Seite das Menüsymbol (≡) aus.

3. Um die Details einer Subnetzgruppe anzuzeigen, wählen Sie den Namen der Subnetzgruppe.



Using the AWS CLI

Um die Details einer Amazon DocumentDB-Subnetzgruppe zu finden, verwenden Sie den `describe-db-subnet-groups` Vorgang mit dem folgenden Parameter.

Parameter

- `--db-subnet=group-name`— Optional. Falls angegeben, werden Details für die benannte Subnetzgruppe aufgelistet. Falls nicht angegeben, werden Details für bis zu 100 Subnetzgruppen aufgelistet.

Example

Der folgende Code listet die Details für die Subnetzgruppe `sample-subnet-group` auf, die im Abschnitt Eine Amazon DocumentDB-Subnetzgruppe erstellen erstellt wurde.

Für Linux, macOS oder Unix:

```
aws docdb describe-db-subnet-groups \
    --db-subnet-group-name sample-subnet-group
```

Für Windows:

```
aws docdb describe-db-subnet-groups ^
    --db-subnet-group-name sample-subnet-group
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus (JSON-Format).

```
{
    "DBSubnetGroup": {
        "DBSubnetGroupArn": "arn:aws:rds:us-east-1:123SAMPLE012:subgrp:sample-
subnet-group",
        "VpcId": "vpc-91280df6",
        "SubnetGroupStatus": "Complete",
        "DBSubnetGroupName": "sample-subnet-group",
        "Subnets": [
            {
                "SubnetAvailabilityZone": {
                    "Name": "us-east-1a"
                },
                "SubnetStatus": "Active",
                "SubnetIdentifier": "subnet-4e26d263"
```

```
            },
            {
                "SubnetAvailabilityZone": {
                    "Name": "us-east-1c"
                },
                "SubnetStatus": "Active",
                "SubnetIdentifier": "subnet-afc329f4"
            },
            {
                "SubnetAvailabilityZone": {
                    "Name": "us-east-1e"
                },
                "SubnetStatus": "Active",
                "SubnetIdentifier": "subnet-b3806e8f"
            }
        ],
        "DBSubnetGroupDescription": "A sample subnet group"
    }
}
```

Ändern einer Amazon DocumentDB-Subnetzgruppe

Sie können das AWS-Managementkonsole oder verwenden AWS CLI , um die Beschreibung einer Subnetzgruppe zu ändern oder Subnetze zu einer Amazon DocumentDB-Subnetzgruppe hinzuzufügen oder zu entfernen. Sie können die `default`-Subnetzgruppe jedoch nicht ändern.

Using the AWS-Managementkonsole

Sie können das verwenden AWS-Managementkonsole , um die Beschreibung einer Subnetzgruppe zu ändern oder Subnetze hinzuzufügen oder zu entfernen. Denken Sie daran, dass beim Abschluss des Vorgangs mindestens zwei Availability Zones mit Ihrer Subnetzgruppe verbunden sein müssen.

So ändern Sie Ihre Subnetzgruppe

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Wählen Sie im Navigationsbereich Subnetzgruppe aus. Klicken Sie dann auf die Schaltfläche links neben dem Namen der Subnetzgruppe. Denken Sie daran, dass Sie die `default`-Subnetzgruppe nicht ändern können.

> **Tip**
>
> Wenn der Navigationsbereich auf der linken Seite des Bildschirms nicht angezeigt wird, wählen Sie links oben auf der Seite das Menüsymbol (≡) aus.

3. Wählen Sie Actions (Aktionen) und dann Modify (Ändern) aus.
4. Beschreibung — Um die Beschreibung Ihrer Subnetzgruppe zu ändern, geben Sie eine neue Beschreibung ein.
5. Wenn Sie die mit Ihrer Subnetzgruppe verbundenen Subnetze ändern möchten, führen Sie im Abschnitt Add subnets (Subnetze hinzufügen) eine oder mehrere der folgenden Aktionen durch:
   - Um alle Subnetze aus dieser Subnetzgruppe zu entfernen, wählen Sie Remove all (Alle entfernen) aus.
   - Wenn Sie bestimmte Subnetze aus dieser Subnetzgruppe entfernen möchten, wählen Sie für jedes einzelne Subnetz, das Sie entfernen möchten, Remove (Entfernen) aus.
   - Wenn Sie alle mit dieser VPC verbundenen Subnetze hinzufügen möchten, wählen Sie Add all the subnets related to this VPC (Alle zu dieser VPC gehörenden Subnetze hinzufügen) aus.
   - Wenn Sie bestimmte Subnetze zu dieser Subnetzgruppe hinzufügen möchten, führen Sie die folgenden Aufgaben für jede Availability Zone aus, der Sie ein Subnetz hinzufügen möchten.
     a. Availability Zone — Wählen Sie in der Liste eine neue Availability Zone aus.
     b. Subnetz — Wählen Sie in der Liste ein Subnetz aus der ausgewählten Availability Zone für diese Subnetzgruppe aus.
     c. Wählen Sie Add subnet (Subnetz hinzufügen) aus.
6. Im Bestätigungsdialogfeld:
   - Wählen Sie Modify (Ändern), um diese Änderungen an der Subnetzgruppe vorzunehmen.
   - Wenn die Subnetzgruppe unverändert bleiben soll, wählen Sie Cancel (Abbrechen) aus.

Using the AWS CLI

Sie können den verwenden AWS CLI , um die Beschreibung einer Subnetzgruppe zu ändern oder Subnetze hinzuzufügen oder zu entfernen. Denken Sie daran, dass beim Abschluss des Vorgangs mindestens zwei Availability Zones mit Ihrer Subnetzgruppe verbunden sein müssen. Es ist nicht möglich, die `default`- Subnetzgruppe zu ändern.

Parameter:

- `--db-subnet-group-name`—Erforderlich. Der Name der Amazon DocumentDB-Subnetzgruppe, die Sie ändern.
- `--subnet-ids`—Erforderlich. Eine Liste aller Subnetze, die nach dieser Änderung Teil der Subnetzgruppe sein sollen.

  > **Important**
  >
  > Alle Subnetze, die sich derzeit in der Subnetzgruppe befinden und die nicht in dieser Liste aufgeführt sind, werden aus der Subnetzgruppe entfernt. Wenn Sie Subnetze, die sich derzeit in der Subnetzgruppe befinden, beibehalten möchten, müssen Sie diese in die Liste aufnehmen.

- `--db-subnet-group-description`— Fakultativ. Beschreibung der Subnetzgruppe.

Example

Der folgende Code ändert die Beschreibung und ersetzt die vorhandenen Subnetze durch die Subnetze `subnet-991cb8d0`, `subnet-53ab3636` und `subnet-29ab1025`.

Für Linux, macOS oder Unix:

```
aws docdb modify-db-subnet-group \
    --db-subnet-group-name sample-subnet-group \
    --subnet-ids subnet-991cb8d0 subnet-53ab3636 subnet-29ab1025 \
    --db-subnet-group-description "Modified subnet group"
```

Für Windows:

```
aws docdb modify-db-subnet-group ^
    --db-subnet-group-name sample-subnet-group ^
```

```
    --subnet-ids subnet-991cb8d0 subnet-53ab3636 subnet-29ab1025 ^
    --db-subnet-group-description "Modified subnet group"
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus (JSON-Format). Beachten Sie, dass dies die gleiche Subnetzgruppe ist, die im Abschnitt Eine Amazon DocumentDB-Subnetzgruppe erstellen erstellt wurde. Die Subnetze in der Subnetzgruppe werden jedoch durch die in der Operation`modify-db-subnet-group` angegebenen ersetzt.

```
{
    "DBSubnetGroup": {
        "DBSubnetGroupArn": "arn:aws:rds:us-east-1:123SAMPLE012:subgrp:sample-
subnet-group",
        "DBSubnetGroupDescription": "Modified subnet group",
        "SubnetGroupStatus": "Complete",
        "Subnets": [
            {
                "SubnetAvailabilityZone": {
                    "Name": "us-east-1d"
                },
                "SubnetStatus": "Active",
                "SubnetIdentifier": "subnet-53ab3636"
            },
            {
                "SubnetAvailabilityZone": {
                    "Name": "us-east-1b"
                },
                "SubnetStatus": "Active",
                "SubnetIdentifier": "subnet-991cb8d0"
            },
            {
                "SubnetAvailabilityZone": {
                    "Name": "us-east-1f"
                },
                "SubnetStatus": "Active",
                "SubnetIdentifier": "subnet-29ab1025"
            }
        ],
        "VpcId": "vpc-91280df6",
        "DBSubnetGroupName": "sample-subnet-group"
    }
}
```

Löschen einer Amazon DocumentDB-Subnetzgruppe

Sie können das AWS-Managementkonsole oder verwenden AWS CLI , um eine Amazon DocumentDB-Subnetzgruppe zu löschen. Sie können jedoch nicht die `default`-Subnetzgruppe löschen.

Using the AWS-Managementkonsole

Sie können den verwenden AWS-Managementkonsole , um eine Subnetzgruppe zu löschen. Die `default`-Subnetzgruppe kann jedoch nicht gelöscht werden.

So löschen Sie eine Subnetzgruppe

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Wählen Sie im Navigationsbereich Subnetzgruppe aus. Klicken Sie dann auf die Schaltfläche links neben dem Namen der Subnetzgruppe. Denken Sie daran, dass Sie die `default`-Subnetzgruppe nicht löschen können.

   > **Tip**
   >
   > Wenn der Navigationsbereich auf der linken Seite des Bildschirms nicht angezeigt wird, wählen Sie links oben auf der Seite das Menüsymbol (≡) aus.

3. Wählen Sie Aktionen und anschließend Löschen aus.
4. Im Bestätigungsdialogfeld:
   - Wählen Sie Delete (Löschen), um die Subnetzgruppe zu löschen.
   - Wählen Sie Cancel (Abbrechen), um die Subnetzgruppe zu erhalten.

Using the AWS CLI

Um eine Amazon DocumentDB-Subnetzgruppe mithilfe von zu löschen AWS CLI, verwenden Sie den `delete-db-subnet-group` Vorgang mit dem folgenden Parameter.

Parameter

- `--db-subnet-group-name`—Erforderlich. Der Name der Amazon DocumentDB-Subnetzgruppe, die gelöscht werden soll. Denken Sie daran, dass Sie die `default`-Subnetzgruppe nicht löschen können.

Example

Der folgende Code löscht `sample-subnet-group`.

Für Linux, macOS oder Unix:

```
aws docdb delete-db-subnet-group \
    --db-subnet-group-name sample-subnet-group
```

Für Windows:

```
aws docdb delete-db-subnet-group ^
    --db-subnet-group-name sample-subnet-group
```

Diese Operation erzeugt keine Ausgabe.

Amazon DocumentDB Hochverfügbarkeit und Replikation

Sie können Hochverfügbarkeit und Leseskalierung in Amazon DocumentDB (mit MongoDB-Kompatibilität) erreichen, indem Sie Replica-Instances verwenden. Ein einzelner Amazon DocumentDB-Cluster unterstützt eine einzelne primäre Instance und bis zu 15 Replikat-Instances. Diese Instances können über mehrere Availability Zones innerhalb der Cluster-Region verteilt werden. Die primäre Instance akzeptiert Lese- und Schreibverkehr, und Replikat-Instances akzeptieren nur Leseanforderungen.

Das Cluster-Volume besteht aus mehreren Kopien der Daten für den Cluster. Die Daten im Cluster-Volume werden jedoch als einzelnes logisches Volume für die primäre Instance und für Amazon DocumentDB DocumentDB-Replikate im Cluster dargestellt. Replikat-Instances sind „Eventually Consistent“. Sie geben Abfrageergebnisse mit minimaler Replikatverzögerung zurück – im Normalfall beträgt die Verzögerung weniger als 100 Millisekunden, nachdem die primäre Instance eine Aktualisierung geschrieben hat. Die Replica-Verzögerung variiert in Abhängigkeit

vom Veränderungsgrad in der Datenbank. Das heißt, in Zeiten, in denen eine große Anzahl von Schreiboperationen für die Datenbank durchgeführt wird, kann es zu einer Erhöhung der Replikationsverzögerung kommen.

Skalierung von Lesevorgängen

Amazon DocumentDB DocumentDB-Replikate eignen sich gut für die Leseskalierung, da sie ausschließlich für Lesevorgänge auf Ihrem Cluster-Volume vorgesehen sind. Schreibvorgänge werden von der primären Instance verwaltet. Das Cluster-Volume wird von allen Instances in Ihrem Cluster gemeinsam genutzt. Daher müssen Sie nicht für jedes Amazon DocumentDB DocumentDB-Replikat eine Kopie der Daten replizieren und verwalten.

Hohe Verfügbarkeit

Wenn Sie einen Amazon DocumentDB-Cluster erstellen, stellt Amazon DocumentDB je nach Anzahl der Availability Zones in der Subnetzgruppe (es müssen mindestens zwei vorhanden sein) Instances in den Availability Zones bereit. Wenn Sie Instances im Cluster erstellen, verteilt Amazon DocumentDB die Instances automatisch auf die Availability Zones in einer Subnetzgruppe, um den Cluster auszugleichen. Diese Vorgehensweise verhindert auch, dass sich alle Instances in derselben Availability Zone befinden.

Beispiel

Zur Veranschaulichung nehmen wir ein Beispiel, in dem ein Cluster erstellt wird, das eine Subnetzgruppe mit drei Availability Zones hat AZ1, AZ2 und AZ3.

Wenn die erste Instance im Cluster erstellt wird, ist diese die primäre Instance und befindet sich in einer der Availability Zones. In diesem Beispiel handelt es sich um AZ1. Die zweite erstellte Instance ist eine Replikat-Instance und befindet sich in einer der beiden anderen Availability Zones, z.B. AZ2. Die dritte Instance, die erstellt wird, ist eine Replikat-Instance und befindet sich in der verbleibenden Availability ZoneAZ3. Wenn Sie mehrere Instances erstellen, werden diese über die Availability Zones verteilt, sodass der Cluster ausbalanciert ist.

Tritt in der primären Instance (AZ1) ein Fehler auf, wird ein Failover ausgelöst und eine der bestehenden Replikat-Instances wird zur primären Instance heraufgestuft. Wenn die alten primäre Instance wiederhergestellt wurde, wird sie zu einem Replikat in der gleichen Availability Zone, in der sie bereitgestellt wurde (AZ1). Wenn Sie einen Drei-Instanz-Cluster bereitstellen, behält Amazon DocumentDB diesen Drei-Instanz-Cluster weiterhin bei. Amazon DocumentDB kümmert sich

automatisch um die Erkennung, den Failover und die Wiederherstellung von Instance-Ausfällen ohne manuelles Eingreifen.

Wenn Amazon DocumentDB einen Failover durchführt und eine Instance wiederherstellt, verbleibt die wiederhergestellte Instance in der Availability Zone, in der sie ursprünglich bereitgestellt wurde. Die Rolle der Instance ändert sich möglicherweise von der primären Instance zum Replikat. Dadurch wird ein Szenario verhindert, in dem eine Reihe von Failovers in allen Instances auftreten könnten, die sich in derselben Availability Zone befinden.

Sie können Amazon DocumentDB DocumentDB-Replikate als Failover-Ziele angeben. Das heißt, wenn die primäre Instance ausfällt, wird das angegebene Amazon DocumentDB DocumentDB-Replikat oder das Replikat aus einer Stufe zur primären Instance heraufgestuft. Es gibt dann eine kurze Unterbrechung, während der Lese- und Schreibanfragen an die primäre Instance mit einer Ausnahme fehlschlagen. Wenn Ihr Amazon DocumentDB-Cluster keine Amazon DocumentDB DocumentDB-Replikate enthält und die primäre Instance ausfällt, wird sie neu erstellt. Das Heraufstufen eines Amazon DocumentDB-Replikats ist viel schneller als das Neuerstellen der primären Instance.

Für Hochverfügbarkeitsszenarien empfehlen wir, ein oder mehrere Amazon DocumentDB DocumentDB-Replikate zu erstellen. Diese Replikate sollten derselben Instance-Klasse wie die primäre Instance angehören und sich in unterschiedlichen Availability Zones für Ihren Amazon DocumentDB-Cluster befinden.

Weitere Informationen finden Sie hier:

- Grundlegendes zur Amazon DocumentDB-Cluster-Fehlertoleranz
- Amazon DocumentDB-Failover
  - Steuerung des Failover-Ziels

In den Amazon DocumentDB DocumentDB-Versionen 5.0 und 8.0 werden Replikat-Instances nicht neu gestartet, wenn die primäre Instance neu gestartet wird. Sie bearbeiten weiterhin Leseanfragen bei Neustarts der primären Instance und sorgen so für eine verbesserte Verfügbarkeit.

Hohe Verfügbarkeit mit globalen Clustern

Um eine hohe Verfügbarkeit für mehrere zu gewährleisten AWS-Regionen, können Sie globale Amazon DocumentDB-Cluster einrichten. Jeder globale Cluster erstreckt sich über mehrere Regionen und ermöglicht globale Lesevorgänge mit geringer Latenz sowie die Notfallwiederherstellung nach

Ausfällen in einem Land. AWS-Region Amazon DocumentDB übernimmt automatisch die Replikation aller Daten und Updates von der primären Region in jede der sekundären Regionen.

Hinzufügen von -Replicas

Die erste dem Cluster hinzugefügte Instance ist die primäre Instance. Jede Instance, die nach der ersten Instance hinzugefügt wird, ist eine Replikat-Instance. Ein Cluster kann zusätzlich zur primären bis zu 15 Replikatinstanzen haben.

Wenn Sie mit dem einen Cluster erstellen AWS-Managementkonsole, wird gleichzeitig automatisch eine primäre Instanz erstellt. Um ein Replikat gleichzeitig mit der Erstellung des Clusters und der primären Instance zu erstellen, wählen Sie Create replica in different zone (Replikat in unterschiedlicher Zone erstellen) aus. Weitere Informationen finden Sie in Schritt 4.d unter Einen Amazon DocumentDB-Cluster erstellen. Informationen zum Hinzufügen weiterer Replikate zu einem Amazon DocumentDB-Cluster finden Sie unter. Hinzufügen einer Amazon DocumentDB DocumentDB-Instance zu einem Cluster

Wenn Sie den AWS CLI zur Erstellung Ihres Clusters verwenden, müssen Sie Ihre Primär- und Replikat-Instances explizit erstellen. Weitere Informationen finden Sie in den folgenden Themen im Abschnitt AWS CLI„Verwenden von“:

- Einen Amazon DocumentDB-Cluster erstellen
- Hinzufügen einer Amazon DocumentDB DocumentDB-Instance zu einem Cluster

Amazon DocumentDB-Failover

In bestimmten Fällen, z. B. bei bestimmten Arten von geplanten Wartungsarbeiten oder in dem unwahrscheinlichen Fall, dass ein primärer Knoten oder eine Availability Zone ausfällt, erkennt Amazon DocumentDB (mit MongoDB-Kompatibilität) den Ausfall und ersetzt den primären Knoten. Während eines Failovers wird die Ausfallzeit für Schreibvorgänge minimiert. Das liegt daran, dass die Rolle des primären Knotens auf eine der Read Replicas übergeht, statt dass ein neuer primärer Knoten erstellt und bereitgestellt werden muss. Durch Ausfallerkennung und Replikatheraufstufung wird sichergestellt, dass Sie weiter in den neuen primären Knoten schreiben können, sobald die Heraufstufung abgeschlossen wurde.

Damit der Failover funktioniert, muss Ihr Cluster über mindestens zwei Instances verfügen — eine primäre und mindestens eine Replikat-Instance.

> **Note**
>
> Dieses Thema bezieht sich nur auf originale, auf Amazon DocumentDB DocumentDB-Instances basierende Cluster. Es gilt nicht für elastische oder globale Cluster.

Steuerung des Failover-Ziels

Amazon DocumentDB bietet Ihnen Failover-Stufen, mit denen Sie kontrollieren können, welche Replikat-Instance bei einem Failover zur primären Instanz heraufgestuft wird.

Failover-Stufen

Jede Replikat-Instance ist einer Failover-Stufe (0—15) zugeordnet. Wenn aufgrund von Wartungsarbeiten oder eines unwahrscheinlichen Hardwarefehlers ein Failover auftritt, wechselt die primäre Instanz zu einem Replikat mit der höchsten Priorität (der niedrigsten Stufe). Wenn mehrere Replikate dieselbe Prioritätsstufe haben, erfolgt für die primäre Replikation ein Failover auf das Replikat dieser Stufe, dessen Größe der vorherigen Primärstufe am nächsten kommt.

Indem Sie die Failover-Stufe für eine Gruppe ausgewählter Replikate auf `0` (höchste Priorität) setzen, können Sie sicherstellen, dass ein Failover auf eines der Replikate in dieser Gruppe wechselt. Sie können effektiv verhindern, dass bestimmte Replikate im Falle eines Failover zur primären Instance hochgestuft werden, indem Sie diesen Replikaten eine niedrige Stufe (hohe Anzahl) zuweisen. Dies ist nützlich, wenn bestimmte Replikate von einer Anwendung stark genutzt werden und ein Failover auf eine von ihnen eine kritische Anwendung negativ beeinflussen würde.

Sie können die Failover-Stufe einer Instance beim Erstellen oder später festlegen. Das Festlegen einer Instance-Failover-Stufe durch Ändern der Instance löst keinen Failover aus. Weitere Informationen finden Sie in den folgenden Themen:

- Hinzufügen einer Amazon DocumentDB DocumentDB-Instance zu einem Cluster
- Ändern einer Amazon DocumentDB DocumentDB-Instance

Wenn Sie einen Failover manuell einleiten, haben Sie zwei Möglichkeiten zur Steuerung, welche Replikat-Instance auf primär umgestellt wird: die Failover-Stufen wie zuvor beschrieben und den Parameter `--target-db-instance-identifier`.

`-- Ziel-DB-Instance-ID`

Zum Testen können Sie mit der Operation `failover-db-cluster` ein Failover-Ereignis erzwingen. Mit dem Parameter `--target-db-instance-identifier` können Sie festlegen, welches Replikat auf primär umgestellt werden soll. Die Verwendung des Parameters `--target-db-instance-identifier` ersetzt die Failover-Prioritätsstufe. Wenn Sie den Parameter `--target-db-instance-identifier` nicht angeben, entspricht die Primär-Failover-Funktion der Failover-Prioritätsstufe.

Was passiert bei einem Failover

Das Failover wird automatisch von Amazon DocumentDB durchgeführt, sodass Ihre Anwendungen den Datenbankbetrieb so schnell wie möglich wieder aufnehmen können, ohne dass ein Administrator eingreifen muss.

- Wenn Sie beim Failover eine Amazon DocumentDB-Replikat-Instance in derselben oder einer anderen Availability Zone haben: Amazon DocumentDB dreht den Canonical Name Record (CNAME) für Ihre Instance um, sodass er auf das fehlerfreie Replikat verweist, das wiederum zum neuen primären Replikat heraufgestuft wird. Das Failover wird in der Regel innerhalb von 30 Sekunden vom Anfang bis zum Ende abgeschlossen.
- Wenn Sie keine Amazon DocumentDB-Replikatinstanz haben (z. B. einen einzelnen Instance-Cluster): Amazon DocumentDB versucht, eine neue Instance in derselben Availability Zone wie die ursprüngliche Instance zu erstellen. Dieser Austausch der ursprünglichen Instance wird nach bestem Bemühen durchgeführt, ist aber nicht immer erfolgreich, z. B. wenn ein Problem vorliegt, das sich allgemein auf die Availability Zone auswirkt.

Bei Verbindungsunterbrechung muss Ihre Anwendung versuchen, die Verbindung zur Datenbank wiederherzustellen.

Testen eines Failovers

Bei einem Failover für einen Cluster wird eine der Amazon DocumentDB DocumentDB-Repliken (schreibgeschützte Instances) im Cluster zur primären Instance (Cluster-Writer) heraufgestuft.

Wenn die primäre Instance ausfällt, wechselt Amazon DocumentDB automatisch zu einem Amazon DocumentDB DocumentDB-Replikat, falls eines existiert. Sie können ein Failover erzwingen, wenn Sie einen Ausfall einer primären Instance zum Testen simulieren möchten. Jede Instance in einem Cluster hat eine eigene Endpunkt-Adresse. Aus diesem Grund müssen Sie alle bestehenden Verbindungen, die diese Endpunktadressen verwenden, bereinigen und wiederherstellen, wenn der Failover abgeschlossen ist.

Um einen Failover zu erzwingen, verwenden Sie die Operation `failover-db-cluster` mit diesen Parametern.

- `--db-cluster-identifier`—Erforderlich. Der Name des Clusters, der einen Failover durchführen soll.
- `--target-db-instance-identifier`— Fakultativ. Der Name der Instance, die zur primären Instance befördert werden soll.

Example

Die folgende Operation erzwingt einen Failover des Clusters `sample-cluster`. Es wird nicht angegeben, welche Instance zur neuen primären Instance gemacht werden soll, sodass Amazon DocumentDB die Instance entsprechend der Priorität der Failover-Tier-Priorität auswählt.

Für Linux, macOS oder Unix:

```
aws docdb failover-db-cluster \
   --db-cluster-identifier sample-cluster
```

Für Windows:

```
aws docdb failover-db-cluster ^
   --db-cluster-identifier sample-cluster
```

Die folgende Operation erzwingt einen Failover des Clusters `sample-cluster` und legt fest, dass `sample-cluster-instance` in die primäre Rolle befördert werden soll. (Beachten Sie `"IsClusterWriter": true` in der Ausgabe.)

Für Linux, macOS oder Unix:

```
aws docdb failover-db-cluster \
   --db-cluster-identifier sample-cluster \
   --target-db-instance-identifier sample-cluster-instance
```

Für Windows:

```
aws docdb failover-db-cluster ^
   --db-cluster-identifier sample-cluster ^
   --target-db-instance-identifier sample-cluster-instance
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus (JSON-Format).

```
{
    "DBCluster": {
        "HostedZoneId": "Z2SUY0A1719RZT",
        "Port": 27017,
        "EngineVersion": "3.6.0",
        "PreferredMaintenanceWindow": "thu:04:05-thu:04:35",
        "BackupRetentionPeriod": 1,
        "ClusterCreateTime": "2018-06-28T18:53:29.455Z",
        "AssociatedRoles": [],
        "DBSubnetGroup": "default",
        "MasterUsername": "master-user",
        "Engine": "docdb",
        "ReadReplicaIdentifiers": [],
        "EarliestRestorableTime": "2018-08-21T00:04:10.546Z",
        "DBClusterIdentifier": "sample-cluster",
        "ReaderEndpoint": "sample-cluster.node.us-east-1.docdb.amazonaws.com",
        "DBClusterMembers": [
            {
                "DBInstanceIdentifier": "sample-cluster-instance",
                "DBClusterParameterGroupStatus": "in-sync",
                "PromotionTier": 1,
                "IsClusterWriter": true
            },
            {
                "DBInstanceIdentifier": "sample-cluster-instance-00",
                "DBClusterParameterGroupStatus": "in-sync",
                "PromotionTier": 1,
                "IsClusterWriter": false
            },
            {
                "DBInstanceIdentifier": "sample-cluster-instance-01",
                "DBClusterParameterGroupStatus": "in-sync",
                "PromotionTier": 1,
                "IsClusterWriter": false
            }
        ],
        "AvailabilityZones": [
            "us-east-1b",
            "us-east-1c",
            "us-east-1a"
        ],
        "DBClusterParameterGroup": "default.docdb3.6",
```

```
        "Endpoint": "sample-cluster.node.us-east-1.docdb.amazonaws.com",
        "IAMDatabaseAuthenticationEnabled": false,
        "AllocatedStorage": 1,
        "LatestRestorableTime": "2018-08-22T21:57:33.904Z",
        "PreferredBackupWindow": "00:00-00:30",
        "StorageEncrypted": false,
        "MultiAZ": true,
        "Status": "available",
        "DBClusterArn": "arn:aws:rds:us-east-1:123456789012:cluster:sample-cluster",
        "VpcSecurityGroups": [
            {
                "Status": "active",
                "VpcSecurityGroupId": "sg-12345678"
            }
        ],
        "DbClusterResourceId": "cluster-ABCDEFGHIJKLMNOPQRSTUVWXYZ"
    }
}
```

Replikationsverzögerung

Die Verzögerung bei der Replikation beträgt in der Regel 50 ms oder weniger. Die häufigsten Gründe für eine erhöhte Replikatverzögerung sind:

- Eine hohe Schreibrate auf der Primärseite, die dazu führt, dass die Lesereplikate hinter die Primärreplikate zurückfallen.
- Konflikt auf den Read Replicas zwischen Abfragen mit langer Laufzeit (z. B. umfangreiche sequentielle Scans, Aggregationsabfragen) und eingehender Schreibreplikation.
- Sehr große Anzahl gleichzeitiger Abfragen an den Read Replicas.

Um die Verzögerung bei der Replikation zu minimieren, sollten Sie die folgenden Methoden zur Problembehandlung ausprobieren:

- Wenn Sie eine hohe Schreibrate oder eine hohe CPU-Auslastung haben, empfehlen wir Ihnen, die Instances in Ihrem Cluster zu skalieren.
- Wenn Ihre Read Replicas lang andauern und die abgefragten Dokumente sehr häufig aktualisiert werden, sollten Sie in Erwägung ziehen, Ihre Abfragen mit langer Laufzeit zu ändern oder sie für das Replikat auszuführen, um Konflikte bei den primary/write Read Replicas zu vermeiden.

- Wenn es nur bei den Read Replicas eine sehr große Anzahl gleichzeitiger Abfragen oder eine hohe CPU-Auslastung gibt, besteht eine weitere Möglichkeit darin, die Anzahl der Read Replicas zu skalieren, um die Arbeitslast zu verteilen.
- Da die Verzögerung bei der Replikation auf einen hohen Schreibdurchsatz und lange laufende Abfragen zurückzuführen ist, empfehlen wir, die Replikationsverzögerung mithilfe der DBClusterReplicaLagMaximum CW-Metrik in Kombination mit dem langsamen Abfrage-Logger und den /-Metriken zu beheben. `WriteThroughput` `WriteIOPS`

Im Allgemeinen empfehlen wir, dass alle Ihre Replikate vom gleichen Instance-Typ sind, damit ein Cluster-Failover nicht zu Leistungseinbußen führt.

Wenn Sie zwischen Hochskalierung und Ausskalierung wählen (z. B. sechs kleinere Instances gegenüber drei größeren Instances), empfehlen wir generell, zuerst zu versuchen, vor dem Skalieren zu versuchen, bevor Sie die Skalierung verlassen, da Sie so einen größeren Puffer-Cache pro DB-Instance erhalten.

Proaktiv sollten Sie einen Alarm für die Verzögerung bei der Replikation einrichten und den Schwellenwert auf einen Wert setzen, der Ihrer Meinung nach die Obergrenze dafür darstellt, wie weit Ihre Daten auf Replikatinstanzen zurückliegen (oder „veraltet“) sein können, bevor sie die Funktionalität Ihrer Anwendung beeinträchtigen. Im Allgemeinen empfehlen wir, den Schwellenwert für die Replikationsverzögerung aufgrund vorübergehender Workloads für mehrere Datenpunkte zu überschreiten, bevor ein Alarm ausgelöst wird.

> **Note**
>
> Darüber hinaus empfehlen wir, einen weiteren Alarm für Replikationsverzögerungen von mehr als 10 Sekunden einzurichten. Wenn Sie diesen Schwellenwert für mehrere Datenpunkte überschreiten, empfehlen wir Ihnen, Ihre Instances zu skalieren oder Ihren Schreibdurchsatz auf der primären Instance zu reduzieren.

Amazon DocumentDB DocumentDB-Indizes verwalten

Themen

- Amazon DocumentDB DocumentDB-Indexerstellung
- Pflege Amazon DocumentDB DocumentDB-Indizes

Amazon DocumentDB DocumentDB-Indexerstellung

Für die Erstellung von Indizes in Amazon DocumentDB müssen eine Reihe von Entscheidungen getroffen werden:

- Wie schnell muss es abgeschlossen werden?
- Kann während der Erstellung nicht auf die Sammlung zugegriffen werden?
- Wie viel Rechenleistung einer Instanz kann dem Build zugewiesen werden?
- Welche Art von Index sollte erstellt werden?

Dieser Abschnitt hilft Ihnen bei der Beantwortung dieser Fragen und enthält die Befehle und Überwachungsbeispiele, um einen Amazon DocumentDB DocumentDB-Index für Ihre instanzbasierte Clustersammlung zu erstellen.

Richtlinien

Die folgenden Richtlinien enthalten grundlegende Grenzwerte und Kompromisse bei der Konfiguration bei der Erstellung neuer Indizes:

- Unterstützung für Amazon DocumentDB DocumentDB-Versionen — Während die Single-Worker-Indizierung in allen Amazon DocumentDB DocumentDB-Versionen unterstützt wird, wird die Multi-Worker-Indizierung nur in den Amazon DocumentDB DocumentDB-Versionen 4.0, 5.0 und 8.0 unterstützt.
- Leistungseinbußen — Eine Erhöhung der Anzahl von Workern bei der Indexerstellung erhöht die CPU-Auslastung und die Lese-I/O auf der primären Instance Ihrer Amazon DocumentDB DocumentDB-Datenbank. Die Ressourcen, die für die Erstellung eines neuen Indexes benötigt werden, stehen Ihrem laufenden Workload nicht zur Verfügung.
- Elastische Cluster — Parallele Indizierung wird auf elastischen Amazon DocumentDB-Clustern nicht unterstützt.
- Maximale Anzahl an Workern — Die maximale Anzahl von Workern, die Sie konfigurieren können, hängt von der Größe Ihrer primären Instance in Ihrem Datenbank-Cluster ab. Das ist die Hälfte der Gesamtzahl der vCPUs auf der primären Instance Ihres Datenbank-Clusters. Sie können beispielsweise maximal 32 Worker auf einer db.r6g.16xlarge-Instance mit 64 vCPUs ausführen.

> **Note**
>
> Parallele Worker werden in den Instance-Klassen 2xlarge und niedriger nicht unterstützt.

- Mindestanzahl an Workern — Die Mindestanzahl an Workern, die Sie konfigurieren können, ist eins. Die Standardeinstellung für die Indexerstellung auf instanzbasierten Clustern ist zwei Worker. Sie können die Anzahl der Worker jedoch auf einen reduzieren, indem Sie die Option „Worker-Threads“ verwenden. Dadurch wird der Prozess mit einem einzigen Worker ausgeführt.
- Indexkomprimierung — Amazon DocumentDB unterstützt keine Indexkomprimierung. Die Datengrößen für Indizes sind möglicherweise größer als bei Verwendung anderer Optionen.
- Indizierung mehrerer Sammlungen — Die Hälfte der vCPUs auf der primären Instance Ihres Datenbank-Clusters kann für konfigurierte Worker verwendet werden, die Indexerstellung für mehrere Sammlungen durchführen.
- Indextypen — In diesem Blogbeitrag finden Sie eine vollständige Erklärung der unterstützten Indextypen in Amazon DocumentDB.

Erste Schritte

Verwenden Sie den `createIndexes` Befehl, um die Indexerstellung für eine Sammlung zu starten. Standardmäßig führt der Befehl zwei parallel Worker aus, wodurch die Geschwindigkeit des Indexerstellungsprozesses um das Zweifache erhöht wird.

Der folgende Befehlsprozess zeigt beispielsweise, wie ein Index für das Feld „user_name“ in einem Dokument erstellt und die Geschwindigkeit des Indizierungsvorgangs auf vier Worker erhöht wird:

1. Erstellen Sie Indizes mit zwei parallel Workern auf dem Cluster:

   ```
   db.runCommand({"createIndexes":"test","indexes":[{"key": {"user_name":1},
    "name":"username_idx"}]})
   ```

2. Um die Geschwindigkeit der Indexerstellung zu optimieren, können Sie die Anzahl der Worker mithilfe der Option „Worker-Threads“ (`"workers":<number>`) im `db.runCommand` `createIndexes` Befehl angeben.

   Erhöhen Sie die Geschwindigkeit des Prozesses auf vier parallel Mitarbeiter:

```
db.runCommand({"createIndexes":"test","indexes":[{"key": {"user_name":1},
 "name":"username_idx", "workers":4}]})
```

> **Note**
>
> Je höher die Anzahl der Mitarbeiter, desto schneller schreitet die Indexerstellung voran. Je höher jedoch die Anzahl der Worker steigt, desto höher steigt die Auslastung der vCPUs und der Lese-I/O Ihrer primären Instance. Stellen Sie sicher, dass Ihr Cluster ausreichend bereitgestellt ist, um die erhöhte Belastung zu bewältigen, ohne andere Workloads zu beeinträchtigen.

Status des Indizierungsfortschritts

Bei der Indexerstellung werden Sammlungen initialisiert, gescannt, Schlüssel sortiert und schließlich Schlüssel mithilfe eines Indexgenerators eingefügt. Der Prozess besteht aus bis zu sechs Phasen, wenn Sie ihn im Vordergrund ausführen, und bis zu neun Phasen, wenn Sie ihn im Hintergrund ausführen. Sie können Statusmetriken wie die prozentuale Fertigstellung, die Gesamtzahl der gescannten Speicherblöcke, die sortierten Schlüssel und die eingefügten Schlüssel Schritt für Schritt anzeigen.

Überwachen Sie den Fortschritt des Indizierungsprozesses, indem Sie den `db.currentOp()` Befehl in der Mongo-Shell verwenden. Ein 100-prozentiger Abschluss der letzten Phase zeigt, dass alle Indizes erfolgreich erstellt wurden:

```
db.currentOp({"command.createIndexes": { $exists : true } })
```

> **Note**
>
> Das Anzeigen des Fortschrittsstatus der Indizierung wird nur in Amazon DocumentDB 5.0 unterstützt.

Typen der Indexerstellung

Die vier Arten von Indexerstellungen sind:

- Vordergrund — Der Vordergrund-Index-Build blockiert alle anderen Datenbankoperationen, bis der Index erstellt ist. Der Amazon DocumentDB DocumentDB-Vordergrundaufbau besteht aus fünf Phasen.
- Vordergrund (einzigartig) — Index-Builds im Vordergrund für ein einzelnes Dokument (eindeutig) blockieren andere Datenbankoperationen wie reguläre Vordergrund-Builds. Im Gegensatz zum einfachen Vordergrund-Build verwendet der Unique-Build eine zusätzliche Stufe (Sortierung von Schlüsseln 2), um nach doppelten Schlüsseln zu suchen. Der (einzigartige) Build im Vordergrund besteht aus sechs Stufen.
- Hintergrund — Die Indexerstellung im Hintergrund ermöglicht die Ausführung anderer Datenbankoperationen im Vordergrund, während der Index erstellt wird. Der Amazon DocumentDB DocumentDB-Hintergrundaufbau besteht aus acht Phasen.
- Hintergrund (einzigartig) — Index-Builds für ein einzelnes Dokument (eindeutig) im Hintergrund ermöglichen die Ausführung anderer Datenbankoperationen im Vordergrund, während der Index erstellt wird. Im Gegensatz zum grundlegenden Hintergrundbuild verwendet der Unique-Build eine zusätzliche Phase (Sortierung von Schlüsseln 2), um nach doppelten Schlüsseln zu suchen. Der (einzigartige) Background-Build besteht aus neun Stufen.

Phasen der Indexerstellung

Stage	Vordergrund	Vordergrund (einzigartig)	Hintergrund	Hintergrund (einzigartig)
Initialisieren	1	1	1	1
Gebäudeindex: initialisieren	2	2	2	2
Gebäudeindex: Sammlung wird gescannt	3	3	3	3
Gebäudeindex: Schlüssel sortieren 1	4	4	4	4

Stage	Vordergrund	Vordergrund (einzigartig)	Hintergrund	Hintergrund (einzigartig)
Gebäudeindex: Sortieren von Schlüsseln 2		5		5
Gebäudeindex: Schlüssel einfügen	5	6	5	6
validieren: Index scannen			6	7
validieren: Tupel sortieren			7	8
validieren: Sammlung scannen			8	9

- initialisieren — CreateIndex bereitet den Index Builder vor. Diese Phase sollte sehr kurz sein.
- Index erstellen: Initialisieren — Der Index Builder bereitet die Erstellung des Indexes vor. Diese Phase sollte sehr kurz sein.
- Index erstellen: Sammlung scannen — Der Index Builder führt einen Sammlungsscan durch, um Indexschlüssel zu sammeln. Die Maßeinheit ist „Blöcke“.

> **Note**
>
> Wenn mehr als ein Worker für den Indexaufbau konfiguriert ist, wird dieser in dieser Phase angezeigt. Die Phase „Erfassung des Scannens“ ist die einzige Phase, in der während der Indexerstellung mehrere Worker verwendet werden. In allen anderen Phasen wird ein einziger Worker angezeigt.

- Index erstellen: Schlüssel sortieren 1 — Der Indexgenerator sortiert die gesammelten Indexschlüssel. Die Maßeinheit ist „Schlüssel“.

- Index erstellen: Schlüssel sortieren 2 — Der Index Builder sortiert die gesammelten Indexschlüssel, die toten Tupeln entsprechen. Diese Phase ist nur für die Erstellung eines eindeutigen Indexes vorgesehen. Die Maßeinheit ist „Schlüssel“.
- Gebäudeindex: Schlüssel einfügen — Der Index Builder fügt Indexschlüssel in den neuen Index ein. Die Maßeinheit ist „Schlüssel“.
- validieren: Index scannen — CreateIndex durchsucht den Index nach Schlüsseln, die validiert werden müssen. Die Maßeinheit ist „Blöcke“.
- validieren: Tupel sortieren — CreateIndex sortiert die Ausgabe der Indexscanphase.
- validieren: Sammlung scannen — CreateIndex scannt die Sammlung, um die Indexschlüssel zu validieren, die in den beiden vorherigen Phasen gefunden wurden. Die Maßeinheit ist „Blöcke“.

Beispiel für die Ausgabe einer Indexerstellung

Im folgenden Ausgabebeispiel (Indexerstellung im Vordergrund) wird der Status der Indexerstellung angezeigt. Das Feld „msg“ fasst den Baufortschritt zusammen, indem es die Phase und den Prozentsatz der Fertigstellung des Builds angibt. Das Feld „Arbeiter“ gibt die Anzahl der Arbeiter an, die in dieser Phase der Indexerstellung eingesetzt wurden. Das Feld „Fortschritt“ zeigt die tatsächlichen Zahlen, die zur Berechnung des Prozentsatzes der Fertigstellung verwendet wurden.

> **Note**
>
> Die Felder „currentIndexBuildName“, „msg“ und „progress“ werden in Amazon DocumentDB Version 4.0 nicht unterstützt.

```
{
    "inprog" : [{
    …
        "command": {
            "createIndexes": "test",
            "indexes": [{
                "v": 2,
                "key": {
                    "user_name": 1
                },
                "name": "user_name_1"
            }],
            "lsid": {
```

```
                "id": UUID("094d0fba-8f41-4373-82c3-7c4c7b5ff13b")
            },
            "$db": "test"
        },
        "currentIndexBuildName": user_name_1,
        "msg": "Index Build: building index number_1, stage 6/6 building index:
 656860/1003520 (keys) 65%",
        "workers": 1,
        "progress": {
            "done": 656861,
            "total": 1003520
        },
    …
    ],

    "ok" : 1
}
```

Pflege Amazon DocumentDB DocumentDB-Indizes

Themen

- Indexblähung
- Indexverwaltung mit ReIndex

Indexblähung

Amazon DocumentDB verwendet Multi-Version Concurrency Control (MVCC) zur Verwaltung gleichzeitiger Transaktionen. Wenn Dokumente gelöscht oder aktualisiert werden, verbleiben ihre vorherigen Versionen als „tote“ Versionen in Sammlungen und Indizes. Durch den Garbage-Collection-Prozess wird automatisch Speicherplatz aus diesen toten Versionen für future Operationen zurückgewonnen.

Ein aufgeblähter Index tritt auf, wenn die Indizes einer Sammlung aufgrund der Anhäufung toter oder veralteter Indexeinträge oder der Fragmentierung innerhalb der Seiten größer werden. Der angegebene Prozentsatz entspricht der Menge an Indexspeicher, die von future Indexeinträgen verwendet werden kann. Diese Aufblähung beansprucht Speicherplatz sowohl im Puffer-Cache als auch im Speicher. Wenn Sie den Bloat entfernen möchten, müssen Sie die Indizes neu erstellen.

Example Beispiel

Führen Sie den folgenden Befehl aus, um den ungenutzten Speicherplatz für Ihren Index zu ermitteln:

```
db.coll.aggregate({$indexStats:{}});
```

Das Ergebnis sieht in etwa so aus:

```
{
    "name" : "_id_",
    "key" : {
        "_id" : 1
    },
    "host" : "devbox-test.localhost.a2z.com:27317",
    "size" : NumberLong(827392),
    "accesses" : {
        "ops" : NumberLong(40000),
        "docsRead" : NumberLong(46049),
        "since" : ISODate("2025-04-03T21:44:51.251Z")
    },
    "cacheStats" : {
        "blksRead" : NumberLong(264),
        "blksHit" : NumberLong(140190),
        "hitRatio" : 99.8121
    },
    "unusedStorageSize" : {
        "unusedSizeBytes" : 409600,
        "unusedSizePercent" : 49.51
    }
}
```

Mit dem `reIndex` Befehl können Sie Indizes ohne Ausfallzeiten neu erstellen. Dazu ist ein Scan der gesamten Sammlung erforderlich. Siehe Indexverwaltung mit `ReIndex`.

Indexverwaltung mit **`ReIndex`**

`reIndex`ist ein Befehl, der verwendet wird, um einen Index neu aufzubauen. Er wird normalerweise verwendet, wenn ein Index beschädigt oder ineffizient geworden ist. Im Laufe der Zeit können Indizes aufgrund vieler Aktualisierungen, Einfügungen oder Löschungen ungenutzten Speicherplatz ansammeln, was zu Leistungseinbußen führt. Eine Neuindizierung hilft dabei, diesen ungenutzten Speicherplatz zu entfernen und die Effizienz des Index wiederherzustellen.

Richtlinien für den reIndex

- `reIndex`wird nur auf Amazon DocumentDB 5.0 unterstützt.
- Amazon DocumentDB unterstützt `reindex` einen einzelnen Index im Hintergrund, sodass mehrere Worker verwendet werden können. Der alte Index kann für Abfragen verwendet werden, wenn der `reIndex` Prozess läuft.
- Amazon DocumentDB unterstützt die Indexierung von Fortschrittsberichten bis. `currentOp` Sie können die Phasen der Indexerstellung sehen, die denen bei der Phasen der Indexerstellung Indexerstellung ähneln. Der einzige Unterschied besteht darin, dass es `reIndex` immer acht Stufen gibt, unabhängig davon, ob es sich um eine eindeutige Phase handelt oder nicht. Es gibt keine Phase „Index erstellen: Schlüssel sortieren 2“.
- `reIndex`kann gleichzeitig mit jedem Befehl ausgeführt werden, mit Ausnahme von indexbezogenen Befehlen in derselben Sammlung:`createIndexes`,`dropIndexes`, `collMod` und. `renameCollection`
- `reIndex`wird derzeit nicht für Text-, Geodaten-, Vektor- und Teilindizes unterstützt.

Build reIndex indizieren

Verwenden Sie den folgenden Befehl, um Ihren Index neu zu erstellen:

```
db.runCommand({ reIndex: "collection-name", index: "index-name"})
```

Optional können Sie auch die Anzahl der Mitarbeiter steuern, die dem Neuaufbauprozess zugewiesen sind:

```
db.runCommand({ reIndex: "collection-name", index: "index-name", workers: number })
```

Verwaltung der Dokumentenkomprimierung auf Sammlungsebene

Mit der Dokumentenkomprimierung auf Sammlungsebene von Amazon DocumentDB 5.0 können Sie die Speicher- und I/O-Kosten senken, indem Sie die Dokumente in Ihren Sammlungen komprimieren. Sie können die Dokumentenkomprimierung auf Sammlungsebene aktivieren und bei Bedarf Komprimierungsmetriken anzeigen, indem Sie den Speicherzuwachs anhand von Komprimierungsmetriken wie der Speichergröße komprimierter Dokumente und dem Komprimierungsstatus messen. Amazon DocumentDB 5.0 verwendet den LZ4-Komprimierungsalgorithmus, um Dokumente zu komprimieren.

Amazon DocumentDB unterstützt die Dokumentenkomprimierung ab Version 5.0. Im Folgenden finden Sie Funktionen zur Komprimierung von Dokumenten auf Sammlungsebene:

- Standardverhalten — Die Standardkomprimierungseinstellung für neue Sammlungen auf einem 5.0-Cluster wird durch den Cluster-Parameter bestimmt. `default_collection_compression` Dieser Parameter ist standardmäßig auf „deaktiviert“ gesetzt.
- Komprimieren vorhandener Sammlungen — Die Komprimierungseinstellungen für bestehende Sammlungen können mit dem `collMod` Befehl geändert werden.
- Ändern des Komprimierungsschwellenwerts — Der Standardschwellenwert für die Komprimierung beträgt 2 KB. Dieser Wert kann für neue Sammlungen mit dem `createCollection` Befehl angegeben und für bestehende Sammlungen mit dem `collMod` Befehl geändert werden.

> **Note**
>
> Die Amazon DocumentDB DocumentDB-Dokumentenkomprimierung wird in den Amazon DocumentDB DocumentDB-Versionen 3.6 und 4.0 nicht unterstützt.

Themen

- Verwaltung der Dokumentenkomprimierung
- Überwachung der Dokumentenkomprimierung

Verwaltung der Dokumentenkomprimierung

Aktivieren der Dokumentenkomprimierung in einer Sammlung

Aktivieren Sie die Dokumentenkomprimierung beim Erstellen einer Sammlung in Amazon DocumentDB 5.0 mithilfe der folgenden `db.createCollection()` Methode:

```
db.createCollection( sample_collection,{
    storageEngine : {
        documentDB: {
            compression:{enable: <true | false>}
        }
    }
})
```

Aktivieren der Dokumentenkomprimierung in einem Cluster

Die Dokumentenkomprimierung kann standardmäßig für alle neuen Sammlungen auf Clusterebene aktiviert werden, indem der Cluster-Parameter `default_collection_compression` auf „enabled“ gesetzt wird. Wenn dieser Parameter auf „aktiviert“ gesetzt ist, ist für neu erstellte Sammlungen auf dem Cluster die Komprimierung standardmäßig aktiviert, wobei der Komprimierungsschwellenwert 2 KB beträgt.

Komprimieren vorhandener Sammlungen

Sie können auch die Komprimierungseinstellungen für eine vorhandene Sammlung ändern, indem Sie den `collMod` Vorgang verwenden und die folgende `storageEngine` Konfiguration angeben. Beachten Sie, dass die mit diesem Befehl vorgenommene Änderung nur für neue inserted/updated Dokumente gilt und dass sich die Komprimierung zuvor eingefügter Dokumente nicht ändert.

```
db.runCommand({
    collMod: "orders",
    storageEngine: {
        documentDB: {compression: {enable: <true | false>} }
    }
})
```

Einstellung der Schwellenwerte für die Komprimierung

Standardmäßig liegt der Komprimierungsschwellenwert für komprimierte Sammlungen bei 2032 Byte. Dieser Schwellenwert kann im `createCollection` Befehl festgelegt werden, wenn eine neue Sammlung mit aktivierter Komprimierung erstellt wird:

```
db.createCollection( sample_collection, {
    storageEngine : {
        documentDB: {
            compression: {
                enable: true,
                threshold: <128 - 8000>
            }
        }
    }
})
```

Sie können den Komprimierungsschwellenwert für eine vorhandene komprimierte Sammlung auch ändern, indem Sie den `collMod` Vorgang verwenden und die folgende `storageEngine` Konfiguration angeben:

```
db.runCommand({
    collMod: "orders",
    storageEngine: {
        documentDB: {
            compression: {
                enable: true,
                threshold: <128 - 8000>
            }
        }
    }
})
```

Beachten Sie, dass der Komprimierungsschwellenwert nur auf einen Wert zwischen 128 und 8000 Byte festgelegt werden kann. Außerdem muss die `enable` Option bei der Angabe des Komprimierungsschwellenwerts auf „true“ gesetzt werden.

Überwachung der Dokumentenkomprimierung

Sie können überprüfen, ob eine Sammlung komprimiert ist, und ihr Komprimierungsverhältnis wie folgt berechnen.

Zeigen Sie die Komprimierungsstatistiken an, indem Sie den `db.collection.stats()` Befehl `db.printCollectionStats()` oder in der Mongo-Shell ausführen. Die Ausgabe zeigt Ihnen die Originalgröße und die komprimierte Größe, die Sie vergleichen können, um die Speichergewinne durch die Dokumentenkomprimierung zu analysieren. In diesem Beispiel werden die Statistiken für eine Sammlung mit dem Namen „sample_collection“ unten angezeigt. Im Folgenden wird ein Skalierungsfaktor von 1024*1024 verwendet, um die Werte und in MB auszugeben. `size` `storageSize`

```
db.sample_collection.stats(1024*1024)
```

Das Folgende ist ein Beispiel für die Ausgabe für den obigen Befehl:

```
{
    "ns" : "test.sample_collection",
    "count" : 1000000,
```

```
    "size" : 3906.3,
    "avgObjSize" : 4096,
    "storageSize" : 1953.1,
    compression:{"enabled" : true,"threshold" : 2032},
    ...
}
```

- Größe — Die Originalgröße der Dokumentensammlung.
- avg ObjSize — Die durchschnittliche Dokumentgröße vor der Komprimierung, abgerundet auf die erste Dezimalzahl. Die Maßeinheit ist Byte.
- StorageSize — Die Speichergröße der Sammlung nach der Komprimierung. Die Maßeinheit ist Byte.
- aktiviert — Zeigt an, ob die Komprimierung aktiviert oder deaktiviert ist.

Um das tatsächliche Komprimierungsverhältnis zu berechnen, dividieren Sie die Sammlungsgröße durch die Speichergröße (size/storageSize). Für das obige Beispiel lautet die Berechnung 3906. 3/1953.1 was einem Kompressionsverhältnis von 2:1 entspricht.

Verwaltung der wörterbuchbasierten Komprimierung in Amazon DocumentDB 8.0

Amazon DocumentDB 8.0 führt einen neuen Algorithmus zur Dokumentenkomprimierung, zstd, als verbesserte Alternative zu LZ4 ein. Wenn Sie die Wörterbuchkomprimierung für eine Amazon DocumentDB 8.0-Sammlung aktivieren, indem Sie Zstd als Komprimierungsalgorithmus auswählen, werden Dokumente aus Ihrer Sammlung ausgewählt, um ein benutzerdefiniertes Komprimierungswörterbuch zu erstellen. Neue und aktualisierte Dokumente werden mit diesem Wörterbuch und dem zstd-Algorithmus komprimiert. Mit diesem Ansatz werden in der Regel höhere Komprimierungsraten erzielt als mit Standardkomprimierungsmethoden, insbesondere bei Sammlungen mit konsistenten Dokumentschemas oder wiederholten Feldnamen.

Lz4 ist ein Algorithmus, der für schnelle Komprimierung und Dekomprimierung entwickelt wurde. Es ist bekannt, dass er die CPU wenig belastet und gleichzeitig eine spürbare Komprimierung erreicht. Zstd ist ein Allzweckalgorithmus, der mit Standardeinstellungen mehr CPU verbraucht, aber bessere Komprimierungsraten als lz4 erzielt. Durch die Verwendung von Wörterbüchern wird die Komprimierung für die meisten JSON-Dokumente noch weiter verbessert. Einige Vorteile des Zstd-Algorithmus sind:

- Geringere Speicherkosten: Höhere Komprimierungsraten bedeuten weniger Speicherverbrauch und niedrigere Kosten.
- Niedriger I/O: Komprimierte Dokumente benötigen weniger I/O, was möglicherweise die Leistung verbessert.
- Optimiert für Ihre Sammlung: Das Wörterbuch wurde speziell für die Datenmuster Ihrer Sammlung trainiert.

> **Note**
>
> Dictionary-based Die Komprimierung wird in den Amazon DocumentDB DocumentDB-Versionen 3.6, 4.0 und 5.0 nicht unterstützt.

Performanceaspekte

Die Zstd-Komprimierung beinhaltet die folgenden Kompromisse:

- Speicher im Vergleich zur CPU: Die Zstd-Komprimierung erzielt bessere Komprimierungsraten, verbraucht aber möglicherweise etwas mehr CPU-Ressourcen als die LZ4-Komprimierung.
- Anfängliche Komprimierung: Neue Sammlungen erreichen möglicherweise erst dann eine optimale Komprimierung, wenn genügend Dokumente eingefügt wurden, um ein effektives Wörterbuch zu trainieren. Derzeit wird ein Wörterbuch trainiert, wenn die Sammlung mindestens 100 Dokumente enthält.
- Workload-Typ: Bei Read-intensive Workloads, bei denen die gesamten Daten in den Puffercache passen, kann es aufgrund des Dekomprimierungsaufwands zu einem Anstieg der Latenz und der CPU-Auslastung kommen.

Die Zstd-Komprimierung ist besonders effektiv für Sammlungen mit kleinen Dokumenten, Dokumentarrays und sich wiederholenden Feldnamen.

Aktivierung der wörterbuchbasierten Komprimierung

Für neue Sammlungen können Sie den folgenden Befehl verwenden, um die Zstd-Komprimierung zu aktivieren:

```
db.createCollection("myCollection",
    {
        storageEngine: {
            documentDB: {
                compression: {
                    enable: true,
                    algorithm: "zstd"
                }
            }
        }
    }
 )
```

Sie können die Komprimierung auch für eine bestehende Sammlung aktivieren oder ändern:

```
db.runCommand({
    collMod: "myCollection",
    storageEngine: {
        documentDB: {
            compression: {
                enable: true,
                algorithm: "zstd"
            }
        }
    }
 })
```

Um den Zstd-Algorithmus für alle Sammlungen auf Ihrem Cluster zu aktivieren, können Sie die Cluster-Parametergruppe so ändern, dass „zstd“ als Wert für den Parameter „default_collection_compression“ ausgewählt wird.

Erste Schritte

Bei Amazon DocumentDB 8.0 ist die Zstd-Komprimierung standardmäßig aktiviert. Sie können sie jederzeit ausschalten, indem Sie den Wert von 'default_compression' in Ihrer Cluster-Parametergruppe auf disabled setzen. Es muss beachtet werden, dass ab Amazon DocumentDB 8.0 'enabled' keine gültige Wahl mehr für default_compression ist und Sie zwischen Zstd und LZ4 wählen müssen.

Überwachen

Sie können die Komprimierungsinformationen für eine Sammlung mit einem der folgenden Befehle anzeigen:

- db.runCommand ({collStats: „MyCollection“}) ODER
- db.collection.stats ()

Diese Befehle geben wichtige Statistiken zurück, anhand derer Sie das Kompressionsverhältnis berechnen können:

- compression.algorithm: Der verwendete Algorithmus („lz4" oder „zstd“)
- StorageSize: Der tatsächliche Speicherplatz, der von der Sammlung nach der Komprimierung verwendet wird. Beachten Sie, dass diese Zahl die Fragmentierung (d. h. den ungenutzten Speicherplatz auf Datenbankseiten) beinhaltet
- avgObjSize: Die durchschnittliche logische Größe der Dokumente der Sammlung, dekomprimiert. Beachten Sie: Wenn Ihre Sammlung mehr als 20.000 Dokumente umfasst, handelt es sich bei dieser Zahl um eine ungefähre Zahl, die auf einer Stichprobe von 20.000 Dokumenten basiert.
- Größe: Die logische Größe der Sammlung ohne Komprimierung. Diese Zahl ergibt sich aus der Multiplikation ObjSize von avg mit der Gesamtzahl der Dokumente in der Sammlung. Wenn avg also eine Näherung ObjSize ist, ist diese Zahl auch eine Näherung.
- Anzahl: Anzahl der Dokumente in der Sammlung

Die folgenden CloudWatch Messwerte können bei der Bewertung der wörterbuchbasierten Komprimierung hilfreich sein:

- CPUUtilization
- FreeableMemory
- VolumeBytesUsed
- VolumeReadIOPs
- VolumeWriteIOPs

CollStats-Metriken:

- storageSize

- size

Darüber hinaus kann es nützlich sein, anwendungsspezifische Kennzahlen wie Latenz und Durchsatz pro Abfragetyp oder API im Auge zu behalten.

Amazon DocumentDB DocumentDB-Ereignisse verwalten

Amazon DocumentDB (mit MongoDB-Kompatibilität) zeichnet Ereignisse auf, die sich auf Ihre Cluster, Instances, Snapshots, Sicherheitsgruppen und Cluster-Parametergruppen beziehen. Diese Informationen beinhalten Datum und Zeit eines Ereignisses, den Quellnamen und Quelltyp des Ereignisses und eine dem Ereignis zugehörige Benachrichtigung.

> **Important**
>
> Für bestimmte Verwaltungsfunktionen verwendet Amazon DocumentDB Betriebstechnologie, die mit Amazon RDS und Amazon Neptune gemeinsam genutzt wird. Regionsgrenzen, Grenzwerte, die auf Regionsebene geregelt werden, werden von Amazon DocumentDB, Amazon RDS und Amazon Neptune gemeinsam genutzt. Weitere Informationen finden Sie unter Regionale Kontingente.

Themen

- Amazon DocumentDB DocumentDB-Ereigniskategorien anzeigen
- Amazon DocumentDB DocumentDB-Ereignisse anzeigen

Amazon DocumentDB DocumentDB-Ereigniskategorien anzeigen

Jeder Amazon DocumentDB DocumentDB-Ressourcentyp hat bestimmte Ereignistypen, die ihm zugeordnet werden können. Sie können den AWS CLI `describe-event-categories` Vorgang verwenden, um die Zuordnung zwischen Ereignistypen und Amazon DocumentDB DocumentDB-Ressourcentypen anzuzeigen.

Parameters

- **`--source-type`**— Fakultativ. Verwenden Sie den `--source-type`-Parameter, um die Ereigniskategorien für einen bestimmten Quelltyp anzuzeigen. Die folgenden Werte sind zulässig:

- `db-cluster`
- `db-instance`
- `db-parameter-group`
- `db-security-group`
- `db-cluster-snapshot`

- **`--filters`**—Fakultativ. Verwenden Sie den Filter`--filter Name=engine,Values=docdb`, um die Ereigniskategorien nur für Amazon DocumentDB anzuzeigen.

Example

Der folgende Code listet die Ereigniskategorien im Zusammenhang mit Clustern auf.

Für Linux, macOS oder Unix:

```
aws docdb describe-event-categories \
    --filter Name=engine,Values=docdb \
    --source-type db-cluster
```

Für Windows:

```
aws docdb describe-event-categories ^
    --filter Name=engine,Values=docdb ^
    --source-type db-cluster
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus (JSON-Format).

```
{
    "EventCategoriesMapList": [
        {
            "EventCategories": [
                "notification",
                "failure",
                "maintenance",
                "failover"
            ],
            "SourceType": "db-cluster"
        }
    ]
}
```

Der folgende Code listet die Ereigniskategorien auf, die jedem Amazon DocumentDB DocumentDB-Quelltyp zugeordnet sind.

```
aws docdb describe-event-categories
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus (JSON-Format).

```
{
    "EventCategoriesMapList": [
        {
            "SourceType": "db-instance",
            "EventCategories": [
                "notification",
                "failure",
                "creation",
                "maintenance",
                "deletion",
                "recovery",
                "restoration",
                "configuration change",
                "read replica",
                "backtrack",
                "low storage",
                "backup",
                "availability",
                "failover"
            ]
        },
        {
            "SourceType": "db-security-group",
            "EventCategories": [
                "configuration change",
                "failure"
            ]
        },
        {
            "SourceType": "db-parameter-group",
            "EventCategories": [
                "configuration change"
            ]
        },
        {
            "SourceType": "db-cluster",
```

```
            "EventCategories": [
                "notification",
                "failure",
                "maintenance",
                "failover"
            ]
        },
        {
            "SourceType": "db-cluster-snapshot",
            "EventCategories": [
                "backup"
            ]
        }
    ]
}
```

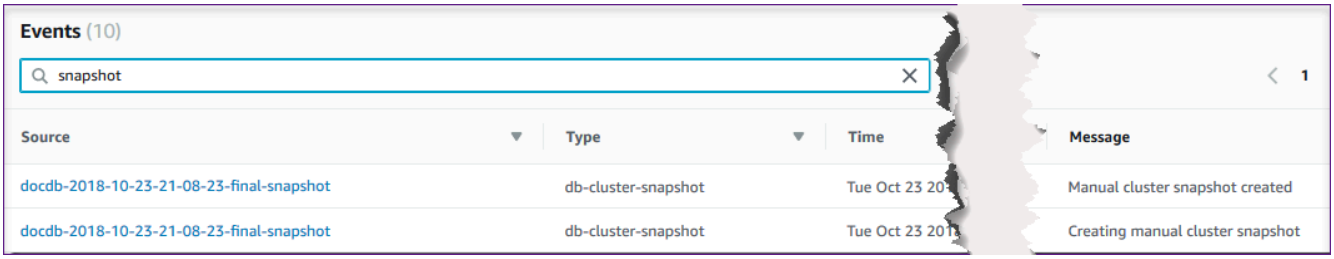
Amazon DocumentDB DocumentDB-Ereignisse anzeigen

Sie können Ereignisse für Ihre Amazon DocumentDB DocumentDB-Ressourcen über die Amazon DocumentDB DocumentDB-Konsole abrufen, in der Ereignisse der letzten 24 Stunden angezeigt werden. Sie können auch Ereignisse für Ihre Amazon DocumentDB DocumentDB-Ressourcen abrufen, indem Sie den AWS CLI Befehl describe-events oder den DescribeEventsAmazon DocumentDB DocumentDB-API-Vorgang verwenden. Wenn Sie die AWS CLI oder die Amazon DocumentDB DocumentDB-API verwenden, um Ereignisse anzuzeigen, können Sie Ereignisse der letzten 14 Tage abrufen.

Using the AWS-Managementkonsole

Um alle Amazon DocumentDB DocumentDB-Instance-Ereignisse der letzten 24 Stunden anzuzeigen

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Wählen Sie im Navigationsbereich die Option Events. Die verfügbaren Ereignisse erscheinen in einer Liste.
3. Verwenden Sie die Liste Filter, um die Ereignisse nach Typ zu filtern. Geben Sie einen Begriff in das Textfeld ein, um Ihre Ergebnisse weiter zu filtern. Der folgende Screenshot zeigt beispielsweise, wie alle Amazon DocumentDB DocumentDB-Ereignisse nach Snapshot-Ereignissen gefiltert werden.



Using the AWS CLI

Um alle Amazon DocumentDB DocumentDB-Instance-Ereignisse der letzten 7 Tage anzuzeigen

Sie können alle Amazon DocumentDB DocumentDB-Instance-Ereignisse der letzten 7 Tage anzeigen, indem Sie den AWS CLI Vorgang describe-events ausführen, wobei der `--duration` Parameter auf `10080` (10.080 Minuten) gesetzt ist.

```
aws docdb describe-events --duration 10080
```

Filtern nach Amazon DocumentDB DocumentDB-Ereignissen

Um bestimmte Amazon DocumentDB DocumentDB-Ereignisse zu sehen, verwenden Sie den `describe-events` Vorgang mit den folgenden Parametern.

Parameters

- **`--filter`**— Erforderlich, um zurückgegebene Werte auf Amazon DocumentDB DocumentDB-Ereignisse zu beschränken. Wird verwendet**`Name=engine,Values=docdb`**, um alle Ereignisse nur für Amazon DocumentDB zu filtern.
- **`--source-identifier`**— Fakultativ. ID der Ereignisquelle, für die Ereignisse zurückgegeben werden. Wenn diese Option weggelassen wird, werden Ereignisse aus allen Quellen in die Ergebnisse einbezogen.
- **`--source-type`**— Optional, sofern nicht `--source-identifier` angegeben, dann erforderlich. Wenn `--source-identifier` angegeben wird, muss `--source-type` mit dem Typ der `--source-identifier` übereinstimmen. Die folgenden Werte sind zulässig:
  - `db-cluster`
  - `db-instance`
  - `db-parameter-group`
  - `db-security-group`

- db-cluster-snapshot

Das folgende Beispiel listet alle Ihre Amazon DocumentDB DocumentDB-Ereignisse auf.

```
aws docdb describe-events --filters Name=engine,Values=docdb
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus (JSON-Format).

```
{
    "Events": [
        {
            "SourceArn": "arn:aws:rds:us-east-1:123SAMPLE012:db:sample-cluster-
instance3",
            "Message": "instance created",
            "SourceType": "db-instance",
            "Date": "2018-12-11T21:17:40.023Z",
            "SourceIdentifier": "sample-cluster-instance3",
            "EventCategories": [
                "creation"
            ]
        },
        {
            "SourceArn": "arn:aws:rds:us-
east-1:123SAMPLE012:db:docdb-2018-12-11-21-08-23",
            "Message": "instance shutdown",
            "SourceType": "db-instance",
            "Date": "2018-12-11T21:25:01.245Z",
            "SourceIdentifier": "docdb-2018-12-11-21-08-23",
            "EventCategories": [
                "availability"
            ]
        },
        {
            "SourceArn": "arn:aws:rds:us-
east-1:123SAMPLE012:db:docdb-2018-12-11-21-08-23",
            "Message": "instance restarted",
            "SourceType": "db-instance",
            "Date": "2018-12-11T21:25:11.441Z",
            "SourceIdentifier": "docdb-2018-12-11-21-08-23",
            "EventCategories": [
                "availability"
            ]
```

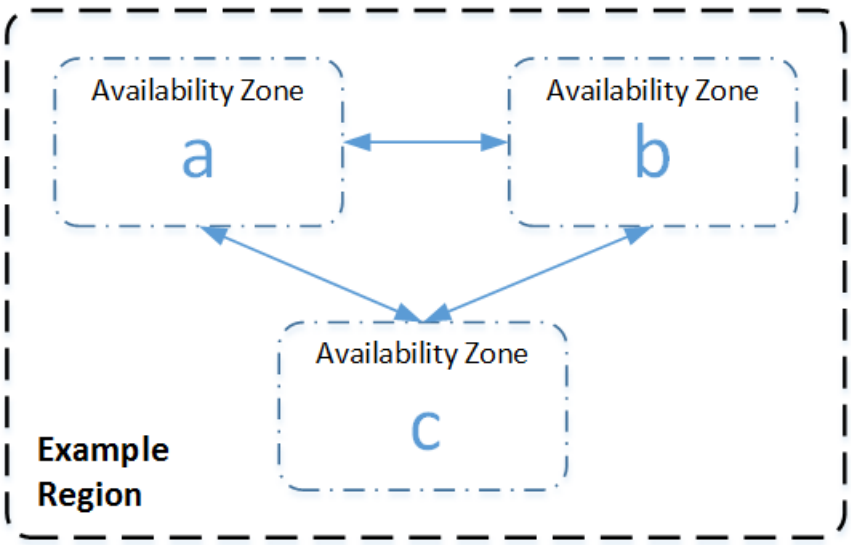
```
        }
    ]
}
```

Weitere Informationen finden Sie unter Amazon DocumentDB DocumentDB-Ereignisse prüfen.

Auswahl von Regionen und Availability Zones

Amazon Cloud Computing-Ressourcen werden an mehreren Standorten weltweit gehostet. Diese Standorte bestehen aus AWS-Regionen Availability Zones. Jeder AWS-Regionist ein separates geografisches Gebiet. Jede Region verfügt über mehrere isolierte Standorte, die als Availability Zones bezeichnet werden. Amazon DocumentDB bietet Ihnen die Möglichkeit, Ressourcen wie Instances und Daten an mehreren Standorten zu platzieren. Ressourcen werden nur repliziert, AWS-Regionen wenn Sie dies ausdrücklich tun.

Amazon betreibt hochmoderne, hoch verfügbare Rechenzentren. In seltenen Fällen kann es aber zu Ausfällen kommen, die die Verfügbarkeit von Instances desselben Standorts beeinträchtigen. Wenn Sie Ihre gesamten Instances an einem einzelnen Standort hosten, der von einem Ausfall dieser Art betroffen ist, ist keine Ihrer Instances verfügbar. Das folgende Diagramm zeigt eine AWS-Region mit drei Availability Zones.



Beachten Sie, dass alle Regionen voneinander unabhängig sind. Jede Amazon DocumentDB DocumentDB-Aktivität, die Sie initiieren (z. B. Instances erstellen oder verfügbare Instances auflisten), wird nur in Ihrer aktuellen Standardeinstellung AWS-Region ausgeführt. Sie können die Standardregion in der Konsole ändern, indem Sie die Umgebungsvariable `EC2_REGION`

festlegen. Oder Sie können sie überschreiben, indem Sie den Parameter `--region` in der AWS CLI verwenden. Weitere Informationen finden Sie unter Konfiguration der AWS Command Line Interface Abschnitte zu Umgebungsvariablen und Befehlszeilenoptionen.

Wenn Sie mit der Amazon DocumentDB-Konsole einen Cluster erstellen und sich dafür entscheiden, ein Replikat in einer anderen Availability Zone zu erstellen, erstellt Amazon DocumentDB zwei Instances. Es erstellt die primäre Instance in einer Availability Zone und die Replikat-Instance in einer anderen Availability Zone. Das Cluster-Volumen wird immer über drei Availability Zones repliziert.

Um eine Amazon DocumentDB DocumentDB-Instance in einer bestimmten Instanz zu erstellen oder mit ihr zu arbeiten AWS-Region, verwenden Sie den entsprechenden regionalen Service-Endpunkt.

Verfügbarkeit in Regionen

Amazon DocumentDB ist in den folgenden AWS Regionen verfügbar.

Von Amazon DocumentDB unterstützte Regionen

Name der Region	Region	Verfügbarkeitszonen (Datenverarbeitung)
USA Ost (Ohio)	`us-east-2`	3
USA Ost (Nord-Virginia)	`us-east-1`	6
USA West (Oregon)	`us-west-2`	4
Afrika (Kapstadt)	`af-south-1`	3
Südamerika (São Paulo)	`sa-east-1`	3
Asien-Pazifik (Hongkong)	`ap-east-1`	3
Asien-Pazifik (Hyderabad)	`ap-south-2`	3
Asien-Pazifik (Malaysia)	`ap-southeast-5`	3

Name der Region	Region	Verfügbarkeitszonen (Datenverarbeitung)
Asien-Pazifik (Mumbai)	ap-south-1	3
Asien-Pazifik (Osaka)	ap-northeast-3	3
Asien-Pazifik (Seoul)	ap-northeast-2	4
Asien-Pazifik (Singapur)	ap-southeast-1	3
Asien-Pazifik (Sydney)	ap-southeast-2	3
Asien-Pazifik (Jakarta)	ap-southeast-3	3
Asien-Pazifik (Melbourne)	ap-southeast-4	3
Asien-Pazifik (Thailand)	ap-southeast-7	3
Asien-Pazifik (Tokio)	ap-northeast-1	3
Kanada (Zentral)	ca-central-1	3
Kanada West (Calgary)	ca-west-1	3
Region China (Peking)	cn-north-1	3
China (Ningxia)	cn-northwest-1	3
Europa (Frankfurt)	eu-central-1	3
Europa (Zürich)	eu-central-2	3
Europa (Irland)	eu-west-1	3

Name der Region	Region	Verfügbarkeitszonen (Datenverarbeitung)
Europa (London)	`eu-west-2`	3
Europa (Milan)	`eu-south-1`	3
Europa (Paris)	`eu-west-3`	3
Europa (Spain)	`eu-south-2`	3
Europa (Stockholm)	`eu-north-1`	3
Mexiko (Zentral)	`mx-central-1`	3
Naher Osten (VAE)	`me-central-1`	3
Israel (Tel Aviv)	`il-central-1`	3
AWS GovCloud (US-West)	`us-gov-west-1`	3
AWS GovCloud (US-East)	`us-gov-east-1`	3

Standardmäßig ist die Zeitzone für einen Amazon DocumentDB-Cluster Universal Time Coordinated (UTC).

Informationen zum Suchen der Verbindungsendpunkte für Cluster und Instances in einer bestimmten Region finden Sie unter Grundlegendes zu Amazon DocumentDB DocumentDB-Endpunkten.

Verwaltung von Amazon DocumentDB-Cluster-Parametergruppen

Sie können die Amazon DocumentDB DocumentDB-Engine-Konfiguration verwalten, indem Sie Parameter in einer Cluster-Parametergruppe verwenden. Eine Cluster-Parametergruppe ist eine Sammlung von Amazon DocumentDB-Konfigurationswerten, die die Verwaltung der Parameter Ihrer Amazon DocumentDB-Cluster erleichtern. Cluster-Parametergruppen dienen als Container für Engine-Konfigurationswerte, die auf jede alle Instances im Cluster angewendet werden.

In diesem Abschnitt wird beschrieben, wie Cluster-Parametergruppen erstellt, angezeigt und geändert werden. Es wird auch gezeigt, wie Sie ermitteln können, welche Cluster-Parametergruppe einem bestimmten Cluster zugeordnet ist.

Themen

- Beschreibung von Amazon DocumentDB-Cluster-Parametergruppen
- Amazon DocumentDB-Cluster-Parametergruppen erstellen
- Amazon DocumentDB-Cluster-Parametergruppen ändern
- Ändern von Amazon DocumentDB-Clustern zur Verwendung benutzerdefinierter Cluster-Parametergruppen
- Amazon DocumentDB-Cluster-Parametergruppen kopieren
- Amazon DocumentDB-Cluster-Parametergruppen zurücksetzen
- Löschen von Amazon DocumentDB-Cluster-Parametergruppen
- Referenz zu den Amazon DocumentDB-Clusterparametern

Beschreibung von Amazon DocumentDB-Cluster-Parametergruppen

Eine `default` Cluster-Parametergruppe wird automatisch erstellt, wenn Sie den ersten Amazon DocumentDB-Cluster in einer neuen Engine erstellen AWS-Region oder eine neue Engine verwenden. Nachfolgende Cluster, die in derselben Region erstellt werden und dieselbe Engine-Version haben, werden mit der `default` Cluster-Parametergruppe erstellt.

Themen

- Beschreibung der Details einer Amazon DocumentDB-Cluster-Parametergruppe
- Ermitteln der Parametergruppe eines Amazon DocumentDB-Clusters
- Ermitteln von Clustern und Instances, die einer Amazon DocumentDB-Cluster-Parametergruppe zugeordnet sind

Beschreibung der Details einer Amazon DocumentDB-Cluster-Parametergruppe

Um die Details einer bestimmten Cluster-Parametergruppe zu beschreiben, führen Sie die folgenden Schritte mit dem AWS-Managementkonsole oder dem AWS Command Line Interface (AWS CLI) aus.

Using the AWS-Managementkonsole

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Wählen Sie im Navigationsbereich Parameter groups (Parametergruppen) aus.

   > **Tip**
   >
   > Wenn der Navigationsbereich auf der linken Seite des Bildschirms nicht angezeigt wird, wählen Sie links oben auf der Seite das Menüsymbol (≡) aus.

3. Wählen Sie im Bereich Cluster parameter groups (Cluster-Parametergruppen) den Namen der Parametergruppe aus, deren Details Sie anzeigen möchten.
4. Auf der anschließend angezeigten Seite werden die Parameter der Parametergruppe, die letzte Aktivität und Tags angezeigt.

   - In Cluster parameters (Cluster-Parameter) werden Ihnen der Name, der aktuelle Wert, die zulässigen Werte, der Anwendungstyp, der Datentyp und die Beschreibung des Parameters angezeigt. Sie können auch erkennen, ob der Parameter geändert werden kann. Sie können einzelne Parameter ändern, indem Sie den Parameter auswählen und dann im Abschnitt Cluster-Parameter auf Bearbeiten klicken. Weitere Informationen finden Sie unter Amazon DocumentDB-Cluster-Parameter ändern.
   - In Recent events (Aktuelle Ereignisse) werden Ihnen die jeweils aktuellen Ereignisse für diese Parametergruppe angezeigt. Sie können diese Ereignisse über die Suchleiste in diesem Abschnitt filtern. Weitere Informationen finden Sie unter Amazon DocumentDB DocumentDB-Ereignisse verwalten.
   - Unter Tags werden die Tags angezeigt, die sich in dieser Cluster-Parametergruppe befinden. Sie können Tags hinzufügen oder entfernen, indem Sie im Abschnitt „Tags“ die Option „Bearbeiten“ wählen. Weitere Informationen finden Sie unter Taggen von Amazon DocumentDB DocumentDB-Ressourcen.

Using the AWS CLI

Sie können den `describe-db-cluster-parameter-groups` AWS CLI Befehl verwenden, um den Amazon-Ressourcennamen (ARN), die Familie, die Beschreibung und den Namen einer

einzelnen Cluster-Parametergruppe oder aller Cluster-Parametergruppen, die Sie für Amazon DocumentDB haben, anzuzeigen. Sie können den `describe-db-cluster-parameters` AWS CLI Befehl auch verwenden, um die Parameter und ihre Details innerhalb einer einzelnen Cluster-Parametergruppe anzuzeigen.

- **`--describe-db-cluster-parameter-groups`**— Um eine Liste all Ihrer Cluster-Parametergruppen und ihrer Details zu sehen.
  - **`--db-cluster-parameter-group-name`**— Fakultativ. Der Name der Cluster-Parametergruppe, die beschrieben werden soll. Wenn dieser Parameter weggelassen wird, werden alle Cluster-Parametergruppen beschrieben.
- **`--describe-db-cluster-parameters`**— Um alle Parameter innerhalb einer Parametergruppe und ihre Werte aufzulisten.
  - **`--db-cluster-parameter-group name`** – Erforderlich. Der Name der Cluster-Parametergruppe, die beschrieben werden soll.

Example

Der folgende Code listet bis zu 100 Cluster-Parametergruppen zusammen mit ARN, Familie, Beschreibung und Name auf.

```
aws docdb describe-db-cluster-parameter-groups
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus (JSON-Format).

```
{
          "DBClusterParameterGroups": [
              {
                  "DBClusterParameterGroupArn": "arn:aws:rds:us-
east-1:012345678912:cluster-pg:default.docdb4.0",
                  "DBParameterGroupFamily": "docdb4.0",
                  "Description": "Default cluster parameter group for docdb4.0",
                  "DBClusterParameterGroupName": "default.docdb4.0"
              },
              {
                  "DBClusterParameterGroupArn": "arn:aws:rds:us-
east-1:012345678912:cluster-pg:sample-parameter-group",
                  "DBParameterGroupFamily": "docdb4.0",
                  "Description": "Custom docdb4.0 parameter group",
                  "DBClusterParameterGroupName": "sample-parameter-group"
```

```
            }
        ]
}
```

Example

Der folgende Code listet den ARN, die Familie, die Beschreibung und den Namen für `sample-parameter-group` auf.

Für Linux, macOS oder Unix:

```
aws docdb describe-db-cluster-parameter-groups \
        --db-cluster-parameter-group-name sample-parameter-group
```

Für Windows:

```
aws docdb describe-db-cluster-parameter-groups ^
        --db-cluster-parameter-group-name sample-parameter-group
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus (JSON-Format).

```
{
        "DBClusterParameterGroups": [
            {
                "DBClusterParameterGroupArn": "arn:aws:rds:us-
east-1:123456789012:cluster-pg:sample-parameter-group",
                "Description": "Custom docdb4.0 parameter group",
                "DBParameterGroupFamily": "docdb4.0",
                "DBClusterParameterGroupName": "sample-parameter-group"
            }
        ]
}
```

Example

Der folgende Code listet die Werte der Parameter in `sample-parameter-group` auf.

Für Linux, macOS oder Unix:

```
aws docdb describe-db-cluster-parameters \
    --db-cluster-parameter-group-name sample-parameter-group
```

Für Windows:

```
aws docdb describe-db-cluster-parameters ^
    --db-cluster-parameter-group-name sample-parameter-group
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus (JSON-Format).

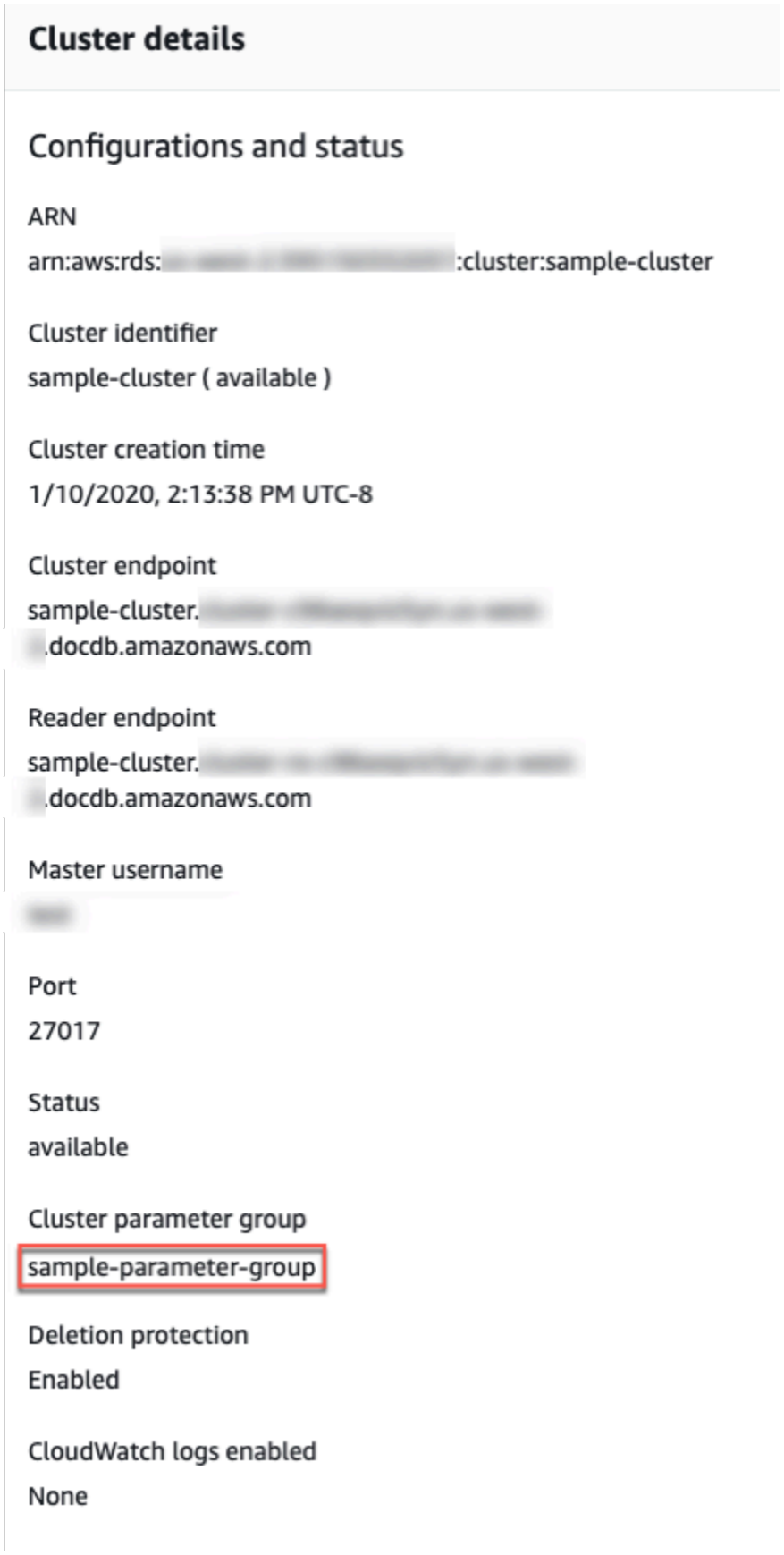
```
{
   "Parameters": [
         {
            "ParameterName": "audit_logs",
            "ParameterValue": "disabled",
            "Description": "Enables auditing on cluster.",
            "Source": "system",
            "ApplyType": "dynamic",
            "DataType": "string",
            "AllowedValues": "enabled,disabled",
            "IsModifiable": true,
            "ApplyMethod": "pending-reboot"
         },
         {
            "ParameterName": "change_stream_log_retention_duration",
            "ParameterValue": "17777",
            "Description": "Duration of time in seconds that the change stream log
 is retained and can be consumed.",
            "Source": "user",
            "ApplyType": "dynamic",
            "DataType": "integer",
            "AllowedValues": "3600-86400",
            "IsModifiable": true,
            "ApplyMethod": "pending-reboot"
         }
   ]
}
```

Ermitteln der Parametergruppe eines Amazon DocumentDB-Clusters

Um zu ermitteln, welche Parametergruppe einem bestimmten Cluster zugeordnet ist, führen Sie die folgenden Schritte mit dem AWS-Managementkonsole oder dem aus AWS CLI.

Using the AWS-Managementkonsole

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Wählen Sie im linken Navigationsbereich Cluster aus.
3. Wählen Sie aus der Liste der Cluster den Namen des Clusters aus, an dem Sie interessiert sind.
4. Auf der anschließend angezeigten Seite werden die Details des von Ihnen ausgewählten Clusters angezeigt. Scrollen Sie nach unten zu Cluster details (Clusterdetails). Sie finden den Namen der Parametergruppe unten in diesem Abschnitt unterhalb von Cluster parameter group (Cluster-Parametergruppe).


Cluster details
Configurations and status
ARN
arn:aws:rds:
:cluster:sample-cluster
Cluster identifier
sample-cluster (available)
Cluster creation time
1/10/2020, 2:13:38 PM UTC-8
Cluster endpoint
sample-cluster.
.docdb.amazonaws.com
Reader endpoint
sample-cluster.
.docdb.amazonaws.com
Master username
Port
27017
Status
available
Cluster parameter group
sample-parameter-group
Deletion protection
Enabled
CloudWatch logs enabled
None

Using the AWS CLI

Der folgende AWS CLI Code bestimmt, welche Parametergruppe den Cluster `sample-cluster` steuert.

```
aws docdb describe-db-clusters \
      --db-cluster-identifier sample-cluster \
      --query 'DBClusters[*].[DBClusterIdentifier,DBClusterParameterGroup]'
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus (JSON-Format).

```
[
       [
           "sample-cluster",
           "sample-parameter-group"
       ]
]
```

Ermitteln von Clustern und Instances, die einer Amazon DocumentDB-Cluster-Parametergruppe zugeordnet sind

Um zu ermitteln, wie viele Cluster und Instances jeder Parametergruppe zugeordnet sind, führen Sie die folgenden Schritte mit dem aus AWS CLI.

Using the AWS CLI

Der folgende AWS CLI Code bestimmt, mit wie vielen Clustern und Instances verknüpft ist`sample-parameter-group`.

Für Linux, macOS oder Unix:

```
aws docdb describe-db-clusters \
      --query 'DBClusters[*].
[DBClusterParameterGroup,DBClusterIdentifier,DBClusterMembers[*].DBInstanceIdentifier]'
 \
      --output json | \
      jq -r 'group_by(.[0]) | map({
         parameter_group_name: .[0][0],
         total_clusters: length,
         total_instances: map(.[2] | length) | add // 0
```

```
      }) | .[]'
```

Für Windows:

```
aws docdb describe-db-clusters ^
      --query 'DBClusters[*].
[DBClusterParameterGroup,DBClusterIdentifier,DBClusterMembers[*].DBInstanceIdentifier]'
 ^
      --output json | ^
      jq -r 'group_by(.[0]) | map({
         parameter_group_name: .[0][0],
         total_clusters: length,
         total_instances: map(.[2] | length) | add // 0
      }) | .[]'
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus (JSON-Format).

```
{
   "parameter_group_name": "sample-parameter-group",
   "total_clusters": 50,
   "total_instances": 150
}
```

Amazon DocumentDB-Cluster-Parametergruppen erstellen

Standard-Cluster-Parametergruppen wie`default.docdb5.0`, oder`default.docdb4.0`, werden erstellt`default.docdb3.6`, wenn Sie einen Cluster mit einer neuen Engine-Version und in einer neuen erstellen. AWS-Region Nachfolgende Cluster, die in derselben Region und mit derselben Engine-Version erstellt wurden, erben die `default` Cluster-Parametergruppe. Nach der Erstellung können die `default` Parametergruppen nicht gelöscht oder umbenannt werden. Sie können das Engine-Verhalten von Cluster-Instances ändern, indem Sie eine benutzerdefinierte Parametergruppe mit bevorzugten Parameterwerten erstellen und sie an Ihren Amazon DocumentDB-Cluster anhängen.

Das folgende Verfahren führt Sie durch die Erstellung einer benutzerdefinierten Cluster-Parametergruppe. Anschließend können Sie die Parameter innerhalb dieser Parametergruppe ändern.

> **Note**
>
> Sie sollten nach der Erstellung einer Cluster-Parametergruppe mindestens 5 Minuten warten, bevor Sie diese Cluster-Parametergruppe verwenden. Dadurch kann Amazon DocumentDB die `create` Aktion vollständig abschließen, bevor die Cluster-Parametergruppe für einen neuen Cluster verwendet wird. Sie können die Operation AWS-Managementkonsole oder die `describe-db-cluster-parameter-groups` AWS CLI Operation verwenden, um zu überprüfen, ob Ihre Cluster-Parametergruppe erstellt wurde. Weitere Informationen finden Sie unter Beschreibung von Amazon DocumentDB-Cluster-Parametergruppen.

Using the AWS-Managementkonsole

So erstellen Sie eine Cluster-Parametergruppe

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Wählen Sie im Navigationsbereich Parameter groups (Parametergruppen) aus.

   > **Tip**
   >
   > Wenn der Navigationsbereich auf der linken Seite des Bildschirms nicht angezeigt wird, wählen Sie links oben auf der Seite das Menüsymbol (≡) aus.

3. Wählen Sie im Bereich Cluster parameter groups (Cluster-Parametergruppen) die Option Create (Erstellen) aus.
4. Geben Sie im Bereich Create cluster parameter group (Cluster-Parametergruppe erstellen) Folgendes ein:

   a. Neuer Name der Cluster-Parametergruppe — Geben Sie einen Namen für die Cluster-Parametergruppe ein. Beispiel, `sample-parameter-group`. Für Cluster-Parametergruppen gelten die folgenden Benennungseinschränkungen:

      - Die Länge muss [1 bis 255] alphanumerische Zeichen betragen.
      - Muss mit einem Buchstaben beginnen.
      - Darf nicht mit einem Bindestrich enden oder zwei aufeinanderfolgende Bindestriche enthalten.

b. Family — Wählen Sie eine DocumentDB-Version, die Sie für Ihren Cluster verwenden möchten.

c. Beschreibung — Geben Sie eine Beschreibung für diese Cluster-Parametergruppe ein.

5. Um die Cluster-Parametergruppe zu erstellen, wählen Sie Erstellen aus. Um die Operation abzubrechen, wählen Sie Abbrechen aus.

6. Nach der Auswahl von Create (Erstellen) wird oben auf der Seite der folgende Text angezeigt, um zu bestätigen, dass die Cluster-Parametergruppe erfolgreich erstellt wurde:

```
Successfully created cluster parameter group 'sample-parameter-group'.
```

Using the AWS CLI

Um eine neue Cluster-Parametergruppe für Amazon DocumentDB 4.0-Cluster zu erstellen, verwenden Sie den AWS CLI `create-db-cluster-parameter-group` Vorgang mit den folgenden Parametern:

- **`--db-cluster-parameter-group-name`**— Der Name der benutzerdefinierten Cluster-Parametergruppe. Beispiel, `sample-parameter-group`.
- **`--db-cluster-parameter-group-family`**— Die Cluster-Parametergruppen-Familie, die als Vorlage für die benutzerdefinierte Cluster-Parametergruppe verwendet wird.
- **`--description`**— Die vom Benutzer bereitgestellte Beschreibung für diese Cluster-Parametergruppe. Das folgende Beispiel verwendet "`Custom docdb4.0 parameter group`“.

Für Linux, macOS oder Unix:

Example

```
aws docdb create-db-cluster-parameter-group \
 --db-cluster-parameter-group-name sample-parameter-group \
 --db-parameter-group-family docdb5.0 \
 --description "Custom docdb5.0 parameter group"
```

Für Windows:

```
aws docdb create-db-cluster-parameter-group ^
 --db-cluster-parameter-group-name sample-parameter-group ^
```

```
  --db-parameter-group-family docdb5.0 ^
  --description "Custom docdb5.0 parameter group"
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus (JSON-Format).

```
{
    "DBClusterParameterGroup": {
        "DBClusterParameterGroupName": "sample-parameter-group",
        "DBParameterGroupFamily": "docdb5.0",
        "Description": "Custom docdb4.0 parameter group",
        "DBClusterParameterGroupArn": "sample-parameter-group-arn"
    }
}
```

Amazon DocumentDB-Cluster-Parametergruppen ändern

In diesem Abschnitt wird erklärt, wie Sie eine benutzerdefinierte Amazon DocumentDB DocumentDB-Parametergruppe ändern. In Amazon DocumentDB können Sie eine `default` Cluster-Parametergruppe nicht ändern, die erstellt wird, wenn Sie zum ersten Mal einen Cluster mit einer neuen Engine-Version in einer neuen Region erstellen. Wenn Ihr Amazon DocumentDB-Cluster die Standard-Cluster-Parametergruppe verwendet und Sie einen Wert darin ändern möchten, müssen Sie zuerst eine neue Parametergruppe erstellen oder eine bestehende Parametergruppe kopieren, sie ändern und dann die geänderte Parametergruppe auf Ihren Cluster anwenden.

Gehen Sie wie folgt vor, um eine benutzerdefinierte Cluster-Parametergruppe zu ändern. Die Übertragung von Änderungsaktionen kann eine Weile dauern. Warten Sie, bis die geänderte Cluster-Parametergruppe verfügbar ist, bevor Sie sie Ihrem Cluster hinzufügen. Sie können den AWS CLI `describe-db-cluster-parameters` Vorgang AWS-Managementkonsole oder verwenden, um zu überprüfen, ob Ihre Cluster-Parametergruppe geändert wurde. Weitere Informationen finden Sie unter Beschreibung von Cluster-Parametergruppen.

Using the AWS-Managementkonsole

Gehen Sie wie folgt vor, um eine benutzerdefinierte Amazon DocumentDB DocumentDB-Parametergruppe zu ändern. Sie können eine `default`-Parametergruppe nicht ändern. Wenn Sie einen Wert in der `default`-Parametergruppe ändern möchten, können Sie die standardmäßige Cluster-Parametergruppe kopieren, sie ändern und die geänderte Parametergruppe anschließend auf Ihren Cluster anwenden. Weitere Hinweise zum Anwenden von Parametergruppen auf Ihren Cluster finden Sie unter Ändern eines Amazon DocumentDB-Clusters.

So ändern Sie eine benutzerdefinierte Cluster-Parametergruppe

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Wählen Sie im Navigationsbereich auf der linken Seite der Konsole Parameter groups (Parametergruppen) aus. Wählen Sie in der Liste der Parametergruppen den Namen der Parametergruppe, die Sie ändern möchten.

   > **Tip**
   >
   > Wenn der Navigationsbereich auf der linken Seite des Bildschirms nicht angezeigt wird, wählen Sie links oben auf der Seite das Menüsymbol (≡) aus.

3. Gehen Sie bei jedem Parameter in der Parametergruppe, die Sie ändern möchten, wie folgt vor:

   a. Suchen Sie den Parameter, den Sie ändern möchten, und überprüfen Sie, ob er änderbar ist, indem Sie überprüfen, ob er in der `true` Spalte Modifizierbar aufgeführt ist.

   b. Wenn der Parameter geändert werden kann, wählen Sie ihn aus und wählen oben rechts auf der Konsolenseite Edit (Bearbeiten) aus.

   c. Nehmen Sie im Dialogfeld Modify **<parameter-name>** die gewünschten Änderungen vor. Wählen Sie anschließend Modify cluster parameter (Cluster-Parameter ändern) aus. Um die Änderungen zu verwerfen, wählen Sie Cancel (Abbrechen) aus.

Using the AWS CLI

Sie können den `ParameterValueDescription`, oder `ApplyMethod` eines beliebigen modifizierbaren Parameters in einer benutzerdefinierten Amazon DocumentDB-Cluster-Parametergruppe mit dem ändern. AWS CLI Sie können eine standardmäßige Cluster-Parametergruppe nicht direkt ändern.

Um die Parameter einer benutzerdefinierten Cluster-Parametergruppe zu ändern, verwenden Sie die Operation `modify-db-cluster-parameter-group` mit den folgenden Parametern.

- **`--db-cluster-parameter-group-name`** – Erforderlich. Der Name der Cluster-Parametergruppe, die Sie ändern.

- **`--parameters`** – Erforderlich. Die Parameter, die von Ihnen geändert werden. Eine Liste der Parameter, die für alle Instances in einem Amazon DocumentDB-Cluster gelten, finden Sie unter. Referenz zu den Amazon DocumentDB-Clusterparametern Jeder Parametereintrag muss Folgendes enthalten:
  - **`ParameterName`**— Der Name des Parameters, den Sie ändern.
  - **`ParameterValue`**— Der neue Wert für diesen Parameter.
  - **`ApplyMethod`**— Wie die Änderungen an diesem Parameter angewendet werden sollen. Zugelassene Werte sind `immediate` und `pending-reboot`.

    > **Note**
    >
    > Parameter mit dem `ApplyType` von `static` müssen über einen `ApplyMethod` von `pending-reboot` verfügen.

Example- Ändern eines Parameterwerts

In diesem Beispiel listen Sie die Parameterwerte von `sample-parameter-group` auf und ändern den `tls`-Parameter. Anschließend listen Sie nach einer Wartezeit von 5 Minuten die Parameterwerte von `sample-parameter-group` erneut auf, um die geänderten Parameterwerte anzuzeigen.

1. Listen Sie die Parameter von `sample-parameter-group` und ihre Werte auf.

   Für Linux, macOS oder Unix:

   ```
   aws docdb describe-db-cluster-parameters \
          --db-cluster-parameter-group-name sample-parameter-group
   ```

   Für Windows:

   ```
   aws docdb describe-db-cluster-parameters ^
          --db-cluster-parameter-group-name sample-parameter-group
   ```

   Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus (JSON-Format).

   ```
   {
          "Parameters": [
   ```

```
            {
                "Source": "system",
                "ApplyType": "static",
                "AllowedValues": "disabled,enabled",
                "ParameterValue": "enabled",
                "ApplyMethod": "pending-reboot",
                "DataType": "string",
                "ParameterName": "tls",
                "IsModifiable": true,
                "Description": "Config to enable/disable TLS"
            },
            {
                "Source": "user",
                "ApplyType": "dynamic",
                "AllowedValues": "disabled,enabled",
                "ParameterValue": "enabled",
                "ApplyMethod": "pending-reboot",
                "DataType": "string",
                "ParameterName": "ttl_monitor",
                "IsModifiable": true,
                "Description": "Enables TTL Monitoring"
            }
        ]
}
```

2. Ändern Sie den Parameter `tls`, sodass der Wert `disabled` ist.

   Sie können den `ApplyMethod` nicht ändern, da der `ApplyType` `static` ist.

   Für Linux, macOS oder Unix:

```
aws docdb modify-db-cluster-parameter-group \
       --db-cluster-parameter-group-name sample-parameter-group \
       --parameters
 "ParameterName"=tls,"ParameterValue"=disabled,"ApplyMethod"=pending-reboot
```

   Für Windows:

```
aws docdb modify-db-cluster-parameter-group ^
       --db-cluster-parameter-group-name sample-parameter-group ^
       --parameters
 "ParameterName"=tls,"ParameterValue"=disabled,"ApplyMethod"=pending-reboot
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus (JSON-Format).

```
{
       "DBClusterParameterGroupName": "sample-parameter-group"
   }
```

3. Warten Sie mindestens 5 Minuten.
4. Listen Sie die Parameterwerte von `sample-parameter-group` auf, um zu überprüfen, ob der Parameter `tls` geändert wurde.

   Für Linux, macOS oder Unix:

```
aws docdb describe-db-cluster-parameters \
       --db-cluster-parameter-group-name sample-parameter-group
```

   Für Windows:

```
aws docdb describe-db-cluster-parameters ^
       --db-cluster-parameter-group-name sample-parameter-group
```

   Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus (JSON-Format).

```
{
       "Parameters": [
           {
               "ParameterValue": "false",
               "ParameterName": "enable_audit_logs",
               "ApplyType": "dynamic",
               "DataType": "string",
               "Description": "Enables auditing on cluster.",
               "AllowedValues": "true,false",
               "Source": "system",
               "IsModifiable": true,
               "ApplyMethod": "pending-reboot"
           },
           {
               "ParameterValue": "disabled",
               "ParameterName": "tls",
               "ApplyType": "static",
               "DataType": "string",
```

```
                "Description": "Config to enable/disable TLS",
                "AllowedValues": "disabled,enabled",
                "Source": "system",
                "IsModifiable": true,
                "ApplyMethod": "pending-reboot"
            }
        ]
}
```

Ändern von Amazon DocumentDB-Clustern zur Verwendung benutzerdefinierter Cluster-Parametergruppen

Wenn Sie einen Amazon DocumentDB-Cluster erstellen, wird automatisch eine `default.docdb4.0` Parametergruppe für diesen Cluster erstellt. Sie können die Cluster-Parametergruppe `default` nicht ändern. Stattdessen können Sie Ihren Amazon DocumentDB-Cluster ändern, um ihm eine neue benutzerdefinierte Parametergruppe zuzuordnen.

In diesem Abschnitt wird erklärt, wie ein vorhandener Amazon DocumentDB-Cluster so geändert wird, dass er eine benutzerdefinierte Cluster-Parametergruppe mit AWS-Managementkonsole und AWS Command Line Interface (AWS CLI) verwendet.

Using the AWS-Managementkonsole

Um einen Amazon DocumentDB-Cluster so zu ändern, dass er eine neue, nicht standardmäßige Cluster-Parametergruppe verwendet

1. Bevor Sie beginnen, stellen Sie sicher, dass Sie einen Amazon DocumentDB-Cluster und eine Cluster-Parametergruppe erstellt haben. Weitere Anweisungen finden Sie unter Einen Amazon DocumentDB-Cluster erstellen und Amazon DocumentDB-Cluster-Parametergruppen erstellen.
2. Nachdem Sie Ihre Cluster-Parametergruppe erstellt haben, öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unterhttps://console.aws.amazon.com/docdb. Wählen Sie im Navigationsbereich Clusters (Cluster) aus, um die neue Parametergruppe einem Cluster hinzuzufügen.
3. Wählen Sie den Cluster aus, dem Sie die Parametergruppe zuordnen möchten. Wählen Sie Actions (Aktionen= und anschließend Modify (Ändern) aus, um den Cluster zu ändern.
4. Wählen Sie unter Cluster options (Clusteroptionen) die neue Parametergruppe aus, der Sie den Cluster zuordnen möchten.

5. Wählen Sie Continue (Weiter) aus, um eine Übersicht Ihrer Änderungen anzuzeigen.
6. Nachdem Sie Ihre Änderungen überprüft haben, können Sie diese sofort oder während des nächsten Wartungsfensters unter Scheduling of modifications (Planen von Änderungen) anwenden.
7. Wählen Sie Modify cluster (Cluster ändern) aus, um den Cluster mit der neuen Parametergruppe zu aktualisieren.

Using the AWS CLI

Bevor Sie beginnen, stellen Sie sicher, dass Sie einen Amazon DocumentDB-Cluster und eine Cluster-Parametergruppe erstellt haben. Mit diesem AWS CLI `create-db-cluster` Vorgang können Sie einen Amazon DocumentDB-Cluster erstellen. Sie können mithilfe des AWS CLI `create-db-cluster-parameter-group` Vorgangs eine Cluster-Parametergruppe erstellen.

Verwenden Sie den AWS CLI `modify-db-cluster` Vorgang mit den folgenden Parametern, um Ihrem Cluster Ihre neue Cluster-Parametergruppe hinzuzufügen.

- --db-cluster-identifier — Der Name Ihres Clusters (z. B.). `sample-cluster`
- --db-cluster-parameter-group-name — Der Name der Parametergruppe, der Sie Ihren Cluster zuordnen möchten (z. B.). `sample-parameter-group`

Example

```
aws docdb modify-db-cluster \
    --db-cluster-identifier sample-cluster \
    --db-cluster-parameter-group-name sample-parameter-group
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus (JSON-Format).

```
"DBCluster": {
    "AvailabilityZones": [
            "us-west-2c",
            "us-west-2b",
            "us-west-2a"
    ],
    "BackupRetentionPeriod": 1,
    "DBClusterIdentifier": "sample-cluster",
    "DBClusterParameterGroup": "sample-parameter-group",
```

```
    "DBSubnetGroup": "default",
   ...
}
```

Amazon DocumentDB-Cluster-Parametergruppen kopieren

Sie können eine Kopie einer Cluster-Parametergruppe in Amazon DocumentDB mit dem AWS-Managementkonsole oder dem AWS Command Line Interface (AWS CLI) erstellen.

Using the AWS-Managementkonsole

Das folgende Verfahren führt Sie durch die Erstellung einer neuen Cluster-Parametergruppe, indem Sie eine vorhandene Cluster-Parametergruppe kopieren.

So kopieren Sie eine Cluster-Parametergruppe

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Wählen Sie im Navigationsbereich Parameter groups (Parametergruppen) aus.
3. Wählen Sie im Bereich Cluster parameter groups (Cluster-Parametergruppen) den Namen der Cluster-Parametergruppe aus, die Sie kopieren möchten.
4. Wählen Sie Actions (Aktionen) und anschließend Copy (Kopieren) aus, um diese Parametergruppe zu kopieren.
5. Geben Sie in Copy options (Kopieroptionen) einen Namen und eine Beschreibung für die neue Cluster-Parametergruppe ein. Wählen Sie anschließend Copy (Kopieren) aus, um Ihre Änderungen zu speichern.

Using the AWS CLI

Um eine Kopie einer Cluster-Parametergruppe zu erstellen, verwenden Sie die `copy-db-cluster-parameter-group`-Operation mit den folgenden Parametern.

- **`--source-db-cluster-parameter-group-identifier`** – Erforderlich. Der Name oder Amazon-Ressourcenname (ARN) der Cluster-Parametergruppe, von der Sie eine Kopie erstellen möchten.

  Wenn sich die Quell- und Zielcluster-Parametergruppen in derselben Gruppe befinden AWS-Region, kann der Identifier entweder ein Name oder ein ARN sein.

Wenn sich die Quell- und Zielcluster-Parametergruppen unterscheiden AWS-Regionen, muss es sich bei dem Bezeichner um einen ARN handeln.

- **`--target-db-cluster-parameter-group-identifier`** – Erforderlich. Der Name oder ARN der Kopie der Cluster-Parametergruppe.

  Einschränkungen:

  - Kann nicht Null, leer oder negativ sein.
  - Muss 1—255 Buchstaben, Zahlen oder Bindestriche enthalten.
  - Muss mit einem Buchstaben beginnen.
  - Darf nicht mit einem Bindestrich enden oder zwei aufeinanderfolgende Bindestriche enthalten.
- **`--target-db-cluster-parameter-group-description`** – Erforderlich. Eine vom Benutzer angegebene Beschreibung für die Kopie der Cluster-Parametergruppe.

Example

Der folgende Code erstellt eine Kopie von `sample-parameter-group` und benennt die Kopie `sample-parameter-group-copy`.

Für Linux, macOS oder Unix:

```
aws docdb copy-db-cluster-parameter-group \
    --source-db-cluster-parameter-group-identifier sample-parameter-group \
    --target-db-cluster-parameter-group-identifier sample-parameter-group-copy \
    --target-db-cluster-parameter-group-description "Copy of sample-parameter-group"
```

Für Windows:

```
aws docdb copy-db-cluster-parameter-group ^
    --source-db-cluster-parameter-group-identifier sample-parameter-group ^
    --target-db-cluster-parameter-group-identifier sample-parameter-group-copy ^
    --target-db-cluster-parameter-group-description "Copy of sample-parameter-group"
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus (JSON-Format).

```
{
    "DBClusterParameterGroup": {
```

```
        "DBClusterParameterGroupArn": "arn:aws:rds:us-east-1:123456789012:cluster-
pg:sample-parameter-group-copy",
        "DBClusterParameterGroupName": "sample-parameter-group-copy",
        "DBParameterGroupFamily": "docdb4.0",
        "Description": "Copy of sample-parameter-group"
    }
}
```

Amazon DocumentDB-Cluster-Parametergruppen zurücksetzen

Sie können einige oder alle Parameterwerte einer Amazon DocumentDB-Cluster-Parametergruppe auf ihre Standardwerte zurücksetzen, indem Sie das AWS-Managementkonsole oder das AWS Command Line Interface (AWS CLI) verwenden, um die Cluster-Parametergruppe zurückzusetzen.

Using the AWS-Managementkonsole

Führen Sie die folgenden Schritt aus, um einige oder alle Parameterwerte einer Cluster-Parametergruppe auf die Standardwerte zurückzusetzen.

So setzen Sie die Parameterwerte einer Cluster-Parametergruppe zurück

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Wählen Sie im Navigationsbereich auf der linken Seite der Konsole Parameter groups (Parametergruppen) aus.
3. Wählen Sie im Bereich Cluster parameter groups (Cluster-Parametergruppen) den Namen der Cluster-Parametergruppe aus, die Sie zurücksetzen möchten.
4. Wählen Sie Actions (Aktionen) und anschließend Reset (Zurücksetzen) aus, um diese Parametergruppe zurückzusetzen.
5. Bestätigen Sie auf der Seite Cluster parameter group reset confirmation (Zurücksetzen der Cluster-Parametergruppe bestätigen), dass Sie alle Cluster-Parameter für diese Parametergruppe auf die Standardwerte zurücksetzen möchten. Wählen Sie anschließend Reset (Zurücksetzen) aus, um die Parametergruppe zurückzusetzen. Sie können auch Cancel (Abbrechen) auswählen, um die Änderungen zu verwerfen.

Using the AWS CLI

Um einige oder alle Parameterwerte einer Cluster-Parametergruppe auf ihre Standardwerte zurückzusetzen, verwenden Sie die `reset-db-cluster-parameter-group`-Operation mit den folgenden Parametern.

- **`--db-cluster-parameter-group-name`** – Erforderlich. Der Name der zurückzusetzenden Cluster-Parametergruppe.
- **`--parameters`**— Fakultativ. Eine Liste von `ParameterName` und `ApplyMethod` in der Cluster-Parametergruppe, die auf ihre Standardwerte zurücksetzt werden sollen. Statische Parameter müssen auf `pending-reboot` gesetzt sein, damit sie beim nächsten Neustart der Instance oder `reboot-db-instance`-Anforderung wirksam werden. Sie müssen `reboot-db-instance` für alle Instances in Ihrem Cluster aufrufen, auf die der aktualisierte statische Parameter angewendet werden soll.

  Dieser Parameter und `--reset-all-parameters` schließen sich gegenseitig aus. Sie können jede der beiden Optionen verwenden, jedoch nicht beide.
- **`--reset-all-parameters`**oder **`--no-reset-all-parameters`** — Fakultativ. Gibt an, ob alle Parameter (`--reset-all-parameters`) oder nur einige der Parameter (`--no-reset-all-parameters`) auf ihre Standardwerte zurückgesetzt werden sollen. Der `--reset-all-parameters`-Parameter und `--parameters` schließen sich gegenseitig aus. Sie können jede der beiden Optionen verwenden, jedoch nicht beide.

  Wenn Sie die gesamte Gruppe zurücksetzen, werden dynamische Parameter sofort aktualisiert. Statische Parameter werden auf `pending-reboot` festgelegt, damit sie beim nächsten Neustart der Instance oder bei der nächsten `reboot-db-instance`-Anforderung wirksam werden. Sie müssen `reboot-db-instance` für alle Instances in Ihrem Cluster aufrufen, auf die der aktualisierte statische Parameter angewendet werden soll.

Example

Beispiel 1: Zurücksetzen aller Parameter auf ihre Standardwerte

Der folgende Code setzt alle Parameter in der Cluster-Parametergruppe `sample-parameter-group` auf ihre Standardwerte zurück.

Für Linux, macOS oder Unix:

```
aws docdb reset-db-cluster-parameter-group \
```

```
        --db-cluster-parameter-group-name sample-parameter-group \
        --reset-all-parameters
```

Für Windows:

```
aws docdb reset-db-cluster-parameter-group ^
        --db-cluster-parameter-group-name sample-parameter-group ^
        --reset-all-parameters
```

Beispiel 2: Zurücksetzen von angegebenen Parametern auf ihre Standardwerte

Der folgende Code setzt den `tls`-Parameter in der Cluster-Parametergruppe `sample-parameter-group` auf seinen Standardwert zurück.

Für Linux, macOS oder Unix:

```
aws docdb reset-db-cluster-parameter-group \
        --db-cluster-parameter-group-name sample-parameter-group \
        --no-reset-all-parameters \
        --parameters ParameterName=tls,ApplyMethod=pending-reboot
```

Für Windows:

```
aws docdb reset-db-cluster-parameter-group ^
        --db-cluster-parameter-group-name sample-parameter-group ^
        --no-reset-all-parameters ^
        --parameters ParameterName=tls,ApplyMethod=pending-reboot
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus (JSON-Format).

```
{
        "DBClusterParameterGroupName": "sample-parameter-group"
   }
```

Neustarten einer Cluster-Instance

Bevor ein statischer Parameterwert geändert wird, muss die Cluster-Instance neu gestartet werden. Starten Sie alle Instances in Ihrem Cluster neu, auf die der aktualisierte statische Parameter angewendet werden soll.

Für Linux, macOS oder Unix:

```
aws docdb reboot-db-instance \
       --db-instance-identifier sample-cluster-instance
```

Für Windows:

```
aws docdb reboot-db-instance ^
       --db-instance-identifier sample-cluster-instance
```

Löschen von Amazon DocumentDB-Cluster-Parametergruppen

Sie können eine benutzerdefinierte Amazon DocumentDB-Cluster-Parametergruppe mit dem AWS-Managementkonsole oder dem AWS Command Line Interface (AWS CLI) löschen. Sie können die Cluster-Parametergruppe `default.docdb4.0` nicht löschen.

Using the AWS-Managementkonsole

So löschen Sie eine Cluster-Parametergruppe

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Wählen Sie im Navigationsbereich Parameter groups (Parametergruppen) aus.

   > **Tip**
   >
   > Wenn der Navigationsbereich auf der linken Seite des Bildschirms nicht angezeigt wird, wählen Sie links oben auf der Seite das Menüsymbol (≡) aus.

3. Wählen Sie im Bereich Parametergruppen das Optionsfeld links neben der Cluster-Parametergruppe aus, die Sie löschen möchten.
4. Wählen Sie Aktionen und anschließend Löschen aus.
5. Wählen Sie im Bestätigungsbereich Delete (Löschen) die Option Delete (Löschen) aus, um die Cluster-Parametergruppe zu löschen. Um die Cluster-Parametergruppe beizubehalten, wählen Sie Cancel (Abbrechen) aus.

Using the AWS CLI

Um eine Cluster-Parametergruppe zu löschen, verwenden Sie die `delete-db-cluster-parameter-group`-Operation mit dem folgenden Parameter.

- **`--db-cluster-parameter-group-name`** – Erforderlich. Der Name der zu löschenden Cluster-Parametergruppe. Dabei muss es sich um eine vorhandene Cluster-Parametergruppe handeln. Sie können die Cluster-Parametergruppe *`default.docdb4.0`* nicht löschen.

Example- Löschen einer Cluster-Parametergruppe

Das folgende Beispiel führt Sie durch die drei Schritte zum Löschen einer Cluster-Parametergruppe:

1. Ermitteln des Namens der Cluster-Parametergruppe, die Sie löschen möchten.
2. Löschen der angegebene Cluster-Parametergruppe.
3. Überprüfen, ob die Cluster-Parametergruppe gelöscht wurde.

1. Suchen Sie den Namen der Cluster-Parametergruppe, die Sie löschen möchten.

Der folgende Code listet die Namen aller Cluster-Parametergruppen auf.

Für Linux, macOS oder Unix:

```
aws docdb describe-db-cluster-parameter-groups \
       --query 'DBClusterParameterGroups[*].[DBClusterParameterGroupName]'
```

Für Windows:

```
aws docdb describe-db-cluster-parameter-groups ^
       --query 'DBClusterParameterGroups[*].[DBClusterParameterGroupName]'
```

Die Ausgabe der vorherigen Operation ist eine Liste der Namen der Cluster-Parametergruppen ähnlich der folgenden (JSON-Format).

```
[
       [
           "default.docdb4.0"
       ],
```

```
        [
            "sample-parameter-group"
        ],
        [
            "sample-parameter-group-copy"
        ]
    ]
```

2. Löschen Sie eine angegebene Cluster-Parametergruppe.

Der folgenden Code löscht die Cluster-Parametergruppe `sample-parameter-group-copy`.

Für Linux, macOS oder Unix:

```
aws docdb delete-db-cluster-parameter-group \
       --db-cluster-parameter-group-name sample-parameter-group-copy
```

Für Windows:

```
aws docdb delete-db-cluster-parameter-group ^
       --db-cluster-parameter-group-name sample-parameter-group-copy
```

Diese Operation erzeugt keine Ausgabe.

3. Überprüfen Sie, ob die angegebene Cluster-Parametergruppe gelöscht wurde.

Der folgende Code listet die Namen aller verbleibenden Cluster-Parametergruppen auf.

Für Linux, macOS oder Unix:

```
aws docdb describe-db-cluster-parameter-groups \
       --query 'DBClusterParameterGroups[*].[DBClusterParameterGroupName]'
```

Für Windows:

```
aws docdb describe-db-cluster-parameter-groups ^
       --query 'DBClusterParameterGroups[*].[DBClusterParameterGroupName]'
```

Die Ausgabe der obigen Operation ist eine Liste der Cluster-Parametergruppen, die der folgenden ähnelt (JSON-Format). Die Cluster-Parametergruppe, die Sie gerade gelöscht haben, sollte nicht in der Liste enthalten sein.

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus (JSON-Format).

```
[
       [
           "default.docdb4.0"
       ],
       [
           "sample-parameter-group"
       ]
   ]
```

Referenz zu den Amazon DocumentDB-Clusterparametern

Wenn Sie einen dynamischen Parameter ändern und die Cluster-Parametergruppe speichern, wird diese Änderung sofort übernommen, ungeachtet der Einstellung von Apply immediately (Sofort anwenden). Wenn Sie einen statischen Parameter ändern und eine Cluster-Parametergruppe speichern, wird die Änderung des Parameters nach einem manuellen Neustart der Instance angewendet. Sie können eine Instance über die Amazon DocumentDB DocumentDB-Konsole oder durch expliziten Aufruf `reboot-db-instance` neu starten.

Die folgende Tabelle zeigt die Parameter, die für alle Instances in einem Amazon DocumentDB-Cluster gelten.

Amazon DocumentDB DocumentDB-Parameter auf Clusterebene

Parameter	Standardwert	Zulässige Werte	Anpassbar	Typ anwenden	Datentyp	Description
`audit_logs`	disabled	aktiviert, deaktiviert, ddl, dml_read, dml_write, all, none	Ja	Dynamisch	Zeichenfolge	Definiert, ob CloudWatch Amazon-Audit-Logs aktiviert sind. • **`enabled`**—CloudWatch Audit-

Parameter	Standardwert	Zulässige Werte	Anpassbar	Typ anwenden	Datentyp	Description
						Logs sind aktiviert. • **disabled**— CloudWatch Audit-Logs sind deaktiviert. • **ddl**— Die Überwachung von DDL-Ereignissen ist aktiviert. • **dml_read**— Die Prüfung auf DML-Leseereignisse ist aktiviert. • **dml_write** — Die Überwachung von DML-Schre

Parameter	Standardwert	Zulässige Werte	Anpassbar	Typ anwenden	Datentyp	Description
						ibereignissen ist aktiviert. • **`all`**— Das Auditing für alle Datenbankereignisse ist aktiviert. • **`none`**— Auditing ist deaktiviert.
`change_stream_log_retention_duration`	10800	3600-604800	Ja	Dynamisch	Ganzzahl	Definiert den Zeitraum (in Sekunden), den das Change Stream-Protokoll aufbewahrt und genutzt werden kann.

Parameter	Standardwert	Zulässige Werte	Anpassbar	Typ anwenden	Datentyp	Description
`default_collection_compression`	disabled	aktiviert, deaktiviert (Amazon DocumentDB 5.0)/zstd, lz4, keine (Amazon) DocumentDB8.0	Ja	Dynamisch	Zeichenfolge	Definiert die Standardkomprimierungseinstellung für neue Sammlungen in einem Cluster • **enabled**— Die Lz4-Komprimierung ist in Amazon DocumentDB 5.0 standardmäßig aktiviert. Die zstd-Komprimierung ist in Amazon DocumentDB 8.0 standardmäßig aktiviert. • **disabled, none**—

Parameter	Standardwert	Zulässige Werte	Anpassbar	Typ anwenden	Datentyp	Description
						Die Komprimierung ist standardmäßig deaktiviert (in Amazon DocumentDB 5.0 deaktiviert, in Amazon DocumentDB 8.0 keine).

Parameter	Standardwert	Zulässige Werte	Anpassbar	Typ anwenden	Datentyp	Description
`profiler`	disabled	aktiviert, deaktiviert	Ja	Dynamisch	Zeichenfolge	Aktiviert die Profilerstellung für langsame Operationen. • **`enabled`**— Vorgänge, die länger dauern als ein vom Kunden definierter Schwellenwert (z. B. 100 ms), werden in Amazon Logs protokolliert. CloudWatch • **`disabled`**— Langsame Operationen

Parameter	Standardwert	Zulässige Werte	Anpassbar	Typ anwenden	Datentyp	Description
						werden nicht in Logs protokolliert. CloudWatch
`profiler_sampling_rate`	1,0	0,0 – 1,0	Ja	Dynamisch	Gleitkommazahl	Definiert die Sampling-Rate für protokollierte Operationen.

Parameter	Standardwert	Zulässige Werte	Anpassbar	Typ anwenden	Datentyp	Description
`profiler_threshold_ms`	100	50 – 2147483646	Ja	Dynamisch	Ganzzahl	Definiert den Schwellenwert für `profiler`. • Alle Operationen, die größer als `profiler_threshold_ms` sind, werden in CloudWatch Logs protokolliert.

Parameter	Standardwert	Zulässige Werte	Anpassbar	Typ anwenden	Datentyp	Description
`planner_version`	3.0	1.0, 2.0, 3.0	Ja	Dynamisch	Gleitkommazahl	Definiert die Query Planner-Version, die für Abfragen verwendet werden soll. • **`1.0`**— Wird in Amazon DocumentDB 5.0 unterstützt. • **`2.0`**— Verbesserungen beim Suchen und Aktualisieren von Operatoren. Wird in Amazon DocumentDB 5.0 unterstützt.

Parameter	Standardwert	Zulässige Werte	Anpassbar	Typ anwenden	Datentyp	Description
						• **`3.0`**— Verbesserungen beim Suchen, Aktualisieren und Aggregieren von Operatoren. Standard-Abfrageplaner in Amazon DocumentDB 8.0.

Parameter	Standardwert	Zulässige Werte	Anpassbar	Typ anwenden	Datentyp	Description
`tls`	aktiviert	aktiviert, deaktiviert, fips-140-3, tls1.2+, tls1.3+	Ja	Statisch	Zeichenfolge	Gibt an, ob TLS-Verbindungen (Transport Layer Security) erforderlich sind. • **`enabled`**— Für die Verbindung sind TLS-Verbindungen erforderlich. Für Amazon DocumentDB 5.0 und früher ermöglicht dies TLS 1.0 bis 1.3, wir empfehlen jedoch TLS 1.2 oder höher. Ab der

Parameter	Standardwert	Zulässige Werte	Anpassbar	Typ anwenden	Datentyp	Description
						Nebenversion 5.0.1, Amazon DocumentDB 8.0 und neuer wird nur TLS 1.2 und höher auf Amazon DocumentDB 5.0 unterstützt. • **disabled**— TLS-Verbindungen können nicht zum Herstellen einer Verbindung verwendet werden. • **fips-140-3** — Für die

Parameter	Standardwert	Zulässige Werte	Anpassbar	Typ anwenden	Datentyp	Description
						Verbindung sind TLS-Verbindungen mit FIPS-Attributen (Federal Information Processing Standards) erforderlich. Der Cluster akzeptiert nur sichere Verbindungen gemäß FIPS-Publikation 140-3. Dies wird erst ab Amazon DocumentDB 5.0-Clustern

Parameter	Standardwert	Zulässige Werte	Anpassbar	Typ anwenden	Datentyp	Description
						(Engine-Version 3.0.3727) in diesen Regionen unterstützt: ca-central-1, us-west-2, us-east-1, us-east-2, us-gov-east-1, us-gov-west-1. • **tls1.2+** — TLS-Verbindungen, die TLS Version 1.2 und höher verwenden, sind für die Verbindung erforderlich. Dies wird

Parameter	Standardwert	Zulässige Werte	Anpassbar	Typ anwenden	Datentyp	Description
						erst ab Amazon DocumentDB 4.0 (Engine-Version 2.0.10980) und Amazon DocumentDB 5.0 (Engine-Version 3.0.11051) unterstützt. • **`tls1.3+`**— TLS-Verbindungen, die TLS Version 1.3 und höher verwenden, sind für die Verbindung erforderlich. Dies wird erst ab

Parameter	Standardwert	Zulässige Werte	Anpassbar	Typ anwenden	Datentyp	Description
						Amazon DocumentDB 4.0 (Engine-Version 2.0.10980) und Amazon DocumentDB 5.0 (Engine-Version 3.0.11051) unterstützt.

Parameter	Standardwert	Zulässige Werte	Anpassbar	Typ anwenden	Datentyp	Description
`ttl_monitor`	aktiviert	aktiviert, deaktiviert	Ja	Dynamisch	Zeichenfolge	Gibt an, ob TTL-Überwachung (Time to Live) für den Cluster aktiviert ist. • **`enabled`**— Die TTL-Überwachung ist aktiviert. • **`disabled`**— Die TTL-Überwachung ist deaktiviert.

Amazon DocumentDB-Cluster-Parameter ändern

In Amazon DocumentDB bestehen Cluster-Parametergruppen aus Parametern, die für alle Instances gelten, die Sie im Cluster erstellen. Im Fall benutzerdefinierter Cluster-Parametergruppen können Sie für alle von Ihnen erstellten Parametergruppen die Parameterwerte jederzeit ändern oder alle Parameterwerte jederzeit auf die Standardwerte für Parametergruppen zurücksetzen. In diesem Abschnitt wird beschrieben, wie Sie die Parameter, aus denen eine Amazon DocumentDB-Cluster-Parametergruppe besteht, und ihre Werte anzeigen und wie Sie diese Werte ändern oder aktualisieren können.

Parameter können dynamisch oder statisch sein. Wenn Sie einen dynamischen Parameter ändern und die Cluster-Parametergruppe speichern, wird die Änderung sofort übernommen, ungeachtet der

Einstellung für `Apply Immediately`. Wenn Sie einen statischen Parameter ändern und die Cluster-Parametergruppe speichern, wird die Änderung des Parameters erst nach einem manuellen Neustart der Instances angewendet.

Parameter einer Amazon DocumentDB-Cluster-Parametergruppe anzeigen

Sie können die Parameter eines Amazon DocumentDB-Clusters und ihre Werte mit dem AWS-Managementkonsole oder AWS CLI sehen.

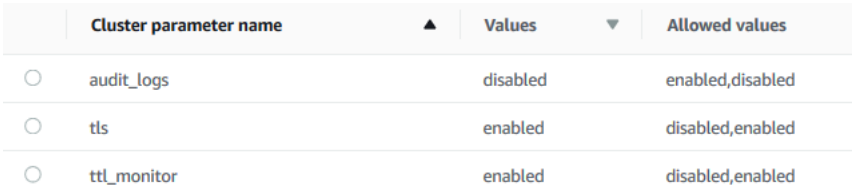
Using the AWS-Managementkonsole

So zeigen Sie die Details einer Cluster-Parametergruppe an

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Wählen Sie im Navigationsbereich Parameter groups (Parametergruppen) aus.

   > **Tip**
   >
   > Wenn der Navigationsbereich auf der linken Seite des Bildschirms nicht angezeigt wird, wählen Sie links oben auf der Seite das Menüsymbol (≡) aus.

3. Wählen Sie im Bereich Parameter groups (Parametergruppen) den Namen der Cluster-Parametergruppe aus, für die Sie die Details anzeigen möchten.
4. Auf der anschließend angezeigten Seite werden Ihnen für die einzelnen Parameter die folgenden Werte angezeigt: Name, aktueller Wert, zulässige Werte, ob der Parameter geändert werden kann, Anwendungstyp, Datentyp und Beschreibung.



	Cluster parameter name ▲	Values ▼	Allowed values
○	audit_logs	disabled	enabled,disabled
○	tls	enabled	disabled,enabled
○	ttl_monitor	enabled	disabled,enabled

Using the AWS CLI

Um die Parameter einer Cluster-Parametergruppe und deren Werte anzuzeigen, verwenden Sie die `describe-db-cluster-parameters`-Operation mit den folgenden Parametern.

- **`--db-cluster-parameter-group-name`** – Erforderlich. Der Name der Cluster-Parametergruppe, für die Sie eine detaillierte Parameterliste möchten.
- **`--source`**— Fakultativ. Wenn angegeben, werden nur Parameter für eine bestimmte Quelle zurückgegeben. Parameterquellen können `engine-default`, `system` oder `user` sein.

Example

Der folgende Code listet die Parameter und deren Werte für die Parametergruppe `custom3-6-param-grp` auf. Um weitere Informationen zur Parametergruppe zu erhalten, lassen Sie die Zeile `--query` aus. Um Informationen zu allen Parametergruppen zu erhalten, lassen Sie die Zeile `--db-cluster-parameter-group-name` aus.

Für Linux, macOS oder Unix:

```
aws docdb describe-db-cluster-parameters \
   --db-cluster-parameter-group-name custom3-6-param-grp \
   --query 'Parameters[*].[ParameterName,ParameterValue]'
```

Für Windows:

```
aws docdb describe-db-cluster-parameters ^
   --db-cluster-parameter-group-name custom3-6-param-grp ^
   --query 'Parameters[*].[ParameterName,ParameterValue]'
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus (JSON-Format).

```
[
    [
        "audit_logs",
        "disabled"
    ],
    [
        "tls",
        "enabled"
    ],
    [
        "ttl_monitor",
        "enabled"
    ]
]
```

Parameter einer Amazon DocumentDB-Cluster-Parametergruppe ändern

Sie können die Parameter einer Parametergruppe mit dem AWS-Managementkonsole oder AWS CLIändern.

Using the AWS-Managementkonsole

So aktualisieren Sie die Parameter einer Cluster-Parametergruppe

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Wählen Sie im Navigationsbereich Parameter groups (Parametergruppen) aus.

   > **Tip**
   >
   > Wenn der Navigationsbereich auf der linken Seite des Bildschirms nicht angezeigt wird, wählen Sie links oben auf der Seite das Menüsymbol (≡) aus.

3. Wählen Sie im Bereich Parameter groups (Parametergruppen) die Cluster-Parametergruppe aus, deren Parameter Sie aktualisieren möchten.
4. Auf der resultierenden Seite werden die Parameter und die entsprechenden Details zu dieser Cluster-Parametergruppe angezeigt. Wählen Sie einen zu aktualisierenden Parameter aus.
5. Klicken Sie oben rechts auf der Seite auf Edit (Bearbeiten), um den Wert des Parameters zu ändern. Weitere Informationen zu den Typen von Cluster-Parametern finden Sie unter Referenz zu den Amazon DocumentDB-Clusterparametern.
6. Führen Sie die Änderung aus. Wählen Sie anschließend Modify cluster parameter (Cluster-Parameter ändern) aus, um die Änderungen zu speichern. Um die Änderungen zu verwerfen, wählen Sie Cancel (Abbrechen) aus.

Using the AWS CLI

Um die Parameter einer Cluster-Parametergruppe zu ändern, verwenden Sie die `modify-db-cluster-parameter-group`-Operation mit den folgenden Parametern:

- **`--db-cluster-parameter-group-name`** – Erforderlich. Der Name der Cluster-Parametergruppe, die Sie ändern.

- **`--parameters`** – Erforderlich. Der Parameter oder die Parameter, die Sie ändern. Jeder Parametereintrag muss Folgendes enthalten:
  - **`ParameterName`**— Der Name des Parameters, den Sie ändern.
  - **`ParameterValue`**— Der neue Wert für diesen Parameter.
  - **`ApplyMethod`**— Wie die Änderungen an diesem Parameter angewendet werden sollen. Zugelassene Werte sind `immediate` und `pending-reboot`.

    > **Note**
    >
    > Parameter mit dem `ApplyType` von `static` müssen über einen `ApplyMethod` von `pending-reboot` verfügen.

Um die Werte der Parameter einer Cluster-Parametergruppe zu ändern (AWS CLI)

Im folgenden Beispiel wird der Parameter `tls` geändert.

1. Listen Sie die Parameter von **`sample-parameter-group`** und ihre Werte auf.

   Für Linux, macOS oder Unix:

   ```
   aws docdb describe-db-cluster-parameters \
       --db-cluster-parameter-group-name sample-parameter-group
   ```

   Für Windows:

   ```
   aws docdb describe-db-cluster-parameters ^
       --db-cluster-parameter-group-name sample-parameter-group
   ```

   Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus (JSON-Format).

   ```
   {
       "Parameters": [
           {
               "Source": "system",
               "ApplyType": "static",
               "AllowedValues": "disabled,enabled",
               "ParameterValue": "enabled",
               "ApplyMethod": "pending-reboot",
   ```

```
            "DataType": "string",
            "ParameterName": "tls",
            "IsModifiable": true,
            "Description": "Config to enable/disable TLS"
        },
        {
            "Source": "user",
            "ApplyType": "dynamic",
            "AllowedValues": "disabled,enabled",
            "ParameterValue": "enabled",
            "ApplyMethod": "pending-reboot",
            "DataType": "string",
            "ParameterName": "ttl_monitor",
            "IsModifiable": true,
            "Description": "Enables TTL Monitoring"
        }
    ]
}
```

2. Ändern Sie den **`tls`**-Parameter, sodass sein Wert **`disabled`** ist. Sie können den `ApplyMethod` nicht ändern, da der `ApplyType` `static` ist.

   Für Linux, macOS oder Unix:

```
aws docdb modify-db-cluster-parameter-group \
    --db-cluster-parameter-group-name sample-parameter-group \
    --parameters
 "ParameterName"=tls,ParameterValue=disabled,ApplyMethod=pending-reboot"
```

   Für Windows:

```
aws docdb modify-db-cluster-parameter-group ^
    --db-cluster-parameter-group-name sample-parameter-group ^
    --parameters "ParameterName=tls,ParameterValue=disabled,ApplyMethod=pending-
reboot"
```

   Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus (JSON-Format).

```
{
    "DBClusterParameterGroupName": "sample-parameter-group"
}
```

3. Warten Sie mindestens 5 Minuten.
4. Listen Sie die Parameterwerte von **`sample-parameter-group`** auf.

   Für Linux, macOS oder Unix:

```
aws docdb describe-db-cluster-parameters \
    --db-cluster-parameter-group-name sample-parameter-group
```

   Für Windows:

```
aws docdb describe-db-cluster-parameters ^
    --db-cluster-parameter-group-name sample-parameter-group
```

   Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus (JSON-Format).

```
{
    "Parameters": [
        {
            "ParameterName": "audit_logs",
            "ParameterValue": "disabled",
            "Description": "Enables auditing on cluster.",
            "Source": "system",
            "ApplyType": "dynamic",
            "DataType": "string",
            "AllowedValues": "enabled,disabled",
            "IsModifiable": true,
            "ApplyMethod": "pending-reboot"
        },
        {
            "ParameterName": "tls",
            "ParameterValue": "disabled",
            "Description": "Config to enable/disable TLS",
            "Source": "user",
            "ApplyType": "static",
            "DataType": "string",
            "AllowedValues": "disabled,enabled",
            "IsModifiable": true,
            "ApplyMethod": "pending-reboot"
        }
    ]
}
```

Grundlegendes zu Amazon DocumentDB DocumentDB-Endpunkten

Sie können Amazon DocumentDB DocumentDB-Endpunkte (mit MongoDB-Kompatibilität) verwenden, um eine Verbindung zu einem Cluster oder einer Instance herzustellen. Amazon DocumentDB hat drei verschiedene Arten von Endpunkten, von denen jeder seinen eigenen Zweck hat.

Themen

- Die Endpunkte eines Clusters finden
- Den Endpunkt einer Instanz finden
- Verbindung zu Endpunkten herstellen

Cluster-Endpunkt

Ein Cluster-Endpunkt ist ein Endpunkt für einen Amazon DocumentDB-Cluster, der eine Verbindung zur aktuellen primären Instance für den Cluster herstellt. Jeder Amazon DocumentDB-Cluster hat einen einzelnen Cluster-Endpunkt und eine primäre Instance. Im Falle eines Failovers wird der Cluster-Endpunkt auf die neue primäre Instance umgeschaltet.

Leser-Endpunkt

Ein Reader-Endpunkt ist ein Endpunkt für einen Amazon DocumentDB-Cluster, der eine Verbindung zu einem der verfügbaren Replikate für diesen Cluster herstellt. Jeder Amazon DocumentDB-Cluster hat einen Leser-Endpunkt. Wenn es mehr als ein Replikat gibt, leitet der Leser-Endpunkt jede Verbindungsanfrage an eines der Amazon DocumentDB DocumentDB-Replikate weiter.

Instance-Endpunkt

Ein Instance-Endpunkt ist ein Endpunkt, der sich mit einer bestimmten Instance verbindet. Jede Instance in einem Cluster, unabhängig davon, ob es sich um eine primäre oder eine Replikat-Instance handelt, hat ihren eigenen eindeutigen Instance-Endpunkt. Sie sollten keine Instance-Endpunkte in Ihrer Anwendung verwenden. Denn diese können im Falle eines Failovers Rollen ändern, sodass Code-Änderungen in Ihrer Anwendung erforderlich sind.

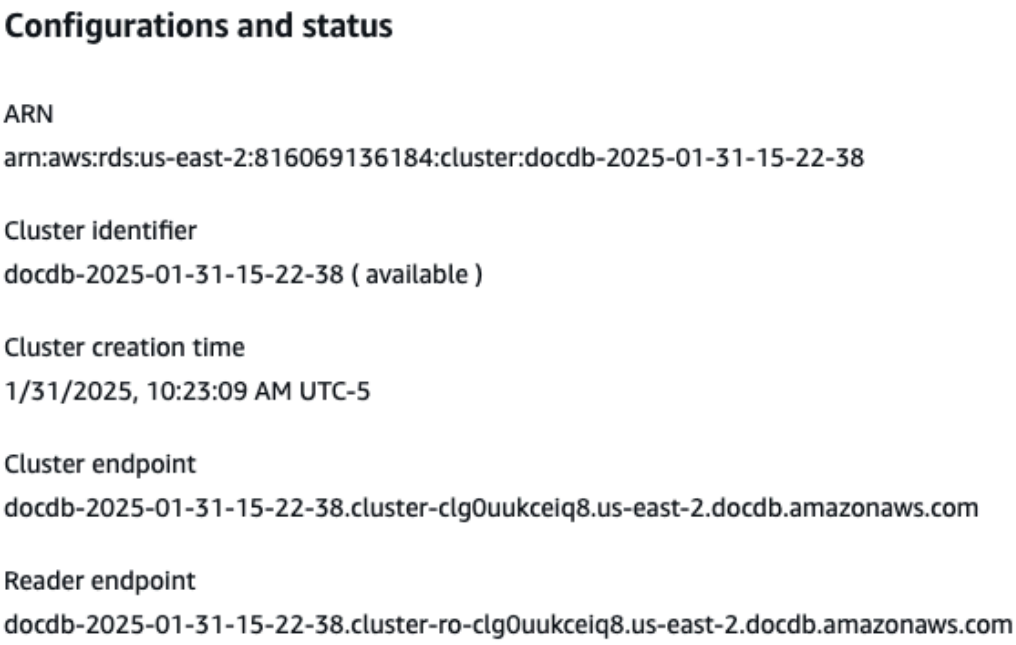
Die Endpunkte eines Clusters finden

Sie können den Cluster-Endpunkt und den Reader-Endpunkt eines Clusters mithilfe der Amazon DocumentDB DocumentDB-Konsole oder AWS CLI finden.

Using the AWS-Managementkonsole

Um die Endpunkte eines Clusters mithilfe der Konsole zu finden:

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Klicken Sie im Navigationsbereich auf Cluster.
3. Wählen Sie aus der Liste der Cluster den Namen des Clusters, der Sie interessiert.
4. Wählen Sie auf der Seite mit den Cluster-Details die Registerkarte Konfiguration aus. Im Abschnitt Konfigurationen und Status finden Sie den Cluster-Endpunkt und den Reader-Endpunkt.



5. Um eine Verbindung zu diesem Cluster herzustellen, wählen Sie die Registerkarte Konnektivität und Sicherheit. Suchen Sie die Verbindungszeichenfolge für die `mongo` Shell und die Verbindungszeichenfolge, die im Anwendungscode verwendet werden kann, um eine Verbindung zu Ihrem Cluster herzustellen.

Using the AWS CLI

Um die Cluster- und Reader-Endpunkte für Ihren Cluster mithilfe von zu finden AWS CLI, führen Sie den `describe-db-clusters` Befehl mit diesen Parametern aus.

Parameters

- **`--db-cluster-identifier`**— Optional. Gibt den Cluster an, für den die Endpunkte zurückgegeben werden sollen. Wenn diese Option weggelassen wird, werden Endpunkte für bis zu 100 Ihrer Cluster zurückgegeben.
- **`--query`**—Fakultativ. Gibt die anzuzeigenden Felder an. Dies ist hilfreich, da die Datenmenge, die Sie anzeigen müssen, um die Endpunkte zu finden, reduziert wird. Wenn diese Option weggelassen wird, werden alle Informationen über einen Cluster zurückgegeben.
- **`--region`**—Fakultativ. Verwenden Sie den Parameter `--region`, um die Region anzugeben, für die Sie den Befehl anwenden möchten. Wenn diese Angabe weggelassen wird, wird Ihre Standardregion verwendet.

Example

Das folgende Beispiel liefert die Werte `DBClusterIdentifier`, Endpunkt (Cluster-Endpunkt) und `ReaderEndpoint` für `sample-cluster`.

Für Linux, macOS oder Unix:

```
aws docdb describe-db-clusters \
   --region us-east-1 \
   --db-cluster-identifier sample-cluster \
   --query 'DBClusters[*].[DBClusterIdentifier,Port,Endpoint,ReaderEndpoint]'
```

Für Windows:

```
aws docdb describe-db-clusters ^
   --region us-east-1 ^
   --db-cluster-identifier sample-cluster ^
   --query 'DBClusters[*].[DBClusterIdentifier,Port,Endpoint,ReaderEndpoint]'
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus (JSON-Format).

```
[
  [
     "sample-cluster",
     27017,
     "sample-cluster.cluster-corlsfccjozr.us-east-1.docdb.amazonaws.com",
     "sample-cluster.cluster-ro-corlsfccjozr.us-east-1.docdb.amazonaws.com"
  ]
]
```

Nachdem Sie nun den Cluster-Endpunkt haben, können Sie sich mit `mongo` oder `mongodb` mit dem Cluster verbinden. Weitere Informationen finden Sie unter Verbindung zu Endpunkten herstellen.

Den Endpunkt einer Instanz finden

Sie können den Endpunkt für eine Instance mithilfe der Amazon DocumentDB DocumentDB-Konsole oder der AWS CLI finden.

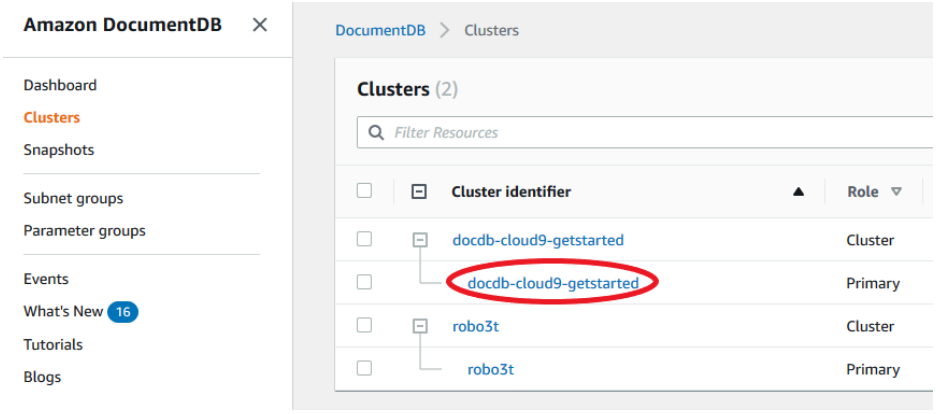
Using the AWS-Managementkonsole

So suchen Sie den Endpunkt einer Instance über die Konsole:

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Klicken Sie im Navigationsbereich auf Cluster.

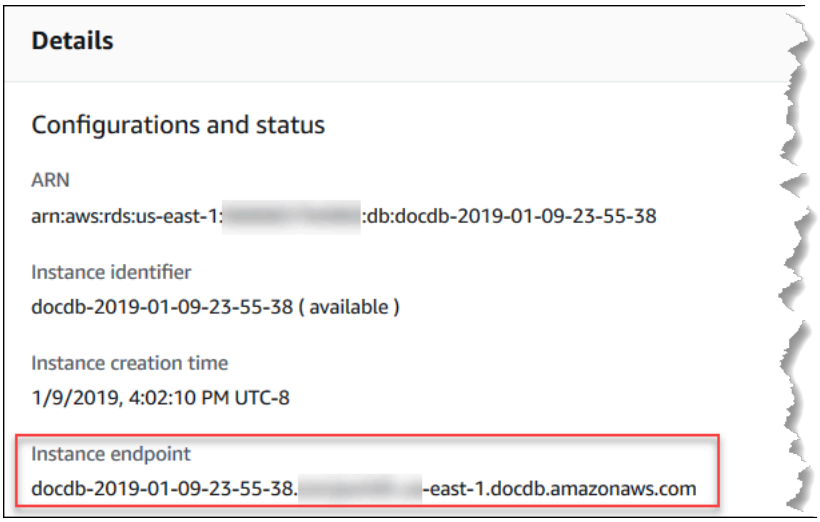
> **Tip**
>
> Wenn der Navigationsbereich auf der linken Seite des Bildschirms nicht angezeigt wird, wählen Sie links oben auf der Seite das Menüsymbol (≡) aus.

3. Im Cluster-Navigationsfeld sehen Sie die Spalte Cluster-ID. Ihre Instances werden unter Clustern aufgeführt, ähnlich wie im folgenden Screenshot.



4. Markieren Sie das Kästchen links neben der Instanz, an der Sie interessiert sind.

5. Scrollen Sie nach unten zum Abschnitt Details und suchen Sie dann den Instance-Endpunkt.



6. Um eine Verbindung zu dieser Instance herzustellen, scrollen Sie nach oben zum Abschnitt Connect (Verbinden). Suchen Sie die Verbindungszeichenfolge für die mongo-Shell und eine Verbindungszeichenfolge, die im Anwendungscode verwendet werden kann, um eine Verbindung zu Ihrer Instance herzustellen.

Using the AWS CLI

Führen Sie den folgenden Befehl mit diesen Argumenten aus AWS CLI, um den Instanzendpunkt mithilfe von zu finden.

Argumente

- **`--db-instance-identifier`**— Optional. Gibt die Instance an, für die der Endpunkt zurückgegeben werden soll. Wenn diese Option weggelassen wird, wird der Endpunkt für bis zu 100 Ihrer Instances zurückgegeben.
- **`--query`**—Fakultativ. Gibt die anzuzeigenden Felder an. Dies ist hilfreich, da die Datenmenge, die Sie anzeigen müssen, um die Endpunkte zu finden, reduziert wird. Wenn diese Option weggelassen wird, werden alle Informationen zu einer Instance zurückgegeben. Das Feld `Endpoint` hat drei Mitglieder, sodass die Auflistung in der Abfrage wie im folgenden Beispiel alle drei Mitglieder zurückgibt. Wenn Sie nur an einigen der `Endpoint`-Mitglieder interessiert sind, ersetzen Sie `Endpoint` in der Abfrage durch die Mitglieder, die Sie interessieren, wie im zweiten Beispiel.
- **`--region`**—Fakultativ. Verwenden Sie den Parameter `--region`, um die Region anzugeben, für die Sie den Befehl anwenden möchten. Wenn diese Angabe weggelassen wird, wird Ihre Standardregion verwendet.

Example

Für Linux, macOS oder Unix:

```
aws docdb describe-db-instances \
    --region us-east-1 \
    --db-instance-identifier sample-cluster-instance \
    --query 'DBInstances[*].[DBInstanceIdentifier,Endpoint]'
```

Für Windows:

```
aws docdb describe-db-instances ^
    --region us-east-1 ^
    --db-instance-identifier sample-cluster-instance ^
    --query 'DBInstances[*].[DBInstanceIdentifier,Endpoint]'
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus (JSON-Format).

```
[
    [
        "sample-cluster-instance",
        {
            "Port": 27017,
            "Address": "sample-cluster-instance.corcjozrlsfc.us-
east-1.docdb.amazonaws.com",
            "HostedZoneId": "Z2R2ITUGPM61AM"
        }
    ]
]
```

Wenn Sie die Ausgabe reduzieren, um die `HostedZoneId` des Endpunkts zu eliminieren, können Sie Ihre Abfrage ändern, indem Sie `Endpoint.Port` und `Endpoint.Address` festlegen.

Für Linux, macOS oder Unix:

```
aws docdb describe-db-instances \
    --region us-east-1 \
    --db-instance-identifier sample-cluster-instance \
    --query 'DBInstances[*].[DBInstanceIdentifier,Endpoint.Port,Endpoint.Address]'
```

Für Windows:

```
aws docdb describe-db-instances ^
    --region us-east-1 ^
    --db-instance-identifier sample-cluster-instance ^
    --query 'DBInstances[*].[DBInstanceIdentifier,Endpoint.Port,Endpoint.Address]'
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus (JSON-Format).

```
[
    [
        "sample-cluster-instance",
        27017,
        "sample-cluster-instance.corcjozrlsfc.us-east-1.docdb.amazonaws.com"
    ]
]
```

Nachdem Sie nun den Instance-Endpunkt haben, können Sie sich mit mongo oder mongodb mit der Instance verbinden. Weitere Informationen finden Sie unter Verbindung zu Endpunkten herstellen.

Verbindung zu Endpunkten herstellen

Wenn Sie Ihren Endpunkt, entweder Cluster oder Instance, haben, können Sie sich über die mongo-Shell oder eine Verbindungszeichenfolge mit ihm verbinden.

Verbindung über die Mongo-Shell herstellen

Verwenden Sie die folgende Struktur, um die Zeichenfolge zu erstellen, die Sie für die Verbindung zu Ihrem Cluster oder Ihrer Instance über die mongo-Shell benötigen:

```
mongo \
    --ssl \
    --host Endpoint:Port \
    --sslCAFile global-bundle.pem \
    --username UserName \
    --password Password
```

Beispiele für **Mongo-Shell**

Verbinden mit einem Cluster:

```
mongo \
    --ssl \
    --host sample-cluster.corcjozrlsfc.us-east-1.docdb.amazonaws.com:27017 \
    --sslCAFile global-bundle.pem \
    --username UserName \
    --password Password
```

Verbindung zu einer Instance herstellen:

```
mongo \
    --ssl \
    --host sample-cluster-instance.corcjozrlsfc.us-east-1.docdb.amazonaws.com:27017 \
    --sslCAFile global-bundle.pem \
    --username UserName \
```

```
    --password Password
```

Verbindung über eine Verbindungszeichenfolge herstellen

Verwenden Sie die folgende Struktur, um die Verbindungszeichenfolge zu erstellen, die Sie für die Verbindung zu Ihrem Cluster oder Ihrer Instance benötigen.

```
mongodb://UserName:Password@endpoint:port?replicaSet=rs0&ssl_ca_certs=global-
bundle.pem
```

Beispiele für Verbindungszeichenfolgen

Verbinden mit einem Cluster:

```
mongodb://UserName:Password@sample-cluster.cluster-corlsfccjozr.us-
east-1.docdb.amazonaws.com:27017?replicaSet=rs0&ssl_ca_certs=global-bundle.pem
```

Verbindung zu einer Instance herstellen:

```
mongodb://UserName:Password@sample-cluster-instance.cluster-corlsfccjozr.us-
east-1.docdb.amazonaws.com:27017?replicaSet=rs0&ssl_ca_certs=global-bundle.pem
```

Grundlegendes zu Amazon DocumentDB Amazon Resource Names (ARNs)

Ressourcen, die Sie in erstellen, AWS werden jeweils eindeutig mit einem Amazon-Ressourcennamen (ARN) identifiziert. Für bestimmte Amazon DocumentDB DocumentDB-Operationen (mit MongoDB-Kompatibilität) müssen Sie eine Amazon DocumentDB DocumentDB-Ressource eindeutig identifizieren, indem Sie ihren ARN angeben. Wenn Sie beispielsweise ein Tag zu einer Ressource hinzufügen, müssen Sie den ARN der Ressource angeben.

Themen

- Einen ARN für eine Amazon DocumentDB DocumentDB-Ressource erstellen
- Einen ARN für eine Amazon DocumentDB DocumentDB-Ressource finden

Einen ARN für eine Amazon DocumentDB DocumentDB-Ressource erstellen

Sie können einen ARN für eine Amazon DocumentDB DocumentDB-Ressource mit der folgenden Syntax erstellen. Amazon DocumentDB verwendet das Format von Amazon Relational Database Service (Amazon RDS) ARNs. Amazon DocumentDB DocumentDB-ARNs enthalten `rds` und nicht. `docdb`

`arn:aws:rds:`*`region`*`:`*`account_number`*`:`*`resource_type`*`:`*`resource_id`*

Name der Region	Region	Verfügbarkeitszonen (Datenverarbeitung)
USA Ost (Ohio)	`us-east-2`	3
USA Ost (Nord-Virginia)	`us-east-1`	6
USA West (Oregon)	`us-west-2`	4
Afrika (Kapstadt)	`af-south-1`	3
Südamerika (São Paulo)	`sa-east-1`	3
Asien-Pazifik (Hongkong)	`ap-east-1`	3
Asien-Pazifik (Hyderabad)	`ap-south-2`	3
Asien-Pazifik (Malaysia)	`ap-southeast-5`	3
Asien-Pazifik (Mumbai)	`ap-south-1`	3
Asien-Pazifik (Osaka)	`ap-northeast-3`	3
Asien-Pazifik (Seoul)	`ap-northeast-2`	4

Name der Region	Region	Verfügbarkeitszonen (Datenverarbeitung)
Asien-Pazifik (Singapur)	ap-southeast-1	3
Asien-Pazifik (Sydney)	ap-southeast-2	3
Asien-Pazifik (Jakarta)	ap-southeast-3	3
Asien-Pazifik (Melbourne)	ap-southeast-4	3
Asien-Pazifik (Thailand)	ap-southeast-7	3
Asien-Pazifik (Tokio)	ap-northeast-1	3
Kanada (Zentral)	ca-central-1	3
Kanada West (Calgary)	ca-west-1	3
Region China (Peking)	cn-north-1	3
China (Ningxia)	cn-northwest-1	3
Europa (Frankfurt)	eu-central-1	3
Europa (Zürich)	eu-central-2	3
Europa (Irland)	eu-west-1	3
Europa (London)	eu-west-2	3
Europa (Milan)	eu-south-1	3
Europa (Paris)	eu-west-3	3

Name der Region	Region	Verfügbarkeitszonen (Datenverarbeitung)
Europa (Spain)	`eu-south-2`	3
Europa (Stockholm)	`eu-north-1`	3
Mexiko (Zentral)	`mx-central-1`	3
Naher Osten (VAE)	`me-central-1`	3
Israel (Tel Aviv)	`il-central-1`	3
AWS GovCloud (US-West)	`us-gov-west-1`	3
AWS GovCloud (US-East)	`us-gov-east-1`	3

> **Note**
>
> Die Amazon DocumentDB DocumentDB-Architektur trennt Speicher und Datenverarbeitung. Für die Speicherebene repliziert Amazon DocumentDB sechs Kopien Ihrer Daten in drei AWS Availability Zones (AZs). Die AZs in der obigen Tabelle sind die Anzahl an AZs, die Sie in einer bestimmten Region für die Bereitstellung von Datenverarbeitungs-Instances verwenden können. Wenn Sie beispielsweise einen Amazon DocumentDB-Cluster in ap-northeast-1 starten, wird Ihr Speicher auf sechs Arten über drei AZs repliziert, Ihre Compute-Instances sind jedoch nur in zwei AZs verfügbar.

Die folgende Tabelle zeigt das Format, das Sie verwenden sollten, wenn Sie einen ARN für eine bestimmte Amazon DocumentDB DocumentDB-Ressource erstellen. Amazon DocumentDB teilt das Format von Amazon RDS-ARNs. Amazon DocumentDB DocumentDB-ARNs enthalten `rds` und nicht. `docdb`

Ressourcentyp	ARN-Format/Beispiel
Instance (db)	`arn:aws:rds:` *`region`*`:`*`account_number`*`:db:`*`resource_id`*

Ressourcentyp	ARN-Format/Beispiel
	`arn:aws:rds:us-east-1:` *1234567890* `:db:`*sample-db-instance*
Cluster (`cluster`)	`arn:aws:rds:` *region*`:`*account_number* `:cluster:` *resource_id* `arn:aws:rds:us-east-1:` *1234567890* `:cluster:` *sample-db-cluster*
Cluster-Parametergruppe (`cluster-pg`)	`arn:aws:rds:` *region*`:`*account_number* `:cluster-pg:` *resource_id* `arn:aws:rds:us-east-1:` *1234567890* `:cluster-pg:` *sample-db-cluster-parameter-group*
Sicherheitsgruppe (`secgrp`)	`arn:aws:rds:` *region*`:`*account_number* `:secgrp:`*resource_id* `arn:aws:rds:us-east-1:` *1234567890* `:secgrp:`*sample-public-secgrp*
Cluster-Snapshot (`cluster-snapshot`)	`arn:aws:rds:` *region*`:`*account_number* `:cluster-snapshot:` *resource_id* `arn:aws:rds:us-east-1:` *1234567890* `:cluster-snapshot:` *sample-db-cluster-snapshot*
Subnetzgruppe (`subgrp`)	`arn:aws:rds:` *region*`:`*account_number* `:subgrp:`*resource_id* `arn:aws:rds:us-east-1:` *1234567890* `:subgrp:`*sample-subnet-10*

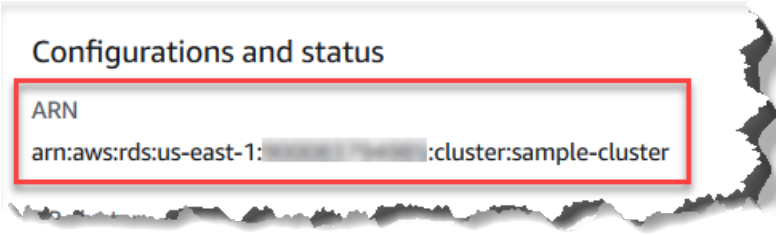
Einen ARN für eine Amazon DocumentDB DocumentDB-Ressource finden

Sie können den ARN einer Amazon DocumentDB DocumentDB-Ressource mit dem AWS-Managementkonsole oder dem AWS CLI ermitteln.

Using the AWS-Managementkonsole

Um einen ARN über die Konsole zu suchen, navigieren Sie zu der Ressource, für die Sie einen ARN erhalten möchten, und zeigen Sie die Details für diese Ressource an.

Sie können beispielsweise den ARN für einen Cluster abrufen, indem Sie auf der Cluster-Detailseite die Registerkarte Konfiguration auswählen. Die ARN finden Sie im Abschnitt Konfigurationen und Status, wie im folgenden Screenshot gezeigt.



Using the AWS CLI

Um einen ARN mit der AWS CLI für eine bestimmte Amazon DocumentDB DocumentDB-Ressource zu erhalten, verwenden Sie den `describe` Vorgang für diese Ressource. Die folgende Tabelle zeigt jeden AWS CLI Vorgang und die ARN-Eigenschaft, die mit dem Vorgang zum Abrufen eines ARN verwendet wird.

AWS CLI Befehl	ARN-Eigenschaft
`describe-db-instances`	`DBInstanceArn`
`describe-db-clusters`	`DBClusterArn`
`describe-db-parameter-groups`	`DBParameterGroupArn`
`describe-db-cluster-parameter-groups`	`DBClusterParameterGroupArn`
`describe-db-security-groups`	`DBSecurityGroupArn`
`describe-db-snapshots`	`DBSnapshotArn`

AWS CLI Befehl	ARN-Eigenschaft
`describe-db-cluster-snapshots`	`DBClusterSnapshotArn`
`describe-db-subnet-groups`	`DBSubnetGroupArn`

Example- ARN Ihres Clusters suchen

Der folgende AWS CLI Vorgang findet den ARN für den Clusters`sample-cluster`.

Für Linux, macOS oder Unix:

```
aws docdb describe-db-clusters \
    --db-cluster-identifier sample-cluster \
    --query 'DBClusters[*].DBClusterArn'
```

Für Windows:

```
aws docdb describe-db-clusters ^
    --db-cluster-identifier sample-cluster \
    --query 'DBClusters[*].DBClusterArn'
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus (JSON-Format).

```
[
    "arn:aws:rds:us-east-1:123456789012:cluster:sample-cluster"
]
```

Example- ARNs für mehrere Parametergruppen suchen

Für Linux, macOS oder Unix:

```
aws docdb describe-db-cluster-parameter-groups \
   --query 'DBClusterParameterGroups[*].DBClusterParameterGroupArn'
```

Für Windows:

```
aws docdb describe-db-cluster-parameter-groups ^
```

```
    --query 'DBClusterParameterGroups[*].DBClusterParameterGroupArn'
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus (JSON-Format).

```
[
    "arn:aws:rds:us-east-1:123456789012:cluster-pg:custom3-6-param-grp",
    "arn:aws:rds:us-east-1:123456789012:cluster-pg:default.aurora5.6",
    "arn:aws:rds:us-east-1:123456789012:cluster-pg:default.docdb3.6"
]
```

Taggen von Amazon DocumentDB DocumentDB-Ressourcen

Sie können Amazon DocumentDB-Tags (mit MongoDB-Kompatibilität) verwenden, um Metadaten zu Ihren Amazon DocumentDB DocumentDB-Ressourcen hinzuzufügen. Diese Tags können zusammen mit AWS Identity and Access Management (IAM-) Richtlinien verwendet werden, um den Zugriff auf Amazon DocumentDB DocumentDB-Ressourcen zu verwalten und zu kontrollieren, welche Aktionen auf die Ressourcen angewendet werden können. Sie können Tags auch verwenden, um Kosten zu verfolgen, indem Ausgaben für ähnlich markierte Ressourcen gruppiert werden.

Sie können die folgenden Amazon DocumentDB DocumentDB-Ressourcen taggen:

- Cluster
- Instances
- -Snapshots
- Cluster-Snapshots
- Parametergruppen
- Cluster-Parametergruppen
- Sicherheitsgruppen
- Subnetzgruppen

Übersicht über Amazon DocumentDB DocumentDB-Ressourcen-Tags

Ein Amazon DocumentDB-Tag ist ein Name-Wert-Paar, das Sie definieren und mit einer Amazon DocumentDB DocumentDB-Ressource verknüpfen. Der Name wird als der Schlüssel bezeichnet. Die Angabe eines Wertes für den Schlüssel ist optional. Sie können Tags verwenden, um einer Amazon DocumentDB DocumentDB-Ressource beliebige Informationen zuzuweisen. Sie können

einen Tag-Schlüssel z. B. dazu verwenden, um eine Kategorie zu definieren, und ein Tag-Wert könnte ein Element in dieser Kategorie sein. Sie könnten beispielsweise einen Tag-Schlüssel `project` und einen Tag-Wert von definieren`Salix`, was angibt, dass die Amazon DocumentDB DocumentDB-Ressource dem Salix-Projekt zugewiesen ist. Sie können Tags auch verwenden, um Amazon DocumentDB DocumentDB-Ressourcen so zu kennzeichnen, dass sie für Test- oder Produktionszwecke verwendet werden, indem Sie einen Schlüssel wie `environment=test` oder verwenden. `environment=production` Wir empfehlen Ihnen, einen konsistenten Satz von Tag-Schlüsseln zu verwenden, um die Nachverfolgung von Metadaten zu erleichtern, die Amazon DocumentDB DocumentDB-Ressourcen zugeordnet sind.

Sie können Tags verwenden, um Ihre AWS Rechnung so zu organisieren, dass sie Ihrer eigenen Kostenstruktur entspricht. Melden Sie sich dazu an, um Ihre AWS-Konto Rechnung mit den Tag-Schlüsselwerten zu erhalten. Um dann die Kosten kombinierter Ressourcen anzuzeigen, organisieren Sie Ihre Fakturierungsinformationen nach Ressourcen mit gleichen Tag-Schlüsselwerten. Beispielsweise können Sie mehrere Ressourcen mit einem bestimmten Anwendungsnamen markieren und dann Ihre Fakturierungsinformationen so organisieren, dass Sie die Gesamtkosten dieser Anwendung über mehrere Services hinweg sehen können. Weitere Informationen finden Sie unter Verwendung von Kostenzuordnungs-Tags im AWS Benutzerhandbuch für Fakturierung und Kostenmanagement.

Jede Amazon DocumentDB DocumentDB-Ressource hat einen Tagsatz, der alle Tags enthält, die dieser Ressource zugewiesen sind. Ein Tag-Satz kann bis zu zehn Tags enthalten oder leer sein. Wenn Sie einer Amazon DocumentDB DocumentDB-Ressource ein Tag hinzufügen, das denselben Schlüssel wie ein vorhandenes Tag auf einer Ressource hat, überschreibt der neue Wert den alten Wert.

AWS weist Ihren Tags keine semantische Bedeutung zu; Tags werden ausschließlich als Zeichenketten interpretiert. Amazon DocumentDB kann Tags für eine Instance oder andere Amazon DocumentDB DocumentDB-Ressourcen festlegen, abhängig von den Einstellungen, die Sie bei der Erstellung der Ressource verwenden. Amazon DocumentDB könnte beispielsweise ein Tag hinzufügen, das angibt, dass eine Instance für die Produktion oder zum Testen bestimmt ist.

Sie können ein Tag an einen Snapshot anfügen. Diese Gruppierung taucht jedoch nicht in Ihrer Rechnung auf.

Sie können das AWS-Managementkonsole oder das verwenden, um Tags AWS CLI zu Amazon DocumentDB DocumentDB-Ressourcen hinzuzufügen, aufzulisten und zu löschen. Wenn Sie den verwenden AWS CLI, müssen Sie den Amazon-Ressourcennamen (ARN) für die Ressource angeben, mit der Sie arbeiten möchten. Weitere Informationen zu Amazon DocumentDB

DocumentDB-ARNs finden Sie unter. Grundlegendes zu Amazon DocumentDB Amazon Resource Names (ARNs)

Tag-Einschränkungen

Die folgenden Einschränkungen gelten für Amazon DocumentDB-Tags:

- Maximale Anzahl von Tags pro Ressource: 10
- Maximale Schlüssellänge – 128 Unicode-Zeichen
- Maximale Wertlänge – 256 Unicode-Zeichen
- Gültige Zeichen für Schlüssel und Wert — Groß- und Kleinbuchstaben im UTF-8 Zeichensatz, Ziffern, Leerzeichen und die folgenden Zeichen: `_ . : / = + -` und `@` (Java-Regex:) `"^([\\p{L}\\p{Z}\\p{N}_.:/=+\\-]*)$"`
- Bei Tag-Schlüsseln und -Werten muss die Groß- und Kleinschreibung beachtet werden.
- Das Präfix `aws:` kann nicht für die Tag-Schlüssel oder Werte verwendet werden. Dieses Präfix ist für AWS reserviert.

Hinzufügen und Aktualisieren von Tags in einer Amazon DocumentDB DocumentDB-Ressource

Mit dem AWS-Managementkonsole oder dem können Sie einer Ressource bis zu 10 Tags hinzufügen. AWS CLI

Using the AWS-Managementkonsole

Der Prozess für das Hinzufügen eines Tags zu einer Ressource ist ähnlich, unabhängig davon, welcher Ressource Sie das Tag hinzufügen. In diesem Beispiel fügen Sie ein Tag zu einem Cluster hinzu.

So fügen Sie Tags einem Cluster über die Konsole hinzu oder aktualisieren sie

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Wählen Sie im Navigationsbereich Cluster aus.
3. Wählen Sie den Namen des Clusters aus, zu dem Sie Tags hinzufügen möchten.
4. Scrollen Sie nach unten zum Abschnitt Tags und wählen Sie anschließend Bearbeiten aus.

5. Für alle Tags, die Sie dieser Ressource hinzufügen möchten, gehen Sie wie folgt vor:

   a. Um ein neues Tag hinzuzufügen, geben Sie den Namen des Tags in das Feld Schlüssel ein. Um den Wert eines Tags zu ändern, suchen Sie den Namen des Tags in der Spalte Schlüssel.

   b. Um dem Tag einen neuen oder aktualisierten Wert zu geben, geben Sie einen Wert für das Tag in das Feld Wert ein.

   c. Wenn Sie mehrere Tags hinzufügen möchten, klicken Sie auf Hinzufügen. Andernfalls klicken Sie auf Speichern, sobald Sie fertig sind.

Using the AWS CLI

Der Prozess für das Hinzufügen eines Tags zu einer Ressource ist ähnlich, unabhängig davon, welcher Ressource Sie die Tags hinzufügen. In diesem Beispiel fügen Sie drei Tags zu einem Cluster hinzu. Das zweite Tag, `key2`, hat keinen Wert.

Verwenden Sie den AWS CLI Vorgang `add-tags-to-resource` mit diesen Parametern.

Parameters

- **`--resource-name`**— Der ARN der Amazon DocumentDB DocumentDB-Ressource, der Sie Tags hinzufügen möchten.
- **`--tags`**—Eine Liste der Tags (Schlüssel-Wert-Paar), die Sie dieser Ressource hinzufügen möchten, im folgenden Format. `Key=`*`key-name`*`,Value=`*`tag-value`*

Example

Für Linux, macOS oder Unix:

```
aws docdb add-tags-to-resource \
    --resource-name arn:aws:rds:us-east-1:1234567890:cluster:sample-cluster \
    --tags Key=key1,Value=value1 Key=key2 Key=key3,Value=value3
```

Für Windows:

```
aws docdb add-tags-to-resource ^
    --resource-name arn:aws:rds:us-east-1:1234567890:cluster:sample-cluster \
    --tags Key=key1,Value=value1 Key=key2 Key=key3,Value=value3
```

Die `add-tags-to-resource`-Operation erzeugt keine Ausgabe. Um die Ergebnisse der Operation anzuzeigen, verwenden Sie die `list-tags-for-resource`-Operation.

Tags in einer Amazon DocumentDB DocumentDB-Ressource auflisten

Sie können das AWS-Managementkonsole oder das verwenden AWS CLI , um eine Liste der Tags für eine Amazon DocumentDB DocumentDB-Ressource zu erhalten.

Using the AWS-Managementkonsole

Der Prozess für das Auflisten von Tags in einer Ressource ist ähnlich, unabhängig davon, welcher Ressource Sie das Tag hinzufügen. In diesem Beispiel listen Sie die Tags für einen Cluster auf.

So listen Sie die Tags in einem Cluster mithilfe der Konsole auf

1. Öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Wählen Sie im Navigationsbereich Cluster aus.
3. Wählen Sie den Namen des Clusters aus, für den Sie Tags auflisten möchten.
4. Um eine Liste der Tags in dieser Ressource anzuzeigen, scrollen Sie nach unten zum Abschnitt Tags.

Using the AWS CLI

Der Prozess für das Auflisten der Tags in einer Ressource ist ähnlich, unabhängig davon, für welche Ressource Sie das Tag auflisten. In diesem Beispiel listen Sie die Tags in einem Cluster auf.

Verwenden Sie die AWS CLI Operation `list-tags-for-resource` mit diesen Parametern.

Parameters

- **`--resource-name`**—Erforderlich. Der ARN der Amazon DocumentDB DocumentDB-Ressource, für die Sie Tags auflisten möchten.

Example

Für Linux, macOS oder Unix:

```
aws docdb list-tags-for-resource \
    --resource-name arn:aws:rds:us-east-1:1234567890:cluster:sample-cluster
```

Für Windows:

```
aws docdb list-tags-for-resource ^
    --resource-name arn:aws:rds:us-east-1:1234567890:cluster:sample-cluster
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus (JSON-Format).

```
{
    "TagList": [
        {
            "Key": "key1",
            "Value": "value1"
        },
        {
            "Key": "key2",
            "Value": ""
        },
        {
            "Key": "key3",
            "Value": "value3"
        }
    ]
}
```

Tags aus einer Amazon DocumentDB DocumentDB-Ressource entfernen

Sie können das AWS-Managementkonsole oder das verwenden, AWS CLI um Tags aus Amazon DocumentDB DocumentDB-Ressourcen zu entfernen.

Using the AWS-Managementkonsole

Der Prozess für das Entfernen von Tags aus einer Ressource ist ähnlich, unabhängig davon, welcher Ressource Sie das Tag hinzufügen. In diesem Beispiel entfernen Sie Tags aus einem Cluster.

So entfernen Sie Tags aus einem Cluster mithilfe der Konsole

1. Öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Wählen Sie im Navigationsbereich Cluster aus.
3. Wählen Sie den Namen des Clusters aus, aus dem Sie Tags entfernen möchten.
4. Scrollen Sie nach unten zum Abschnitt Tags und wählen Sie anschließend Bearbeiten aus.
5. Wenn Sie alle Tags aus dieser Ressource entfernen möchten, wählen Sie Remove all (Alle entfernen) aus. Andernfalls gehen Sie für alle Tags, die Sie aus dieser Ressource entfernen möchten, wie folgt vor:

   a. Suchen Sie den Namen des Tags in der Spalte Schlüssel.
   b. Wählen Sie Entfernen auf derselben Zeile wie der Tag-Schlüssel aus.
   c. Wenn Sie fertig sind, wählen Sie Speichern aus.

Using the AWS CLI

Der Prozess für das Entfernen eines Tags aus einer Ressource ist ähnlich, unabhängig davon, aus welcher Ressource Sie das Tag entfernen. In diesem Beispiel entfernen Sie ein Tag aus einem Cluster.

Verwenden Sie die AWS CLI Operation `remove-tags-from-resource` mit diesen Parametern.

- **`--resource-name`**—Erforderlich. Der ARN der Amazon DocumentDB DocumentDB-Ressource, aus der Sie Tags entfernen möchten.
- **`--tag-keys`**—Erforderlich. Eine Liste der Tag-Schlüssel, die von dieser Ressource entfernt werden sollen.

Example

Für Linux, macOS oder Unix:

```
aws docdb remove-tags-from-resource \
    --resource-name arn:aws:rds:us-east-1:1234567890:cluster:sample-cluster \
    --tag-keys key1 key3
```

Für Windows:

```
aws docdb remove-tags-from-resource ^
    --resource-name arn:aws:rds:us-east-1:1234567890:cluster:sample-cluster \
    --tag-keys key1 key3
```

Die `removed-tags-from-resource`-Operation erzeugt keine Ausgabe. Um die Ergebnisse der Operation anzuzeigen, verwenden Sie die `list-tags-for-resource`-Operation.

Wartung von Amazon DocumentDB

Amazon DocumentDB führt regelmäßig zwei Arten von Wartungsarbeiten durch:

- Die Cluster-Wartung aktualisiert die Datenbank-Engine. Engine-Updates enthalten Sicherheitsupdates, Bugfixes, neue Funktionen und andere Engine-Verbesserungen.
- Durch die Instanzwartung wird das Betriebssystem (OS) auf der Instanz aktualisiert.

Engine-Patches und Betriebssystemupdates verwenden dieselben drei Lebenszykluskategorien — optional, erforderlich und erzwungen — mit demselben Benachrichtigungs- und Anwendungsverhalten für jede Kategorie. Engine-Versionen haben auch eine vierte Kategorie: Nebenversionen, auf die Sie manuell aktualisieren. Es gibt folgende Kategorien:

- Optional — enthält unkritische Verbesserungen. Kein automatisches Bewerbungsdatum und keine AHD-Benachrichtigung; bewerben Sie sich, wann es Ihnen passt. (Für Betriebssystem-Updates können Sie abonnieren, um benachrichtigt `RDS-EVENT-0230` zu werden, sobald eines verfügbar ist.)
- Erforderlich — enthält Sicherheits- und andere wichtige Korrekturen. Sie erhalten eine Benachrichtigung per Health Dashboard (AHD) und per E-Mail. Eine erforderliche Aktion wird automatisch während Ihres Clusters oder Ihrer Instance nach Ablauf des Wartungsfensters angewendet. `AutoAppliedAfterDate` Sie können es verschieben, indem Sie das Wartungsfenster vor diesem Datum ändern.
- Erzwungen — eine seltene, äußerst kritische Lösung. Auto-applies außerhalb Ihres Wartungsfensters, nachdem es`ForcedApplyDate`. Amazon DocumentDB bezeichnet nur eine Aktion, die erzwungen wird, wenn keine andere Option verfügbar ist.
- Nebenversion (nur Engine-Releases) — eine nummerierte Engine-Version zusätzlich zu einer Hauptversion (z. B.). `5.0.1` User-driven: Sie aktualisieren, indem Sie die Engine-Version des Clusters ändern. Gilt nie automatisch; keine AHD-Benachrichtigung. Nebenversionen für Hauptversionen vor 5.0 werden nicht veröffentlicht.

Engine-Patches werden in einer einzigen Kategorie (optional, erforderlich oder erzwungen) veröffentlicht und bleiben dort. Aktualisierung der Betriebssysteme: Die meisten Updates sind zunächst optional und werden, falls sie nicht angewendet werden, zu „erforderlich“ und schließlich erzwungen. Der genaue Zeitpunkt hängt vom jeweiligen Patch ab und wird in der AHD-Benachrichtigung und in den Datumsfeldern veröffentlicht, die von zurückgegeben werden `describe-pending-maintenance-actions` (siehe Termine anwenden). In den Versionshinweisen von Amazon DocumentDB werden diese Kategorienamen verwendet, wenn Engine-Änderungen angekündigt werden.

Durch das Anwenden eines Engine-Patches wird der Cluster kurzzeitig offline geschaltet. Im Rest dieses Themas wird beschrieben, wie Wartungsfenster funktionieren, wie ausstehende Aufgaben gefunden werden, wie Engine-Patches und Nebenversionen installiert werden, wie Betriebssystemupdates funktionieren und wie spezielle Verfahren für globale Cluster behandelt werden.

Themen

- Nummerierung der Engine-Versionen
- Verwaltung Ihrer Amazon DocumentDB DocumentDB-Wartungsfenster
- Benachrichtigungen für Amazon DocumentDB DocumentDB-Engine-Patches
- Ausstehende Amazon DocumentDB DocumentDB-Wartungsaktionen anzeigen
- Aktualisierungen der Amazon DocumentDB DocumentDB-Engine
- Unterversion-Upgrades
- Betriebssystem-Updates für Amazon DocumentDB
- User-initiated Aktualisierungen
- Patchen globaler Cluster

Nummerierung der Engine-Versionen

Amazon DocumentDB verwendet zwei separate Versions-IDs:

- Engine-Version — eine dreiteilige Nummer in der Form *`major`*`.`*`major`*`.`*`minor` (z. B. `5.0.0` oder). `5.0.1` Die ersten beiden Teile (`5.0`) sind die MongoDB-Kompatibilitätsversion; der dritte Teil ist die Nebenversion, die erhöht wird, wenn Amazon DocumentDB eine Nebenversion veröffentlicht, die Fehlerkorrekturen und wichtige Verbesserungen enthält. Dies ist die Version, die Sie bei der Erstellung oder Aktualisierung eines Clusters angeben.

- Engine-Patch-Version — eine separate dreiteilige Nummer in der Form *major*`.0.`*patch* (z. B.`3.0.17983`), die das auf Ihren Cluster angewendete Patch-Level angibt. Die mittlere Ziffer ist immer`0`. Patch-Versionen enthalten wichtige Sicherheits- und Stabilitätsverbesserungen.

Sie können die Engine-Version anhand des Präfixes der Engine-Patch-Version ermitteln, wie in der folgenden Tabelle dargestellt.

Versionspräfix für den Engine-Patch	Version der Amazon DocumentDB DocumentDB-Engine
`1.0.`*x*	3.6
`2.0.`*x*	4,0
`3.0.`*x*	5.0
`4.0.`*x*	8.0

Um zu überprüfen, welche Patch-Version Ihr Cluster gerade läuft, stellen Sie eine Verbindung her und starten `db.runCommand({getEngineVersion: 1})` Sie ihn.

Eine Liste der veröffentlichten Engine-Patch-Versionen und deren Inhalt finden Sie unterVersionshinweise.

Verwaltung Ihrer Amazon DocumentDB DocumentDB-Wartungsfenster

Jeder Cluster und jede Instanz hat ihr eigenes wöchentliches Wartungsfenster von 30 Minuten — den Zeitraum, in dem geplante Änderungen und Software-Patches ausgeführt werden. Die meisten Ereignisse werden innerhalb von 30 Minuten abgeschlossen, größere können länger dauern.

Wenn Sie bei der Erstellung der Ressource kein Fenster auswählen, weist Amazon DocumentDB innerhalb eines für die Region definierten 8-Stunden-Tagesblocks an einem zufällig ausgewählten Tag eines nach dem Zufallsprinzip ausgewählten Tages zu. Wählen Sie Fenster, die die Auswirkungen auf Ihre Anwendung so gering wie möglich halten — zum Beispiel abends oder am Wochenende.

Für Datenbank-Engine-Upgrades verwendet Amazon DocumentDB das Fenster des Clusters, nicht die Fenster einzelner Instances.

Die folgende Tabelle zeigt die Standard-Zeitblöcke pro Region.

Name der Region	Region	UTC-Zeitblock
USA Ost (Ohio)	us-east-2	03:00-11:00
USA Ost (Nord-Virginia)	us-east-1	03:00-11:00
USA West (Oregon)	us-west-2	06:00-14:00
Afrika (Kapstadt)	af-south-1	03:00 — 11:00
Asien-Pazifik (Hongkong)	ap-east-1	06:00-14:00
Asien-Pazifik (Hyderabad)	ap-south-2	06:30 — 14:30
Asien-Pazifik (Malaysia)	ap-southeast-5	13:00-21:00
Asien-Pazifik (Mumbai)	ap-south-1	06:00-14:00
Asia Pacific (Osaka)	ap-northeast-3	12:00-20:00
Asien-Pazifik (Seoul)	ap-northeast-2	13:00-21:00
Asien-Pazifik (Singapur)	ap-southeast-1	14:00-22:00
Asien-Pazifik (Sydney)	ap-southeast-2	12:00-20:00
Asien-Pazifik (Jakarta)	ap-southeast-3	08:00-16:00
Asien-Pazifik (Melbourne)	ap-southeast-4	11:00-19:00
Asien-Pazifik (Thailand)	ap-southeast-7	15:00-23:00
Asien-Pazifik (Tokio)	ap-northeast-1	13:00-21:00
Kanada (Zentral)	ca-central-1	03:00-11:00
Kanada West (Calgary)	ca-west-1	18:00-02:00
China (Beijing)	cn-north-1	06:00-14:00

Name der Region	Region	UTC-Zeitblock
China (Ningxia)	cn-northwest-1	06:00-14:00
Europa (Frankfurt)	eu-central-1	21:00-05:00
Europa (Zürich)	eu-central-2	02:00-10:00
Europa (Irland)	eu-west-1	22:00-06:00
Europa (London)	eu-west-2	22:00-06:00
Europa (Milan)	eu-south-1	02:00-10:00
Europa (Paris)	eu-west-3	23:59-07:29
Europa (Spain)	eu-south-2	02:00 — 10:00
Europa (Stockholm)	eu-north-1	04:00 — 12:00
Mexiko (Zentral)	mx-central-1	03:00-11:00
Naher Osten (VAE)	me-central-1	05:00 — 13:00
Südamerika (São Paulo)	sa-east-1	00:00-08:00
Israel (Tel Aviv)	il-central-1	04:00-12:00
AWS GovCloud (US-East)	us-gov-east-1	17:00-01:00
AWS GovCloud (US-West)	us-gov-west-1	06:00-14:00

Ihre Amazon DocumentDB DocumentDB-Wartungsfenster ändern

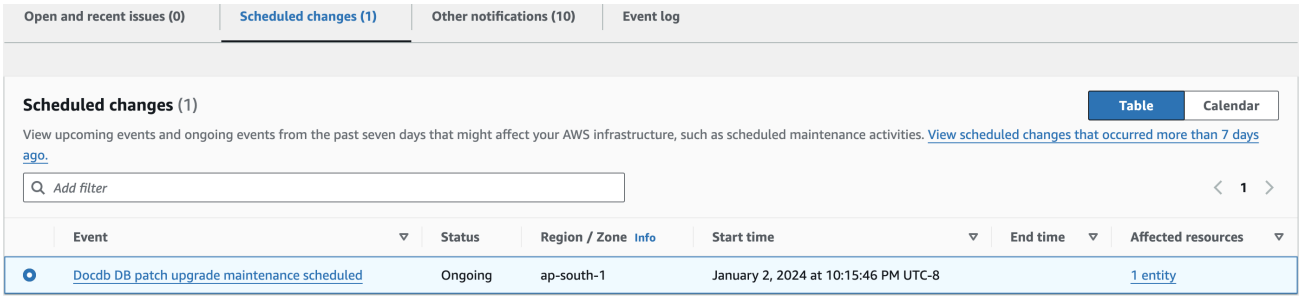
Wählen Sie das Fenster mit dem geringsten Verkehrsaufkommen, und passen Sie es im Laufe der Zeit an, wenn sich Ihre Verkehrsmuster ändern. Der Cluster oder die Instance ist während des Zeitfensters nur dann nicht verfügbar, wenn eine Systemänderung — zum Beispiel ein Skalierungsspeichervorgang oder eine Änderung der Instance-Klasse — einen Ausfall erfordert, und nur so lange, wie diese Änderung tatsächlich erforderlich ist.

So ändern Sie das Wartungsfenster

- Für einen Cluster: Weitere Informationen finden Sie unter Ändern eines Amazon DocumentDB-Clusters.
- Für eine Instance: Weitere Informationen finden Sie unter Ändern einer Amazon DocumentDB DocumentDB-Instance.

Benachrichtigungen für Amazon DocumentDB DocumentDB-Engine-Patches

Wenn ein erforderlicher Engine-Patch in einer AWS Region verfügbar wird, erhält jedes AWS Konto mit einem betroffenen Amazon DocumentDB-Cluster in dieser Region eine Benachrichtigung per Health Dashboard (AHD) und per E-Mail (gesendet an die Root-Benutzeradresse des AWS Kontos). Pro betroffener Version der Amazon DocumentDB DocumentDB-Engine wird eine Benachrichtigung zugestellt. Sie finden sie im AHD unter Geplante Änderungen. In jeder Benachrichtigung werden der Zeitpunkt der Patch-Verfügbarkeit, der Zeitplan für die automatische Anwendung, die betroffenen Cluster und die Versionshinweise aufgeführt.



Benachrichtigungen werden ungefähr zwei Tage vor dem Öffnen des Fensters für die automatische Bewerbung versendet. Beispielsweise kann ein erforderlicher Patch, der am Montag um 00:00 Uhr UTC veröffentlicht wurde, am Mittwoch um 00:00 Uhr UTC automatisch angewendet werden. Wenn das Wartungsfenster Ihres Clusters Mittwoch um 12:00 Uhr UTC ist, wird der Patch an diesem Mittwoch automatisch angewendet — etwa 12 Stunden, nachdem das Fenster für die automatische Anwendung geöffnet wurde. Wenn Ihr Wartungsfenster Dienstag um 12:00 Uhr UTC ist, wartet der Patch eine ganze Woche, bevor er automatisch angewendet wird.

Nachdem Sie die Benachrichtigung erhalten haben, haben Sie zwei Möglichkeiten: Sie können den Patch vor dem Datum der automatischen Installation selbst anwenden oder warten, bis er während eines bevorstehenden Wartungsfensters automatisch angewendet wird (Standardeinstellung). Um die

Anwendung selbst durchzuführen, öffnen Sie die Registerkarte Wartung und Backups des Clusters und suchen Sie nach dem Eintrag vom Typ. `system-update`

> **Note**
>
> Der Status der Benachrichtigung im AHD bleibt in Bearbeitung, bis Amazon DocumentDB einen weiteren Engine-Patch mit einer neuen Patch-Version veröffentlicht.
> Nachdem der Patch installiert wurde, wird die Engine-Patch-Version des Clusters aktualisiert, sodass sie der Version in der Benachrichtigung entspricht. Überprüfen Sie die neue Version, indem Sie den Befehl ausführen`db.runCommand({getEngineVersion: 1})`.

Optionale Patches und neue Nebenversionen generieren keine AHD- oder E-Mail-Benachrichtigungen. Um sie zu verfolgen, sehen Sie sich die Amazon DocumentDB DocumentDB-Versionshinweise an.

Erzwungene Patches (die seltenste Kategorie, die den kritischsten Sicherheitsupdates vorbehalten ist) werden ebenfalls per AHD und E-Mail angekündigt. Im Gegensatz zu erforderlichen Patches werden sie außerhalb Ihres Wartungsfensters angewendet, sodass das obige Beispiel für den Zeitpunkt der automatischen Anwendung nicht gilt.

Programmgesteuertes Reagieren auf Patch-Benachrichtigungen

AWS Health ist in Amazon integriert EventBridge, sodass Sie ereignisgesteuerte Anwendungen für mehr als 20 Ziele erstellen können, darunter AWS Lambda Amazon Simple Queue Service (SQS). Um programmgesteuert auf die Verfügbarkeit von Engine-Patches zu reagieren, konfigurieren Sie die Konfiguration entsprechend dem Ereignis. EventBridge `AWS_DOCDB_DB_PATCH_UPGRADE_MAINTENANCE_SCHEDULED` Von dort aus können Sie Ereignisdaten erfassen, zusätzliche Ereignisse auslösen, Push-Benachrichtigungen über das senden oder jede andere Aktion ergreifen AWS Console Mobile Application, die Sie benötigen.

Wenn Amazon DocumentDB einen Patch storniert (selten), erhalten Sie eine AHD-Benachrichtigung und eine E-Mail über die Kündigung. Verwenden Sie den `AWS_DOCDB_DB_PATCH_UPGRADE_MAINTENANCE_CANCELLED` Eventcode bei Amazon EventBridge , um diesen Fall zu behandeln. Weitere Informationen zum Schreiben von Regeln finden Sie im EventBridge Amazon-Benutzerhandbuch.

Ausstehende Amazon DocumentDB DocumentDB-Wartungsaktionen anzeigen

Verwenden Sie das AWS-Managementkonsole oder AWS CLI , um zu überprüfen, welche Wartungsarbeiten für einen Cluster oder eine Instanz ausstehen.

Ausstehende Updates werden mit dem Aktionstyp angezeigt`system-update`, der sowohl Engine-Patches als auch Betriebssystemupdates umfasst.

Wenn ein Update aussteht, können Sie:

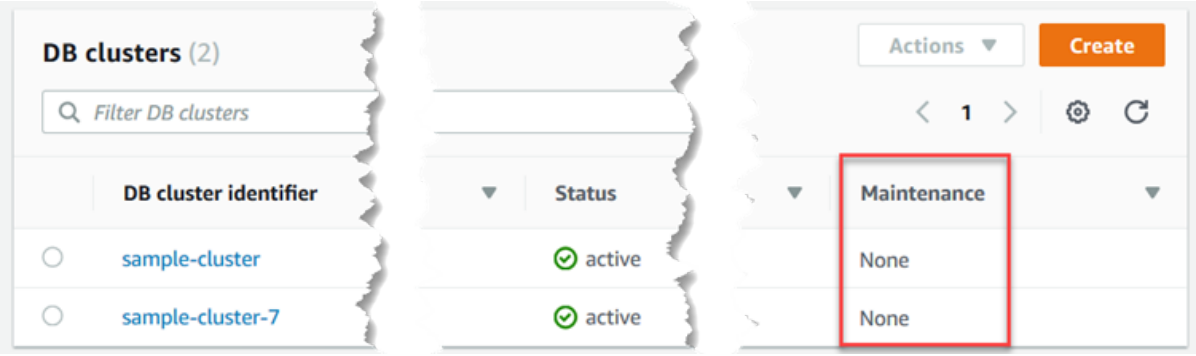
- Wenden Sie es sofort an.
- Planen Sie es für das nächste Wartungsfenster ein.
- Verschieben Sie den Wartungszeitraum (nur Engine-Patches und Betriebssystemupdates), indem Sie vorher `AutoAppliedAfterDate` Ihr Wartungsfenster ändern. Sobald dieses Datum verstrichen ist, wird die Aktion automatisch im nächsten Wartungsfenster angewendet. Nach Ablauf `ForcedApplyDate` dieser Frist ist kein weiterer Aufschub mehr möglich.

> **Note**
>
> Wenn Sie keine Maßnahmen ergreifen, werden erforderliche Wartungsmaßnahmen, wie z. B. erforderliche Engine-Patches, während eines bevorstehenden Wartungsfensters automatisch angewendet. Optionale Patches und Nebenversionen werden nie automatisch angewendet.

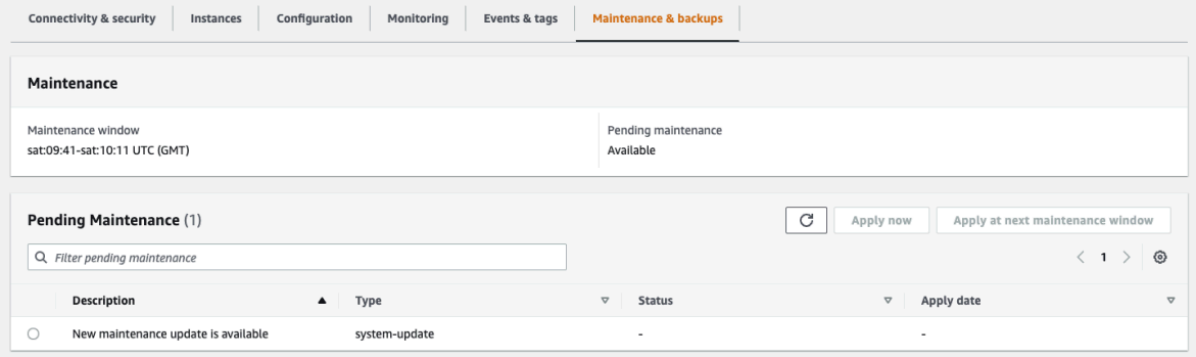
Das Wartungsfenster steuert, wann ausstehende Vorgänge gestartet werden, und nicht, wie lange es dauert, bis sie abgeschlossen sind.

Using the AWS-Managementkonsole

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Klicken Sie im Navigationsbereich auf Cluster.
3. In der Spalte Wartung des Clusters wird Verfügbar, Erforderlich oder Nächstes Fenster angezeigt, wenn ein Update aussteht.



4. Öffnen Sie den Cluster und wählen Sie dann Wartung und Backups aus, um die ausstehenden Wartungsarbeiten zu sehen und entsprechende Maßnahmen zu ergreifen.



Using the AWS CLI

Führen Sie das `describe-pending-maintenance-actions` Programm aus, um zu sehen, was noch aussteht. Das folgende Beispiel zeigt ein Konto ohne ausstehende Aktionen.

```
aws docdb describe-pending-maintenance-actions
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus (JSON-Format).

```
{
    "PendingMaintenanceActions": []
}
```

Ein Konto mit einer ausstehenden Aktion gibt eine Ausgabe zurück, die wie folgt aussieht:

```
{
    "PendingMaintenanceActions": [
        {
```

```
            "ResourceIdentifier": "arn:aws:rds:us-
east-1:123456789012:cluster:sample-cluster",
            "PendingMaintenanceActionDetails": [
                {
                    "Action": "system-update",
                    "Description": "db-version-upgrade",
                    "CurrentApplyDate": "2026-05-15T03:01:00Z",
                    "AutoAppliedAfterDate": "2026-05-15T03:01:00Z"
                }
            ]
        }
    ]
}
```

Mithilfe des Formulars können Sie die Liste auf bestimmte Cluster beschränken`Name=`*`filter-name`*`,Values=`*`resource-id`*`,...`. `--filters` Der akzeptierte Filter `Name` ist`db-cluster-id`, der eine Liste von Cluster-Identifikatoren oder ARNs verwendet.

Example

Für Linux, macOS oder Unix:

```
aws docdb describe-pending-maintenance-actions \
   --filters Name=db-cluster-id,Values=sample-cluster1,sample-cluster2
```

Für Windows:

```
aws docdb describe-pending-maintenance-actions ^
   --filters Name=db-cluster-id,Values=sample-cluster1,sample-cluster2
```

Termine anwenden

Für jede ausstehende Wartungsmaßnahme gelten bis zu drei Gültigkeitsdaten. Sie erscheinen in der AWS CLI Ausgabe für `describe-pending-maintenance-actions` und geben an, wann die Aktion ausgeführt wird. Felder sind `null` für die optionale Wartung vorgesehen.

- **`CurrentApplyDate`**— wann die Ausführung der Aktion geplant ist, entweder jetzt oder im nächsten Wartungsfenster. Befüllt mit erforderlichen und erzwungenen Aktionen.
- **`AutoAppliedAfterDate`**— das Datum, nach dem die automatische Anwendung während des Wartungsfensters für Cluster oder Instance beginnt. Für die erforderlichen Aktionen aufgefüllt.

- **`ForcedApplyDate`**— die harte Frist. Nach diesem Datum wird die Aktion unabhängig von Ihrem Wartungsfenster automatisch ausgeführt. Für erzwungene Aktionen aufgefüllt.

Um eine ausstehende Aktion zu verschieben, verschieben Sie Ihr Wartungsfenster auf einen späteren Tag zuvor`AutoAppliedAfterDate`. Sobald `AutoAppliedAfterDate` die Aktion erfolgreich abgeschlossen ist, wird sie automatisch im nächsten Wartungsfenster angewendet. Sobald der `ForcedApplyDate` Vorgang abgeschlossen ist, ist kein weiterer Aufschub möglich. Das genaue Zeitfenster für die Verzögerung ist je nach Patch unterschiedlich. Die Daten werden in der AHD-Benachrichtigung und der Ausgabe veröffentlicht. AWS CLI

Aktualisierungen der Amazon DocumentDB DocumentDB-Engine

Wenn Sie einen ausstehenden Engine-Patch identifiziert haben, wenden Sie eines der folgenden Verfahren an, um ihn anzuwenden oder zu planen. Sie können diese Verfahren entweder vom AWS-Managementkonsole oder vom aus ausführen AWS CLI.

Using the AWS-Managementkonsole

Um ein Update für einen Cluster zu verwalten

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Klicken Sie im Navigationsbereich auf Cluster.
3. Wählen Sie den Cluster aus, den Sie aktualisieren möchten.
4. Wählen Sie im Menü Aktionen eine der folgenden Optionen aus:
   - Jetzt aktualisieren: Führen Sie die ausstehenden Wartungsarbeiten sofort aus.
   - Im nächsten Fenster aktualisieren — Führen Sie es während des nächsten Wartungsfensters des Clusters aus.

   Sie können auch im Bereich Ausstehende Wartung auf der Registerkarte Wartung und Backups des Clusters die Option Jetzt anwenden oder Beim nächsten Wartungsfenster anwenden verwenden (sieheAusstehende Amazon DocumentDB DocumentDB-Wartungsaktionen anzeigen).

> **Note**
>
> Wenn nichts aussteht, sind alle diese Optionen inaktiv.

Using the AWS CLI

Wenden Sie ein ausstehendes Update mit an`apply-pending-maintenance-action`.

Parameters

- **`--resource-identifier`**— Der Amazon Resource Name (ARN) von Amazon DocumentDB der Ressource, auf die die ausstehende Aktion abzielt.
- **`--apply-action`**— die ausstehende Wartungsmaßnahme, die angewendet werden soll. Zulässige Werte: `system-update`, `db-upgrade`.
- **`--opt-in-type`**— die Art der Opt-in-Anfrage oder ob eine rückgängig gemacht werden soll. Zulässige Werte:
  - `immediate`— bewerben Sie sich jetzt. Kann nach dem Absenden nicht rückgängig gemacht werden.
  - `next-maintenance`— während des nächsten Wartungsfensters der Ressource anwenden.
  - `undo-opt-in`— storniert ein `next-maintenance` vorhandenes Opt-In.

Example

Für Linux, macOS oder Unix:

```
aws docdb apply-pending-maintenance-action \
    --resource-identifier arn:aws:rds:us-east-1:123456789012:db:sample-cluster-instance-1 \
    --apply-action system-update \
    --opt-in-type immediate
```

Für Windows:

```
aws docdb apply-pending-maintenance-action ^
    --resource-identifier arn:aws:rds:us-east-1:123456789012:db:sample-cluster-instance-1 ^
    --apply-action system-update ^
```

```
    --opt-in-type immediate
```

Lesen Sie die Verfügbarkeit während des Patchens

Die Amazon DocumentDB DocumentDB-Engine 5.0 und 8.0 behalten die Leseverfügbarkeit beim Patchen bei, wenn der Cluster mehrere Instances umfasst. Amazon DocumentDB patcht Leser-Instances fortlaufend in drei Gruppen, sodass die verbleibenden Reader weiterhin Traffic bereitstellen. Der Writer ist während des Patches kurzzeitig nicht verfügbar. Um keine Ausfallzeiten beim Lesen zu erreichen, stellen Sie Ihre Lesepräferenz so ein, dass Lesevorgänge auf den Writer zurückfallen können: `secondaryPreferred` oder sie `primaryPreferred` funktionieren `primary` oder `secondary` alleine zu Leseausfällen führen können.

Bevorzugter Lesemodus	Während des Writer-Upgrades	Während des Reader-Upgrades	Minimale Anzahl an Lesegeräten erforderlich, um Ausfallzeiten beim Lesen zu vermeiden
`primary`	Read/write Ausfallzeit	Keine Auswirkungen	N/A
`primaryPreferred`	Ausfallzeiten schreiben	Keine Auswirkungen	1
`secondary`	Ausfallzeiten schreiben	Ausfallzeit beim Lesen (wenn nur ein Lesegerät vorhanden ist)	2
`secondaryPreferred`	Ausfallzeit beim Schreiben	Keine Auswirkungen	1
`nearest`	Ausfallzeiten schreiben	Keine Auswirkungen	1

Während Lesegeräte Patches durchführen, sinkt der gesamte Cluster-Lesedurchsatz vorübergehend. Um den Durchsatz konstant zu halten, sollten Sie vor dem Upgrade zusätzliche Lesegeräte bereitstellen und diese nach Abschluss des Upgrades entfernen.

Auf Engine 3.6 und 4.0 gelten diese Funktionen für Leseverfügbarkeit nicht: Ein Engine-Patch verursacht längere Ausfallzeiten, die sich sowohl auf Lese- als auch auf Schreibvorgänge auswirken. Informationen zum Upgrade auf eine Hauptversion, bei der dies der Fall ist, finden Sie unter. Direktes Upgrade der Hauptversion von Amazon DocumentDB

Dauer der Patch-Ausfallzeit

Engine-patch Die Ausfallzeiten variieren. Die wichtigsten Faktoren sind die CPU-Auslastung und der Speicherdruck auf der Instance zum Zeitpunkt des Patches. Daher ist es wichtig, die richtige Größe Ihrer Instances zu wählen. Um Ausfallzeiten zu minimieren, führen Sie die neueste Version der Amazon DocumentDB DocumentDB-Hauptengine aus und verteilen Sie die Instances auf mehrere Availability Zones.

Patch-Updates und Ersatzprodukte

Amazon DocumentDB überwacht Patches nach der Veröffentlichung. In dem seltenen Fall, dass ein Problem festgestellt wird, unterbricht Amazon DocumentDB den Rollout, während eine aktualisierte Version vorbereitet wird. In diesem Fall wird der Patch von Clustern, die den Patch noch nicht erhalten haben, nicht mehr als verfügbare Wartungsaktion angesehen und die entsprechende Benachrichtigung über geplante Änderungen in der wird zurückgezogen. Health Dashboard Cluster, auf denen die betroffene Version bereits ausgeführt wird, funktionieren weiterhin normal und erfordern keine Aktion von Ihnen.

Ein aktualisierter Patch folgt in Kürze. Sobald er in Ihrer Region verfügbar ist, erhalten Sie per E-Mail eine neue Benachrichtigung, genau wie unter beschriebenBenachrichtigungen für Amazon DocumentDB DocumentDB-Engine-Patches. Health Dashboard

Unterversion-Upgrades

Amazon DocumentDB veröffentlicht Nebenversionen zusätzlich zur Hauptversion 5.0 und höher (z. B.`5.0.1`). Nebenversionen für Hauptversionen vor 5.0 werden nicht veröffentlicht. Nebenversionen verhalten sich anders als erforderliche und optionale Engine-Patches:

- Sie werden nicht als ausstehende Wartungsmaßnahme angezeigt und werden auch nicht automatisch angewendet.
- Sie generieren keine AHD- oder E-Mail-Benachrichtigungen. Neue Nebenversionen werden in den Amazon DocumentDB DocumentDB-Versionshinweisen angekündigt.
- Um ein Upgrade durchzuführen, ändern Sie die Engine-Version des Clusters (sofort oder während des nächsten Wartungsfensters). Upgrades kleinerer Versionen erfordern kurze Ausfallzeiten und

sind unidirektional — ein Downgrade auf eine frühere Nebenversion ist nicht möglich. Führen Sie bei globalen Clustern ein Upgrade der sekundären Cluster vor den primären Clustern durch.

Lesen Sie mehr:Upgrade der Nebenversion von Amazon DocumentDB.

Betriebssystem-Updates für Amazon DocumentDB

Instanzen benötigen gelegentlich Betriebssystem-Updates. Amazon DocumentDB aktualisiert das Betriebssystem, um die Leistung zu verbessern und die Sicherheit zu erhöhen. Bei Betriebssystem-Updates bleiben die Cluster-Engine-Version und die Instance-Klasse unverändert. Wie Engine-Patches verwenden Betriebssystem-Updates den optionalen Lebenszyklus / required /forced, der oben in diesem Thema beschrieben wird. Im Gegensatz zu Engine-Patches kann ein Betriebssystemupdate im Laufe der Zeit diese Kategorien durchlaufen, wenn Sie es verschieben. Installieren Sie Betriebssystem-Updates, sobald sie verfügbar sind, und legen Sie das Wartungsfenster Ihrer Instanz auf einen Zeitpunkt fest, der zu Ihrem Unternehmen passt.

Wenn Sie über ein neues optionales Update informiert werden möchten, abonnieren Sie es `RDS-EVENT-0230` in der Kategorie Sicherheitspatching-Ereignisse. Einzelheiten finden Sie unter Abonnieren von Amazon DocumentDB DocumentDB-Veranstaltungsabonnements. Nachdem Sie eine Benachrichtigung erhalten haben, können Sie den Betriebssystem-Patch selbst auf jede Instance anwenden.

Wenn Sie einen Cluster patchen, aktualisieren Sie zuerst die Reader-Instanzen und zuletzt den Writer-Instances. Vermeiden Sie es, Reader und Writer gleichzeitig zu patchen — ein Failover während des Patches kann die Ausfallzeit verlängern. Die Wartung der primären Instanz löst einen Failover aus. Führen Sie also mehr als eine Instanz pro Cluster aus, um verfügbar zu bleiben. Details hierzu finden Sie unter Amazon DocumentDB-Failover.

> **Important**
>
> Ihre Amazon DocumentDB DocumentDB-Instance geht für das Betriebssystem-Upgrade offline. Multi-instance Cluster minimieren die Auswirkungen. Wenn Sie einen Cluster mit einer einzigen Instanz ausführen, können Sie vorübergehend einen sekundären Cluster für das Upgrade hinzufügen und ihn anschließend entfernen. Für das sekundäre System fallen die üblichen Gebühren an, solange es existiert.

> **Note**
>
> Aus Compliance-Gründen kann es erforderlich sein, über optionale und erforderliche Updates auf dem Laufenden zu bleiben. Wenden Sie die verfügbaren Updates während Ihrer Wartungsfenster routinemäßig an.

Betriebssystem-Updates sind an bestimmte Engine-Versionen und Instanzklassen gebunden, sodass verschiedene Instanzen zu unterschiedlichen Zeiten in Frage kommen. Wenn eine Instanz berechtigt ist, wird das Update in der Konsole angezeigt. Sie können es auch über den AWS CLI `describe-pending-maintenance-actions` Befehl oder die `DescribePendingMaintenanceActions` API einsehen.

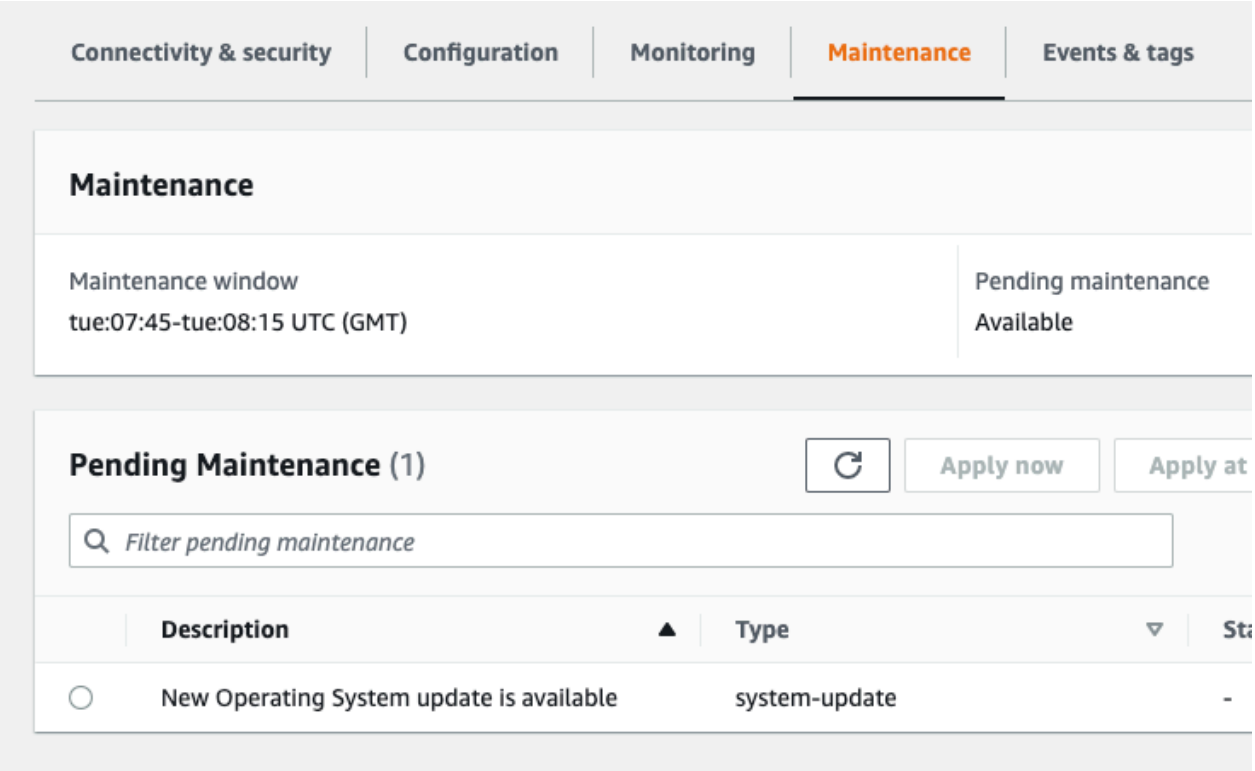
> **Note**
>
> Wenn Ihr Cluster nicht auf der neuesten Patch-Version seiner Amazon DocumentDB-Engine installiert ist, wird ein Betriebssystem-Update möglicherweise nicht als verfügbar angezeigt. Wenden Sie zuerst den neuesten Engine-Patch an und überprüfen Sie es dann erneut.

Verwenden Sie das AWS-Managementkonsole oder AWS CLI , um zu überprüfen, ob ein Update verfügbar ist.

Using the AWS-Managementkonsole

Um von der Konsole aus nach einem Betriebssystem-Update zu suchen:

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Klicken Sie im Navigationsbereich auf Cluster. Die Liste zeigt sowohl Cluster als auch die darin enthaltenen Instances, unterschieden durch die Spalte Rolle.
3. Wählen Sie die Zeile aus, deren Rolle Instanz ist (nicht die Clusterzeile). Betriebssystemupdates gelten für Instanzen, nicht für Cluster.
4. Wählen Sie Wartung.
5. Suchen Sie unter Ausstehende Wartung nach dem Betriebssystem-Update.



Wählen Sie im Bereich „Ausstehende Wartung“ das Betriebssystem-Update aus und wählen Sie „Jetzt anwenden“ oder „Beim nächsten Wartungsfenster anwenden“. Wenn der Wartungswert „Nächstes Fenster“ lautet, können Sie das Update mit „Upgrade aufschieben“ verschieben, solange es noch nicht gestartet wurde.

Sie können dies auch über die Cluster-Liste tun: Wählen Sie im Navigationsbereich Clusters aus, wählen Sie die Zeile aus, deren Rolle Instance ist, und wählen Sie im Menü Aktionen die Option Jetzt anwenden oder Beim nächsten Wartungsfenster anwenden aus.

Using the AWS CLI

Führen Sie im AWS CLI folgenden Befehl aus`describe-pending-maintenance-actions`:

```
aws docdb describe-pending-maintenance-actions
```

```
{
  "PendingMaintenanceActions": [
    {
      "ResourceIdentifier": "arn:aws:rds:us-east-1:123456789012:db:sample-cluster-
instance-1",
      "PendingMaintenanceActionDetails": [
        {
```

```
          "Action": "system-update",
          "Description": "New Operating System update is available"
        }
      ]
    }
  ]
}
```

User-initiated Aktualisierungen

Einige Änderungen können Sie selbst vornehmen, z. B. das Austauschen einer Instance-Klasse gegen eine mit mehr oder weniger Arbeitsspeicher oder das Ändern der Parametergruppe des Clusters. Amazon DocumentDB behandelt diese anders als Updates, die es initiiert. Details hierzu finden Sie unter:

- Ändern eines Amazon DocumentDB-Clusters
- Ändern einer Amazon DocumentDB DocumentDB-Instance

Um vom Benutzer initiierte Änderungen aufzulisten, die noch ausstehen:

Example

Um ausstehende, vom Benutzer initiierte Änderungen für Ihre Instances aufzulisten

Für Linux, macOS oder Unix:

```
aws docdb describe-db-instances \
    --query 'DBInstances[*].
[DBClusterIdentifier,DBInstanceIdentifier,PendingModifiedValues]'
```

Für Windows:

```
aws docdb describe-db-instances ^
    --query 'DBInstances[*].
[DBClusterIdentifier,DBInstanceIdentifier,PendingModifiedValues]'
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus (JSON-Format).

In diesem Beispiel `sample-cluster-instance` hat eine ausstehende Änderung zu`db.r5.xlarge`; `sample-cluster-instance-2` hat keine.

```
[
    [
        "sample-cluster",
        "sample-cluster-instance",
        {
            "DBInstanceClass": "db.r5.xlarge"
        }
    ],
    [
        "sample-cluster",
        "sample-cluster-instance-2",
        {}
    ]
]
```

Patchen globaler Cluster

In einem globalen Cluster wird jeder Mitgliedscluster — primärer und sekundärer — während seines eigenen Wartungsfensters aktualisiert. Wenn ein erforderlicher Engine-Patch in jeder Region verfügbar ist, erhalten Sie eine AHD- und E-Mail-Benachrichtigung. Optionale Patches und neue Nebenversionen generieren keine Benachrichtigungen. Weitere Informationen finden Sie in den Amazon DocumentDB DocumentDB-Versionshinweisen.

Wenn Sie die Patches selbst anwenden, patchen Sie immer zuerst die sekundären Patches und die primären Patches zuletzt. Diese Reihenfolge sorgt dafür, dass Failover und Switchover während des gesamten Rollouts verfügbar sind.

> **Important**
>
> Wenn Sie versehentlich die primäre Version zuerst patchen, aktualisieren Sie alle sekundären Versionen so bald wie möglich auf dieselbe Version. Failover und Switchover bleiben deaktiviert, bis sich alle Cluster auf derselben Version befinden.

Wenn Sie keine Maßnahmen ergreifen, wird der Patch automatisch während des nächsten Wartungsfensters jedes Clusters angewendet: zuerst die sekundären, dann der primäre Patch in seinem Fenster, sobald die sekundären Wartungsfenster abgeschlossen sind.

Behalten Sie die gleiche Version für den primären und den sekundären DB-Cluster bei. Das verwaltete regionsübergreifende Failover funktioniert nur in einer globalen Datenbank, wenn jeder

Cluster dieselbe Engine-Version und dasselbe Patch-Level verwendet. Das Gleiche gilt, wenn Sie eine neue sekundäre Engine-Version hinzufügen, die eine neuere Engine-Version als die primäre verwendet. Erstellen Sie neue sekundäre Engine-Versionen auf der primären Version, bevor Sie sie mit der globalen Datenbank verbinden.

Führen Sie nach einer Patch-Benachrichtigung zum frühestmöglichen Zeitpunkt ein Upgrade der primären und sekundären Version auf die neueste Version durch, damit Failover und Switchover weiterhin funktionieren. Wenn eine Failover- oder Switchover-Anfrage abgelehnt wird, vergleichen Sie die Engine-Patch-Versionen der einzelnen Cluster. Wenn sie nicht übereinstimmen, wenden Sie den verfügbaren Patch auf den verzögerten Clustern an.

Grundlegendes zu Rollen im Zusammenhang mit Services

Amazon DocumentDB (mit MongoDB-Kompatibilität) verwendet AWS Identity and Access Management (IAM) service-verknüpfte Rollen. Eine serviceverknüpfte Rolle ist eine einzigartige Art von IAM-Rolle, die direkt mit Amazon DocumentDB verknüpft ist. Service-linked Rollen sind von Amazon DocumentDB vordefiniert und beinhalten alle Berechtigungen, die der Service benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen.

Eine serviceverknüpfte Rolle erleichtert die Verwendung von Amazon DocumentDB, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Amazon DocumentDB definiert die Berechtigungen seiner serviceverknüpften Rollen, und sofern nicht anders definiert, kann nur Amazon DocumentDB seine Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Sie können die Rollen nur nach dem Löschen der zugehörigen Ressourcen löschen. Dadurch werden Ihre Amazon DocumentDB DocumentDB-Ressourcen geschützt, da Sie nicht versehentlich die Zugriffsberechtigung für die Ressourcen entziehen können.

Informationen zu anderen Diensten, die dienstbezogene Rollen unterstützen, finden Sie unter AWS Services That Work with IAM und suchen Sie nach den Services, für die in der Spalte Rolle Ja steht. Service-Linked Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Mit dem Service verknüpfte Amazon DocumentDB DocumentDB-Rollenberechtigungen

Amazon DocumentDB (mit MongoDB-Kompatibilität) verwendet die benannte dienstbezogene Rolle AWSServiceRoleForRDS, damit Amazon DocumentDB AWS Dienste im Namen Ihrer Cluster aufrufen kann.

Die AWSServiceRoleForRDS serviceverknüpfte Rolle vertraut darauf, dass die folgenden Dienste die Rolle übernehmen:

- `docdb.amazonaws.com`

Die Rollenberechtigungsrichtlinie ermöglicht es Amazon DocumentDB, die folgenden Aktionen für die angegebenen Ressourcen durchzuführen:

- Aktionen auf `ec2`:
  - `AssignPrivateIpAddresses`
  - `AuthorizeSecurityGroupIngress`
  - `CreateNetworkInterface`
  - `CreateSecurityGroup`
  - `DeleteNetworkInterface`
  - `DeleteSecurityGroup`
  - `DescribeAvailabilityZones`
  - `DescribeInternetGateways`
  - `DescribeSecurityGroups`
  - `DescribeSubnets`
  - `DescribeVpcAttribute`
  - `DescribeVpcs`
  - `ModifyNetworkInterfaceAttribute`
  - `RevokeSecurityGroupIngress`
  - `UnassignPrivateIpAddresses`
- Aktionen auf `sns`:
  - `ListTopic`

  - `Publish`
- Aktionen auf `cloudwatch`:
  - `PutMetricData`
  - `GetMetricData`
  - `CreateLogStream`
  - `PullLogEvents`
  - `DescribeLogStreams`
  - `CreateLogGroup`

> **Note**
>
> Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Möglicherweise erhalten Sie die folgende Fehlermeldung:
> Unable to create the resource. Überprüfen Sie, ob Sie die Berechtigung haben, eine serviceverknüpfte Rolle zu erstellen. Andernfalls warten Sie und versuchen Sie es später noch einmal.
> Wenn Sie diesen Fehler erhalten, stellen Sie sicher, dass Sie die folgenden Berechtigungen aktiviert haben:
>
> ```
> {
>     "Action": "iam:CreateServiceLinkedRole",
>     "Effect": "Allow",
>     "Resource": "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/
> AWSServiceRoleForRDS",
>     "Condition": {
>         "StringLike": {
>             "iam:AWSServiceName":"rds.amazonaws.com"
>         }
>     }
> }
> ```

Weitere Informationen finden Sie unter Service-Linked Rollenberechtigungen im IAM-Benutzerhandbuch.

Eine serviceverknüpfte Amazon DocumentDB DocumentDB-Rolle erstellen

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie einen Cluster erstellen, erstellt Amazon DocumentDB die serviceverknüpfte Rolle für Sie.

Wenn Sie diese serviceverknüpfte Rolle löschen und dann erneut erstellen müssen, können Sie die Rolle in Ihrem Konto mit demselben Verfahren neu anlegen. Wenn Sie einen Cluster erstellen, erstellt Amazon DocumentDB die serviceverknüpfte Rolle erneut für Sie.

Änderung einer serviceverknüpften Amazon DocumentDB DocumentDB-Rolle

Amazon DocumentDB erlaubt es Ihnen nicht, die AWSServiceRoleForRDS serviceverknüpfte Rolle zu ändern. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach dem Erstellen einer serviceverknüpften Rolle nicht mehr geändert werden. Sie können die Beschreibung der Rolle jedoch mithilfe von IAM ändern. Weitere Informationen finden Sie unter Bearbeiten einer Service-Linked Rolle im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Amazon DocumentDB DocumentDB-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 alle Ihre -Cluster löschen, bevor Sie die serviceverknüpfte Rolle löschen können.

Bereinigen einer serviceverknüpften Rolle mit Amazon DocumentDB

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 über die Konsole, ob die servicegebundene Rolle eine aktive Sitzung hat:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die IAM-Konsole unter. https://console.aws.amazon.com/iam/
2. Wählen Sie im Navigationsbereich der IAM-Konsole Rollen und dann den Namen (nicht das Kontrollkästchen) der AWSServiceRoleForRDSRolle aus.

3. Wählen Sie auf der Seite Summary für die ausgewählte Rolle die Registerkarte Access Advisor.
4. Überprüfen Sie auf der Registerkarte Access Advisor (Advisor aufrufen) die jüngsten Aktivitäten für die serviceverknüpfte Rolle.

> **Note**
>
> Wenn Sie sich nicht sicher sind, ob Amazon DocumentDB die AWSServiceRoleForRDS Rolle verwendet, können Sie versuchen, die Rolle zu löschen. Wenn der Service die Rolle verwendet, schlägt die Löschung fehl und Sie können die -Regionen 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. Die Sitzung für eine serviceverknüpfte Rolle können Sie nicht widerrufen.

Wenn Sie die AWSServiceRoleForRDS Rolle entfernen möchten, müssen Sie zuerst alle Ihre Instances und Cluster löschen. Informationen zum Löschen von Instances und Clustern finden Sie in den folgenden Themen:

- Löschen einer Amazon DocumentDB DocumentDB-Instance
- Löschen eines Amazon DocumentDB-Clusters

Unterstützte Regionen für serviceverknüpfte Amazon DocumentDB DocumentDB-Rollen

Amazon DocumentDB unterstützt die Verwendung von serviceverknüpften Rollen in allen Regionen, in denen der Service verfügbar ist. Weitere Informationen finden Sie unter https://docs.aws.amazon.com/documentdb/latest/devguide/regions-and-azs.html#regions-and-azs-availability.

Change-Streams mit Amazon DocumentDB verwenden

Die Change-Streams-Funktion in Amazon DocumentDB (mit MongoDB-Kompatibilität) bietet eine zeitlich geordnete Abfolge von Änderungsereignissen, die in den Sammlungen Ihres Clusters auftreten. Sie können Ereignisse aus einem Change Stream lesen, um zahlreiche verschiedene Anwendungsfälle zu implementieren, einschließlich:

- Änderungsbenachrichtigung
- Full-text Suche mit Amazon OpenSearch Service (OpenSearch Service)
- Analytik mit Amazon Redshift

Anwendungen können Änderungsstreams verwenden, um Datenveränderungen bei individuellen Sammlungen zu abonnieren. Die Ereignisse werden in Change Streams in der Reihenfolge angeordnet, wie sie im Cluster auftreten, und nach der Aufzeichnung des Ereignisses 3 Stunden (Standardeinstellung) gespeichert. Die Aufbewahrungsfrist kann mithilfe des `change_stream_log_retention_duration` Parameters auf bis zu 7 Tage verlängert werden. Informationen zum Ändern der Aufbewahrungsdauer für Change-Stream-Protokolle finden Sie unter Ändern der Aufbewahrungsdauer für das Change-Stream-Protokoll.

Themen

- Unterstützte Vorgänge
- Fakturierung
- Einschränkungen
- Change-Streams aktivieren
- Beispiel: Change-Streams mit Python verwenden
- Vollständige Suche nach Dokumenten
- Wiederaufnahme eines Change-Streams
- Wiederaufnahme eines Change-Streams mit Start AtOperationTime
- Wiederaufnahme eines Change-Streams mit Post BatchResumeToken
- Transaktionen in Change-Streams
- Änderung der Aufbewahrungsdauer des Change-Stream-Protokolls
- Verwendung von Change-Streams auf sekundären Instanzen

Unterstützte Vorgänge

Amazon DocumentDB unterstützt die folgenden Operationen für Change-Streams:

- Alle Änderungsereignisse werden in der MongoDB `db.collection.watch()` `db.watch()` und der `client.watch()` API unterstützt.
- Vollständige Dokumentsuche nach Aktualisierungen.

- Aggregationsphasen:`$match`, `$project``$redact`, und und`$addFields`. `$replaceRoot`
- Einen Change-Stream von einem Resume-Token aus fortsetzen
- Wiederaufnahme eines Change-Streams aus einem Zeitstempel mit `startAtOperation` (gilt für Amazon DocumentDB 4.0+)

Fakturierung

Die Amazon DocumentDB DocumentDB-Funktion zum Ändern von Streams ist standardmäßig deaktiviert und es fallen keine zusätzlichen Gebühren an, bis die Funktion aktiviert ist. Die Verwendung von Change-Streams in einem Cluster verursacht zusätzliche Lese- und Schreib-IOs sowie Speicherkosten. Sie können den `modifyChangeStreams` API-Vorgang verwenden, um diese Funktion für Ihren Cluster zu aktivieren. Weitere Informationen zur Preisgestaltung finden Sie unter Amazon DocumentDB DocumentDB-Preise.

Einschränkungen

Für Change-Streams gelten in Amazon DocumentDB die folgenden Einschränkungen:

- Auf Amazon DocumentDB 3.6 und Amazon DocumentDB 4.0 können Change-Streams nur über eine Verbindung zur primären Instance eines Amazon DocumentDB-Clusters geöffnet werden. Das Lesen aus Change-Streams auf einer Replikat-Instance wird in Amazon DocumentDB 3.6 und Amazon DocumentDB 4.0 nicht unterstützt. Beim Aufruf der API-Operation `watch()` müssen Sie die Leseeinstellung `primary` angeben, um sicherzustellen, dass alle Lesevorgänge an die primäre Instance weitergeleitet werden (siehe den Abschnitt Beispiel).
- In Amazon DocumentDB 5.0 können Change-Streams sowohl von primären Instances als auch von sekundären Instances, einschließlich globaler Cluster, geöffnet werden. Sie können eine sekundäre Lesepräferenz angeben, um die Change-Streams an sekundäre Instances umzuleiten. Verwendung von Change-Streams auf sekundären InstanzenWeitere bewährte Methoden und Einschränkungen finden Sie unter.
- Ereignisse, die in einen Change-Stream für eine Sammlung geschrieben wurden, sind bis zu 7 Tage lang verfügbar (die Standardeinstellung ist 3 Stunden). Änderungsstream-Daten werden nach dem Zeitfenster der Protokollaufbewahrungsdauer gelöscht, auch wenn keine neuen Änderungen vorgenommen wurden.
- Eine über längere Zeit für eine Sammlung ausgeführte Schreiboperation wie `updateMany` oder `deleteMany` kann das Schreiben von Change Stream-Ereignissen vorübergehend bis zum Abschluss der über längere Zeit ausgeführten Schreiboperation blockieren.

- Amazon DocumentDB unterstützt das MongoDB-Betriebsprotokoll () `oplog` nicht.
- Bei Amazon DocumentDB müssen Sie Change-Streams für eine bestimmte Sammlung explizit aktivieren.
- Wenn die Gesamtgröße eines Change Stream-Ereignisses (einschließlich der Änderungsdaten und des vollständigen Dokuments, wenn angefordert) größer als 16 `MB` ist, tritt auf dem Client ein Lesefehler für die Change Streams auf.
- Der Ruby-Treiber wird derzeit nicht unterstützt, wenn `db.watch()` und `client.watch()` mit Amazon DocumentDB 3.6 verwendet wird.
- Die Ausgabe des `updateDescription` Befehls in Change-Streams unterscheidet sich in Amazon DocumentDB von der in MongoDB, wenn der aktualisierte Wert des Felds derselbe ist wie der vorherige:
  - Amazon DocumentDB gibt kein Feld in der `updateDescription` Ausgabe zurück, wenn das angegebene Feld im `$set` Befehl angegeben ist und sein Zielwert bereits dem Quellwert entspricht.
  - MongoDB gibt das Feld in der Ausgabe zurück, auch wenn der angegebene Wert dem aktuellen Wert entspricht.

Change-Streams aktivieren

Sie können Amazon DocumentDB DocumentDB-Change-Streams für alle Sammlungen innerhalb einer bestimmten Datenbank oder nur für ausgewählte Sammlungen aktivieren. Im Folgenden finden Sie Beispiele für die Aktivierung von Change Streams für verschiedene Anwendungsfälle über die Mongo-Shell. Leere Zeichenfolgen werden bei der Angabe von Datenbank- und Sammlungsnamen als Platzhalter behandelt.

```
//Enable change streams for the collection "foo" in database "bar"
db.adminCommand({modifyChangeStreams: 1,
    database: "bar",
    collection: "foo",
    enable: true});
```

```
//Disable change streams on collection "foo" in database "bar"
db.adminCommand({modifyChangeStreams: 1,
    database: "bar",
    collection: "foo",
    enable: false});
```

```
//Enable change streams for all collections in database "bar"
db.adminCommand({modifyChangeStreams: 1,
    database: "bar",
    collection: "",
    enable: true});
```

```
//Enable change streams for all collections in all databases in a cluster
db.adminCommand({modifyChangeStreams: 1,
    database: "",
    collection: "",
    enable: true});
```

Change Streams werden für eine Sammlung aktiviert, wenn eine der folgenden Bedingungen erfüllt ist:

- Sowohl die Datenbank als auch die Sammlung sind explizit aktiviert.
- Die Datenbank, die die Sammlung enthält, ist aktiviert.
- Alle Datenbanken sind aktiviert.

Wenn Sie eine Sammlung aus einer Datenbank löschen, werden Change Streams für diese Sammlung nicht deaktiviert, wenn Change Streams für die übergeordnete Datenbank auch aktiviert sind oder wenn alle Datenbanken im Cluster aktiviert sind. Wenn eine neue Sammlung mit demselben Namen wie die gelöschte Sammlung erstellt wird, werden Change Streams für diese Sammlung aktiviert.

Sie können alle aktivierten Change Streams Ihres Clusters mithilfe der `$listChangeStreams`-Aggregationspipeline-Phase auflisten. Alle von Amazon DocumentDB unterstützten Aggregationsphasen können in der Pipeline für die weitere Verarbeitung verwendet werden. Wenn eine zuvor aktivierte Sammlung deaktiviert wurde, wird sie nicht in der `$listChangeStreams`-Ausgabe angezeigt.

```
//List all databases and collections with change streams enabled
cursor = new DBCommandCursor(db,
    db.runCommand(
        {aggregate: 1,
        pipeline: [{$listChangeStreams: 1}],
        cursor:{}}));
```

```
//List of all databases and collections with change streams enabled
{ "database" : "test", "collection" : "foo" }
{ "database" : "bar", "collection" : "" }
{ "database" : "", "collection" : "" }
```

```
//Determine if the database “bar” or collection “bar.foo” have change streams enabled
cursor = new DBCommandCursor(db,
  db.runCommand(
      {aggregate: 1,
       pipeline: [{$listChangeStreams: 1},
                  {$match: {$or: [{database: "bar", collection: "foo"},
                                  {database: "bar", collection: ""},
                                  {database: "", collection: ""}]}}
                 ],
      cursor:{}}));
```

Beispiel: Change-Streams mit Python verwenden

Im Folgenden finden Sie ein Beispiel für die Verwendung eines Amazon DocumentDB DocumentDB-Change-Streams mit Python auf Sammlungsebene.

```
import os
import sys
from pymongo import MongoClient, ReadPreference

username = "DocumentDBusername"
password = <Insert your password>

clusterendpoint = "DocumentDBClusterEndpoint”
client = MongoClient(clusterendpoint, username=username, password=password, tls='true',
 tlsCAFile='global-bundle.pem')

db = client['bar']

#While ‘Primary’ is the default read preference, here we give an example of
#how to specify the required read preference when reading the change streams
coll = db.get_collection('foo', read_preference=ReadPreference.PRIMARY)
#Create a stream object
stream = coll.watch()
#Write a new document to the collection to generate a change event
coll.insert_one({'x': 1})
#Read the next change event from the stream (if any)
```

```
print(stream.try_next())

"""
Expected Output:
{'_id': {'_data': '015daf94f600000002010000000200009025'},
'clusterTime': Timestamp(1571788022, 2),
'documentKey': {'_id': ObjectId('5daf94f6ea258751778163d6')},
'fullDocument': {'_id': ObjectId('5daf94f6ea258751778163d6'), 'x': 1},
'ns': {'coll': 'foo', 'db': 'bar'},
'operationType': 'insert'}
"""

#A subsequent attempt to read the next change event returns nothing, as there are no
 new changes
print(stream.try_next())

"""
Expected Output:
None
"""

#Generate a new change event by updating a document
result = coll.update_one({'x': 1}, {'$set': {'x': 2}})
print(stream.try_next())

"""
Expected Output:
{'_id': {'_data': '015daf99d400000001010000000100009025'},
'clusterTime': Timestamp(1571789268, 1),
'documentKey': {'_id': ObjectId('5daf9502ea258751778163d7')},
'ns': {'coll': 'foo', 'db': 'bar'},
'operationType': 'update',
'updateDescription': {'removedFields': [], 'updatedFields': {'x': 2}}}
"""
```

Im Folgenden finden Sie ein Beispiel für die Verwendung eines Amazon DocumentDB DocumentDB-Change-Streams mit Python auf Datenbankebene.

```
import os
import sys
from pymongo import MongoClient

username = "DocumentDBusername"
```

```
password = <Insert your password>
clusterendpoint = "DocumentDBClusterEndpoint”
client = MongoClient(clusterendpoint, username=username, password=password, tls='true',
 tlsCAFile='global-bundle.pem')

db = client['bar']
#Create a stream object
stream = db.watch()
coll = db.get_collection('foo')
#Write a new document to the collection foo to generate a change event
coll.insert_one({'x': 1})

#Read the next change event from the stream (if any)
print(stream.try_next())

"""
Expected Output:
{'_id': {'_data': '015daf94f600000002010000000200009025'},
'clusterTime': Timestamp(1571788022, 2),
'documentKey': {'_id': ObjectId('5daf94f6ea258751778163d6')},
'fullDocument': {'_id': ObjectId('5daf94f6ea258751778163d6'), 'x': 1},
'ns': {'coll': 'foo', 'db': 'bar'},
'operationType': 'insert'}
"""
#A subsequent attempt to read the next change event returns nothing, as there are no
 new changes
print(stream.try_next())

"""
Expected Output:
None
"""

coll = db.get_collection('foo1')

#Write a new document to another collection to generate a change event
coll.insert_one({'x': 1})
print(stream.try_next())

"""
Expected Output: Since the change stream cursor was the database level you can see
 change events from different collections in the same database
{'_id': {'_data': '015daf94f600000002010000000200009025'},
'clusterTime': Timestamp(1571788022, 2),
```

```
'documentKey': {'_id': ObjectId('5daf94f6ea258751778163d6')},
'fullDocument': {'_id': ObjectId('5daf94f6ea258751778163d6'), 'x': 1},
'ns': {'coll': 'foo1', 'db': 'bar'},
'operationType': 'insert'}
"""
```

Vollständige Suche nach Dokumenten

Das Änderungsereignis „Aktualisierung“ enthält nicht das vollständige Dokument, sondern lediglich die ausgeführte Änderung. Wenn für Ihren Anwendungsfall das vollständige Dokument erforderlich ist, das von einer Aktualisierung betroffen ist, können Sie beim Öffnen des Datenstroms die vollständige Dokumentsuche aktivieren.

Das `fullDocument`-Dokument für ein Update-Change Stream-Ereignis stellt die neueste Version des aktualisierten Dokuments zum Zeitpunkt der Dokumentsuche dar. Wenn zwischen der Aktualisierungsoperation und der `fullDocument`-Suche Änderungen ausgeführt wurden, besitzt das `fullDocument`-Dokument möglicherweise nicht den Dokumentstatus zur Aktualisierungszeit.

Verwenden Sie dieses Beispiel, um ein Stream-Objekt mit aktivierter Aktualisierungssuche zu erstellen:

```
stream = coll.watch(full_document='updateLookup')

#Generate a new change event by updating a document
result = coll.update_one({'x': 2}, {'$set': {'x': 3}})

stream.try_next()
```

Die Ausgabe des Stream-Objekts sieht ungefähr so aus:

```
{'_id': {'_data': '015daf9b7c000000101000000100009025'},
'clusterTime': Timestamp(1571789692, 1),
'documentKey': {'_id': ObjectId('5daf9502ea258751778163d7')},
'fullDocument': {'_id': ObjectId('5daf9502ea258751778163d7'), 'x': 3},
'ns': {'coll': 'foo', 'db': 'bar'},
'operationType': 'update',
'updateDescription': {'removedFields': [], 'updatedFields': {'x': 3}}}
```

Wiederaufnahme eines Change-Streams

Sie können einen Change Stream zu einem späteren Zeitpunkt mithilfe eines Fortsetzungs-Tokens fortsetzen, das dem Feld `_id` des zuletzt abgerufenen Änderungsereignisdokuments entspricht.

```
import os
import sys
from pymongo import MongoClient

username = "DocumentDBusername"
password = <Insert your password>
clusterendpoint = "DocumentDBClusterEndpoint”
client = MongoClient(clusterendpoint, username=username, password=password, tls='true',
 tlsCAFile='global-bundle.pem', retryWrites='false')

db = client['bar']
coll = db.get_collection('foo')
#Create a stream object
stream = db.watch()
coll.update_one({'x': 1}, {'$set': {'x': 4}})
event = stream.try_next()
token = event['_id']
print(token)

"""
Output: This is the resume token that we will later us to resume the change stream
{'_data': '015daf9c5b0000000101000000100009025'}
"""
#Python provides a nice shortcut for getting a stream’s resume token
print(stream.resume_token)

"""
Output
{'_data': '015daf9c5b0000000101000000100009025'}
"""
#Generate a new change event by updating a document
result = coll.update_one({'x': 4}, {'$set': {'x': 5}})
#Generate another change event by inserting a document
result = coll.insert_one({'y': 5})
#Open a stream starting after the selected resume token
stream = db.watch(full_document='updateLookup', resume_after=token)
#Our first change event is the update with the specified _id
print(stream.try_next())
```

```
"""
#Output: Since we are resuming the change stream from the resume token, we will see all
 events after the first update operation. In our case, the change stream will resume
 from the update operation {x:5}

{'_id': {'_data': '015f7e8f0c0000000601000000006000fe038'},
'operationType': 'update',
'clusterTime': Timestamp(1602129676, 6),
'ns': {'db': 'bar', 'coll': 'foo'},
'documentKey': {'_id': ObjectId('5f7e8f0ac423bafbfd9adba2')},
'fullDocument': {'_id': ObjectId('5f7e8f0ac423bafbfd9adba2'), 'x': 5},
'updateDescription': {'updatedFields': {'x': 5}, 'removedFields': []}}
"""
#Followed by the insert
print(stream.try_next())

"""
#Output:
{'_id': {'_data': '015f7e8f0c0000000701000000007000fe038'},
'operationType': 'insert',
'clusterTime': Timestamp(1602129676, 7),
'ns': {'db': 'bar', 'coll': 'foo'},
'documentKey': {'_id': ObjectId('5f7e8f0cbf8c233ed577eb94')},
'fullDocument': {'_id': ObjectId('5f7e8f0cbf8c233ed577eb94'), 'y': 5}}
"""
```

Wiederaufnahme eines Change-Streams mit Start AtOperationTime

Sie können einen Änderungsstream zu einem späteren Zeitpunkt ab einem bestimmten Zeitstempel wieder aufnehmen, indem Sie `startAtOperationTime`

> **Note**
>
> Die Fähigkeit zur Verwendung `startAtOperationTime` ist in Amazon DocumentDB 4.0+ verfügbar. Bei Verwendung `startAtOperationTime` gibt der Change-Stream-Cursor nur Änderungen zurück, die zu oder nach dem angegebenen Zeitstempel vorgenommen wurden. Die `resumeAfter` Befehle `startAtOperationTime` und schließen sich gegenseitig aus und können daher nicht zusammen verwendet werden.

```
import os
import sys
from pymongo import MongoClient

username = "DocumentDBusername"
password = <Insert your password>
clusterendpoint = "DocumentDBClusterEndpoint”
client = MongoClient(clusterendpoint, username=username, password=password, tls='true',
 tlsCAFile='rds-root-ca-2020.pem',retryWrites='false')
db = client['bar']
coll = db.get_collection('foo')
#Create a stream object
stream = db.watch()
coll.update_one({'x': 1}, {'$set': {'x': 4}})
event = stream.try_next()
timestamp = event['clusterTime']
print(timestamp)
"""
Output
Timestamp(1602129114, 4)
"""
#Generate a new change event by updating a document
result = coll.update_one({'x': 4}, {'$set': {'x': 5}})
result = coll.insert_one({'y': 5})
#Generate another change event by inserting a document
#Open a stream starting after specified time stamp

stream = db.watch(start_at_operation_time=timestamp)
print(stream.try_next())

"""
#Output: Since we are resuming the change stream at the time stamp of our first update
 operation (x:4), the change stream cursor will point to that event
{'_id': {'_data': '015f7e941a0000000301000000003000fe038'},
'operationType': 'update',
'clusterTime': Timestamp(1602130970, 3),
'ns': {'db': 'bar', 'coll': 'foo'},
'documentKey': {'_id': ObjectId('5f7e9417c423bafbfd9adbb1')},
'updateDescription': {'updatedFields': {'x': 4}, 'removedFields': []}}
"""

print(stream.try_next())
"""
```

```
#Output: The second event will be the subsequent update operation (x:5)
{'_id': {'_data': '015f7e9502000000050100000005000fe038'},
'operationType': 'update',
'clusterTime': Timestamp(1602131202, 5),
'ns': {'db': 'bar', 'coll': 'foo'},
'documentKey': {'_id': ObjectId('5f7e94ffc423bafbfd9adbb2')},
'updateDescription': {'updatedFields': {'x': 5}, 'removedFields': []}}
"""

print(stream.try_next())

"""
#Output: And finally the last event will be the insert operation (y:5)
{'_id': {'_data': '015f7e9502000000060100000006000fe038'},
'operationType': 'insert',
'clusterTime': Timestamp(1602131202, 6),
'ns': {'db': 'bar', 'coll': 'foo'},
'documentKey': {'_id': ObjectId('5f7e95025c4a569e0f6dde92')},
'fullDocument': {'_id': ObjectId('5f7e95025c4a569e0f6dde92'), 'y': 5}}
"""
```

Wiederaufnahme eines Change-Streams mit Post BatchResumeToken

Der Amazon DocumentDB DocumentDB-Change-Stream gibt jetzt ein zusätzliches Feld namens `postBatchResumeToken` zurück. Dieses Feld wird von dem `$changestream` Befehl und `getMore` dem Befehl zurückgegeben.

Beispiel für den `$changestream` Befehl in Python:

```
db.command({"aggregate": "sales", "pipeline": [{ "$changeStream": {}}], "cursor":
 {"batchSize": 1}})
```

Erwartete Ausgabe:

```
cursor" : {
   "firstBatch" : [ ],
   "postBatchResumeToken" : {"_data" : "0167c8cbe60000000004"},
   "id" : NumberLong("9660788144470"),
   "ns" : "test.sales"
}
```

Beispiel für den `getMore` Befehl in Python:

```
db.command({"getMore": NumberLong(<cursor id>), "collection": "sales", "batchSize":
 1 })
```

Erwartete Ausgabe

```
cursor" : {
   "nextBatch" : [ ],
   "postBatchResumeToken" : {"_data" : "0167c8cbe60000000004"},
   "id" : NumberLong("9660788144470"),
   "ns" : "test.sales"
}
```

Das `postBatchResumeToken` Feld kann verwendet werden, um neue Change-Stream-Cursor im `resumeAfter` Feld zu öffnen, ähnlich wie das Resume-Token verwendet wird.

Öffnet einen Stream, der nach dem ausgewählten `postBatchResumeToken` beginnt:

```
post_batch_resume_token = output['cursor']['postBatchResumeToken']
stream = db.watch(full_document='updateLookup', resume_after=post_batch_resume_token)
```

Im Gegensatz zu einem regulären Resume-Token, das immer einem Operationsprotokolleintrag (Oplog) entspricht, der ein aktuelles Ereignis widerspiegelt, `postBatchResumeToken` entspricht dies einem Oplog-Eintrag, bis zu dem der Change-Stream auf dem Server gescannt hat. Dabei handelt es sich nicht unbedingt um eine entsprechende Änderung.

Der Versuch, den Vorgang mit einem alten regulären Resume-Token fortzusetzen, zwingt die Datenbank, alle Oplog-Einträge zwischen dem angegebenen Zeitstempel und der aktuellen Uhrzeit zu scannen. Dadurch können intern viele Abfragen generiert werden, wobei jede Unterabfrage für einen kurzen Zeitraum gescannt wird. Dies führt zu einem Anstieg der CPU-Auslastung und beeinträchtigt die Datenbankleistung. Wenn Sie mit dem letzten `postBatchResumeToken` Schritt fortfahren, wird das Scannen nicht übereinstimmender Protokolleinträge übersprungen.

Transaktionen in Change-Streams

Change-Stream-Ereignisse enthalten keine Ereignisse aus nicht bestätigten, and/or abgebrochenen Transaktionen. Wenn Sie beispielsweise eine Transaktion mit einem Vorgang und einem `INSERT` Vorgang starten und Ihr `UPDATE` Vorgang erfolgreich ist, der `INSERT` `UPDATE` Vorgang jedoch

fehlschlägt, wird die Transaktion zurückgesetzt. Da diese Transaktion zurückgesetzt wurde, enthält Ihr Change-Stream keine Ereignisse für diese Transaktion.

Änderung der Aufbewahrungsdauer des Change-Stream-Protokolls

Sie können die Aufbewahrungsdauer für das Change-Stream-Protokoll so ändern, dass sie zwischen 1 Stunde und 7 Tagen liegt, indem Sie die Taste AWS-Managementkonsole oder die verwenden AWS CLI.

Using the AWS-Managementkonsole

So ändern Sie den Aufbewahrungszeitraum für das Change-Stream-Protokoll

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Wählen Sie im Navigationsbereich Parameter groups (Parametergruppen) aus.

   > **Tip**
   >
   > Wenn der Navigationsbereich auf der linken Seite des Bildschirms nicht angezeigt wird, wählen Sie links oben auf der Seite das Menüsymbol (≡) aus.

3. Wählen Sie im Bereich Parameter groups (Parametergruppen) die Cluster-Parametergruppe, die Ihrem Cluster zugeordnet ist. Informationen zum Identifizieren der Clusterparametergruppe, die dem Cluster zugeordnet ist, finden Sie unter Ermitteln der Parametergruppe eines Amazon DocumentDB-Clusters.
4. Auf der resultierenden Seite werden die Parameter und die entsprechenden Details zu Ihrer Cluster-Parametergruppe angezeigt. Wählen Sie den `change_stream_log_retention_duration`-Parameter aus.
5. Klicken Sie oben rechts auf der Seite auf Edit (Bearbeiten), um den Wert des Parameters zu ändern. Der `change_stream_log_retention_duration` Parameter kann so geändert werden, dass er zwischen 1 Stunde und 7 Tagen liegt.
6. Führen Sie die Änderung aus. Wählen Sie anschließend Modify cluster parameter (Cluster-Parameter ändern) aus, um die Änderungen zu speichern. Um die Änderungen zu verwerfen, wählen Sie Cancel (Abbrechen) aus.

Using the AWS CLI

Um den `change_stream_log_retention_duration`-Parameter Ihrer Cluster-Parametergruppe zu ändern, verwenden Sie die `modify-db-cluster-parameter-group`-Operation mit den folgenden Parametern:

- **`--db-cluster-parameter-group-name`** – Erforderlich. Der Name der Cluster-Parametergruppe, die Sie ändern. Informationen zum Identifizieren der Clusterparametergruppe, die dem Cluster zugeordnet ist, finden Sie unter Ermitteln der Parametergruppe eines Amazon DocumentDB-Clusters.
- **`--parameters`** – Erforderlich. Der Parameter, der von Ihnen geändert wird. Jeder Parametereintrag muss Folgendes enthalten:
  - **`ParameterName`**— Der Name des Parameters, den Sie ändern. In diesem Fall ist es `change_stream_log_retention_duration`
  - **`ParameterValue`**— Der neue Wert für diesen Parameter.
  - **`ApplyMethod`**— Wie die Änderungen an diesem Parameter angewendet werden sollen. Zugelassene Werte sind `immediate` und `pending-reboot`.

> **Note**
>
> Parameter mit dem `ApplyType` von `static` müssen über einen `ApplyMethod` von `pending-reboot` verfügen.

1. Um die Werte des Parameters `change_stream_log_retention_duration` zu ändern, führen Sie den folgenden Befehl aus und ersetzen `parameter-value` durch den Wert, auf den Sie den Parameter ändern möchten.

   Für Linux, macOS oder Unix:

   ```
   aws docdb modify-db-cluster-parameter-group \
       --db-cluster-parameter-group-name sample-parameter-group \
       --parameters
    "ParameterName=change_stream_log_retention_duration,ParameterValue=<parameter-
   value>,ApplyMethod=immediate"
   ```

   Für Windows:

```
aws docdb modify-db-cluster-parameter-group ^
    --db-cluster-parameter-group-name sample-parameter-group ^
    --parameters
 "ParameterName=change_stream_log_retention_duration,ParameterValue=<parameter-
value>,ApplyMethod=immediate"
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus (JSON-Format).

```
{
    "DBClusterParameterGroupName": "sample-parameter-group"
}
```

2. Warten Sie mindestens 5 Minuten.
3. Listen Sie die Parameterwerte von `sample-parameter-group` auf, um sicherzustellen, dass Ihre Änderungen übernommen wurden.

   Für Linux, macOS oder Unix:

```
aws docdb describe-db-cluster-parameters \
    --db-cluster-parameter-group-name sample-parameter-group
```

   Für Windows:

```
aws docdb describe-db-cluster-parameters ^
    --db-cluster-parameter-group-name sample-parameter-group
```

   Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus (JSON-Format).

```
{
    "Parameters": [
        {
            "ParameterName": "audit_logs",
            "ParameterValue": "disabled",
            "Description": "Enables auditing on cluster.",
            "Source": "system",
            "ApplyType": "dynamic",
            "DataType": "string",
            "AllowedValues": "enabled,disabled",
            "IsModifiable": true,
```

```
            "ApplyMethod": "pending-reboot"
        },
        {
            "ParameterName": "change_stream_log_retention_duration",
            "ParameterValue": "12345",
            "Description": "Duration of time in seconds that the change stream
 log is retained and can be consumed.",
            "Source": "user",
            "ApplyType": "dynamic",
            "DataType": "integer",
            "AllowedValues": "3600-86400",
            "IsModifiable": true,
            "ApplyMethod": "immediate"
        }
    ]
}
```

> **Note**
>
> Bei der Aufbewahrung von Change-Stream-Protokollen werden Protokolle, die älter als der konfigurierte `change_stream_log_retention_duration` Wert sind, erst gelöscht, wenn die Protokollgröße größer als (>) 51.200 MB ist.

Verwendung von Change-Streams auf sekundären Instanzen

Um mit der Verwendung von Change Stream auf sekundären Instances zu beginnen, öffnen Sie den Change-Stream-Cursor `readPreference` als sekundäre Instanz.

Sie können einen Change-Stream-Cursor öffnen, um nach Änderungsereignissen in einer bestimmten Sammlung oder allen Sammlungen in einem Cluster oder einer Datenbank Ausschau zu halten. Sie können einen Change-Stream-Cursor auf jeder Amazon DocumentDB DocumentDB-Instance öffnen und Change-Stream-Dokumente sowohl von Writer- als auch von Reader-Instances abrufen. Sie können Change-Stream-Tokens (wie `resumeToken` oder`startOperationTime`) für verschiedene Change-Stream-Cursors, die auf einer Writer- und Reader-Instance geöffnet sind, gemeinsam nutzen.

Beispiel

```
import os
```

```
import sys
from pymongo import MongoClient, ReadPreference

username = "DocumentDBusername"
password = <Your password>

clusterendpoint = "DocumentDBClusterEndpoint"

client = MongoClient(clusterendpoint, username=username, password=password, tls='true',
 tlsCAFile='global-bundle.pem')

db = client['bar']

# Make sure to use SECONDARY to redirect cursor reads from secondary instances
coll = db.get_collection('foo', read_preference=ReadPreference.SECONDARY)

# Create a stream object on RO. The token needs to generated from PRIMARY.
stream = coll.watch(resumeAfter=token)

for event in stream:
   print(event)
```

Richtlinien und Einschränkungen für Change-Streams auf sekundären Instanzen

- Change-Stream-Ereignisse müssen von der primären Instance auf die sekundären Instances repliziert werden. Sie können die Verzögerung anhand der `DBInstanceReplicaLag` Metrik in Amazon überwachen CloudWatch.
- Zeitstempel auf sekundären Instances stimmen möglicherweise nicht immer mit denen der primären Instance überein. In diesem Fall müssen Sie mit Verzögerungen beim Zeitstempel der sekundären Instanz rechnen, damit diese aufholen kann. Als bewährte Methode empfehlen wir, die Überwachung auf der sekundären Instanz `resumeToken` zu verwenden `startAtOperationTime` oder zu starten.
- Auf sekundären Instanzen kann es zu einem geringeren Durchsatz kommen als auf der primären Instanz, wenn Ihr Dokument groß ist, Sie dies tun`fullDocumentLookup`, und auf der primären Instanz eine hohe Arbeitslast beim gleichzeitigen Schreiben anfällt. Als bewährte Methode empfehlen wir, die Trefferquote im Puffercache auf der sekundären Ebene zu überwachen und sicherzustellen, dass die Trefferquote im Puffercache hoch ist.

Verwenden der Sortierung in Amazon DocumentDB 8.0

Amazon DocumentDB 8.0 unterstützt jetzt die Sortierung. Die Sortierung ermöglicht es Ihnen, sprachspezifische Regeln für den Zeichenkettenvergleich zu konfigurieren. Mit der Sortierung können Sie Regeln für Vergleiche unter Berücksichtigung der Groß- und Kleinschreibung oder ein Sprachgebietsschema angeben. Die Sortierung kann in DocumentDB 8.0 auf Sammlungs- oder Indexebene konfiguriert werden. Wenn Sie die Sortierung in DocumentDB verwenden, wird intern ein Kollatierungsdokument mit den folgenden Parametern erstellt.

```
{
locale: string,
caseLevel: boolean,
caseFirst: string,
strength: int,
numericOrdering: boolean,
alternate: string,
maxVariable: string,
backwards: boolean,
normalization: boolean
}
```

Einschränkungen

Für die Sortierung gelten in Amazon DocumentDB die folgenden Einschränkungen:

- Die Sortierung ist mit Planner v3 kompatibel, das in Amazon DocumentDB 8.0 verfügbar ist. Der Wechsel zu Plannerv2 oder Plannerv1 kann zu inkonsistentem Verhalten führen, einschließlich der Fehlermeldung „Index nicht gefunden“.
- Wenn eine Mongodb-Sammlung mit Sortierung exportiert wird, müssen Sie aufgrund inhärenter Bibliotheksunterschiede die Dateien metadata.bson aktualisieren und ihre Version vor der Migration von 57.1 auf 60.2 ändern.
- In seltenen Fällen können Ihre Sortierungseinstellungen das interne Limit für die Zeichenanzahl überschreiten und den folgenden Fehler verursachen. „Fehler: Das Sortierungsdokument enthält nicht standardmäßige Attribute, die mehr als unterstützt werden. Bitte reduzieren Sie die Anzahl der Optionen.“ Versuchen Sie in diesem Fall, die Optionen, die Sie im Kollationsdokument angeben, zu reduzieren, oder versuchen Sie, wo immer möglich, Standardwerte zu verwenden.

Verwenden von Ansichten in Amazon DocumentDB 8.0

- Amazon DocumentDB 8.0 unterstützt jetzt Ansichten. Ansichten funktionieren als virtuelle Sammlungen, die Daten basierend auf bestimmten Aggregationsvorgängen präsentieren. Wenn Sie eine Ansicht erstellen, definieren Sie eine Abfrage, die Daten aus einer oder mehreren Quellensammlungen transformiert. Amazon DocumentDB 8.0 führt diese Abfrage bei jedem Zugriff auf die Ansicht aus, ohne zusätzliche Speicherressourcen zu verbrauchen. Im Gegensatz zu Standardsammlungen speichern Ansichten in Amazon DocumentDB 8.0 keine Dokumente auf der Festplatte, was sie zu einer effizienten Lösung für die Präsentation transformierter oder gefilterter Daten für Anwendungen macht. Um eine Ansicht in Amazon DocumentDB zu erstellen, können Sie den Befehl createView oder die Hilfsmethode db.createView () verwenden:

```
db.createView("viewName","sourceCollection",
[
    { $match: { status: "active" } },
    { $project: { _id: 1, name: 1, email: 1 } }
]
)
```

  Dadurch wird eine Ansicht mit dem Namen „ViewName“ erstellt, die auf „sourceCollection“ basiert und nur aktive Dokumente und Projekte enthält, nur die Felder _id, name und email. Ansichten in Amazon DocumentDB sind schreibgeschützt. Schreibvorgänge an Ansichten geben einen Fehler zurück. Für eine optimale Leistung bei großen Datensätzen können Sie Ihre View-Pipelines so strukturieren, dass die Effizienz maximiert wird. Bei komplexen Aggregationspipelines wird empfohlen, die $match-Stufe als erste Phase oder zu Beginn der Pipeline zu verwenden, um die Anzahl der Dokumente zu reduzieren, die in den nachfolgenden Phasen verarbeitet werden müssen, und so die Abfrageleistung zu verbessern.

Bewährte Methoden

Nachfolgend sind einige bewährte Methoden aufgeführt, die Sie bei Views anwenden sollten.

- Früh filtern: Verwenden Sie $match-Stufen zu einem frühen Zeitpunkt in View-Pipelines, um die Menge der verarbeiteten Daten zu reduzieren.

- Vermeiden Sie komplexe Aggregationen: Für häufig aufgerufene Ansichten mit komplexen Aggregationen sollten Sie erwägen, eine separate Sammlung mit vorab berechneten Ergebnissen zu erstellen, die regelmäßig aktualisiert werden.
- Indexplanung: Stellen Sie sicher, dass Felder, die in View-Pipelines verwendet werden, insbesondere bei $match- und $sort-Vorgängen, in der Quellsammlung ordnungsgemäß indexiert sind.
- Abfrageoptimierung: Verwenden Sie den Befehl explain, um zu verstehen, wie Ihre View-Abfragen ausgeführt werden, und um sie entsprechend zu optimieren.
- Alternativen für Ansichten: Angesichts der funktionalen Unterschiede zwischen Amazon DocumentDB- und MongoDB-Ansichten sollten Sie bei Einschränkungen die Verwendung regulärer Sammlungen mit geplanten Aktualisierungen als Alternative zu Ansichten in Betracht ziehen.

Kompatibilität mit Aggregator-Operatoren

Amazon DocumentDB unterstützt viele Aggregationsoperatoren in Ansichtsdefinitionen und erweitert gleichzeitig die Kompatibilität weiter. Konzentrieren Sie sich bei der Verwendung von Ansichten auf die folgenden unterstützten Operatoren:

- $match zum Filtern von Dokumenten
- $project für Feldauswahl und Transformation
- $addFields zum Hinzufügen von berechneten Feldern
- $sort für die Reihenfolge der Ergebnisse
- $limit und $skip für die Paginierung

Einige spezialisierte Operatoren wie $currentOp, $replaceRoot und $geoNear funktionieren derzeit eher in direkten Aggregationsabfragen als in Ansichtsdefinitionen.

Nutzung von Indizes und Ansichten

Ansichten in Amazon DocumentDB 8.0 verwenden die Indizes der zugrunde liegenden Sammlung. Daher können Sie Indizes für eine Ansicht nicht direkt erstellen, löschen oder neu erstellen. Gut entworfene Indizes für die Quellsammlung können jedoch die Leistung von Anzeigeabfragen erheblich verbessern. Nachfolgend finden Sie einige Schritte zur Optimierung der Abfrageleistung für Ansichten:

- Stellen Sie sicher, dass für die Felder der Quellsammlung, die in der Pipeline der Ansicht verwendet werden, geeignete Indizes vorhanden sind, insbesondere bei den Vorgängen $match und $sort
- Verwenden Sie die Methode explain (), um Ausführungspläne für Abfragen zu analysieren und die Indexnutzung zu überprüfen. E.g., `db.viewName.find({...}).explain()`

Verwenden AWS Lambda mit Change-Streams

Amazon DocumentDB ist integriert, AWS Lambda sodass Sie Lambda-Funktionen verwenden können, um Datensätze in einem Change-Stream zu verarbeiten. Die Zuordnung von Lambda-Ereignisquellen ist eine Ressource, mit der Lambda-Funktionen aufgerufen werden können, um Amazon DocumentDB DocumentDB-Ereignisse zu verarbeiten, die Lambda nicht direkt aufrufen. Mit Amazon DocumentDB Change Stream als Ereignisquelle können Sie ereignisgesteuerte Anwendungen erstellen, die auf Änderungen in Ihren Daten reagieren. Sie können Lambda-Funktionen beispielsweise verwenden, um neue Dokumente zu verarbeiten, Aktualisierungen vorhandener Dokumente nachzuverfolgen oder gelöschte Dokumente zu protokollieren.

Sie können eine Ereignisquellenzuordnung so konfigurieren, dass Datensätze aus Ihrem Amazon DocumentDB DocumentDB-Change-Stream an eine Lambda-Funktion gesendet werden. Ereignisse können einzeln oder gebündelt gesendet werden, um die Effizienz zu verbessern. Sie werden der Reihe nach verarbeitet. Sie können das Batchverhalten Ihrer Ereignisquellenzuordnung auf der Grundlage einer bestimmten Zeitfensterdauer (0-300 Sekunden) oder der Anzahl von Batch-Datensätzen (maximale Grenze von 10.000 Datensätzen) konfigurieren. Sie können mehrere Ereignisquellenzuordnungen erstellen, um dieselben Daten mit mehreren Lambda-Funktionen zu verarbeiten oder um unterschiedliche Elemente aus mehreren Streams mit einer einzigen Funktion zu verarbeiten.

Wenn Ihre Funktion einen Fehler zurückgibt, versucht Lambda den Batch erneut, bis er erfolgreich verarbeitet wurde. Falls die Ereignisse im Change-Stream abgelaufen sind, deaktiviert Lambda die Zuordnung der Ereignisquellen. In diesem Fall können Sie eine neue Zuordnung der Ereignisquelle erstellen und diese mit einer Startposition Ihrer Wahl konfigurieren. Lambda-Ereignisquellenzuordnungen verarbeiten Ereignisse aufgrund der verteilten Natur ihrer Poller mindestens einmal. Infolgedessen kann Ihre Lambda-Funktion in seltenen Situationen doppelte Ereignisse erhalten. Folgen Sie den bewährten Methoden für die Arbeit mit AWS Lambda Funktionen und erstellen Sie idempotente Funktionen, um Probleme im Zusammenhang mit doppelten Ereignissen zu vermeiden. Weitere Informationen finden Sie unter Using AWS Lambda console with Amazon DocumentDB im AWS Lambda Developer Guide.

Gemäß bewährten Methoden für die Leistung muss die Lambda-Funktion kurzlebig sein. Um unnötige Verarbeitungsverzögerungen zu vermeiden, sollte sie auch keine komplexe Logik ausführen. Insbesondere bei einem Hochgeschwindigkeits-Stream ist es besser, asynchrone Nachbearbeitungs-Schrittfunktions-Workflows auszulösen als synchrone Lambdas mit langer Laufzeit. Weitere Informationen zu AWS Lambda finden Sie im AWS Lambda Entwicklerhandbuch.

Einschränkungen

Die folgenden Einschränkungen sind bei der Arbeit mit Amazon DocumentDB zu beachten und AWS Lambda:

- AWS Lambda wird derzeit nur auf Amazon DocumentDB 4.0 und 5.0 unterstützt.
- AWS Lambda wird derzeit nicht auf elastischen Clustern oder globalen Clustern unterstützt.
- AWS Lambda Die Größe der Nutzlast darf 6 MB nicht überschreiten. Weitere Informationen zu Lambda-Batchgrößen finden Sie unter „Batchverhalten“ im Abschnitt Lambda-Ereignisquellenzuordnungen im Entwicklerhandbuch.AWS Lambda

Verwendung elastischer Amazon DocumentDB-Cluster

Elastische Amazon DocumentDB-Cluster unterstützen Workloads mit einer reads/writes Speicherkapazität von Millionen pro Sekunde und Petabyte. Elastische Cluster vereinfachen auch die Interaktion von Entwicklern mit Amazon DocumentDB, da sie Instances nicht mehr auswählen, verwalten oder aktualisieren müssen.

> **Note**
>
> Elastic Cluster verwenden ein MongoDB 5.0-kompatibles Wire-Protokoll. Sie werden von der Amazon DocumentDB DocumentDB-Engine Version 8.0 nicht unterstützt und sind in China Regionen oder AWS GovCloud nicht verfügbar.

Elastische Amazon DocumentDB-Cluster wurden erstellt, um:

- Bieten Sie eine Lösung für Kunden, die nach einer Datenbank suchen, die praktisch grenzenlose Skalierbarkeit mit umfangreichen Abfragefunktionen und MongoDB-API-Kompatibilität bietet.
- Bieten Sie Kunden höhere Verbindungslimits und reduzieren Sie Ausfallzeiten aufgrund von Patches.
- Investieren Sie weiterhin in eine cloudnative, elastische und erstklassige Architektur für JSON-Workloads.

Topics

- Anwendungsfälle für elastische Cluster
- Vorteile elastischer Cluster
- Elastische Cluster-Region und Versionsverfügbarkeit
- Einschränkungen
- Elastische Amazon DocumentDB-Cluster: So funktioniert's
- Erste Schritte mit Amazon DocumentDB Elastic Clusters
- Bewährte Methoden für Amazon DocumentDB Elastic Cluster
- Verwaltung elastischer Amazon DocumentDB-Cluster

- Datenverschlüsselung im Ruhezustand für elastische Amazon DocumentDB-Cluster
- Service-linked Rollen in elastischen Clustern

Anwendungsfälle für elastische Cluster

Dokumentdatenbanken sind nützlich für Workloads, die ein flexibles Schema für eine schnelle, iterative Entwicklung benötigen. Beispiele für Amazon DocumentDB DocumentDB-Anwendungsfälle finden Sie unterAnwendungsfälle für Dokumentendatenbanken.

Im Folgenden finden Sie einige Beispiele für Anwendungsfälle, für die elastische Cluster erhebliche Vorteile bieten können:

Benutzerprofile

Da Dokumentendatenbanken über ein flexibles Schema verfügen, können sie Dokumente mit unterschiedlichen Attributen und Datenwerten skaliert speichern. Elastische Cluster sind eine praktische Lösung für Online-Profile, in denen verschiedene Benutzer unterschiedliche Arten von Informationen bereitstellen. Angenommen, Ihre Anwendungen unterstützen Hunderte Millionen von Benutzerprofilen. Sie können elastische Cluster zur Unterstützung solcher Anwendungen verwenden, da sie hoch- und skaliert werden können, um Millionen von Schreib- und Lesevorgängen in diese Benutzerprofile zu unterstützen. Sie können auch außerhalb der Spitzenzeiten herunterskalieren, um die Kosten zu senken.

Inhaltsverwaltung und historische Aufzeichnungen

Um Inhalte effektiv zu verwalten, müssen Sie in der Lage sein, Inhalte aus einer Vielzahl von Quellen zu sammeln, zu aggregieren und dann an den Client zu liefern. Aufgrund ihres flexiblen Schemas sind Dokumentdatenbanken ideal für die Erfassung und Speicherung jeglicher Art von Daten. Sie können sie verwenden, um neue Arten von Inhalten zu erstellen und zu integrieren, einschließlich benutzergenerierter Inhalte wie Bilder, Kommentare und Videos. Im Laufe der Zeit benötigt Ihre Datenbank möglicherweise mehr Speicherplatz. Mit elastischen Clustern können Sie Ihre Daten auf mehr Speichervolumen verteilen, sodass Sie Petabyte an Daten in einem einzigen Cluster speichern können.

Vorteile elastischer Cluster

AWS Serviceintegration

Elastische Amazon DocumentDB-Cluster lassen sich auf dieselbe Weise in andere AWS Services integrieren wie Amazon DocumentDB:

- Migration — Sie können AWS Database Migration Service (DMS) verwenden, um von MongoDB und anderen relationalen Datenbanken zu elastischen Amazon DocumentDB-Clustern zu migrieren.
- Überwachung — Sie können den Zustand und die Leistung Ihres Elastic Clusters mithilfe von Amazon überwachen CloudWatch.
- Sicherheit — Sie können Authentifizierung und Autorisierung über AWS Identity and Access Management (IAM) einrichten, um Ihre Elastic Cluster-Ressourcen wie die Erstellung und Aktualisierung eines Elastic Clusters zu verwalten und Amazon VPC für sichere VPC-only Verbindungen verwenden. Die Anmeldung mit IAM-Authentifizierung für Elastic Clusters wird nicht unterstützt.
- Datenmanagement — Sie können Daten AWS Glue mit from/to anderen AWS Diensten wie Amazon S3, Amazon Redshift und Amazon OpenSearch Service importieren und exportieren.

Elastische Cluster-Region und Versionsverfügbarkeit

Regionale Verfügbarkeit für elastische Cluster

Die folgende Tabelle zeigt die AWS Regionen, in denen Amazon DocumentDB Elastic Cluster derzeit verfügbar sind, sowie den Endpunkt für jede Region.

Name der Region	Region	Availability Zones
USA Ost (Nord-Virginia)	`us-east-1`	5
USA Ost (Ohio)	`us-east-2`	3
USA West (Oregon)	`us-west-2`	3
Asien-Pazifik (Hongkong)	`ap-east-1`	3
Asien-Pazifik (Mumbai)	`ap-south-1`	3

Name der Region	Region	Availability Zones
Asien-Pazifik (Seoul)	ap-northeast-2	3
Asien-Pazifik (Singapur)	ap-southeast-1	3
Asien-Pazifik (Sydney)	ap-southeast-2	3
Asien-Pazifik (Tokio)	ap-northeast-1	3
Kanada (Zentral)	ca-central-1	3
Südamerika (São Paulo)	sa-east-1	3
Europa (Frankfurt)	eu-central-1	3
Europa (Irland)	eu-west-1	3
Europa (London)	eu-west-2	3
Europa (Milan)	eu-south-1	3
Europa (Paris)	eu-west-3	3

Verfügbarkeit der Versionen

Elastic Cluster unterstützen das MongoDB 5.0-kompatible Wire-Protokoll. Unterschiede zwischen instanzbasierten Amazon DocumentDB 4.0-Clustern und elastischen Clustern finden Sie unter. Funktionale Unterschiede zwischen Amazon DocumentDB 4.0 und Elastic Clusters Hinweis: Elastic Clusters werden auf Amazon DocumentDB 8.0 nicht unterstützt

Einschränkungen

Elastisches Cluster-Management

Die folgenden Funktionen und Funktionen zur Clusterverwaltung werden in dieser Version nicht unterstützt:

- Benutzerdefinierter Port (nur 27017 wird unterstützt)

- Möglichkeit, IAM-Benutzer und -Rollen zur Authentifizierung in der Datenbank zu verwenden
- Fähigkeit, globale Cluster zu erstellen
- Bestehende Amazon DocumentDB DocumentDB-Ereignisse und Abonnieren von Veranstaltungen
- Bereichs-Sharding
- Bestehende Sammlung teilen
- Multi-field Schlüssel teilen
- Shard-Schlüssel ändern
- Point-in-time wiederherstellen
- Klonen
- Performance Insights

> **Note**
>
> Hinweise zu den Grenzwerten für elastische Cluster finden Sie unterAmazon DocumentDB Kontingente und Beschränkungen.

Abfrage- und Schreiboperationen

Die folgenden Befehle und Funktionen für Abfrage- und Schreiboperationen werden in dieser Version nicht unterstützt:

- DDL-Befehle bei Skalierungsvorgängen
- Profiler
- Parametergruppen
- AWS Config
- AWS Backup

Sammlungs- und Indexverwaltung

Die folgenden Funktionen zur Erfassung und Indexverwaltung werden in dieser Version nicht unterstützt:

- Eindeutige Indizes
- Nicht vollständige Indizes
- Textindizes
- Vektor-Indizes
- Komprimierung von Dokumenten

Verwaltung und Diagnose

Die folgenden Befehle und Funktionen für Verwaltung und Diagnose werden in dieser Version nicht unterstützt:

- AWS Secrets Manager
- Role-based-access-control (RBAC) benutzerdefinierte Rollen.
- Beim Herstellen einer Verbindung wird das Schreibproblem 0 nicht unterstützt.
- Ändern von Subnetzen, die zu einer VPC gehören, die derzeit keinem vorhandenen Elastic Cluster zugewiesen ist.

Opt-in features

Die folgenden Amazon DocumentDB DocumentDB-Opt-In-Funktionen werden in dieser Version nicht unterstützt:

- ACID-Transaktionen
- DDL/DML Auditing
- Change streams
- Sitzungsbefehle

Elastische Amazon DocumentDB-Cluster: So funktioniert's

Die Themen in diesem Abschnitt enthalten Informationen zu den Mechanismen und Funktionen, die Amazon DocumentDB Elastic Clusters zugrunde liegen.

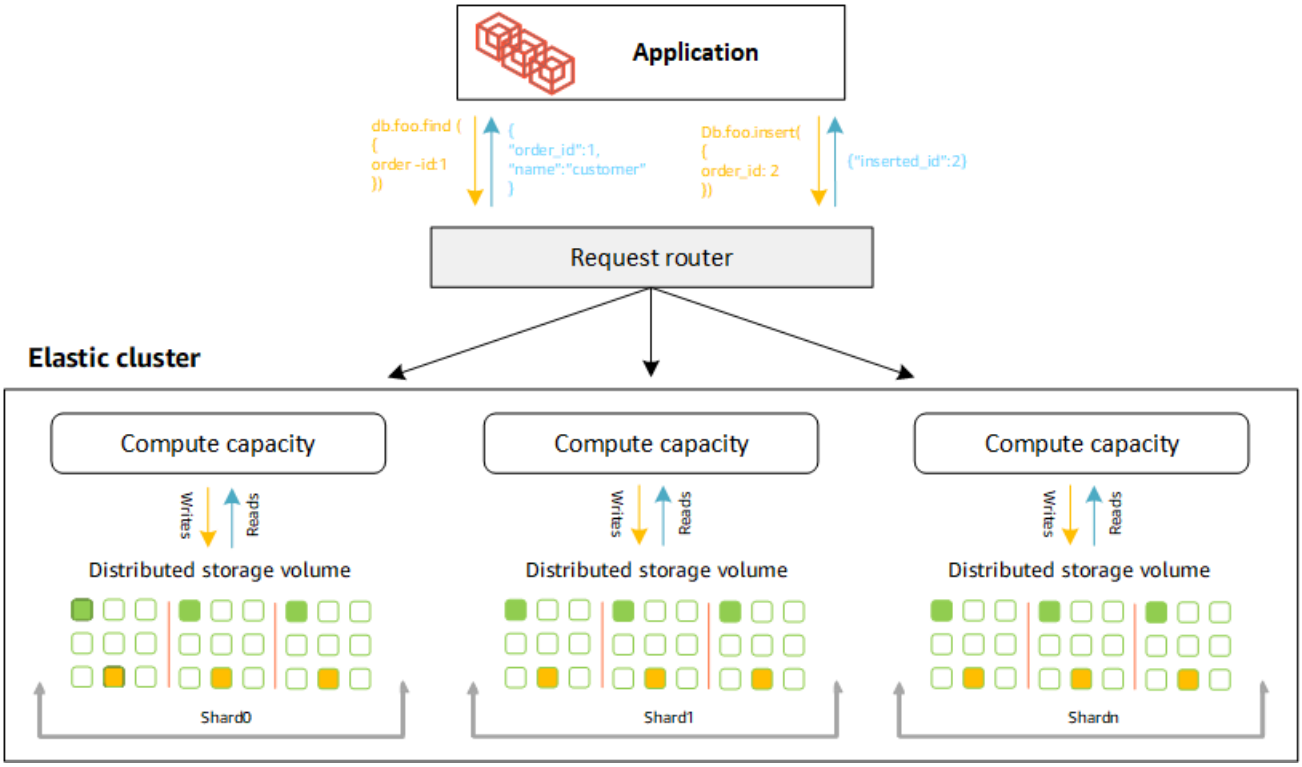
Topics

- Elastisches Cluster-Sharding von Amazon DocumentDB

- Elastische Cluster-Migration
- Elastische Cluster-Skalierung
- Zuverlässigkeit elastischer Cluster
- Elastischer Cluster-Speicher und Verfügbarkeit
- Funktionale Unterschiede zwischen Amazon DocumentDB 4.0 und Elastic Clusters

Elastisches Cluster-Sharding von Amazon DocumentDB

Elastische Amazon DocumentDB-Cluster verwenden Hash-basiertes Sharding, um Daten in einem verteilten Speichersystem zu partitionieren. Sharding, auch Partitionierung genannt, teilt große Datensätze auf mehrere Knoten in kleine Datensätze auf, sodass Sie Ihre Datenbank über vertikale Skalierungsgrenzen hinaus skalieren können. Elastische Cluster nutzen die Trennung oder „Entkopplung“ von Rechenleistung und Speicher in Amazon DocumentDB, sodass Sie unabhängig voneinander skalieren können. Anstatt Sammlungen neu zu partitionieren, indem kleine Datenblöcke zwischen Rechenknoten verschoben werden, kopieren elastische Cluster Daten effizient innerhalb des verteilten Speichersystems.



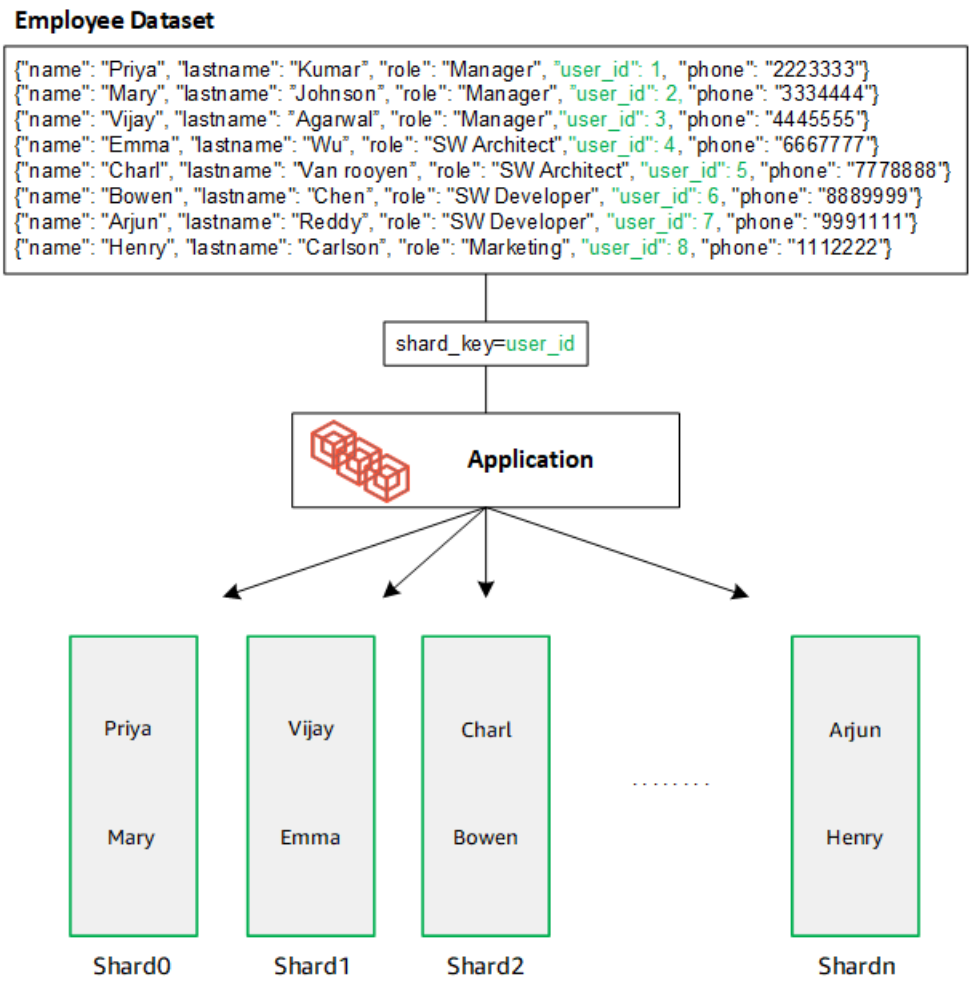
Shard-Definitionen

Definitionen der Shard-Nomenklatur:

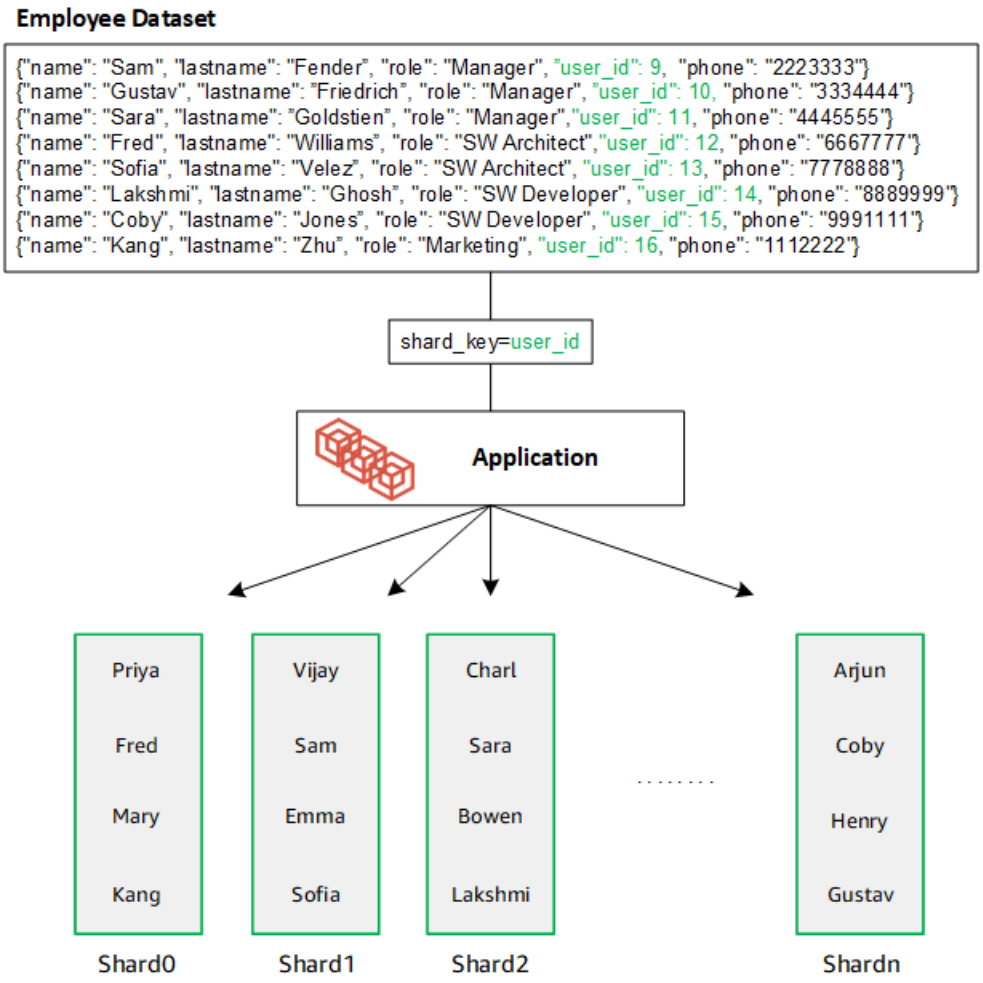
- Shard — Ein Shard stellt Rechenleistung für einen elastischen Cluster bereit. Er wird über eine einzelne Writer-Instance und 0—15 Read Replicas verfügen. Standardmäßig hat ein Shard zwei Instanzen: eine Writer- und eine einzelne Read-Replica. Sie können maximal 32 Shards konfigurieren und jede Shard-Instanz kann maximal 64 vCPUs haben.
- Shard-Schlüssel — Ein Shard-Schlüssel ist ein Pflichtfeld in Ihren JSON-Dokumenten in Sharded-Collections, die Elastic Cluster verwenden, um Lese- und Schreibverkehr auf den entsprechenden Shard zu verteilen.
- Sharded Collection — Eine Sharded Collection ist eine Sammlung, deren Daten über einen Elastic Cluster in Datenpartitionen verteilt sind.
- Partition — Eine Partition ist ein logischer Teil von Shard-Daten. Wenn Sie eine fragmentierte Sammlung erstellen, werden die Daten innerhalb jedes Shards automatisch auf der Grundlage des Shard-Schlüssels in Partitionen organisiert. Jeder Shard hat mehrere Partitionen.

Verteilung von Daten auf konfigurierte Shards

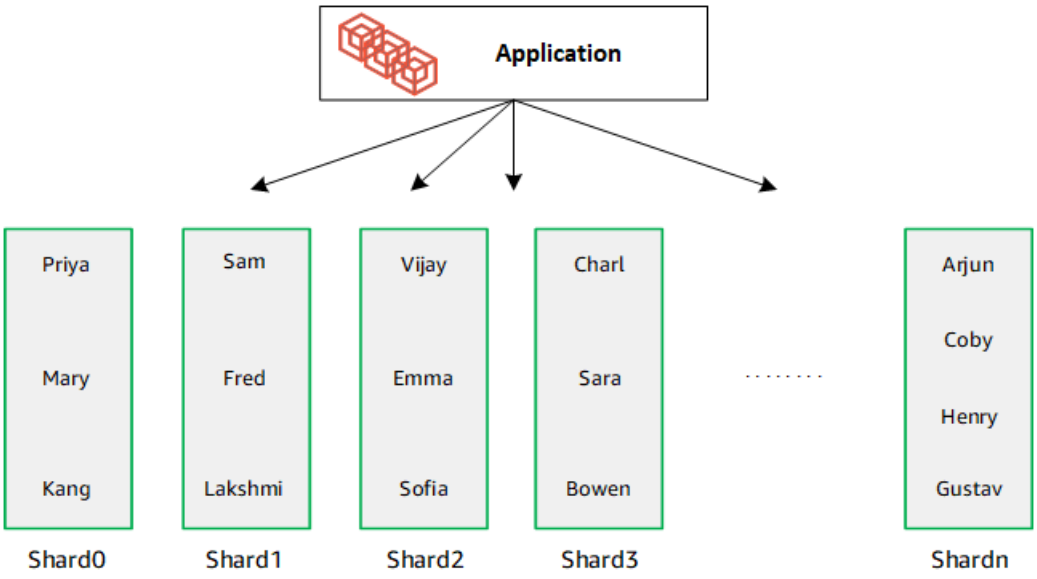
Erstellen Sie einen Shard-Schlüssel mit vielen eindeutigen Werten. Ein guter Shard-Schlüssel verteilt Ihre Daten gleichmäßig auf die zugrunde liegenden Shards, sodass Ihr Workload den besten Durchsatz und die beste Leistung erhält. Das folgende Beispiel zeigt Daten zu Mitarbeiternamen, die einen Shard-Schlüssel mit dem Namen „user_id“ verwenden:



DocumentDB verwendet Hash-Sharding, um Ihre Daten auf die zugrunde liegenden Shards zu partitionieren. Zusätzliche Daten werden auf die gleiche Weise eingefügt und verteilt:



Wenn Sie Ihre Datenbank skalieren, indem Sie zusätzliche Shards hinzufügen, verteilt Amazon DocumentDB die Daten automatisch neu:



Elastische Cluster-Migration

Amazon DocumentDB unterstützt die Migration von mongoDB-Sharded-Daten zu elastischen Clustern. Offline-, Online- und Hybridmigrationsmethoden werden unterstützt. Weitere Informationen finden Sie unter Migration zu Amazon DocumentDB.

Elastische Cluster-Skalierung

Elastische Amazon DocumentDB-Cluster bieten die Möglichkeit, die Anzahl der Shards (Scale Out) in Ihrem Elastic Cluster und die Anzahl der auf jeden Shard angewendeten vCPUs (Scale Up) zu erhöhen. Sie können auch die Anzahl der Shards und die Rechenkapazität (vCPUs) nach Bedarf reduzieren.

Bewährte Methoden zur Skalierung finden Sie unter. Skalierung elastischer Cluster

> **Note**
>
> Cluster-level Skalierung ist ebenfalls verfügbar. Weitere Informationen finden Sie unter Skalierung von Amazon DocumentDB-Clustern.

Zuverlässigkeit elastischer Cluster

Amazon DocumentDB ist darauf ausgelegt, zuverlässig, robust und fehlertolerant zu sein. Um die Verfügbarkeit zu verbessern, stellen Elastic Cluster zwei Knoten pro Shard bereit, die in verschiedenen Availability Zones platziert sind. Amazon DocumentDB umfasst mehrere automatische Funktionen, die es zu einer zuverlässigen Datenbanklösung machen. Weitere Informationen finden Sie unter Zuverlässigkeit von Amazon DocumentDB.

Elastischer Cluster-Speicher und Verfügbarkeit

Amazon DocumentDB DocumentDB-Daten werden in einem Cluster-Volume gespeichert, bei dem es sich um ein einzelnes virtuelles Volume handelt, das Solid-State-Laufwerke (SSDs) verwendet. Ein Cluster-Volume besteht aus sechs Kopien Ihrer Daten, die automatisch über mehrere Availability Zones in einer einzigen Region repliziert werden. AWS Diese Replikation trägt dazu bei, dass Ihre Daten sehr langlebig sind und weniger Datenverlust möglich ist. Sie trägt außerdem dazu bei, dass Ihr Cluster während eines Failovers besser verfügbar ist, da Kopien Ihrer Daten bereits in anderen Availability Zones vorhanden sind. Weitere Informationen zu Speicher, Hochverfügbarkeit und Replikation finden Sie unterAmazon DocumentDB: So funktioniert es.

Funktionale Unterschiede zwischen Amazon DocumentDB 4.0 und Elastic Clusters

Die folgenden funktionalen Unterschiede bestehen zwischen Amazon DocumentDB 4.0 und Elastic Clusters.

- Die Ergebnisse von `top` und `collStats` sind nach Shards partitioniert. Bei Datensammlungen mit mehreren Partitionen werden die Daten auf mehrere Partitionen verteilt, und die `collStats` Berichte werden aus den Partitionen aggregiert. `collScans`
- Sammlungsstatistiken von `top` und `collStats` für Sammlungen mit Sharding werden zurückgesetzt, wenn die Anzahl der Cluster-Shards geändert wird.
- Die integrierte Backup-Rolle unterstützt jetzt. `serverStatus` Aktion — Entwickler und Anwendungen mit Backup-Rolle können Statistiken über den Status des Amazon DocumentDB-Clusters sammeln.
- Das `SecondaryDelaySecs` Feld ersetzt `slaveDelay` in der `replSetGetConfig` Ausgabe.
- Der `hello` Befehl ersetzt `isMaster` — `hello` gibt ein Dokument zurück, das die Rolle des elastischen Clusters beschreibt.
- Der `$elemMatch` Operator in elastischen Clustern entspricht nur Dokumenten in der ersten Verschachtelungsebene eines Arrays. In Amazon DocumentDB 4.0 durchläuft der Operator alle Ebenen, bevor er übereinstimmende Dokumente zurücksendet. Beispiel:

```
db.foo.insert(
[
    {a: {b: 5}},
    {a: {b: [5]}},
    {a: {b: [3, 7]}},
    {a: [{b: 5}]},
    {a: [{b: 3}, {b: 7}]},
    {a: [{b: [5]}]},
    {a: [{b: [3, 7]}]},
    {a: [[{b: 5}]]},
    {a: [[{b: 3}, {b: 7}]]},
    {a: [[{b: [5]}]]},
    {a: [[{b: [3, 7]}]]}
]);
// Elastic clusters
```

```
> db.foo.find({a: {$elemMatch: {b: {$elemMatch: {$lt: 6, $gt: 4}}}}}, {_id: 0})
{ "a" : [ { "b" : [ 5 ] } ] }

// Docdb 4.0: traverse more than one level deep
> db.foo.find({a: {$elemMatch: {b: {$elemMatch: {$lt: 6, $gt: 4}}}}}, {_id: 0})
{ "a" : [ { "b" : [ 5 ] } ] }
{ "a" : [ [ { "b" : [ 5 ] } ] ] }
```

- Die Projektion „$“ in Amazon DocumentDB 4.0 gibt alle Dokumente mit allen Feldern zurück. Bei elastischen Clustern gibt der `find` Befehl mit einer „$“ -Projektion Dokumente zurück, die dem Abfrageparameter entsprechen und nur das Feld enthalten, das der Projektion „$“ entspricht.
- In elastischen Clustern geben die `find` Befehle mit `$regex` und `$options` Abfrageparametern einen Fehler zurück: „Optionen können nicht sowohl in $regex als auch in $options festgelegt werden.“

- Bei elastischen Clustern wird `$indexOfCP` jetzt „-1" zurückgegeben, wenn:
  - Die Teilzeichenfolge wurde nicht in der `string expression` Datei gefunden, oder
  - `start`ist eine Zahl größer als`end`, oder
  - `start`ist eine Zahl, die größer als die Bytelänge der Zeichenfolge ist.

  Gibt in Amazon DocumentDB 4.0 „0" `$indexOfCP` zurück, wenn die `start` Position eine Zahl ist, die größer als `end` oder die Bytelänge der Zeichenfolge ist.
- Bei elastischen Clustern geben Projektionsoperationen z. B. Dokumente zurück`{"_id.nestedField" : 1}`, die nur das projizierte Feld enthalten. `_id fields` In Amazon DocumentDB 4.0 filtern Befehle zur verschachtelten Feldprojektion derweil kein Dokument heraus.

Erste Schritte mit Amazon DocumentDB Elastic Clusters

In diesem Abschnitt „Erste Schritte“ erfahren Sie, wie Sie Ihren ersten Elastic Cluster erstellen und abfragen können.

Es gibt viele Möglichkeiten, eine Verbindung herzustellen und mit Amazon DocumentDB zu beginnen. Das folgende Verfahren ist der schnellste, einfachste und einfachste Weg für Benutzer, mit der Nutzung unserer leistungsstarken Dokumentendatenbank zu beginnen. In diesem Handbuch wird verwendet AWS CloudShell, um eine Verbindung herzustellen und Ihren Amazon DocumentDB-

Cluster direkt vom AWS-Managementkonsole abzufragen. Neukunden, die Anspruch auf das AWS kostenlose Kontingent haben, können Amazon DocumentDB CloudShell kostenlos nutzen. Wenn Ihre AWS CloudShell Umgebung oder Ihr elastischer Amazon DocumentDB-Cluster Ressourcen nutzt, die über das kostenlose Kontingent hinausgehen, werden Ihnen die normalen AWS Tarife für diese Ressourcen berechnet. Mit diesem Handbuch können Sie in weniger als 5 Minuten mit Amazon DocumentDB beginnen.

Topics

- Voraussetzungen
- Schritt 1: Erstellen Sie einen elastischen Cluster
- Schritt 2: Connect zu Ihrem Elastic Cluster her
- Schritt 3: Teilen Sie Ihre Sammlung, fügen Sie Daten ein und fragen Sie sie ab
- Schritt 4: Erkunden

Voraussetzungen

Bevor Sie Ihren ersten Amazon DocumentDB-Cluster erstellen, müssen Sie Folgendes tun:

Erstellen Sie ein Amazon Web Services (AWS) -Konto

Bevor Sie Amazon DocumentDB verwenden können, benötigen Sie ein Amazon Web Services (AWS) -Konto. Das AWS Konto ist kostenlos. Sie zahlen nur für die Services und Ressourcen, die Sie wirklich nutzen.

Wenn Sie noch keinen haben AWS-Konto, führen Sie die folgenden Schritte aus, um einen zu erstellen.

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie https://portal.aws.amazon.com/billing/signup.
2. Folgen Sie den Online-Anweisungen.

   Während der Anmeldung erhalten Sie einen Telefonanruf oder eine Textnachricht und müssen einen Verifizierungscode über die Telefontasten eingeben.

   Wenn Sie sich für eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontoswird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Als bewährte Sicherheitsmethode weisen Sie einem Benutzer Administratorzugriff zu und

verwenden Sie nur den Root-Benutzer, um Aufgaben auszuführen, die Root-Benutzerzugriff erfordern.

Richten Sie die erforderlichen AWS Identity and Access Management (IAM-) Berechtigungen ein.

Für den Zugriff auf die Verwaltung von Amazon DocumentDB DocumentDB-Ressourcen wie Clustern, Instances und Cluster-Parametergruppen sind Anmeldeinformationen erforderlich, mit denen Sie Ihre Anfragen authentifizieren AWS können. Weitere Informationen finden Sie unter Identity and Access Management für Amazon DocumentDB.

1. Geben Sie in der Suchleiste von IAM ein und wählen Sie im Drop-down-Menü IAM aus. AWS-Managementkonsole
2. Sobald Sie sich in der IAM-Konsole befinden, wählen Sie im Navigationsbereich Benutzer aus.
3. Wählen Sie Ihren Nutzernamen aus.
4. Wählen Sie Add permissions (Berechtigungen hinzufügen) aus.
5. Wählen Sie Richtlinien direkt anhängen aus.
6. Geben Sie `AmazonDocDBElasticFullAccess` in die Suchleiste ein und wählen Sie sie aus, sobald sie in den Suchergebnissen erscheint.
7. Wählen Sie Weiter aus.
8. Wählen Sie Add permissions (Berechtigungen hinzufügen) aus.

> **Note**
>
> Ihr AWS Konto enthält in jeder Region eine Standard-VPC. Wenn Sie sich für die Verwendung einer Amazon VPC entscheiden, führen Sie die Schritte im Thema Amazon VPC erstellen im Amazon VPC-Benutzerhandbuch aus.

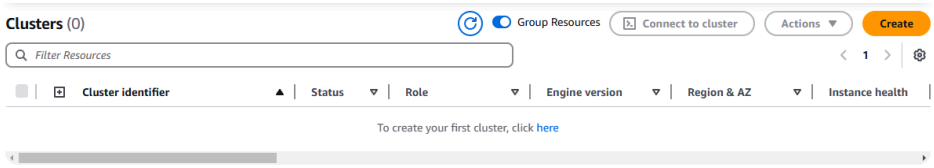
Schritt 1: Erstellen Sie einen elastischen Cluster

In diesem Abschnitt erklären wir, wie Sie einen brandneuen elastischen Cluster erstellen, indem Sie entweder das AWS-Managementkonsole oder AWS CLI verwenden und die folgenden Anweisungen verwenden.

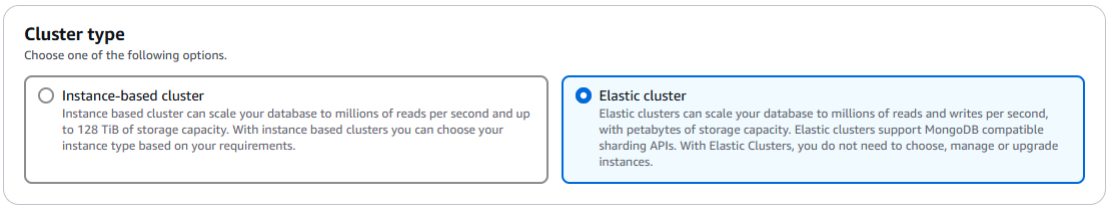
Using the AWS-Managementkonsole

Um eine elastische Cluster-Konfiguration zu erstellen, verwenden Sie AWS-Managementkonsole:

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Wählen Sie in der Amazon DocumentDB Management Console unter Clusters die Option Create aus.



3. Wählen Sie auf der Seite Amazon DocumentDB-Cluster erstellen im Abschnitt Clustertyp die Option Elastic Cluster aus.



4. Konfigurieren Sie im Abschnitt Konfiguration Folgendes:

   a. Geben Sie im Feld Clustername eine eindeutige Cluster-ID ein (gemäß den Benennungsanforderungen unter dem Feld).

   b. Geben Sie im Feld Anzahl der Shards die Anzahl der Shards ein, die Sie in Ihrem Cluster haben möchten. Die maximale Anzahl von Shards pro Cluster ist 32.

   > **Note**
   >
   > Für jeden Shard werden zwei Knoten bereitgestellt. Beide Knoten werden dieselbe Shard-Kapazität haben.

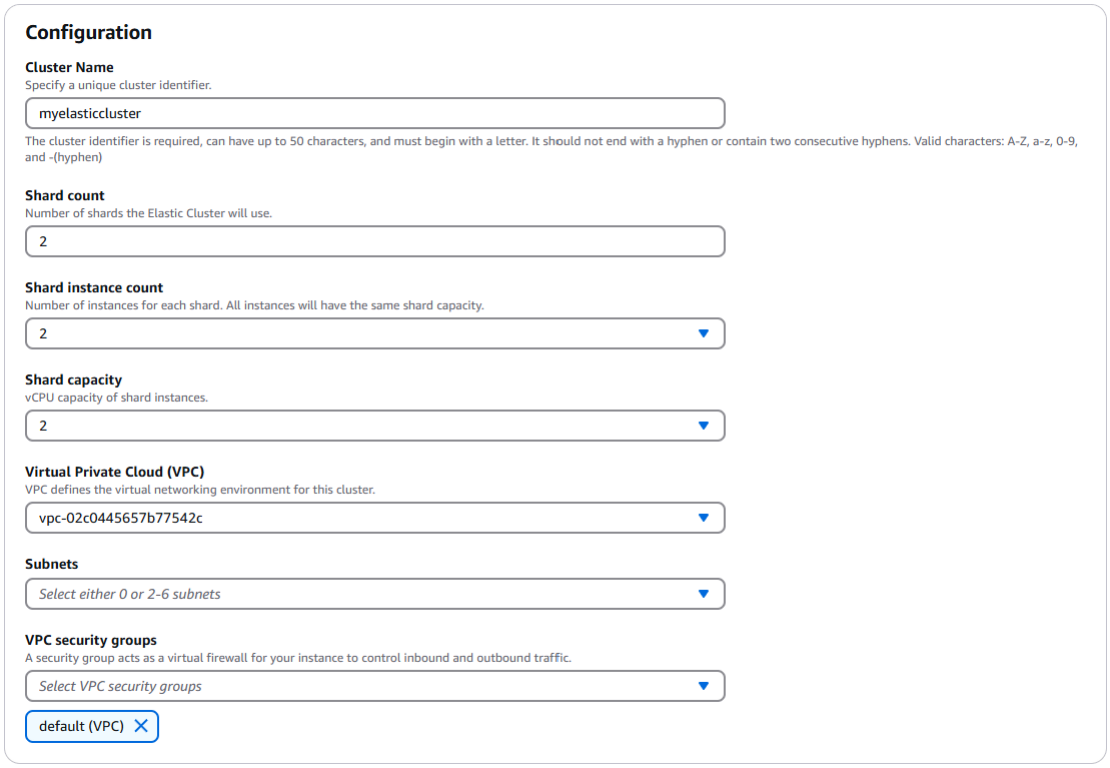
   c. Wählen Sie im Feld Anzahl der Shard-Instanzen die Anzahl der Replikatinstanzen aus, die Sie jedem Shard zuordnen möchten. Die maximale Anzahl von Shard-Instanzen beträgt 16, in Schritten von 1. Alle Replikatinstanzen haben dieselbe Shard-Kapazität, wie im folgenden Feld definiert. Zu Testzwecken sollte der Standardwert 2 ausreichen.

> **Note**
>
> Die Anzahl der Replikatinstanzen gilt für alle Shards im Elastic Cluster. Ein Wert für die Anzahl der Shard-Instances von 1 bedeutet, dass es eine Writer-Instance gibt, und alle weiteren Instances sind Replikate, die für Lesevorgänge und zur Verbesserung der Verfügbarkeit verwendet werden können. Zu Testzwecken sollte der Standardwert 2 ausreichen.

d. Wählen Sie im Feld Shard-Kapazität die Anzahl der virtuellen CPUs (vCPUs) aus, die jeder Shard-Instanz zugeordnet werden sollen. Die maximale Anzahl von vCPUs pro Shard-Instanz beträgt 64. Zulässige Werte sind 2, 4, 8, 16, 32, 64. Zu Testzwecken sollte der Standardwert 2 ausreichen.

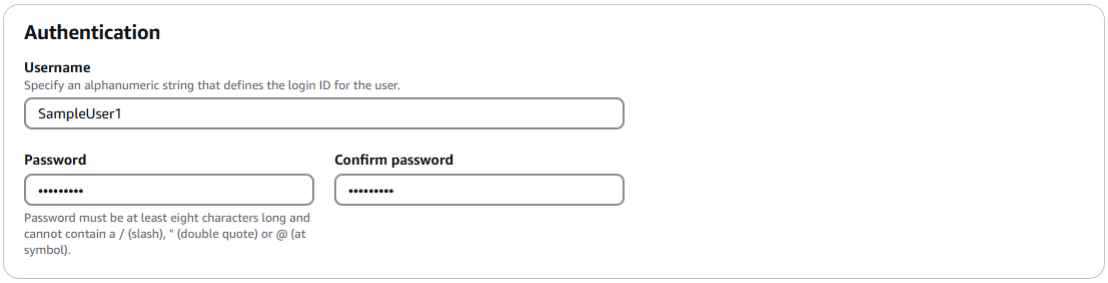
e. Wählen Sie im Feld Virtual Private Cloud (VPC) eine VPC aus der Dropdownliste aus.

f. Für Subnetze und VPC-Sicherheitsgruppen können Sie die Standardeinstellungen verwenden oder drei Subnetze Ihrer Wahl und bis zu drei VPC-Sicherheitsgruppen (mindestens eine) auswählen.



5. Geben Sie im Abschnitt Authentifizierung im Feld Benutzername eine Zeichenfolge ein, die den Anmeldenamen des Hauptbenutzers identifiziert.

Geben Sie im Feld Passwort ein eindeutiges Passwort ein, das den Anweisungen entspricht, und bestätigen Sie es anschließend.



6. Behalten Sie im Abschnitt Verschlüsselung die Standardeinstellung (Standardschlüssel) bei.

   Optional können Sie einen von Ihnen erstellten AWS KMS key ARN eingeben. Weitere Informationen finden Sie unter Datenverschlüsselung im Ruhezustand für elastische Amazon DocumentDB-Cluster.

   > **Important**
   >
   > Die Verschlüsselung muss für elastische Cluster aktiviert sein.

7. Bearbeiten Sie im Abschnitt Backup die Felder entsprechend Ihren Backup-Anforderungen. Zu Testzwecken können Sie die Standardeinstellungen beibehalten.

   a. Aufbewahrungszeitraum für Backup — Wählen Sie in der Liste die Anzahl der Tage aus, für die automatische Backups dieses Clusters aufbewahrt werden sollen, bevor sie gelöscht werden.

   b. Backup-Fenster — Legen Sie die tägliche Uhrzeit und Dauer fest, während der Amazon DocumentDB Backups dieses Clusters erstellen soll.

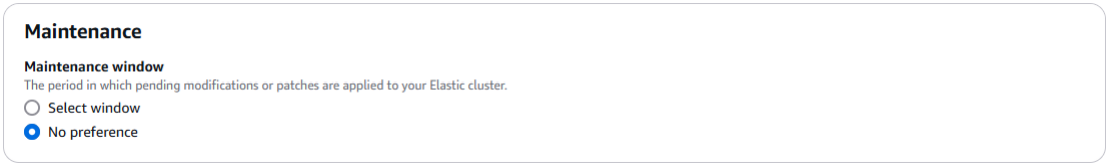
      i. Wählen Sie Fenster auswählen, wenn Sie die Uhrzeit und Dauer der Erstellung von Backups konfigurieren möchten.

Startzeit — Wählen Sie in der ersten Liste die Startzeit (UTC) für den Start Ihrer automatischen Backups aus. Wählen Sie in der zweiten Liste die Minute für den Beginn der automatischen Backups aus.

Dauer — Wählen Sie in der Liste die Anzahl der Stunden aus, die für die Erstellung automatischer Backups reserviert werden sollen.

ii. Wählen Sie Keine Präferenz, wenn Amazon DocumentDB den Zeitpunkt und die Dauer der Erstellung von Backups wählen soll.

8. Wählen Sie im Abschnitt Wartung den Tag, die Uhrzeit und die Dauer aus, an dem Änderungen oder Patches auf Ihren Cluster angewendet werden. Zu Testzwecken können Sie die Standardeinstellungen beibehalten.



9. Wählen Sie Cluster erstellen.

Der elastische Cluster wird jetzt bereitgestellt. Es kann bis zu einigen Minuten dauern, bis dieser Vorgang abgeschlossen ist. Sie können eine Verbindung zu Ihrem Cluster herstellen, wenn der Elastic Cluster-Status in der Cluster-Liste als Verfügbar angezeigt wird.

Using the AWS CLI

Um einen elastischen Cluster mit dem zu erstellen AWS CLI, verwenden Sie den `create-cluster` Vorgang mit den folgenden Parametern:

- --cluster-name—Erforderlich. Der aktuelle Name des Elastic Scale Clusters, wie er bei der Erstellung eingegeben oder zuletzt geändert wurde.
- --shard-capacity—Erforderlich. Die Anzahl der vCPUs, die jedem Shard zugewiesen sind. Das Maximum ist 64. Zulässige Werte sind 2, 4, 8, 16, 32, 64.
- --shard-count—Erforderlich. Die Anzahl der dem Cluster zugewiesenen Shards. Das Maximum ist 32.
- --shard-instance-count— Fakultativ. Die Anzahl der Replikatinstanzen, die für alle Shards in diesem Cluster gelten. Das Maximum ist 16.
- --admin-user-name—Erforderlich. Der dem Admin-Benutzer zugeordnete Benutzername.
- --admin-user-password—Erforderlich. Das dem Admin-Benutzer zugeordnete Passwort.

- --auth-type—Erforderlich. Der Authentifizierungstyp, der verwendet wird, um zu bestimmen, wo das für den Zugriff auf den Elastic Cluster verwendete Passwort abgerufen werden soll. Gültige Typen sind `PLAIN_TEXT` oder`SECRET_ARN`.
- --vpc-security-group-ids— Fakultativ. Konfigurieren Sie eine Liste von EC2-VPC-Sicherheitsgruppen, die diesem Cluster zugeordnet werden sollen.
- --preferred-maintenance-window— Fakultativ. Konfigurieren Sie den wöchentlichen Zeitraum, in dem die Systemwartung erfolgen kann, in UTC (Universal Coordinated Time).

  Das Format ist:`ddd:hh24:mi-ddd:hh24:mi`. Gültige Tage (ddd): Mo, Di, Mi, Do, Fr, Sa, So

  Die Standardeinstellung ist ein 30-minütiges Fenster, das nach dem Zufallsprinzip aus einem 8-Stunden-Zeitblock für jede Amazon Web Services Services-Region ausgewählt wird und an einem zufälligen Wochentag stattfindet.

  Zeitfenster von mindestens 30 Minuten.
- --kms-key-id— Fakultativ. Konfigurieren Sie die KMS-Schlüssel-ID für einen verschlüsselten Cluster.

  Die KMS-Schlüssel-ID ist der Amazon-Ressourcenname (ARN) für den AWS KMS Verschlüsselungsschlüssel. Wenn Sie einen Cluster mit demselben Amazon Web Services Services-Konto erstellen, dem der KMS-Verschlüsselungsschlüssel gehört, der zur Verschlüsselung des neuen Clusters verwendet wird, können Sie den KMS-Schlüsselalias anstelle des ARN für den KMS-Verschlüsselungsschlüssel verwenden.

  Wenn in kein Verschlüsselungsschlüssel angegeben ist KmsKeyId und der `StorageEncrypted` Parameter wahr ist, verwendet Amazon DocumentDB Ihren Standard-Verschlüsselungsschlüssel.
- --preferred-backup-window— Optional. Der bevorzugte tägliche Zeitraum, in dem automatische Backups erstellt werden. Die Standardeinstellung ist ein 30-minütiges Fenster, das nach dem Zufallsprinzip aus einem Zeitblock von jeweils AWS-Region 8 Stunden ausgewählt wird.
- --backup-retention-period— Fakultativ. Die Anzahl von Tagen, über die automatische Backups aufbewahrt werden. Der Standardwert ist 1.
- --storage-encrypted— Fakultativ. Konfiguriert, ob der Cluster verschlüsselt oder nicht verschlüsselt ist.

  `--no-storage-encrypted`gibt an, dass der Cluster nicht verschlüsselt ist.
- --subnet-ids— Fakultativ. Konfigurieren Sie Netzwerk-Subnetz-IDs.

Ersetzen Sie im folgenden Beispiel jede *user input placeholder* durch Ihre eigenen Informationen.

> **Note**
>
> Die folgenden Beispiele beinhalten die Erstellung eines bestimmten KMS-Schlüssels. Um den Standard-KMS-Schlüssel zu verwenden, schließen Sie den `--kms-key-id` Parameter nicht ein.

Für Linux, macOS oder Unix:

```
aws docdb-elastic create-cluster \
     --cluster-name sample-cluster-123 \
     --shard-capacity 8 \
     --shard-count 4 \
     --shard-instance-count 3 \
     --auth-type PLAIN_TEXT \
     --admin-user-name testadmin \
     --admin-user-password testPassword \
     --vpc-security-group-ids ec-65f40350 \
     --kms-key-id arn:aws:docdb-elastic:us-east-1:477568257630:cluster/
b9f1d489-6c3e-4764-bb42-da62ceb7bda2 \
     --subnet-ids subnet-9253c6a3, subnet-9f1b5af9 \
     --preferred-backup-window 18:00-18:30 \
     --backup-retention-period 7
```

Für Windows:

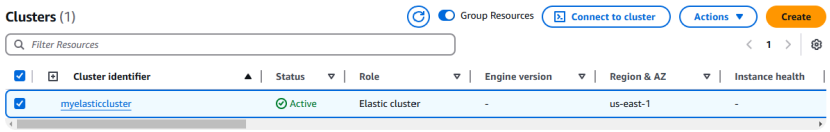
```
aws docdb-elastic create-cluster ^
     --cluster-name sample-cluster-123 ^
     --shard-capacity 8 ^
     --shard-count 4 ^
     --shard-instance-count 3 ^
     --auth-type PLAIN_TEXT ^
     --admin-user-name testadmin ^
     --admin-user-password testPassword ^
     --vpc-security-group-ids ec-65f40350 ^
     --kms-key-id arn:aws:docdb-elastic:us-east-1:477568257630:cluster/
b9f1d489-6c3e-4764-bb42-da62ceb7bda2 ^
     --subnet-ids subnet-9253c6a3, subnet-9f1b5af9 \
```

```
    --preferred-backup-window 18:00-18:30 \
    --backup-retention-period 7
```

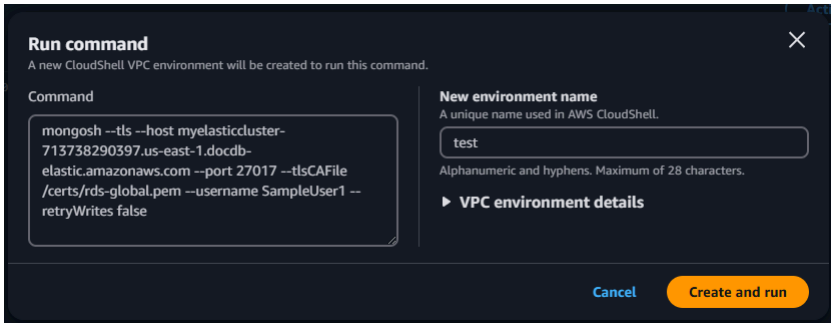
Schritt 2: Connect zu Ihrem Elastic Cluster her

Stellen Sie mithilfe AWS CloudShell von... Connect zu Ihrem Amazon DocumentDB Elastic Cluster her.

1. Suchen Sie auf der Amazon DocumentDB-Managementkonsole unter Clusters den Elastic Cluster, den Sie erstellt haben. Wählen Sie Ihren Cluster aus, indem Sie das Kontrollkästchen daneben aktivieren.



2. Wählen Sie Connect to cluster (neben dem Drop-down-Menü Aktionen). Diese Schaltfläche ist erst aktiviert, nachdem Sie auf das Kontrollkästchen neben Ihrem Cluster geklickt haben und der Status des Clusters als Verfügbar angezeigt wird. Der Befehlsbildschirm CloudShell Ausführen wird angezeigt.
3. Geben Sie im Feld Neuer Umgebungsname einen eindeutigen Namen ein, z. B. „Test“, und wählen Sie Erstellen und ausführen aus. VPC-Umgebungsdetails werden automatisch für Ihre Amazon DocumentDB DocumentDB-Datenbank konfiguriert.



4. Wenn Sie dazu aufgefordert werden, geben Sie das Passwort ein, das Sie in Schritt 1: Amazon DocumentDB Elastic Cluster erstellen (Unterschritt 5) erstellt haben.

Nachdem Sie Ihr Passwort eingegeben haben und Ihre Aufforderung lautet: Sie sind erfolgreich mit Ihrem Amazon DocumentDB-Cluster verbunden `direct: mongos] <env-name>>`

> **Note**
>
> Informationen zur Fehlerbehebung finden Sie unter Problembehandlung bei Amazon DocumentDB.

Schritt 3: Teilen Sie Ihre Sammlung, fügen Sie Daten ein und fragen Sie sie ab

Elastische Cluster bieten Unterstützung für Sharding in Amazon DocumentDB. Jetzt, da Sie mit Ihrem Cluster verbunden sind, können Sie den Cluster teilen, Daten einfügen und einige Abfragen ausführen.

1. Um eine Sammlung zu teilen, geben Sie Folgendes ein:

```
sh.shardCollection("db.Employee1" , { "Employeeid" : "hashed" })
```

2. Um ein einzelnes Dokument einzufügen, geben Sie Folgendes ein:

```
db.Employee1.insertOne({"Employeeid":1, "Name":"Joe", "LastName": "Bruin", "level":
 1 })
```

   Die folgende Ausgabe wird angezeigt:

```
WriteResult({ "nInserted" : 1 })
```

3. Um das Dokument zu lesen, das Sie geschrieben haben, geben Sie den `findOne()` Befehl ein (es wird ein einzelnes Dokument zurückgegeben):

```
db.Employee1.findOne()
```

Die folgende Ausgabe wird angezeigt:

```
{
"_id" : ObjectId("61f344e0594fe1a1685a8151"),
"EmployeeID" : 1,
"Name" : "Joe",
"LastName" : "Bruin",
"level" : 1
}
```

4. Um ein paar weitere Abfragen durchzuführen, sollten Sie einen Anwendungsfall für ein Spieleprofil in Betracht ziehen. Fügen Sie zunächst einige Einträge in eine Sammlung mit dem Titel „Mitarbeiter“ ein. Geben Sie Folgendes ein:

```
db.profiles.insertMany([ { "_id": 1, "name": "Matt", "status": "active", "level":
 12, "score": 202 },
     { "_id": 2, "name": "Frank", "status": "inactive", "level": 2, "score": 9 },
     { "_id": 3, "name": "Karen", "status": "active", "level": 7, "score": 87 },
     { "_id": 4, "name": "Katie", "status": "active", "level": 3, "score": 27 }
])
```

Die folgende Ausgabe wird angezeigt:

```
{ acknowledged: true,
     insertedIds: {
        '0': ObjectId('679d02cd6b5a0581be78bcbd'),
        '1': ObjectId('679d02cd6b5a0581be78bcbe'),
        '2': ObjectId('679d02cd6b5a0581be78bcbf'),
        '3': ObjectId('679d02cd6b5a0581be78bcc0')
    }
}
```

5. Um alle Dokumente in der Profilsammlung zurückzugeben, geben Sie den Befehl `find` () ein:

```
db.Employee.find()
```

Die Daten, die Sie in Schritt 4 eingegeben haben, werden angezeigt.

6. Um ein einzelnes Dokument abzufragen, fügen Sie einen Filter hinzu (z. B.: „Katie“). Geben Sie Folgendes ein:

```
db.Employee.find({name: "Katie"})
```

Die folgende Ausgabe wird angezeigt:

```
[
   {
     _id: ObjectId('679d02cd6b5a0581be78bcc0'),
     Employeeid: 4,
     name: 'Katie',
     lastname: 'Schaper',
     level: 3
   }
]
```

7. Um ein Profil zu finden und es zu ändern, geben Sie den `findAndModify` Befehl ein. In diesem Beispiel erhält der Mitarbeiter „Matt“ eine höhere Stufe von „14":

```
db.Employee.findAndModify({
    query: { "Employeeid" : 1, "name" : "Matt"},
    update: { "Employeeid" : 1, "name" : "Matt", "lastname" : "Winkle", "level" :
 14 }
})
```

Die folgende Ausgabe wird angezeigt (beachten Sie, dass sich der Pegel noch nicht geändert hat):

```
{
```

```
   _id: ObjectId('679d02cd6b5a0581be78bcbd'),

   Employeeid: 1,

   name: 'Matt',

   lastname: 'Winkle',

   level: 12

}
```

8. Geben Sie die folgende Abfrage ein, um den Levelanstieg zu überprüfen:

```
db.Employee.find({name: "Matt"})
```

Die folgende Ausgabe wird angezeigt:

```
[
   {

   _id: ObjectId('679d02cd6b5a0581be78bcbd'),

   Employeeid: 1,

   name: 'Matt',

   lastname: 'Winkle',

   level: 14

   }
]
```

Schritt 4: Erkunden

Herzlichen Glückwunsch! Sie haben das Verfahren Erste Schritte für Amazon DocumentDB Elastic Clusters erfolgreich abgeschlossen.

Was kommt als Nächstes? Erfahren Sie, wie Sie diese Datenbank mit einigen ihrer beliebten Funktionen voll ausschöpfen können:

- Bewährte Methoden für Amazon DocumentDB Elastic Cluster
- Verwaltung elastischer Amazon DocumentDB-Cluster

> **Note**
>
> Für den Elastic Cluster, den Sie im Rahmen dieser ersten Schritte erstellt haben, fallen weiterhin Kosten an, sofern Sie ihn nicht löschen. Eine Anleitung finden Sie unter Löschen eines elastischen Clusters.

Bewährte Methoden für Amazon DocumentDB Elastic Cluster

Lernen Sie bewährte Methoden für die Arbeit mit elastischen Amazon DocumentDB-Clustern kennen. Alle bewährten Methoden für instanzbasierte Amazon DocumentDB-Cluster gelten auch für elastische Cluster. Dieser Abschnitt wird fortlaufend aktualisiert, wenn neue bewährte Methoden identifiziert werden.

Topics

- Shard-Schlüssel auswählen
- Verbindungsverwaltung
- Sammlungen, die nicht geteilt wurden
- Skalierung elastischer Cluster
- Überwachung elastischer Cluster

Shard-Schlüssel auswählen

In der folgenden Liste werden Richtlinien für die Erstellung von Shard-Schlüsseln beschrieben.

- Verwenden Sie einen gleichmäßig verteilten Hashschlüssel, um Ihre Daten auf alle Shards in Ihrem Cluster zu verteilen (vermeiden Sie Hotkeys).
- Verwenden Sie Ihren Shard-Schlüssel in allen read/update /delete-Anfragen, um Scatter-Gather-Abfragen zu vermeiden.
- Vermeiden Sie verschachtelte Shard-Schlüssel, wenn Sie /delete-Operationen ausführen. read/update

- Wenn Sie Batch-Operationen ausführen, sollten Sie `ordered` den Wert auf False setzen, damit alle Shards parallel ausgeführt werden können und die Latenzen verbessert werden.

Verbindungsverwaltung

In der folgenden Liste werden Richtlinien für die Verwaltung Ihrer Verbindungen zu Ihrer Datenbank beschrieben.

- Überwachen Sie die Anzahl Ihrer Verbindungen und wie häufig neue Verbindungen geöffnet und geschlossen werden.
- Verteilen Sie Ihre Verbindungen auf alle Subnetze in der Konfiguration Ihrer Anwendung. Wenn Ihr Cluster in mehreren Subnetzen konfiguriert ist, Sie aber nur eine Teilmenge der Subnetze nutzen, kann es zu Engpässen bei der maximalen Anzahl von Verbindungen kommen.

Sammlungen, die nicht geteilt wurden

Im Folgenden wird eine Richtlinie für Sammlungen ohne Sharding beschrieben.

- Versuchen Sie bei der Arbeit mit Sammlungen ohne Sharded, um die Last zu verteilen, häufig genutzte Sammlungen ohne Sharded in verschiedenen Datenbanken zu speichern. Elastische Amazon DocumentDB-Cluster platzieren Datenbanken auf verschiedenen Shards und legen Sammlungen ohne Shards für dieselbe Datenbank auf demselben Shard zusammen.

Skalierung elastischer Cluster

In der folgenden Liste werden Richtlinien für die Skalierung Ihrer elastischen Cluster beschrieben.

- Skalierungsvorgänge können für einen kurzen Zeitraum zu zeitweiligen Datenbank- und Netzwerkfehlern führen. Vermeiden Sie nach Möglichkeit eine Skalierung zu Spitzenzeiten. Versuchen Sie, während der Wartungsfenster zu skalieren.
- Das Hoch- und Herunterskalieren der Shard-Kapazität (Änderung der vCPU-Anzahl pro Shard) zur Erhöhung der Rechenleistung wird dem Erhöhen oder Verringern der Shard-Anzahl vorgezogen, da dies schneller ist und eine kürzere Dauer von zeitweiligen Datenbank- und Netzwerkfehlern hat.
- Wenn Sie ein Wachstum erwarten, sollten Sie die Anzahl der Shards erhöhen, anstatt die Shard-Kapazität zu skalieren. Auf diese Weise können Sie Ihren Cluster skalieren, indem Sie die Shard-Kapazität für Szenarien erhöhen, in denen Sie schnell skalieren müssen.

- Überwachen Sie Ihre clientseitigen Wiederholungsrichtlinien und versuchen Sie es erneut mit exponentiellem Backoff und Jitter, um eine Überlastung Ihrer Datenbank zu vermeiden, wenn bei der Skalierung Fehler auftreten.
- Das Ändern der Anzahl der Shards kann einige Zeit in Anspruch nehmen, da Daten sicher von einem Shard auf einen anderen übertragen werden müssen. Um das Fehlerrisiko zu minimieren, empfehlen wir, den Clusterstatus während der Änderung nicht zu beenden oder anderweitig zu ändern.

Überwachung elastischer Cluster

In der folgenden Liste werden Richtlinien für die Überwachung Ihrer elastischen Cluster beschrieben.

- Verfolgen Sie das Verhältnis zwischen Spitzenwert und Durchschnitt Ihrer Metriken pro Shard, um festzustellen, ob Sie ungleichmäßigen Traffic generieren (einen Hotspot haben). key/hot Die wichtigsten Kennzahlen zur Erfassung des Verhältnisses zwischen Spitzenwert und Durchschnitt sind:
  - `PrimaryInstanceCPUUtilization`
    - Dies kann auf der Ebene pro Shard überwacht werden.
    - Auf Clusterebene können Sie den Mittelwert bis zur Abweichung von p99 überwachen.
  - `PrimaryInstanceFreeableMemory`
    - Dies kann auf der Ebene pro Shard überwacht werden.
    - Auf Clusterebene können Sie den Mittelwert bis zur Abweichung von p99 überwachen.
  - `DatabaseCursorsMax`
    - Dies sollte auf der Ebene pro Shard überwacht werden, um die Verzerrung zu ermitteln.
  - `Documents-Inserted/Updated/Returned/Deleted`
    - Dies sollte auf der Ebene pro Shard überwacht werden, um die Verzerrung zu ermitteln.

Verwaltung elastischer Amazon DocumentDB-Cluster

Um einen elastischen Amazon DocumentDB-Cluster zu verwalten, benötigen Sie eine IAM-Richtlinie mit den entsprechenden Berechtigungen für die Amazon DocumentDB-Steuerebene. Diese Berechtigungen ermöglichen es Ihnen, Cluster zu erstellen, zu ändern und zu löschen. Die DocumentDBFullAccess Amazon-Richtlinie bietet alle erforderlichen Berechtigungen für die Verwaltung eines elastischen Amazon DocumentDB-Clusters.

Die folgenden Themen zeigen, wie Sie verschiedene Aufgaben bei der Arbeit mit elastischen Amazon DocumentDB-Clustern ausführen.

Topics

- Modifizieren elastischer Cluster-Konfigurationen
- Überwachen eines elastischen Clusters
- Löschen eines elastischen Clusters
- Verwaltung von Elastic Cluster-Snapshots
- Stoppen und Starten eines elastischen Amazon DocumentDB-Clusters
- Wartung elastischer Amazon DocumentDB-Cluster

Modifizieren elastischer Cluster-Konfigurationen

In diesem Abschnitt wird anhand der folgenden Anweisungen erklärt, wie Elastic Cluster entweder AWS CLI mit AWS-Managementkonsole oder geändert werden.

Die Änderung des Clusters wird hauptsächlich zur Skalierung von Shards verwendet, indem die Shard-Rechenkapazität erhöht oder verringert wird. and/or

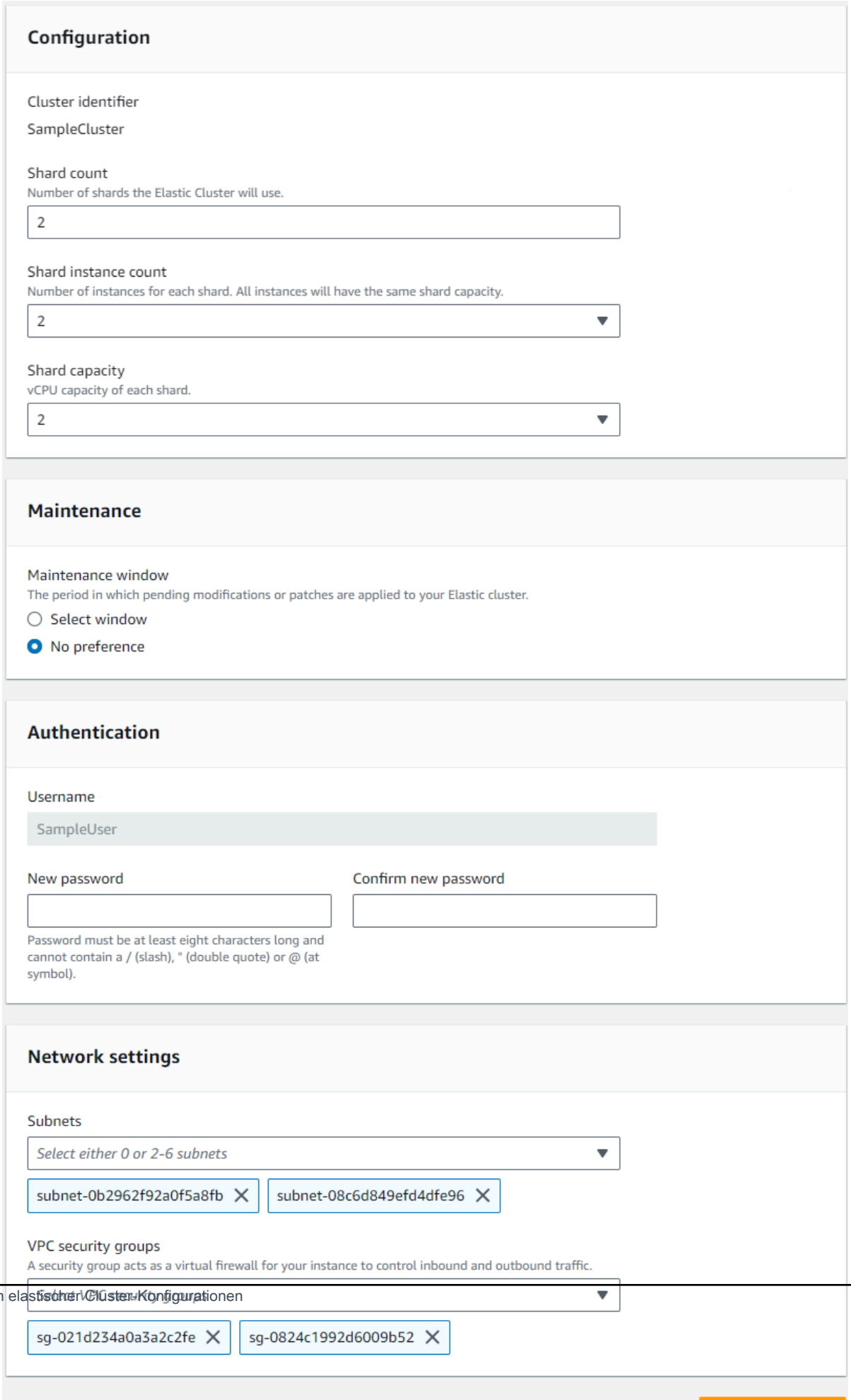
Using the AWS-Managementkonsole

Um eine elastische Cluster-Konfiguration zu ändern, verwenden Sie: AWS-Managementkonsole

1. Melden Sie sich bei der Amazon DocumentDB DocumentDB-Konsole an AWS-Managementkonsoleund öffnen Sie sie.
2. Klicken Sie im Navigationsbereich auf Cluster.

> **Tip**
>
> Wenn Sie den Navigationsbereich nicht auf der linken Seite Ihres Bildschirms sehen, wählen Sie das Menüsymbol in der oberen linken Ecke des Navigationsbereichs.

3. Wählen Sie in der Spalte Cluster-ID den Namen des Clusters aus, den Sie ändern möchten.
4. Wählen Sie Ändern aus.
5. Bearbeiten Sie die Felder, die Sie ändern möchten, und wählen Sie dann Cluster ändern aus.


Configuration
Cluster identifier
SampleCluster
Shard count
Number of shards the Elastic Cluster will use.
2
Shard instance count
Number of instances for each shard. All instances will have the same shard capacity.
2
Shard capacity
vCPU capacity of each shard.
2
Maintenance
Maintenance window
The period in which pending modifications or patches are applied to your Elastic cluster.
Select window
No preference
Authentication
Username
SampleUser
New password
Confirm new password
Password must be at least eight characters long and cannot contain a / (slash), " (double quote) or @ (at symbol).
Network settings
Subnets
Select either 0 or 2-6 subnets
subnet-0b2962f92a0f5a8fb
subnet-08c6d849efd4dfe96
VPC security groups
A security group acts as a virtual firewall for your instance to control inbound and outbound traffic.
sg-021d234a0a3a2c2fe
sg-0824c1992d6009b52

> **Note**
>
> Alternativ können Sie auf das Dialogfeld „Cluster ändern“ zugreifen, indem Sie auf der Seite Cluster das Kästchen neben Ihrem Cluster markieren und Aktionen und dann Ändern auswählen.

Using the AWS CLI

Um eine elastische Cluster-Konfiguration mithilfe von zu ändern AWS CLI, verwenden Sie den `update-cluster` Vorgang mit den folgenden Parametern:

- **`--cluster-arn`**—Erforderlich. Die ARN-ID des Clusters, den Sie ändern möchten.
- **`--shard-capacity`**— Fakultativ. Die Anzahl der vCPUs, die jedem Shard zugewiesen sind. Das Maximum ist 64. Zulässige Werte sind 2, 4, 8, 16, 32, 64.
- **`--shard-count`**— Fakultativ. Die Anzahl der dem Cluster zugewiesenen Shards. Das Maximum ist 32.
- **`--shard-instance`**-Anzahl — optional. Die Anzahl der Replikatinstanzen, die für alle Shards in diesem Cluster gelten. Das Maximum ist 16.
- **`--auth-type`**— Fakultativ. Der Authentifizierungstyp, der verwendet wird, um zu bestimmen, wo das für den Zugriff auf den Elastic Cluster verwendete Passwort abgerufen werden soll. Gültige Typen sind `PLAIN_TEXT` oder`SECRET_ARN`.
- **`--admin-user-password`**— Fakultativ. Das dem Admin-Benutzer zugeordnete Passwort.
- **`--vpc-security-group-ids`**— Fakultativ. Konfigurieren Sie eine Liste von Amazon EC2- und Amazon Virtual Private Cloud (VPC) -Sicherheitsgruppen, die diesem Cluster zugeordnet werden sollen.
- **`--preferred-maintenance-window`**— Optional. Konfigurieren Sie den wöchentlichen Zeitraum, in dem die Systemwartung erfolgen kann, in UTC (Universal Coordinated Time)

  Das Format ist:`ddd:hh24:mi-ddd:hh24:mi`. Gültige Tage (ddd): Mo, Di, Mi, Do, Fr, Sa, So

  Die Standardeinstellung ist ein 30-minütiges Fenster, das nach dem Zufallsprinzip aus einem 8-Stunden-Zeitblock für jede Amazon Web Services Services-Region ausgewählt wird und an einem zufälligen Wochentag stattfindet.

  Zeitfenster von mindestens 30 Minuten.
- **`--subnet-ids`**— Fakultativ. Konfigurieren Sie Netzwerk-Subnetz-IDs.

Ersetzen Sie im folgenden Beispiel jede *user input placeholder* durch Ihre eigenen Informationen.

Für Linux, macOS oder Unix:

```
aws docdb-elastic update-cluster \
    --cluster-arn arn:aws:docdb-elastic:us-east-1:477568257630:cluster/
b9f1d489-6c3e-4764-bb42-da62ceb7bda2 \
    --shard-capacity 8 \
    --shard-count 4 \
    --shard-instance-count 3 \
    --admin-user-password testPassword \
    --vpc-security-group-ids ec-65f40350 \
    --subnet-ids subnet-9253c6a3, subnet-9f1b5af9
```

Für Windows:

```
aws docdb-elastic update-cluster ^
    --cluster-arn arn:aws:docdb-elastic:us-east-1:477568257630:cluster/
b9f1d489-6c3e-4764-bb42-da62ceb7bda2 ^
    --shard-capacity 8 ^
    --shard-count 4 ^
    --shard-instance-count 3 ^
    --admin-user-password testPassword ^
    --vpc-security-group-ids ec-65f40350 ^
    --subnet-ids subnet-9253c6a3, subnet-9f1b5af9
```

Informationen zur Überwachung des Status des Elastic Clusters nach Ihrer Änderung finden Sie unter Elastic Cluster überwachen.

Überwachen eines elastischen Clusters

In diesem Abschnitt wird anhand der folgenden Anweisungen erklärt, wie Sie Ihren Elastic Cluster entweder AWS CLI mithilfe der AWS-Managementkonsole oder überwachen können.

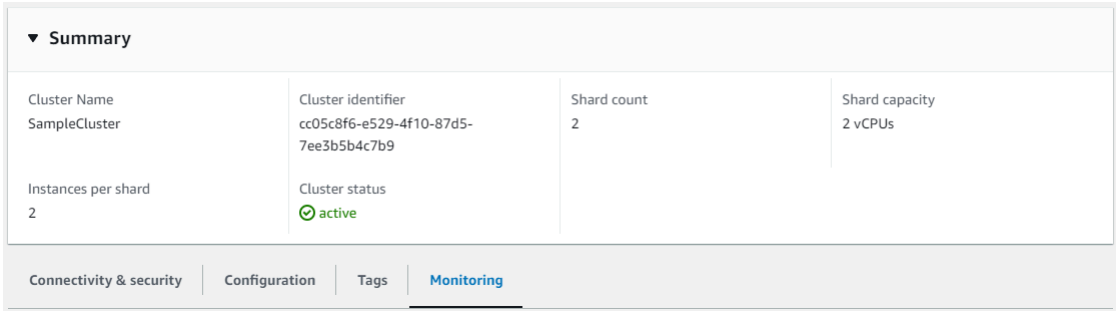
Using the AWS-Managementkonsole

Um eine elastische Cluster-Konfiguration zu überwachen, verwenden Sie AWS-Managementkonsole:

1. Melden Sie sich bei der Amazon DocumentDB DocumentDB-Konsole an AWS-Managementkonsoleund öffnen Sie sie.
2. Klicken Sie im Navigationsbereich auf Cluster.

> **Tip**
>
> Wenn Sie den Navigationsbereich nicht auf der linken Seite Ihres Bildschirms sehen, wählen Sie das Menüsymbol in der oberen linken Ecke des Navigationsbereichs.

3. Wählen Sie in der Spalte Cluster-ID den Namen des Clusters aus, den Sie überwachen möchten.
4. Wählen Sie die Registerkarte Überwachung.



CloudWatch Es werden eine Reihe von Diagrammen von Amazon für die folgenden Überwachungskategorien angezeigt:

- Nutzung der Ressourcen
- Durchsatz
- Operationen
- System (System)

Sie können auch CloudWatch über Amazon zugreifen AWS-Managementkonsole , um Ihre eigene Überwachungsumgebung für Ihre elastischen Cluster einzurichten.

Using the AWS CLI

Um eine bestimmte Elastic Cluster-Konfiguration mithilfe von zu überwachen AWS CLI, verwenden Sie den `get-cluster` Vorgang mit den folgenden Parametern:

- **`--cluster-arn`**—Erforderlich. Die ARN-ID des Clusters, für den Sie Informationen benötigen.

Ersetzen Sie im folgenden Beispiel jede *`user input placeholder`* durch Ihre eigenen Informationen.

Für Linux, macOS oder Unix:

```
aws docdb-elastic get-cluster \
    --cluster-arn arn:aws:docdb-elastic:us-west-2:123456789012:cluster:/68ffcdf8-e3af-40a3-91e4-24736f2dacc9
```

Für Windows:

```
aws docdb-elastic get-cluster ^
    --cluster-arn arn:aws:docdb:-elastic:us-west-2:123456789012:cluster:/68ffcdf8-e3af-40a3-91e4-24736f2dacc9
```

Die Ausgabe dieses Vorgangs sieht etwa wie folgt aus:

```
"cluster": {
        ...
        "clusterArn": "arn:aws:docdb-elastic:us-
west-2:123456789012:cluster:/68ffcdf8-e3af-40a3-91e4-24736f2dacc9",
        "clusterEndpoint": "stretch-11-477568257630.us-east-1.docdb-
elastic.amazonaws.com",
        "readerEndpoint": "stretch-11-477568257630-ro.us-east-1.docdb-
elastic.amazonaws.com",
        "clusterName": "stretch-11",
        "shardCapacity": 2,
        "shardCount": 3,
        "shardInstanceCount: 5,
        "status": "ACTIVE",
        ...
 }
```

Weitere Informationen finden Sie `DescribeClusterSnapshot` in der Amazon DocumentDB Resource Management API-Referenz.

Verwenden Sie den `list-clusters` Vorgang mit den folgenden Parametern AWS CLI, um die Details aller Elastic Cluster anzuzeigen, die den verwenden:

- **`--next-token`**— Optional. Wenn die Anzahl der ausgegebenen Elemente (`--max-results`) geringer als die Gesamtanzahl der Elemente ist, die von den zugrunde liegenden API-Aufrufen

zurückgeliefert werden, enthält die Ausgabe ein `NextToken`. Dieses können Sie in einem anschließenden Befehl zum Abrufen der nächsten Gruppe von Elementen übergeben.

- **`--max-results`**—Fakultativ. Die Gesamtzahl der Elemente, die in der Ausgabe des Befehls zurückgegeben werden sollen. Wenn mehr Ergebnisse als der angegebene `max-results` Wert vorhanden sind, ist ein Paginierungstoken (`next-token`) in der Antwort enthalten, sodass die verbleibenden Ergebnisse abgerufen werden können.
  - Standard: 100
  - Mindestens 20, maximal 100

Ersetzen Sie im folgenden Beispiel jede *`user input placeholder`* durch Ihre eigenen Informationen.

Für Linux, macOS oder Unix:

```
aws docdb-elastic list-clusters \
    --next-token eyJNYXJrZXIiOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQiOiAxfQ== \
    --max-results 2
```

Für Windows:

```
aws docdb-elastic list-clusters ^
    --next-token eyJNYXJrZXIiOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQiOiAxfQ== ^
    --max-results 2
```

Die Ausgabe dieses Vorgangs sieht etwa wie folgt aus:

```
{
   "Clusters": [
      {
         "ClusterIdentifier":"mycluster-1",
         "ClusterArn":"arn:aws:docdb:us-west-2:123456789012:sharded-cluster:sample-
cluster"
         "Status":"available",
         "ClusterEndpoint":"sample-cluster.sharded-cluster-corcjozrlsfc.us-
west-2.docdb.amazonaws.com"
       }
       {
         "ClusterIdentifier":"mycluster-2",
         "ClusterArn":"arn:aws:docdb:us-west-2:987654321098:sharded-cluster:sample-
cluster"
```

```
        "Status":"available",
        "ClusterEndpoint":"sample-cluster2.sharded-cluster-corcjozrlsfc.us-
west-2.docdb.amazonaws.com"
      }
   ]
}
```

Löschen eines elastischen Clusters

In diesem Abschnitt erklären wir, wie Sie einen elastischen Cluster löschen, indem Sie entweder die AWS-Managementkonsole oder AWS CLI verwenden, und die folgenden Anweisungen verwenden.

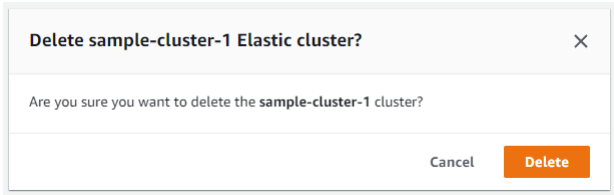
Using the AWS-Managementkonsole

Um eine elastische Cluster-Konfiguration zu löschen, verwenden Sie AWS-Managementkonsole:

1. Melden Sie sich bei der Amazon DocumentDB DocumentDB-Konsole an AWS-Managementkonsoleund öffnen Sie sie.
2. Klicken Sie im Navigationsbereich auf Cluster.

> **Tip**
>
> Wenn Sie den Navigationsbereich nicht auf der linken Seite Ihres Bildschirms sehen, wählen Sie das Menüsymbol in der oberen linken Ecke des Navigationsbereichs.

3. Aktivieren Sie in der Cluster-Listentabelle das Kontrollkästchen links neben dem Clusternamen, den Sie löschen möchten, und wählen Sie dann Aktionen aus. Wählen Sie im Dropdown-Menü Löschen aus.
4. Im elastischen Cluster „Clustername“ löschen? Wählen Sie im Dialogfeld Löschen aus.



Es dauert einige Minuten, bis der Cluster gelöscht ist. Informationen zur Überwachung des Clusterstatus finden Sie unter Überwachen des Status eines Amazon DocumentDB-Clusters.

Using the AWS CLI

Um einen Elastic Cluster mit dem zu löschen AWS CLI, verwenden Sie den `delete-cluster` Vorgang mit den folgenden Parametern:

- **`--cluster-arn`**—Erforderlich. Die ARN-ID des Clusters, den Sie löschen möchten.
- **`--no-skip-final-backup`**— Fakultativ. Wenn Sie eine endgültige Sicherung wünschen, müssen Sie diesen Parameter zusammen mit einem Namen für die endgültige Sicherung angeben. Sie müssen entweder `--final-backup-identifier` oder `--skip-final-backup` angeben.
- **`--skip-final-backup`**— Fakultativ. Verwenden Sie diesen Parameter nur, wenn Sie vor dem Löschen Ihres Clusters kein letztes Backup erstellen möchten. Standardmäßig wird ein letzter Snapshot erstellt.

Die folgenden AWS CLI Codebeispiele löschen einen Cluster mit dem ARN arn:aws:docdb:us-west- 2:123456789012:sharded-cluster:sample-cluster mit einer endgültigen Sicherung.

*`user input placeholder`*Ersetzen Sie im folgenden Beispiel jede durch Ihre eigenen Informationen..

Für Linux, macOS oder Unix:

```
aws docdb-elastic delete-cluster \
    --cluster-arn arn:aws:docdb:us-west-2:123456789012:sharded-cluster:sample-cluster \
    --no-skip-final-backup \
    --final-backup-identifier finalArnBU-arn:aws:docdb:us-west-2:123456789012:sharded-cluster:sample-cluster
```

Für Windows:

```
aws docdb-elastic delete-cluster ^
    --cluster-arn arn:aws:docdb:us-west-2:123456789012:sharded-cluster:sample-cluster ^
    --no-skip-final-backup ^
    --final-backup-identifier finalArnBU-arn:aws:docdb:us-west-2:123456789012:sharded-cluster:sample-cluster
```

Die folgenden AWS CLI Codebeispiele löschen einen Cluster mit dem ARN arn:aws:docdb:us-west- 2:123456789012:sharded-cluster:sample-cluster, ohne eine endgültige Sicherung zu erstellen.

*user input placeholder*Ersetzen Sie im folgenden Beispiel jedes durch Ihre eigenen Informationen.

Für Linux, macOS oder Unix:

```
aws docdb-elastic delete-cluster \
    --cluster-arn arn:aws:docdb:us-west-2:123456789012:sharded-cluster:sample-cluster \
    --skip-final-backup \
```

Für Windows:

```
aws docdb-elastic delete-cluster ^
    --cluster-arn arn:aws:docdb:us-west-2:123456789012:sharded-cluster:sample-cluster ^
    --skip-final-backup ^
```

Die Ausgabe des `delete-cluster` Vorgangs ist eine Anzeige des Clusters, den Sie löschen.

Es dauert einige Minuten, bis der Cluster gelöscht ist. Informationen zur Überwachung des Clusterstatus finden Sie unter Überwachen des Status eines Amazon DocumentDB-Clusters.

Verwaltung von Elastic Cluster-Snapshots

Manuelle Snapshots können erstellt werden, nachdem ein elastischer Cluster erstellt wurde. Automatisierte Backups werden in dem Moment erstellt, in dem der Elastic Cluster-Snapshot erstellt wird.

> **Note**
>
> Ihr Elastic Cluster muss sich in dem `Available` Zustand befinden, in dem ein manueller Snapshot erstellt werden kann.

In diesem Abschnitt wird erklärt, wie Sie Elastic Cluster-Snapshots erstellen, anzeigen, wiederherstellen und löschen können.

Die folgenden Themen zeigen, wie Sie verschiedene Aufgaben bei der Arbeit mit Amazon DocumentDB Elastic Cluster-Snapshots ausführen.

Topics

- Einen manuellen Elastic Cluster-Snapshot erstellen
- Einen Elastic Cluster-Snapshot anzeigen
- Wiederherstellen eines Elastic Clusters aus einem Snapshot
- Einen Elastic Cluster-Snapshot wird kopiert
- Löschen eines Elastic Cluster-Snapshots
- Verwaltung eines automatischen Backups eines Elastic Cluster-Snapshots

Einen manuellen Elastic Cluster-Snapshot erstellen

In diesem Abschnitt erklären wir, wie Sie einen manuellen Elastic Cluster-Snapshot erstellen, indem Sie entweder die AWS-Managementkonsole oder AWS CLI die folgenden Anweisungen verwenden.

Using the AWS-Managementkonsole

Um einen manuellen Elastic Cluster-Snapshot zu erstellen, verwenden Sie AWS-Managementkonsole:

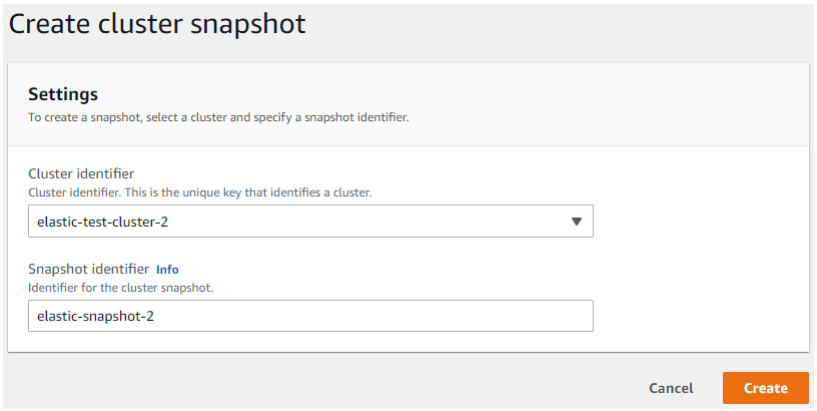
1. Melden Sie sich bei der Amazon DocumentDB DocumentDB-Konsole an AWS-Managementkonsoleund öffnen Sie sie.
2. Wählen Sie im Navigationsbereich die Option Snapshots.

   > **Tip**
   >
   > Wenn Sie den Navigationsbereich nicht auf der linken Seite Ihres Bildschirms sehen, wählen Sie das Menüsymbol in der oberen linken Ecke des Navigationsbereichs.

3. Wählen Sie auf der Seite Snapshots die Option Create (Erstellen) aus.
4. Wählen Sie auf der Seite Cluster-Snapshot erstellen im Feld Cluster-ID Ihren Elastic Cluster aus der Dropdownliste aus.

   Geben Sie im Feld Snapshot-Identifier eine eindeutige Kennung für Ihren Elastic Cluster ein.

   Wählen Sie Erstellen aus.



> **Note**
>
> Alternativ können Sie auf das Dialogfeld Cluster-Snapshot erstellen zugreifen, indem Sie auf der Seite Cluster das Kästchen neben Ihrem Cluster markieren und dann Aktionen und dann Snapshot erstellen auswählen.

Ihr Elastic Cluster-Snapshot wird jetzt bereitgestellt. Es kann bis zu ein paar Minuten dauern, bis dieser Vorgang abgeschlossen ist. Sie können Ihren Snapshot ansehen und aus diesem wiederherstellen, wenn der Status wie `Available` in der Snapshot-Liste angezeigt wird.

Using the AWS CLI

Um einen manuellen Elastic Cluster-Snapshot mit dem zu erstellen AWS CLI, verwenden Sie den `create-cluster-snapshot` Vorgang mit den folgenden Parametern:

- **`--snapshot-name`**—Erforderlich. Der Name des Cluster-Snapshots, den Sie erstellen möchten.
- **`--cluster-arn`**—Erforderlich. Die ARN-ID des Clusters, von dem Sie einen Snapshot erstellen möchten.

Ersetzen Sie im folgenden Beispiel jede *`user input placeholder`* durch Ihre eigenen Informationen.

Für Linux, macOS oder Unix:

```
aws docdb-elastic create-cluster-snapshot \
    --snapshot-name sample-snapshot-1 \
```

```
    --cluster-arn arn:aws:docdb:us-west-2:123456789012:sharded-cluster:sample-
cluster
```

Für Windows:

```
aws docdb-elastic create-cluster-snapshot ^
    --snapshot-name sample-snapshot-1 ^
    --cluster-arn arn:aws:docdb:us-west-2:123456789012:sharded-cluster:sample-
cluster
```

Einen Elastic Cluster-Snapshot anzeigen

In diesem Abschnitt wird anhand der folgenden Anweisungen erklärt, wie Sie Elastic Cluster-Snapshot-Informationen anzeigen können. AWS-Managementkonsole AWS CLI

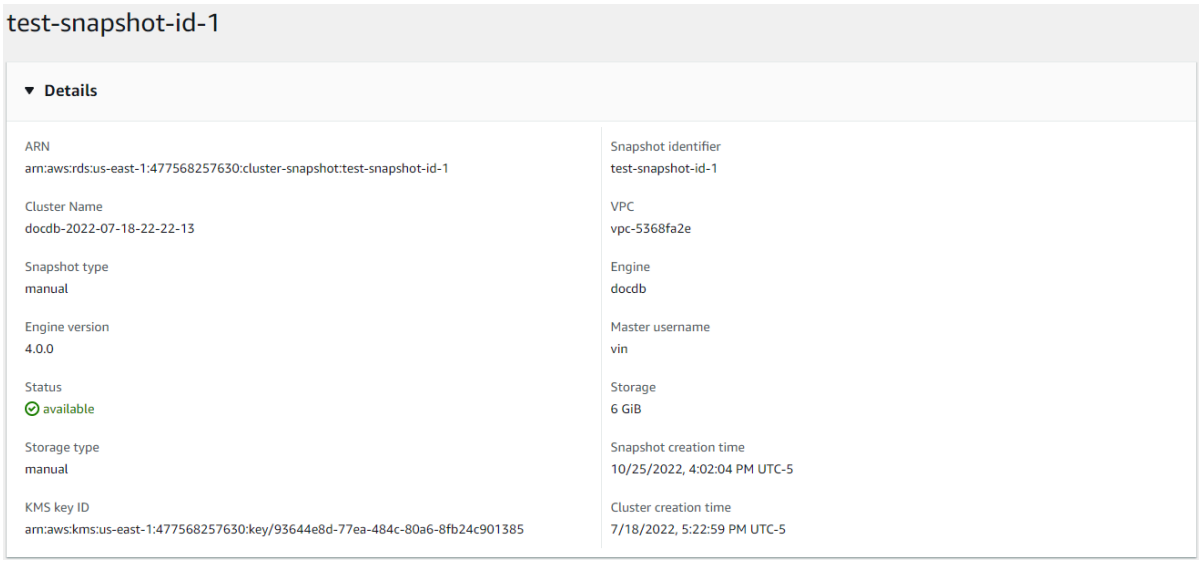
Using the AWS-Managementkonsole

Um Informationen zu einem bestimmten Elastic Cluster-Snapshot anzuzeigen, verwenden Sie AWS-Managementkonsole:

1. Melden Sie sich bei der Amazon DocumentDB DocumentDB-Konsole an AWS-Managementkonsoleund öffnen Sie sie.
2. Wählen Sie im Navigationsbereich die Option Snapshots.

   > **Tip**
   >
   > Wenn Sie den Navigationsbereich nicht auf der linken Seite Ihres Bildschirms sehen, wählen Sie das Menüsymbol in der oberen linken Ecke des Navigationsbereichs.

3. Wählen Sie auf der Seite Snapshots Ihren Snapshot aus der Liste aus, indem Sie in der Spalte Snapshot-ID auf den Namen klicken.
4. Sehen Sie sich die Informationen zu Ihrem Snapshot unter Details an.



Using the AWS CLI

Verwenden Sie den `get-cluster-snapshot` Vorgang mit den folgenden Parametern AWS CLI, um Informationen zu einem bestimmten Elastic Cluster-Snapshot mithilfe von anzuzeigen:

- **`--snapshot-arn`**—Erforderlich. Die ARN-ID des Snapshots, für den Sie Informationen benötigen.

Ersetzen Sie im folgenden Beispiel jede *`user input placeholder`* durch Ihre eigenen Informationen.

Für Linux, macOS oder Unix:

```
aws docdb-elastic get-cluster-snapshot \
    --snapshot-arn sampleResourceName
```

Für Windows:

```
aws docdb-elastic get-cluster-snapshot ^
    --snapshot-arn sampleResourceName
```

Verwenden Sie den `get-cluster-snapshot` Vorgang mit den folgenden Parametern AWS CLI, um Informationen zu einem bestimmten Elastic Cluster-Snapshot mithilfe von anzuzeigen:

- **`--snapshot-arn`**—Erforderlich. Die ARN-ID des Snapshots, für den Sie Informationen benötigen.

Ersetzen Sie im folgenden Beispiel jede *`user input placeholder`* durch Ihre eigenen Informationen.

Für Linux, macOS oder Unix:

```
aws docdb-elastic get-cluster-snapshot \
    --snapshot-arn sampleResourceName
```

Für Windows:

```
aws docdb-elastic get-cluster-snapshot ^
    --snapshot-arn sampleResourceName
```

Verwenden Sie den `list-cluster-snapshots` Vorgang mit den folgenden Parametern, um Informationen zu allen Elastic Cluster-Snapshots anzuzeigen AWS CLI, die den verwenden:

- **`--snapshot-type`**— Optional. Der Typ der Cluster-Snapshots, die zurückgegeben werden sollen. Sie können einen der folgenden Werte angeben:
  - `automated`- Gibt alle Cluster-Snapshots zurück, die Amazon DocumentDB automatisch für Ihr AWS Konto erstellt hat.
  - `manual`- Gibt alle Cluster-Snapshots zurück, die Sie manuell für Ihr Konto erstellt haben. AWS
  - `shared`- Gibt alle manuellen Cluster-Snapshots zurück, die für Ihr AWS Konto freigegeben wurden.
  - `public`- Gibt alle Cluster-Snapshots zurück, die als öffentlich markiert wurden.
- **`--next-token`**— Fakultativ. Ein optionales Paginierungstoken, das von einer vorherigen Anforderung bereitgestellt wird. Wenn dieser Parameter angegeben ist, umfasst die Antwort nur Datensätze, die über dieses Token hinausgehen, bis zu dem von `max-results` angegebenen Wert.
- **`--max-results`**— Optional. Die maximale Anzahl von Ergebnissen, die in die Antwort aufgenommen werden sollen. Wenn mehr Ergebnisse als der angegebene `max-results` Wert

vorhanden sind, ist ein Paginierungstoken (`next-token`) in der Antwort enthalten, sodass die verbleibenden Ergebnisse abgerufen werden können.

- Standard: 100
- Mindestens 20, maximal 100

Ersetzen Sie im folgenden Beispiel jede *`user input placeholder`* durch Ihre eigenen Informationen.

Für Linux, macOS oder Unix:

```
aws docdb-elastic list-cluster-snapshots \
    --snapshot-type  value \
    --next-token  value \
    --max-results 50
```

Für Windows:

```
aws docdb-elastic list-cluster-snapshots ^
    --snapshot-type  value ^
    --next-token  value ^
    --max-results 50
```

Wiederherstellen eines Elastic Clusters aus einem Snapshot

In diesem Abschnitt wird anhand der folgenden Anweisungen erklärt, wie Sie einen Elastic Cluster aus einem Snapshot wiederherstellen, indem Sie entweder die AWS-Managementkonsole oder AWS CLI verwenden.

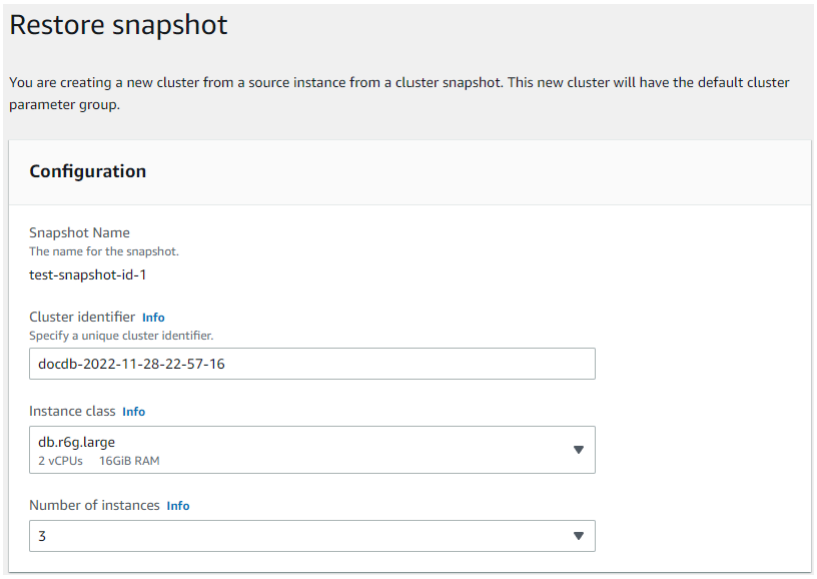
Using the AWS-Managementkonsole

Um einen Elastic Cluster aus einem Snapshot wiederherzustellen, verwenden Sie AWS-Managementkonsole:

1. Melden Sie sich bei der Amazon DocumentDB DocumentDB-Konsole an AWS-Managementkonsoleund öffnen Sie sie.
2. Wählen Sie im Navigationsbereich die Option Snapshots.

> **Tip**
>
> Wenn Sie den Navigationsbereich nicht auf der linken Seite Ihres Bildschirms sehen, wählen Sie das Menüsymbol in der oberen linken Ecke des Navigationsbereichs.

3. Wählen Sie in der Spalte Snapshot-ID die Schaltfläche links neben dem Snapshot, den Sie zum Wiederherstellen eines Clusters verwenden möchten.
4. Wählen Sie Aktionen und dann Wiederherstellen aus.



5. Geben Sie auf der Seite „Snapshot wiederherstellen“ einen Namen für den neuen Cluster in das Feld Cluster-ID ein.

> **Note**
>
> Für jede manuelle Snapshot-Wiederherstellung müssen Sie einen neuen Cluster erstellen.

6. Wählen Sie im Feld Virtual Private Cloud (VPC) eine VPC aus der Drop-down-Liste aus.
7. Für Subnetze und VPC-Sicherheitsgruppen können Sie die Standardeinstellungen verwenden oder drei Subnetze Ihrer Wahl und bis zu drei VPC-Sicherheitsgruppen (mindestens eine) auswählen.
8. Wenn Sie mit der Cluster-Konfiguration zufrieden sind, wählen Sie Restore cluster (Cluster wiederherstellen) aus und warten Sie, bis Ihr Cluster wiederhergestellt ist.

Using the AWS CLI

Verwenden Sie den Vorgang mit den folgenden Parametern, um einen Elastic Cluster aus einem Snapshot mithilfe von wiederherzustellen: AWS CLI`restore-cluster-from-snapshot`

- **`--cluster-name`**—Erforderlich. Der aktuelle Name des elastischen Clusters, wie er bei der Erstellung eingegeben oder zuletzt geändert wurde.
- **`--snapshot-arn`**—Erforderlich. Die ARN-ID des Snapshots, der zur Wiederherstellung des Clusters verwendet wird.
- **`--vpc-security-group-ids`**— Fakultativ. Eine oder mehrere Amazon EC2- und Amazon Virtual Private Cloud (VPC) -Sicherheitsgruppen, die dem Cluster zugeordnet werden sollen.
- **`--kms-key-id`**— Optional. Konfigurieren Sie die KMS-Schlüssel-ID für einen verschlüsselten Cluster.

  Die KMS-Schlüssel-ID ist der Amazon-Ressourcenname (ARN) für den AWS KMS Verschlüsselungsschlüssel. Wenn Sie einen Cluster mit demselben Amazon Web Services Services-Konto erstellen, dem der KMS-Verschlüsselungsschlüssel gehört, der zur Verschlüsselung des neuen Clusters verwendet wird, können Sie den KMS-Schlüsselalias anstelle des ARN für den KMS-Verschlüsselungsschlüssel verwenden.

  Wenn in kein Verschlüsselungsschlüssel angegeben ist KmsKeyId und der `StorageEncrypted` Parameter wahr ist, verwendet Amazon DocumentDB Ihren Standard-Verschlüsselungsschlüssel.
- **`--subnet-ids`**— Optional. Netzwerk-Subnetz-IDs.

Ersetzen Sie im folgenden Beispiel jede *`user input placeholder`* durch Ihre eigenen Informationen.

Für Linux, macOS oder Unix:

```
aws docdb-elastic restore-cluster-from-snapshot \
     --cluster-name elastic-sample-cluster \
     --snapshot-arn sampleResourceName \
     --vpc-security-group-ids value ec-65f40350 \
     --kms-key-id arn:aws:docdb-elastic:us-east-1:477568257630:cluster/
b9f1d489-6c3e-4764-bb42-da62ceb7bda2 \
     --subnet-ids subnet-9253c6a3, subnet-9f1b5af9
```

Für Windows:

```
aws docdb-elastic restore-cluster-from-snapshot ^
     --cluster-name elastic-sample-cluster ^
     --snapshot-arn sampleResourceName ^
     --vpc-security-group-ids value ec-65f40350 ^
     --kms-key-id arn:aws:docdb-elastic:us-east-1:477568257630:cluster/
b9f1d489-6c3e-4764-bb42-da62ceb7bda2 ^
     --subnet-ids subnet-9253c6a3, subnet-9f1b5af9
```

Einen Elastic Cluster-Snapshot wird kopiert

In Amazon DocumentDB können Sie manuelle und automatische Elastic Cluster-Snapshots innerhalb derselben Region und innerhalb desselben Kontos kopieren. In diesem Abschnitt wird erklärt, wie Sie einen Elastic Cluster-Snapshot kopieren, indem Sie entweder das AWS-Managementkonsole oder verwenden. AWS CLI

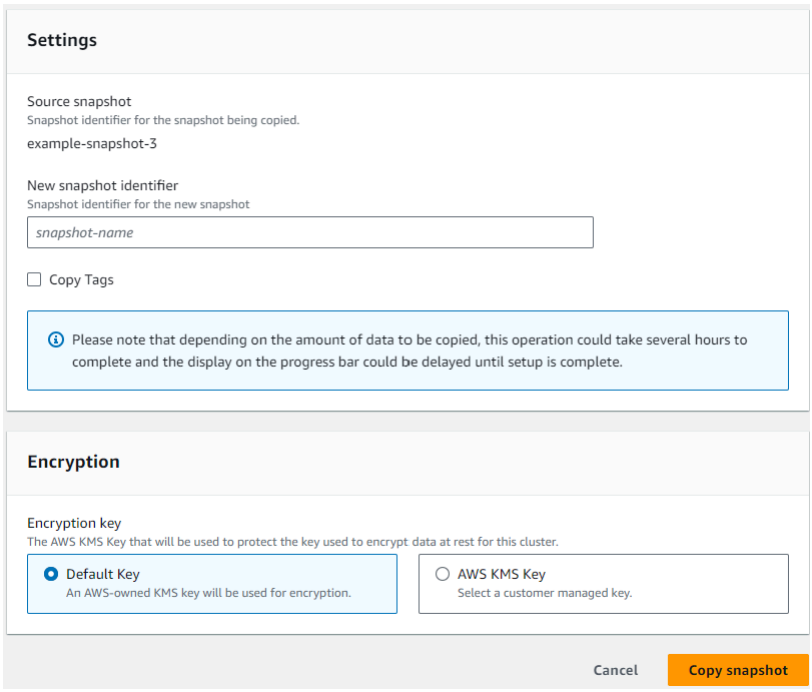
Using the AWS-Managementkonsole

Um einen Elastic Cluster-Snapshot zu kopieren, verwenden Sie AWS-Managementkonsole:

1. Melden Sie sich bei der Amazon DocumentDB DocumentDB-Konsole an AWS-Managementkonsoleund öffnen Sie sie.
2. Wählen Sie im Navigationsbereich die Option Snapshots.

   > **Tip**
   >
   > Wenn Sie den Navigationsbereich nicht auf der linken Seite Ihres Bildschirms sehen, wählen Sie das Menüsymbol in der oberen linken Ecke des Navigationsbereichs.

3. Wählen Sie in der Spalte Snapshot-ID die Schaltfläche links neben dem Snapshot, den Sie kopieren möchten.
4. Wählen Sie „Aktionen“ und dann „Kopieren“.



5. Geben Sie unter Neuer Snapshot-Identifier den Namen des neuen Snapshots ein.
6. Aktivieren Sie für Copy Tags das Kontrollkästchen, wenn Sie alle Tags aus dem Elastic Cluster-Quell-Snapshot in den Elastic Cluster-Ziel-Snapshot kopieren möchten.
7. Wählen Sie für die Verschlüsselung entweder einen AWS Standard-KMS-Schlüssel oder einen KMS-Schlüssel Ihrer Wahl. Mit der zweiten Option können Sie einen vorhandenen KMS-Schlüssel auswählen, den Sie bereits erstellt haben, oder einen neuen erstellen.
8. Wählen Sie Snapshot kopieren, wenn Sie fertig sind.

Using the AWS CLI

Um einen Elastic Cluster-Snapshot mit dem zu kopieren AWS CLI, verwenden Sie den `copy-cluster-snapshot` Vorgang mit den folgenden Parametern:

- **`--source-db-cluster-snapshot-identifier`**—Erforderlich. Die ID des vorhandenen Elastic Cluster-Snapshots, der kopiert wird. Der Elastic Cluster-Snapshot muss vorhanden sein und sich im verfügbaren Zustand befinden. Bei diesem Parameter wird nicht zwischen Groß- und Kleinschreibung unterschieden.
- **`--target-db-cluster-snapshot-identifier`**—Erforderlich. Die ID des neuen Elastic Cluster-Snapshots, der aus dem vorhandenen Cluster-Snapshot erstellt werden soll. Bei diesem Parameter wird nicht zwischen Groß- und Kleinschreibung unterschieden.

Einschränkungen beim Namen des Ziel-Snapshots:

- Kann nicht der Namen eines vorhandenen Snapshots sein.
- Die Länge beträgt [1—63] Buchstaben, Zahlen oder Bindestriche.
- Muss mit einem Buchstaben beginnen.
- Darf nicht mit einem Bindestrich enden oder zwei aufeinanderfolgende Bindestriche enthalten.

Ersetzen Sie im folgenden Beispiel jede durch Ihre *user input placeholder* eigenen Informationen.

Für Linux, macOS oder Unix:

```
aws docdb-elastic copy-cluster-snapshot \
     --source-cluster-snapshot-arn <sample ARN> \
     --target-cluster-snapshot-name my-target-copied-snapshot
```

Für Windows:

```
aws docdb-elastic copy-cluster-snapshot ^
     --source-cluster-snapshot-arn <sample ARN> ^
     --target-cluster-snapshot-name my-target-copied-snapshot
```

Löschen eines Elastic Cluster-Snapshots

In diesem Abschnitt wird erklärt, wie Sie einen Elastic Cluster-Snapshot löschen, indem Sie entweder das AWS-Managementkonsole oder verwenden AWS CLI.

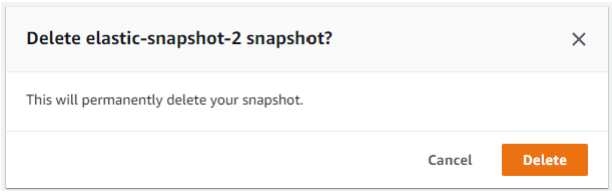
Using the AWS-Managementkonsole

Um einen Elastic Cluster aus einem Snapshot wiederherzustellen, verwenden Sie AWS-Managementkonsole:

1. Melden Sie sich bei der Amazon DocumentDB DocumentDB-Konsole an AWS-Managementkonsoleund öffnen Sie sie.
2. Wählen Sie im Navigationsbereich die Option Snapshots.

> **Tip**
>
> Wenn Sie den Navigationsbereich nicht auf der linken Seite Ihres Bildschirms sehen, wählen Sie das Menüsymbol in der oberen linken Ecke des Navigationsbereichs.

3. Wählen Sie in der Spalte Snapshot-ID die Schaltfläche links neben dem Snapshot, den Sie zum Wiederherstellen eines Clusters verwenden möchten.
4. Wählen Sie Aktionen und dann Löschen aus.



5. Wählen Sie im Dialogfeld „Snapshot-Name“ -Snapshot löschen die Option Löschen aus.

Using the AWS CLI

Um einen Elastic Cluster-Snapshot mit dem zu löschen AWS CLI, verwenden Sie den `delete-cluster-snapshot` Vorgang mit den folgenden Parametern:

- **`--snapshot-arn`**—Erforderlich. Die ARN-ID des Snapshots, der zur Wiederherstellung des Clusters verwendet wird.

Ersetzen Sie im folgenden Beispiel jede *`user input placeholder`* durch Ihre eigenen Informationen.

Für Linux, macOS oder Unix:

```
aws docdb-elastic delete-cluster-snapshot \
     --snapshot-arn sampleResourceName
```

Für Windows:

```
aws docdb-elastic delete-cluster-snapshot ^
     --snapshot-arn sampleResourceName
```

Verwaltung eines automatischen Backups eines Elastic Cluster-Snapshots

Amazon DocumentDB erstellt täglich Schnappschüsse Ihrer elastischen Cluster. Sie können das bevorzugte Backup-Fenster und den Aufbewahrungszeitraum für Backups in einer neuen oder vorhandenen Elastic Cluster-Snapshot-Konfiguration angeben. In diesem Abschnitt wird erklärt, wie Sie automatische Backup-Parameter in einem Elastic Cluster-Snapshot festlegen, indem Sie entweder das AWS-Managementkonsole oder verwenden AWS CLI.

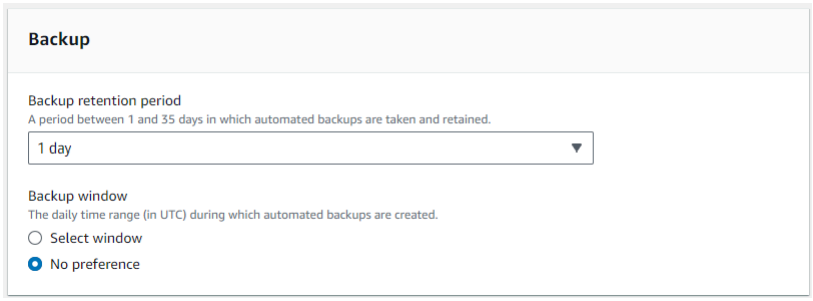
Using the AWS-Managementkonsole

Um ein automatisches Backup für einen neuen Elastic Cluster-Snapshot einzurichten, verwenden Sie AWS-Managementkonsole:

1. Melden Sie sich bei der Amazon DocumentDB DocumentDB-Konsole an AWS-Managementkonsoleund öffnen Sie sie.
2. Klicken Sie im Navigationsbereich auf Cluster.

> **Tip**
>
> Wenn Sie den Navigationsbereich nicht auf der linken Seite Ihres Bildschirms sehen, wählen Sie das Menüsymbol in der oberen linken Ecke des Navigationsbereichs.

3. Wählen Sie in der Spalte Cluster-ID die Schaltfläche links neben dem Cluster, für den Sie die Backup-Einstellungen ändern möchten.
4. Wählen Sie „Aktionen“ und dann „Ändern“.
5. Bearbeiten Sie im Abschnitt Backup die Felder entsprechend Ihren Backup-Anforderungen.



   a. Aufbewahrungszeitraum für Backup — Wählen Sie in der Liste die Anzahl der Tage aus, für die automatische Backups dieses Clusters aufbewahrt werden sollen, bevor sie gelöscht werden.

b. Backup-Fenster — Legen Sie die tägliche Uhrzeit und Dauer fest, während der Amazon DocumentDB Backups dieses Clusters erstellen soll.

   i. Wählen Sie Fenster auswählen, wenn Sie die Uhrzeit und Dauer der Erstellung von Backups konfigurieren möchten.

      Startzeit — Wählen Sie in der ersten Liste die Startzeit (UTC) für den Start Ihrer automatischen Backups aus. Wählen Sie in der zweiten Liste die Minute für den Beginn der automatischen Backups aus.

      Dauer — Wählen Sie in der Liste die Anzahl der Stunden aus, die für die Erstellung automatischer Backups reserviert werden sollen.

   ii. Wählen Sie Keine Präferenz, wenn Amazon DocumentDB den Zeitpunkt und die Dauer der Erstellung von Backups wählen soll.

6. Wählen Sie Cluster modifizieren, wenn der Vorgang abgeschlossen ist.

Using the AWS CLI

Um ein automatisches Backup für einen neuen Elastic Cluster-Snapshot mithilfe von einzurichten AWS CLI, verwenden Sie den `create-cluster-snapshot` Vorgang mit den folgenden Parametern:

- **`--preferred-backup-window`**— Optional. Der bevorzugte tägliche Zeitraum, in dem automatische Backups erstellt werden. Die Standardeinstellung ist ein 30-minütiges Fenster, das nach dem Zufallsprinzip aus einem Zeitblock von jeweils AWS-Region 8 Stunden ausgewählt wird.

  Einschränkungen:

  - Muss im Format `hh24:mi-hh24:mi` angegeben werden.
  - Muss in Universal Coordinated Time (UTC) angegeben werden.
  - Darf nicht mit dem bevorzugten Wartungsfenster in Konflikt treten.
  - Muss mindestens 30 Minuten betragen.
- **`--backup-retention-period`**— Fakultativ. Die Anzahl von Tagen, über die automatische Backups aufbewahrt werden. Der Standardwert ist 1.

  Einschränkungen:

  - Es muss ein Mindestwert von 1 angegeben werden.

- Der Bereich liegt zwischen 1 und 35.

> **Note**
>
> Automatisierte Backups werden nur erstellt, wenn sich der Cluster im Status „aktiv“ befindet.

> **Note**
>
> Sie können auch die `backup-retention-period` Parameter `preferred-backup-window` und eines vorhandenen Elastic Clusters mithilfe des `aws docdb-elastic update-cluster` Befehls ändern.

Ersetzen Sie im folgenden Beispiel jede Information *`user input placeholder`* durch Ihre eigenen Informationen.

Im folgenden `create-cluster` Beispiel wird der elastische Amazon DocumentDB-Cluster *`sample-cluster`* mit einer Aufbewahrungsdauer für automatische Backups von *`7`* Tagen und einem bevorzugten Backup-Fenster von *`18:00-18:30 UTC`* erstellt.

Für Linux, macOS oder Unix:

```
aws docdb-elastic create-cluster \
     --cluster-name sample-cluster \
     --shard-capacity 2 \
     --shard-count 2 \
     --admin-user-name SampleAdmin \
     --auth-type PLAIN_TEXT \
     --admin-user-password SamplePass123! \
     --preferred-backup-window 18:00-18:30 \
     --backup-retention-period 7
```

Für Windows:

```
aws docdb-elastic create-cluster ^
     --cluster-name sample-cluster ^
```

```
    --shard-capacity 2 ^
    --shard-count 2 ^
    --admin-user-name SampleAdmin ^
    --auth-type PLAIN_TEXT ^
    --admin-user-password SamplePass123! ^
    --preferred-backup-window 18:00-18:30 ^
    --backup-retention-period 7
```

Stoppen und Starten eines elastischen Amazon DocumentDB-Clusters

Das Stoppen und Starten von Amazon DocumentDB Elastic Clusters kann Ihnen helfen, die Kosten für Entwicklungs- und Testumgebungen zu verwalten. Anstatt jedes Mal, wenn Sie Amazon DocumentDB verwenden, elastische Cluster zu erstellen und zu löschen, können Sie Ihren Cluster vorübergehend beenden, wenn er nicht benötigt wird. Sie können ihn dann erneut starten, wenn Sie Ihre Tests fortsetzen.

Themen

- Überblick über das Stoppen und Starten eines Elastic Clusters
- Operationen, die Sie auf einem gestoppten Elastic Cluster ausführen können

Überblick über das Stoppen und Starten eines Elastic Clusters

In Zeiten, in denen Sie keinen elastischen Amazon DocumentDB-Cluster benötigen, können Sie den Cluster beenden. Bei Bedarf können Sie den Cluster jederzeit erneut starten. Das Starten und Stoppen vereinfacht die Einrichtungs- und Abbauprozesse für elastische Cluster, die für Entwicklungs-, Test- oder ähnliche Aktivitäten verwendet werden, für die keine kontinuierliche Verfügbarkeit erforderlich ist. Sie können einen Elastic Cluster mithilfe von AWS-Managementkonsole oder AWS CLI mit einer einzigen Aktion beenden und starten.

Während Ihr Elastic Cluster gestoppt ist, bleibt das Cluster-Speichervolumen unverändert. Sie zahlen nur für Speicherung, manuelle Snapshots und automatischen Sicherungsspeicher innerhalb des angegebenen Aufbewahrungsfensters. Amazon DocumentDB startet Ihren Elastic Cluster automatisch nach sieben Tagen, sodass er nicht hinter den erforderlichen Wartungsupdates zurückbleibt. Wenn Ihr Cluster nach sieben Tagen startet, wird Ihnen die Nutzung des Elastic Clusters wieder in Rechnung gestellt. Solange Ihr Cluster gestoppt ist, können Sie Ihr Speichervolume nicht abfragen, da die Abfrage voraussetzt, dass sich der Cluster im verfügbaren Status befindet.

Wenn ein elastischer Amazon DocumentDB-Cluster gestoppt wird, kann der Cluster in keiner Weise geändert werden. Dies beinhaltet das Löschen des Clusters.

Using the AWS-Managementkonsole

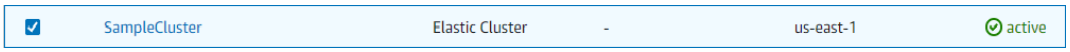
Das folgende Verfahren zeigt Ihnen, wie Sie einen elastischen Cluster im verfügbaren Zustand beenden oder einen gestoppten elastischen Cluster starten.

So beenden oder starten Sie einen elastischen Amazon DocumentDB-Cluster

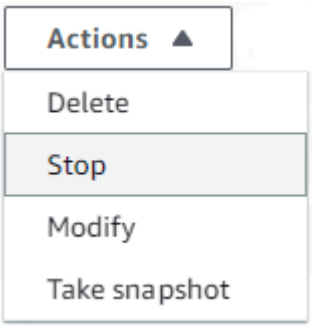
1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Klicken Sie im Navigationsbereich auf Cluster.

> **Tip**
>
> Wenn der Navigationsbereich auf der linken Seite des Bildschirms nicht angezeigt wird, wählen Sie links oben auf der Seite das Menüsymbol (≡) aus.

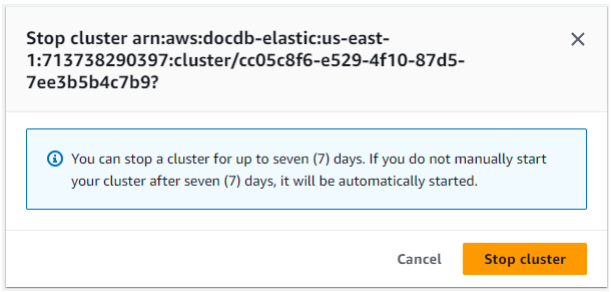
3. Wählen Sie in der Liste der Cluster die Schaltfläche links neben dem Namen des Clusters aus, den Sie stoppen oder starten möchten.



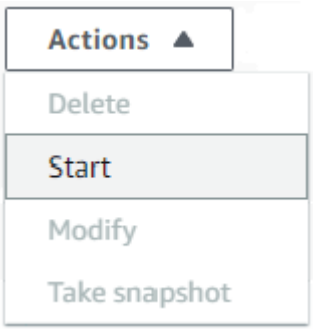
4. Wählen Sie Aktionen aus und dann die Aktion, die Sie auf dem Cluster ausführen möchten.
   - Wenn Sie den Cluster stoppen möchten und der Cluster verfügbar ist:
     a. Wählen Sie Beenden aus.



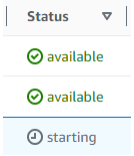
     b. Bestätigen Sie im Bestätigungsdialogfeld, dass Sie den Elastic Cluster beenden möchten, indem Sie Cluster beenden wählen, oder klicken Sie auf Abbrechen, um den Cluster am Laufen zu halten.



- Wenn Sie einen gestoppten Cluster starten möchten, wählen Sie Starten aus.



5. Überwachen Sie den Status des Elastic Clusters. Wenn Sie den Cluster gestartet haben, können Sie den Cluster wieder verwenden, sobald der Cluster verfügbar ist. Weitere Informationen finden Sie unter Den Status eines Clusters ermitteln.



Using the AWS CLI

Die folgenden Codebeispiele zeigen Ihnen, wie Sie einen elastischen Cluster im aktiven oder verfügbaren Zustand beenden oder einen gestoppten elastischen Cluster starten.

Verwenden Sie die `stop-cluster` Operation AWS CLI, um einen elastischen Cluster mithilfe von zu beenden. Verwenden Sie die `start-cluster`-Operation, um einen gestoppten Cluster zu starten. Beide Operationen verwenden den `--cluster-arn`-Parameter.

Parameter:

- **`--cluster-arn`**—Erforderlich. Der ARN-Bezeichner des Elastic Clusters, den Sie beenden oder starten möchten.

Example— Um einen elastischen Cluster mit dem zu beenden AWS CLI

Ersetzen Sie im folgenden Beispiel jede *user input placeholder* durch Ihre eigenen Informationen.

Der folgende Code stoppt den elastischen Cluster mit einem ARN von`arn:aws:docdb-elastic:us-east-1:477568257630:cluster/b9f1d489-6c3e-4764-bb42-da62ceb7bda2`.

> **Note**
>
> Der elastische Cluster muss sich im aktiven oder verfügbaren Zustand befinden.

Für Linux, macOS oder Unix:

```
aws docdb-elastic stop-cluster \
   --cluster-arn arn:aws:docdb-elastic:us-east-1:477568257630:cluster/
b9f1d489-6c3e-4764-bb42-da62ceb7bda2
```

Für Windows:

```
aws docdb-elastic stop-cluster ^
   --cluster-arn arn:aws:docdb-elastic:us-east-1:477568257630:cluster/
b9f1d489-6c3e-4764-bb42-da62ceb7bda2
```

Example— Um einen elastischen Cluster mit dem zu starten AWS CLI

Ersetzen Sie im folgenden Beispiel jede *user input placeholder* durch Ihre eigenen Informationen.

Der folgende Code startet den Elastic Cluster mit einem ARN von`arn:aws:docdb-elastic:us-east-1:477568257630:cluster/b9f1d489-6c3e-4764-bb42-da62ceb7bda2`.

> **Note**
>
> Der elastische Cluster muss derzeit gestoppt werden.

Für Linux, macOS oder Unix:

```
aws docdb-elastic start-cluster \
   --cluster-arn arn:aws:docdb-elastic:us-east-1:477568257630:cluster/
b9f1d489-6c3e-4764-bb42-da62ceb7bda2
```

Für Windows:

```
aws docdb-elastic start-cluster ^
   --cluster-arn arn:aws:docdb-elastic:us-east-1:477568257630:cluster/
b9f1d489-6c3e-4764-bb42-da62ceb7bda2
```

Operationen, die Sie auf einem gestoppten Elastic Cluster ausführen können

Sie können die Konfiguration eines elastischen Amazon DocumentDB-Clusters nicht ändern, solange der Cluster gestoppt ist. Vor solchen administrativen Aktionen müssen Sie den Cluster starten.

Amazon DocumentDB wendet alle geplanten Wartungsarbeiten auf Ihren gestoppten Elastic Cluster erst an, nachdem er erneut gestartet wurde. Nach sieben Tagen startet Amazon DocumentDB automatisch einen gestoppten Elastic Cluster, sodass er in seinem Wartungsstatus nicht zu weit zurückfällt. Wenn der Elastic Cluster neu gestartet wird, werden Ihnen die Shards im Cluster wieder in Rechnung gestellt.

Während ein elastischer Cluster gestoppt ist, führt Amazon DocumentDB keine automatisierten Backups durch und verlängert auch nicht den Aufbewahrungszeitraum für Backups.

Wartung elastischer Amazon DocumentDB-Cluster

Topics

- Ausstehende Wartungsaktionen für elastische Cluster anzeigen
- Aktualisierungen der Elastic Cluster Engine
- Betriebssystem-Updates für Elastic Cluster

Amazon DocumentDB führt regelmäßig Wartungsarbeiten an den Elastic Cluster-Ressourcen von Amazon DocumentDB durch. Die Wartung umfasst in den meisten Fällen Aktualisierungen der Datenbank-Engine (Elastic Cluster-Wartung) oder des dem Elastic Cluster zugrunde liegenden

Betriebssystems (Betriebssystem-Updates). Datenbank-Engine-Updates sind erforderliche Patches und beinhalten Sicherheitskorrekturen, Bugfixes und Verbesserungen der Datenbank-Engine. Die meisten Betriebssystem-Patches sind zwar optional, aber wenn Sie sie eine Zeit lang nicht anwenden, kann es sein, dass der Patch erforderlich ist und auto angewendet wird, um Ihren Sicherheitsstatus aufrechtzuerhalten. Wir empfehlen Ihnen daher, Betriebssystem-Updates auf Ihre elastischen Amazon DocumentDB-Cluster zu installieren, sobald sie verfügbar sind.

Datenbank-Engine-Patches erfordern, dass Sie Ihre elastischen Amazon DocumentDB-Cluster für kurze Zeit offline schalten. Sobald sie verfügbar sind, werden diese Patches automatisch so geplant, dass sie während eines bevorstehenden geplanten Wartungsfensters Ihres Amazon DocumentDB Elastic Clusters installiert werden.

Elastische Cluster haben ihre eigenen jeweiligen Wartungsfenster. Elastic Cluster-Änderungen, die Sie nicht sofort anwenden möchten, werden während des Wartungsfensters angewendet. Wenn Sie einen Elastic Cluster erstellen, weist Amazon DocumentDB standardmäßig ein Wartungsfenster für Ihren Elastic Cluster zu. Sie können das Wartungsfenster wählen, wenn Sie einen elastischen Cluster erstellen. Sie können die Wartungsfenster außerdem jederzeit an Ihre Geschäftspläne oder -praktiken anpassen. Es wird generell empfohlen, Wartungsfenster auszuwählen, die die Auswirkungen der Wartung auf Ihre Anwendung minimieren (z. B. an Abenden oder Wochenenden).

Ausstehende Wartungsaktionen für elastische Cluster anzeigen

Mithilfe von können Sie überprüfen, ob ein Wartungsupdate für Ihren Elastic Cluster verfügbar ist AWS CLI.

Wenn ein Update verfügbar ist, können Sie eine der folgenden Aktionen durchführen:

- Verschieben Sie eine Wartungsaktion, die derzeit für das nächste Wartungsfenster geplant ist (nur für Betriebssystem-Patches).
- Wenden Sie die Wartungsaktionen sofort an.
- Einplanen der Wartungsaktivitäten für das nächste Wartungsfenster.
- Planen Sie die Wartungsaktionen so, dass sie während des ausgewählten Anwendungsfensters beginnen.

Das Wartungsfenster legt fest, wann die ausstehenden Operationen gestartet werden, gibt aber kein Abschlussdatum für diese Operationen vor; die Ausführungsdauer ist weder bekannt noch a priori beschränkt.

Verwenden Sie den folgenden AWS CLI Vorgang, um festzustellen, welche Wartungsaktionen noch ausstehen. Listet alle ausstehenden Wartungsaktionen auf:

```
aws docdb-elastic list-pending-maintenance-actions
```

Die Ausgabe dieses Vorgangs sieht etwa wie folgt aus (JSON-Format):

```
{
'ResourcePendingMaintenanceActions': [
    {
        'ResourceArn': 'string-arn',
        'PendingMaintenanceActionDetails': [
            {
                'Action': 'ENGINE_UPDATE',
                'AutoAppliedAfterDate': 'string',
                'ForcedApplyDate': 'string',
                'OptInStatus': 'string',
                'CurrentApplyDate': 'string',
                'Description': 'string'
            },
        ]
    },
],
'NextToken': 'string'
}
```

Ruft ausstehende Wartungsmaßnahmen (falls vorhanden) für ein bestimmtes Objekt ab`resourceArn`:

```
aws docdb-elastic get-pending-maintenance-action --resource-arn string-arn
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus (JSON-Format).

```
{
    'ResourcePendingMaintenanceAction': {
        'ResourceArn': 'string-arn',
        'PendingMaintenanceActionDetails': [
            {
                'Action': 'ENGINE_UPDATE',
                'AutoAppliedAfterDate': 'string',
                'ForcedApplyDate': 'string',
```

```
                'OptInStatus': 'string',
                'CurrentApplyDate': 'string',
                'Description': 'string'
            }
        ]
    }
}
```

Parameter:

- `ResourceArn`— Der Amazon Resource Name (ARN) von Amazon DocumentDB der Ressource, für die die ausstehende Wartungsaktion gilt.
- `Action`— Die ausstehende Wartungsaktion, die auf die Ressource angewendet wird.

  Zulässige Werte:

  - `ENGINE_UPDATE`
  - `ENGINE_UPGRADE`
  - `SECURITY_UPDATE`
  - `OS_UPDATE`
  - `MASTER_USER_PASSWORD_UPDATE`
- `AutoAppliedAfterDate`— Erstes Wartungsfenster nach diesem Datum. `NEXT_MAINTENANCE` `OPT_IN`wird in diesem Fall ignoriert.
- `ForcedApplyDate`— Wird unabhängig vom Wartungsfenster angewendet. `IMMEDIATE` `OPT_IN`wird in diesem Fall ignoriert.
- `OptInStatus`— Ein Wert, der den Typ der Opt-in-Anfrage angibt oder eine Opt-in-Anfrage rückgängig macht. Eine Opt-in-Anfrage vom Typ `IMMEDIATE` kann nicht rückgängig gemacht werden.

  Zulässige Werte:

  - `IMMEDIATE`— Wendet die Wartungsmaßnahme sofort an.
  - `NEXT_MAINTENANCE`— Wendet die Wartungsaktion im nächsten Wartungsfenster für die Ressource an.
  - `APPLY_ON`— Wendet die Wartungsaktion unabhängig vom nächsten Wartungsfenster für die Ressource am angegebenen Anwendungsdatum an.
  - `UNDO_OPT_IN`— Storniert alle bestehenden Anfragen `NEXT_MAINTENANCE` oder `APPLY_ON` Opt-In-Anfragen.

- `CurrentApplyDate`— Wird angezeigt, wenn der Opt-in-Typ ist. `APPLY_ON`
- `Description`— Eine Beschreibung der Option für die Wartungsaktion.

Aktualisierungen der Elastic Cluster Engine

Mit Amazon DocumentDB können Sie wählen, wann Wartungsarbeiten durchgeführt werden sollen. Mit dem können Sie entscheiden, wann Amazon DocumentDB Updates AWS CLI einführt.

Ausstehende Wartungsmaßnahmen anwenden:

```
aws docdb-elastic apply-pending-maintenance-action
--resource-arn string-arn
--apply-action string-enum
--opt-in-type string-enum
[--apply-on string-date-range]
```

Parameter:

- **`--resource-arn`**— Der Amazon Resource Name (ARN) von Amazon DocumentDB der Ressource, für die die ausstehende Wartungsaktion gilt.
- **`--apply-action`**— Die ausstehende Wartungsaktion, die auf diese Ressource angewendet werden soll.

  Zulässige Werte:

  - `ENGINE_UPDATE`
  - `ENGINE_UPGRADE`
  - `SECURITY_UPDATE`
  - `OS_UPDATE`
  - `MASTER_USER_PASSWORD_UPDATE`
- **`--opt-in-type`**— Ein Wert, der den Typ der Opt-in-Anfrage angibt oder eine Opt-in-Anfrage rückgängig macht. Eine Opt-in-Anfrage vom Typ `IMMEDIATE` kann nicht rückgängig gemacht werden.

  Zulässige Werte:

  - `IMMEDIATE`— Wendet die Wartungsmaßnahme sofort an.
  - `NEXT_MAINTENANCE`— Wendet die Wartungsaktion im nächsten Wartungsfenster für die Ressource an.

- `APPLY_ON`— Wendet die Wartungsaktion unabhängig vom nächsten Wartungsfenster für die Ressource am angegebenen Anwendungsdatum an.
- `UNDO_OPT_IN`— Storniert alle bestehenden Anfragen `NEXT_MAINTENANCE` oder `APPLY_ON` Opt-In-Anfragen.

- **`[--apply-on]`**— Erforderlich, wenn der Opt-in-Typ ist. `APPLY_ON` Format: `yyyy/MM/dd HH:mm-yyyy/MM/dd HH:mm` (Diese Option verwendet UTC-Zeit. Die Startzeit kann ein beliebiger Zeitpunkt in der future sein, zwischen mindestens 30 Minuten und maximal 14 Tagen, oder das force/apply Datum der ausstehenden Aktion, je nachdem, welcher Zeitpunkt früher liegt. Das Zeitfenster von Anfang bis Ende kann mindestens 30 Minuten bis maximal 8 Stunden lang sein.)

Die Ausgabe dieses Vorgangs sieht etwa wie folgt aus (JSON-Format):

```
{
 'ResourcePendingMaintenanceAction': {
        'ResourceArn': 'string-arn',
        'PendingMaintenanceActionDetails': [
            {
                'Action': 'SECURITY_UPDATE',
                'AutoAppliedAfterDate': 'string',
                'ForcedApplyDate': 'string',
                'OptInStatus': 'IMMEDIATE',
                'CurrentApplyDate': 'string',
                'Description': 'string'
            },
        ]
 }
}
```

Parameter:

- `ResourceArn`— Der Amazon Resource Name (ARN) von Amazon DocumentDB der Ressource, für die die ausstehende Wartungsaktion gilt.
- `Action`— Die ausstehende Wartungsaktion, die auf die Ressource angewendet wird.

  Zulässige Werte:

  - `ENGINE_UPDATE`
  - `ENGINE_UPGRADE`
  - `SECURITY_UPDATE`

  - OS_UPDATE
  - MASTER_USER_PASSWORD_UPDATE
- AutoAppliedAfterDate— Erstes Wartungsfenster nach diesem Datum. NEXT_MAINTENANCE OPT_INwird in diesem Fall ignoriert.
- ForcedApplyDate— Wird unabhängig vom Wartungsfenster angewendet. IMMEDIATE OPT_INwird in diesem Fall ignoriert.
- OptInStatus— Ein Wert, der den Typ der Opt-in-Anfrage angibt oder eine Opt-in-Anfrage rückgängig macht. Eine Opt-in-Anfrage vom Typ IMMEDIATE kann nicht rückgängig gemacht werden.

  Zulässige Werte:

  - IMMEDIATE— Wendet die Wartungsmaßnahme sofort an.
  - NEXT_MAINTENANCE— Wendet die Wartungsaktion im nächsten Wartungsfenster für die Ressource an.
  - APPLY_ON— Wendet die Wartungsaktion unabhängig vom nächsten Wartungsfenster für die Ressource am angegebenen Anwendungsdatum an.
  - UNDO_OPT_IN— Storniert alle bestehenden Anfragen NEXT_MAINTENANCE oder APPLY_ON Opt-In-Anfragen.
- CurrentApplyDate— Wird angezeigt, wenn der Opt-in-Typ ist. APPLY_ON
- Description— Eine Beschreibung der Option für die Wartungsaktion.

Termine anwenden

Jede Wartungsaktivität hat ein entsprechendes Anwendungsdatum, das Sie bei der Beschreibung der anstehenden Wartungsaktivität finden. Wenn Sie die Ausgabe der ausstehenden Wartungsmaßnahmen vom lesen AWS CLI, werden drei Daten aufgeführt:

- CurrentApplyDate— Das Datum, an dem die Wartungsaktion entweder sofort oder während des nächsten Wartungsfensters ausgeführt wird. Wenn die Wartung optional ist, kann dieser Wert Null sein.
- ForcedApplyDate— Das Datum, an dem die Wartung unabhängig von Ihrem Wartungsfenster automatisch angewendet wird.
- AutoAppliedAfterDate— Das Datum, nach dem die Wartung während des Wartungsfensters des Clusters angewendet wird.

User-created Wartungsaktionen

Als Benutzer eines Amazon DocumentDBElastic-Clusters können Sie Aktualisierungen Ihrer Clusterkonfigurationen veranlassen.

Das primäre Cluster-Passwort wird aktualisiert

```
aws docdb-elastic update-cluster
--cluster-arn string-arn
[--admin-user-password string]
[--auth-type string-enum]
[--apply-method string-enum]
[--apply-on string-date-range]
#... other parameters of the API that follow here are not relevant for this
 configuration
```

Parameter:

- **`--cluster-arn`**— Der Amazon Resource Name (ARN) von Amazon DocumentDB der Ressource, auf die die Wartungsmaßnahme angewendet wird.
- **`[--admin-user-password]`**— Das dem Admin-Benutzer zugeordnete Passwort.
- **`[--auth-type]`**— Der Authentifizierungstyp, der verwendet wird, um zu bestimmen, wo das für den Zugriff auf den Elastic Cluster verwendete Passwort abgerufen werden soll. Gültige Typen sind `PLAIN_TEXT` oder`SECRET_ARN`.
- **`[--apply-method]`**— Ein Wert, der den Typ der Methode angibt, die angewendet wird. Zulässige Werte sind `IMMEDIATE` und `APPLY_ON`. Der Standardwert ist `IMMEDIATE`.
- **`[--apply-on]`**— Erforderlich, wenn ja`apply-method`. `APPLY_ON` Format: `yyyy/MM/dd HH:mm-yyyy/MM/dd HH:mm` (Diese Option verwendet UTC-Zeit. Die Startzeit kann jederzeit in der future liegen und zwischen mindestens 30 Minuten und maximal 14 Tagen liegen. Das Zeitfenster von Anfang bis Ende kann mindestens 30 Minuten bis maximal 8 Stunden lang sein.)

Die Ausgabe dieses Vorgangs sieht etwa wie folgt aus (JSON-Format):

```
{
 'ResourcePendingMaintenanceAction': {
        'ResourceArn': 'string-arn',
        'PendingMaintenanceActionDetails': [
            {
```

```
                'Action': 'MASTER_USER_PASSWORD_UPDATE',
                'OptInStatus': 'APPLY_ON',
                'CurrentApplyDate': 'string',
                'Description': 'string'
            },
        ]
 }
}
```

Ihre Amazon DocumentDB DocumentDB-Wartungsfenster ändern

Das Wartungsfenster sollte in den Zeitraum mit der geringsten Nutzung fallen und daher unter Umständen von Zeit zu Zeit geändert werden. Ihr Elastic Cluster ist während dieser Zeit nur dann nicht verfügbar, wenn Systemänderungen (z. B. eine Änderung des Speicherbetriebs) vorgenommen werden und ein Ausfall erforderlich ist. Er ist nur für den Mindestzeitraum nicht verfügbar, der erforderlich ist, um die erforderlichen Änderungen vorzunehmen.

Die Standardeinstellung ist ein 30-minütiges Fenster, das nach dem Zufallsprinzip aus einem 8-Stunden-Zeitblock für jede Amazon Web Services Services-Region ausgewählt wird und an einem zufälligen Wochentag stattfindet.

Informationen zum Ändern des Wartungsfensters finden Sie unterModifizieren elastischer Cluster-Konfigurationen.

Betriebssystem-Updates für Elastic Cluster

Elastische Amazon DocumentDB-Cluster erfordern gelegentlich Betriebssystemupdates. Amazon DocumentDB aktualisiert das Betriebssystem auf eine neuere Version, um die Datenbankleistung und die allgemeine Sicherheitslage der Kunden zu verbessern. Betriebssystemupdates ändern nicht die Cluster-Engine-Version eines elastischen Amazon DocumentDB-Clusters.

Die meisten Betriebssystemupdates für Amazon DocumentDB Elastic Clusters sind optional und haben kein festes Datum, an dem sie angewendet werden sollen. Wenn Sie diese Updates jedoch eine Zeit lang nicht installieren, werden sie möglicherweise irgendwann erforderlich und werden während des Wartungsfensters Ihres Clusters automatisch angewendet. Dies soll dazu beitragen, den Sicherheitsstatus Ihrer Datenbank aufrechtzuerhalten. Um unerwartete Ausfallzeiten zu vermeiden, empfehlen wir Ihnen, Betriebssystem-Updates auf Ihren Amazon DocumentDB Elastic Cluster zu installieren, sobald sie verfügbar sind, und Ihr Cluster-Wartungsfenster zu einem Zeitpunkt festzulegen, der Ihren Geschäftsanforderungen entspricht.

Datenverschlüsselung im Ruhezustand für elastische Amazon DocumentDB-Cluster

In den folgenden Themen erfahren Sie mehr über AWS Key Management Service Verschlüsselungsschlüssel für elastische Amazon DocumentDB-Cluster, deren Erstellung und Überwachung:

Topics

- So verwenden elastische Amazon DocumentDB-Cluster Zuschüsse in AWS KMS
- Erstellen eines kundenseitig verwalteten Schlüssels
- Überwachung Ihrer Verschlüsselungsschlüssel für Amazon DocumentDB Elastic Clusters
- Weitere Informationen

Elastische Amazon DocumentDB-Cluster integrieren sich automatisch in AWS Key Management Service (AWS KMS) für die Schlüsselverwaltung und verwenden eine Methode, die als Envelope-Verschlüsselung bekannt ist, um Ihre Daten zu schützen. Weitere Informationen zur Envelope-Verschlüsselung finden Sie unter Envelope-Verschlüsselung im AWS Key Management Service - Entwicklerhandbuch.

An AWS KMS key ist eine logische Darstellung eines Schlüssels. Der KMS-Schlüssel enthält Metadaten wie die Schlüssel-ID, das Erstellungsdatum, die Beschreibung und den Schlüsselstatus. Der KMS-Schlüssel enthält auch das zur Ver- und Entschlüsselung von Daten verwendete Schlüsselmaterial. Weitere Informationen über KMS-Schlüssel finden Sie unter AWS KMS keys im AWS Key Management Service Developer Guide.

Elastic Clusters von Amazon DocumentDB unterstützen die Verschlüsselung mit zwei Arten von Schlüsseln:

- AWS eigene Schlüssel — Elastische Amazon DocumentDB-Cluster verwenden diese Schlüssel standardmäßig, um personenbezogene Daten automatisch zu verschlüsseln. Sie können AWS eigene Schlüssel nicht einsehen, verwalten oder verwenden oder deren Verwendung überprüfen. Sie müssen jedoch keine Maßnahmen ergreifen oder Programme zum Schutz der Schlüssel ändern, die zur Verschlüsselung Ihrer Daten verwendet werden. Weitere Informationen finden Sie unter AWS -eigene Schlüssel im AWS Key Management Service -Entwicklerhandbuch.

- Customer-managed Schlüssel — Symmetrisch AWS KMS keys , die Sie erstellen, besitzen und verwalten. Da Sie die volle Kontrolle über diese Verschlüsselungsebene haben, können Sie beispielsweise folgende Aufgaben ausführen:
  - Festlegung und Pflege wichtiger Richtlinien
  - Festlegung und Aufrechterhaltung von IAM-Richtlinien und -Zuschüssen
  - Aktivieren und Deaktivieren wichtiger Richtlinien
  - Kryptographisches Material mit rotierendem Schlüssel
  - Hinzufügen von -Tags
  - Erstellen von Schlüsselaliasen
  - Schlüssel für das Löschen von Schlüsseln planen

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

> **Important**
>
> Sie müssen einen KMS-Schlüssel für die symmetrische Verschlüsselung verwenden, um Ihren Cluster zu verschlüsseln, da Amazon DocumentDB nur KMS-Schlüssel mit symmetrischer Verschlüsselung unterstützt. Verwenden Sie keinen asymmetrischen KMS-Schlüssel, um zu versuchen, die Daten in Ihren elastischen Amazon DocumentDB-Clustern zu verschlüsseln. Weitere Informationen finden Sie unter Asymmetrische Schlüssel AWS KMS im Entwicklerhandbuch.AWS Key Management Service
> Wenn Amazon DocumentDB keinen Zugriff mehr auf den Verschlüsselungsschlüssel für einen Cluster erhält — zum Beispiel, wenn der Zugriff auf einen Schlüssel gesperrt wird — geht der verschlüsselte Cluster in einen Terminalstatus über. In diesem Fall können Sie den Cluster nur aus einer Sicherung wiederherstellen. Für Amazon DocumentDB sind Backups immer für einen Tag aktiviert. Wenn Sie den Schlüssel für einen verschlüsselten Amazon DocumentDB-Cluster deaktivieren, verlieren Sie außerdem irgendwann den Lese- und Schreibzugriff auf diesen Cluster. Wenn Amazon DocumentDB auf einen Cluster trifft, der mit einem Schlüssel verschlüsselt ist, auf den es keinen Zugriff hat, versetzt es den Cluster in einen Terminalstatus. In diesem Fall ist der Cluster nicht länger verfügbar und der aktuelle Zustand der Datenbank kann nicht mehr wiederhergestellt werden. Um den Cluster wiederherzustellen, müssen Sie den Zugriff auf den Verschlüsselungsschlüssel für Amazon DocumentDB erneut aktivieren und dann den Cluster aus einem Backup wiederherstellen.

> **Important**
>
> Sie können den KMS-Schlüssel für einen verschlüsselten Cluster nicht ändern, nachdem Sie ihn bereits erstellt haben. Stellen Sie sicher, dass Sie Ihre Anforderungen an den Verschlüsselungsschlüssel ermitteln, bevor Sie Ihren verschlüsselten Elastic Cluster erstellen.

So verwenden elastische Amazon DocumentDB-Cluster Zuschüsse in AWS KMS

Elastische Amazon DocumentDB-Cluster benötigen einen Zuschuss, um Ihren vom Kunden verwalteten Schlüssel verwenden zu können.

Wenn Sie einen Cluster erstellen, der mit einem vom Kunden verwalteten Schlüssel verschlüsselt ist, erstellen Amazon DocumentDB Elastic Clusters in Ihrem Namen einen Zuschuss, indem sie eine `CreateGrant` Anfrage an AWS KMS senden. Grants in AWS KMS werden verwendet, um Amazon DocumentDB Elastic Clusters Zugriff auf einen KMS-Schlüssel in einem Kundenkonto zu gewähren.

Elastische Amazon DocumentDB-Cluster benötigen den Zuschuss, um Ihren vom Kunden verwalteten Schlüssel für die folgenden internen Operationen verwenden zu können:

- Senden Sie `DescribeKey` Anfragen, um AWS KMS zu überprüfen, ob die symmetrische, vom Kunden verwaltete KMS-Schlüssel-ID, die Sie bei der Erstellung einer Tracker- oder Geofence-Sammlung eingegeben haben, gültig ist.
- Senden Sie `GenerateDataKey` Anfragen AWS KMS zur Generierung von Datenschlüsseln, die mit Ihrem vom Kunden verwalteten Schlüssel verschlüsselt wurden.
- Senden Sie `Decrypt` Anfragen AWS KMS zur Entschlüsselung der verschlüsselten Datenschlüssel, damit diese zur Verschlüsselung 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, können Amazon DocumentDB Elastic Clusters auf keine der mit dem vom Kunden verwalteten Schlüssel verschlüsselten Daten zugreifen, was sich auf Operationen auswirkt, die von diesen Daten abhängig sind.

Erstellen eines kundenseitig verwalteten Schlüssels

Sie können einen symmetrischen, vom Kunden verwalteten Schlüssel mithilfe der AWS-Managementkonsole oder der AWS KMS API erstellen.

Symmetrische, vom Kunden verwaltete Schlüsselerstellung

Folgen Sie den Schritten zum Erstellen eines symmetrischen kundenverwalteten Schlüssels im Entwicklerhandbuch zum AWS Key Management Service .

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 kundenseitig verwalteten Schlüssel erstellen, können Sie eine Schlüsselrichtlinie angeben. Weitere Informationen finden Sie in den Informationen zum Zugriff auf KMS-Schlüssel in der AWS Key Management Service Übersicht im AWS Key Management Service Developer Guide.

Um Ihren vom Kunden verwalteten Schlüssel mit Amazon DocumentDB Elastic Cluster-Ressourcen zu verwenden, müssen die folgenden API-Operationen in der Schlüsselrichtlinie zugelassen sein:

- `kms:CreateGrant`: Fügt einem kundenverwalteten Schlüssel eine Erteilung hinzu. Gewährt Kontrollzugriff auf einen bestimmten KMS-Schlüssel, der Zugriff auf Grant-Operationen ermöglicht, die Amazon Location Service benötigt. Weitere Informationen zur Verwendung von Zuschüssen finden Sie unter Grants AWS KMS im AWS Key Management Service Developer Guide.
- `kms:DescribeKey`— Stellt dem Kunden verwaltete Schlüsseldetails zur Verfügung, damit Docdb Elastic den Schlüssel validieren kann.
- `kms:Decrypt`— Ermöglicht Docdb Elastic, den gespeicherten verschlüsselten Datenschlüssel für den Zugriff auf verschlüsselte Daten zu verwenden.
- `kms:GenerateDataKey`— Ermöglicht Docdb Elastic, einen verschlüsselten Datenschlüssel zu generieren und ihn zu speichern, da der Datenschlüssel nicht sofort zum Verschlüsseln verwendet wird.

Weitere Informationen finden Sie unter Berechtigungen für AWS Dienste in den wichtigsten Richtlinien und unter Fehlerbehebung beim Schlüsselzugriff im AWS Key Management Service Entwicklerhandbuch.

Einschränkung des vom Kunden verwalteten Schlüsselzugriffs über IAM-Richtlinien

Zusätzlich zu den KMS-Schlüsselrichtlinien können Sie in einer IAM-Richtlinie auch die KMS-Schlüsselberechtigungen einschränken.

Sie können die IAM-Richtlinie auf verschiedene Weise strikter gestalten. Um beispielsweise zu ermöglichen, dass der vom Kunden verwaltete Schlüssel nur für Anfragen verwendet wird, die ihren Ursprung in elastischen Amazon DocumentDB-Clustern haben, können Sie den `kms:ViaService`Bedingungsschlüssel mit dem `docdb-elastic.<region-name>.amazonaws.com` Wert verwenden.

Weitere Informationen finden Sie unter Benutzern in anderen Konten die Verwendung eines KMS-Schlüssels erlauben im AWS Key Management Service -Entwicklerhandbuch.

Überwachung Ihrer Verschlüsselungsschlüssel für Amazon DocumentDB Elastic Clusters

Wenn Sie einen vom AWS KMS key Kunden verwalteten Schlüssel mit Ihren Docdb Elastic-Ressourcen verwenden, können Sie AWS CloudTrail oder Amazon CloudWatch Logs verwenden, um Anfragen zu verfolgen, an die Docdb Elastic sendet. AWS KMS

Die folgenden Beispiele sind AWS CloudTrail Ereignisse für`CreateGrant`,, und `DescribeKey` zur Überwachung von AWS KMS key Vorgängen `GenerateDataKeyWithoutPlainTextDecrypt`, die von Amazon DocumentDB DocumentDB-Elastic-Clustern aufgerufen werden, um auf Daten zuzugreifen, die mit Ihrem vom Kunden verwalteten Schlüssel verschlüsselt wurden:

CreateGrant

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE",
                "arn": "arn:aws:iam::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Sampleuser01"
```

```
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-05-09T23:04:20Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "docdb-elastic.amazonaws.com"
    },
    "eventTime": "2023-05-09T23:55:48Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateGrant",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "docdb-elastic.amazonaws.com",
    "userAgent": "docdb-elastic.amazonaws.com",
    "requestParameters": {
        "retiringPrincipal": "docdb-elastic.us-east-1.amazonaws.com",
        "granteePrincipal": "docdb-elastic.us-east-1.amazonaws.com",
        "operations": [
            "Decrypt",
            "Encrypt",
            "GenerateDataKey",
            "GenerateDataKeyWithoutPlaintext",
            "ReEncryptFrom",
            "ReEncryptTo",
            "CreateGrant",
            "RetireGrant",
            "DescribeKey"
        ],
        "keyId": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "responseElements": {
        "grantId":
 "0ab0ac0d0b000f00ea00cc0a0e00fc00bce000c000f0000000c0bc0a0000aaafSAMPLE",
        "keyId": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": false,
    "resources": [
        {
            "accountId": "AWS Internal",
```

```
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

GenerateDataKey

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE",
                "arn": "arn:aws:iam::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Sampleuser01"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-05-10T18:02:59Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "docdb-elastic.amazonaws.com"
    },
    "eventTime": "2023-05-10T18:03:25Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "docdb-elastic.amazonaws.com",
    "userAgent": "docdb-elastic.amazonaws.com",
```

```
    "requestParameters": {
        "keySpec": "AES_256",
        "keyId": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "AWS Internal",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Decrypt

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE",
                "arn": "arn:aws:iam::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Sampleuser01"
            },
            "webIdFederationData": {},
            "attributes": {
```

```
                "creationDate": "2023-05-10T18:05:49Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "docdb-elastic.amazonaws.com"
    },
    "eventTime": "2023-05-10T18:06:19Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "docdb-elastic.amazonaws.com",
    "userAgent": "docdb-elastic.amazonaws.com",
    "requestParameters": {
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT"
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "AWS Internal",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


DescribeKey


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
```

```
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE",
                "arn": "arn:aws:iam::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Sampleuser01"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-05-09T23:04:20Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "docdb-elastic.amazonaws.com"
    },
    "eventTime": "2023-05-09T23:55:48Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DescribeKey",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "docdb-elastic.amazonaws.com",
    "userAgent": "docdb-elastic.amazonaws.com",
    "requestParameters": {
        "keyId": "alias/SampleKmsKey"
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "AWS Internal",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Weitere Informationen

Die folgenden Ressourcen bieten weitere Informationen zur Datenverschlüsselung im Ruhezustand:

- Weitere Informationen zu AWS KMS Konzepten finden Sie unter AWS Key Management Service Grundbegriffe im AWS Key Management Service Entwicklerhandbuch.
- Weitere Informationen zur AWS KMS Sicherheit finden Sie unter Bewährte Sicherheitsmethoden für AWS Key Management Service im AWS Key Management Service Entwicklerhandbuch.

Service-linked Rollen in elastischen Clustern

Elastische Amazon DocumentDB-Cluster verwenden AWS Identity and Access Management (IAM) service-verknüpfte Rollen. Eine serviceverknüpfte Rolle ist eine einzigartige Art von IAM-Rolle, die direkt mit elastischen Amazon DocumentDB-Clustern verknüpft ist. Service-linked Rollen sind von Amazon DocumentDB Elastic Clusters vordefiniert und beinhalten alle Berechtigungen, die der Service benötigt, um andere AWS Services in Ihrem Namen aufzurufen.

Eine serviceverknüpfte Rolle erleichtert die Verwendung von Amazon DocumentDB Elastic Clusters, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Amazon DocumentDB Elastic Clusters definiert die Berechtigungen seiner serviceverknüpften Rollen. Sofern nicht anders definiert, können nur Amazon DocumentDB Elastic Clusters diese Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden. Sie können die Rollen nur nach dem Löschen der zugehörigen Ressourcen löschen. Dadurch werden Ihre Amazon DocumentDB Elastic Cluster-Ressourcen geschützt, da Sie nicht versehentlich die Zugriffsberechtigung für die Ressourcen entziehen können.

Informationen zu anderen Diensten, die serviceverknüpfte Rollen unterstützen, finden Sie unter AWS Dienste, die mit IAM funktionieren. Suchen Sie in der Spalte Rolle nach den Diensten, die mit Ja markiert sind. Service-Linked Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Service-linked Rollenberechtigungen für elastische Cluster

Amazon DocumentDB Elastic Clusters verwendet die benannte serviceverknüpfte RolleAWS `ServiceRoleForDocDB-Elastic`, um es Amazon DocumentDB Elastic Clusters zu ermöglichen, AWS Dienste im Namen Ihrer Cluster aufzurufen.

Dieser dienstgebundenen Rolle ist eine Berechtigungsrichtlinie namens `AmazonDocDB-ElasticServiceRolePolicy` zugeordnet, die ihr Berechtigungen für den Betrieb in Ihrem Konto erteilt. Die Rollenberechtigungsrichtlinie ermöglicht es Amazon DocumentDB Elastic Clusters, die folgenden Aktionen für die angegebenen Ressourcen durchzuführen:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": [
                        "AWS/DocDB-Elastic"
                    ]
                }
            }
        }
    ]
}
```

> **Note**
>
> Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Wenn Sie auf die folgende Fehlermeldung stoßen: „Die Ressource konnte nicht erstellt werden. Überprüfen Sie, ob Sie die Berechtigung haben, eine serviceverknüpfte Rolle zu erstellen. Andernfalls warten Sie und versuchen Sie es später erneut.“ , stellen Sie sicher, dass Sie die folgenden Berechtigungen aktiviert haben:

```
{
"Action": "iam:CreateServiceLinkedRole",
    "Effect": "Allow",
    "Resource": "arn:aws:iam::*:role/aws-service-role/docdb-elastic.amazonaws.com/
AWSServiceRoleForDocDB-Elastic",
    "Condition": {
"StringLike": {
"iam:AWSServiceName":"docdb-elastic.amazonaws.com"
        }
    }
}
```

Weitere Informationen finden Sie unter Service-linked Rollenberechtigungen im AWS Identity and Access Management-Benutzerhandbuch.

Eine serviceverknüpfte Rolle für elastische Amazon DocumentDB-Cluster erstellen

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie eine DB-Instance erstellen, erstellt Amazon DocumentDB Elastic Clusters die serviceverknüpfte Rolle für Sie.

Bearbeiten einer serviceverknüpften Rolle für elastische Amazon DocumentDB-Cluster

Elastische Amazon DocumentDB-Cluster ermöglichen es Ihnen nicht, die `AWS ServiceRoleForDocDB-Elastic` 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 dienstbezogenen Rolle im AWS Identity and Access Management-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für Amazon DocumentDB Elastic Clusters

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 alle Ihre -Cluster löschen, bevor Sie die serviceverknüpfte Rolle löschen können.

Bereinigen einer 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.

Um zu überprüfen, ob die serviceverknüpfte Rolle über eine aktive Sitzung in der IAM-Konsole verfügt:

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die IAM-Konsole.
2. Wählen Sie im Navigationsbereich der IAM Console Roles (Rollen) aus. Wählen Sie dann den Namen (nicht das Kontrollkästchen) der Rolle `AWS ServiceRoleForDocDB-Elastic` aus.
3. Wählen Sie auf der Seite Summary (Zusammenfassung) für die ausgewählte Rolle die Registerkarte Access Advisor (Advisor aufrufen) aus.

> **Note**
>
> Wenn Sie sich nicht sicher sind, ob Amazon DocumentDB Elastic Clusters die `AWS ServiceRoleForDocDB-Elastic` Rolle verwendet, können Sie versuchen, die Rolle zu löschen. Wenn der Service die Rolle verwendet, schlägt das Löschen fehl und Sie können sehen AWS-Regionen , wo die Rolle verwendet wird. Wenn die Rolle verwendet wird, müssen Sie warten, bis die Sitzung beendet wird, bevor Sie die Rolle löschen können. Die Sitzung für eine serviceverknüpfte Rolle können Sie nicht widerrufen.
> Wenn Sie die `AWS ServiceRoleForDocDB-Elastic` Rolle entfernen möchten, müssen Sie zuerst alle Ihre Cluster löschen.

Löschen aller Ihrer Cluster

Um einen Cluster in der Amazon DocumentDB DocumentDB-Konsole zu löschen:

1. Melden Sie sich bei der an AWS-Managementkonsoleund öffnen Sie die Amazon DocumentDB DocumentDB-Konsole.
2. Klicken Sie im Navigationsbereich auf Cluster.
3. Wählen Sie den Cluster aus, den Sie löschen möchten.
4. Klicken Sie bei Actions auf Delete.
5. Wenn Sie aufgefordert werden, den endgültigen Snapshot zu erstellen? , wählen Sie Ja oder Nein.

6. Wenn Sie im vorherigen Schritt Yes (Ja) gewählt haben, geben Sie unter Final snapshot name (Endgültiger Snapshot-Name) den Namen Ihres endgültigen DB-Snapshots ein.
7. Wählen Sie Löschen aus.

> **Note**
>
> Sie können die IAM-Konsole, die IAM-CLI oder die IAM-API verwenden, um die serviceverknüpfte Rolle `AWS ServiceRoleForDocDB-Elastic` zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im AWS Identity and Access Management-Benutzerhandbuch.

Amazon DocumentDB überwachen

Die Überwachung Ihrer AWS Dienste ist ein wichtiger Bestandteil, damit Ihre Systeme gesund bleiben und optimal funktionieren. Es ist ratsam, Überwachungsdaten aus allen Teilen Ihrer AWS Lösung zu sammeln, damit Sie Fehler oder Beeinträchtigungen leichter debuggen und beheben können, falls sie auftreten sollten. Bevor Sie mit der Überwachung Ihrer AWS Lösungen beginnen, empfehlen wir Ihnen, die folgenden Fragen zu prüfen und Antworten darauf zu formulieren:

- Was sind Ihre Überwachungsziele?
- Welche Ressourcen werden Sie überwachen?
- Wie oft werden Sie diese Ressourcen überwachen?
- Welche Überwachungstools werden verwendet?
- Wer ist für die Überwachung verantwortlich?
- Wer ist zu benachrichtigen und auf welche Weise, wenn etwas schief geht?

Um Ihre aktuellen Leistungsmuster zu verstehen, Leistungsanomalien zu identifizieren und Methoden zur Behebung von Problemen zu formulieren, sollten Sie grundlegende Leistungskennzahlen für verschiedene Zeiten und unter unterschiedlichen Lastbedingungen festlegen. Bei der Überwachung Ihrer AWS Lösung empfehlen wir Ihnen, Ihre historischen Monitoring-Daten zu speichern, damit Sie future darauf zurückgreifen und Ihre Baselines erstellen können.

Die zulässigen Werte für Leistungsmetriken sind im Allgemeinen davon abhängig, wie die Ausgangsbasis aussieht und wofür die Anwendung gedacht ist. Prüfen Sie, ob dauerhafte oder tendenzielle Abweichungen von Ihrer Ausgangsbasis vorliegen. Im Folgenden werden Hinweise zu bestimmten Arten von Kennzahlen gegeben:

- Hohe CPU- oder RAM-Auslastung — Hohe Werte für die CPU- oder RAM-Auslastung können angemessen sein, vorausgesetzt, sie entsprechen Ihren Zielen für Ihre Anwendung (wie Durchsatz oder Parallelität) und werden erwartet.
- Speichervolumenverbrauch — Untersuchen Sie den Speicherverbrauch (`VolumeBytesUsed`), wenn der genutzte Speicherplatz konstant 85 Prozent des gesamten Speichervolumens ausmacht oder mehr beträgt. Legen Sie fest, ob Sie Daten aus dem Speicher-Volume löschen oder Daten in ein anderes System archivieren können, um Platz zu schaffen. Weitere Informationen erhalten Sie unter Amazon DocumentDB DocumentDB-Speicher und Amazon DocumentDB Kontingente und Beschränkungen.

- Netzwerkverkehr — Wenden Sie sich bezüglich des Netzwerkverkehrs an Ihren Systemadministrator, um zu erfahren, wie hoch der zu erwartende Durchsatz für Ihr Domänennetzwerk und Ihre Internetverbindung ist. Überprüfen Sie den Netzwerkdatenverkehr, wenn der Durchsatz dauerhaft unter dem erwarteten Wert liegt.
- Datenbankverbindungen — Erwägen Sie, Datenbankverbindungen einzuschränken, wenn Sie eine hohe Anzahl von Benutzerverbindungen in Verbindung mit einer verringerten Instanzleistung und Reaktionszeit feststellen. Die optimale Anzahl der Benutzerverbindungen für Ihre Instance ist von der Instance-Klasse und der Komplexität der Operationen abhängig, die ausgeführt werden.
- IOPS-Metriken — Die erwarteten Werte für IOPS-Metriken hängen von der Festplattenspezifikation und der Serverkonfiguration ab. Verwenden Sie daher Ihren Basiswert, um herauszufinden, was typisch ist. Prüfen Sie, ob dauerhafte Abweichungen von den Werten Ihrer Ausgangsbasis vorliegen. Für eine optimale IOPS-Leistung stellen Sie sicher, dass Ihr typisches Working Set in den Speicher passt, um Lese- und Schreibvorgänge zu minimieren.

Amazon DocumentDB (mit MongoDB-Kompatibilität) bietet eine Vielzahl von CloudWatch Amazon-Metriken, die Sie überwachen können, um den Zustand und die Leistung Ihrer Amazon DocumentDB-Cluster und -Instances zu ermitteln. Sie können Amazon DocumentDB-Metriken mit verschiedenen Tools anzeigen, darunter der Amazon DocumentDB DocumentDB-Konsole AWS CLI, CloudWatch API und Performance Insights.

Themen

- Den Status eines Amazon DocumentDB-Clusters überwachen
- Den Status einer Amazon DocumentDB DocumentDB-Instance überwachen
- Amazon DocumentDB DocumentDB-Empfehlungen anzeigen
- Amazon DocumentDB DocumentDB-Veranstaltungsabonnements verwenden
- Überwachen von Amazon DocumentDB mit CloudWatch
- Protokollieren Amazon DocumentDB DocumentDB-API-Aufrufen mit AWS CloudTrail
- Profilierung von Amazon DocumentDB DocumentDB-Vorgängen
- Überwachung mit Performance Insights

Den Status eines Amazon DocumentDB-Clusters überwachen

Der Status eines Clusters zeigt den Zustand des Clusters an. Sie können den Status eines Clusters mithilfe der Amazon DocumentDB DocumentDB-Konsole oder des AWS CLI `describe-db-clusters` Befehls anzeigen.

Themen

- Werte für den Cluster-Status
- Den Status eines Clusters überwachen

Werte für den Cluster-Status

In der folgenden Tabelle sind die gültigen Werte für den Cluster-Status aufgeführt.

Cluster-Status	Description
`active`	Der Cluster ist aktiv. Dieser Status gilt nur für elastische Cluster.
`available`	Der Cluster ist stabil und verfügbar. Dieser Status gilt nur für instanzbasierte Cluster.
`backing-up`	Der Cluster wird derzeit gesichert.
`creating`	Der Cluster wird gerade erstellt. Ist während der Erstellung unzugänglich.
`deleting`	Der Cluster wird gerade gelöscht. Ist während des Löschvorgangs nicht zugreifbar.
`failing-over`	Ein Failover von der primären Instance zu einem Amazon

Cluster-Status	Description
	DocumentDB DocumentDB-Replikat wird durchgeführt.
`inaccessible-encryption-credentials`	Auf den AWS KMS Schlüssel , der zum Verschlüsseln oder Entschlüsseln des Clusters verwendet wurde, kann nicht zugegriffen werden.
`maintenance`	Ein Wartungsupdate wird auf den Cluster angewende t. Dieser Status wird für Wartungsarbeiten auf Clusterebene verwendet, die Amazon DocumentDB weit im Voraus plant.
`migrating`	Es wird gerade ein Cluster-Snapshot in einen Cluster wiederhergestellt.
`migration-failed`	Eine Migration ist fehlgesch lagen.
`modifying`	Der Cluster wird aufgrund einer Kundenanfrage, den Cluster zu ändern, geändert.
`renaming`	Der Cluster wird aufgrund einer Kundenanfrage auf Instance-Umbenennung umbenannt.
`resetting-master-credentials`	Die Master-Anmeldeinfo rmationen für den Cluster werden auf eine Kundenanf rage auf Zurücksetzung hin zurückgesetzt.

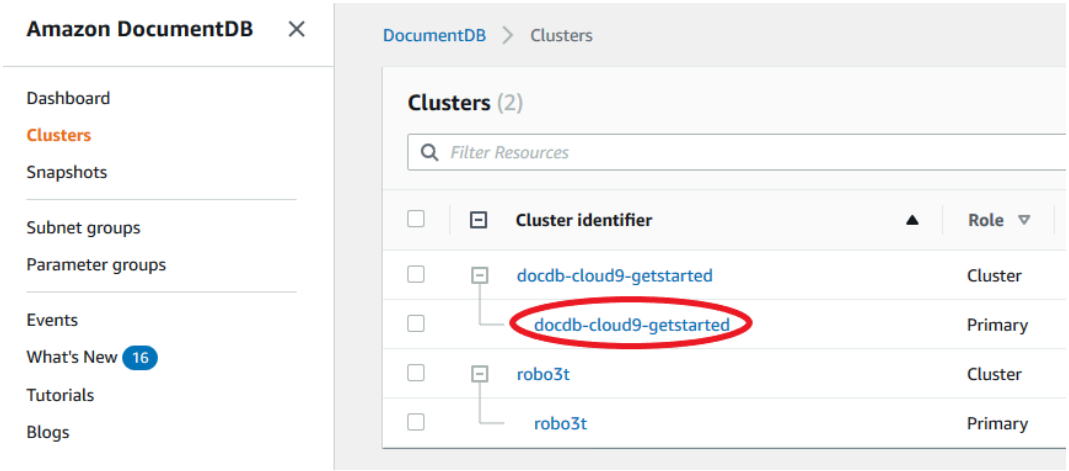
Cluster-Status	Description
`upgrading`	Die Cluster-Engine wird auf eine neue Version aktualisiert.

Den Status eines Clusters überwachen

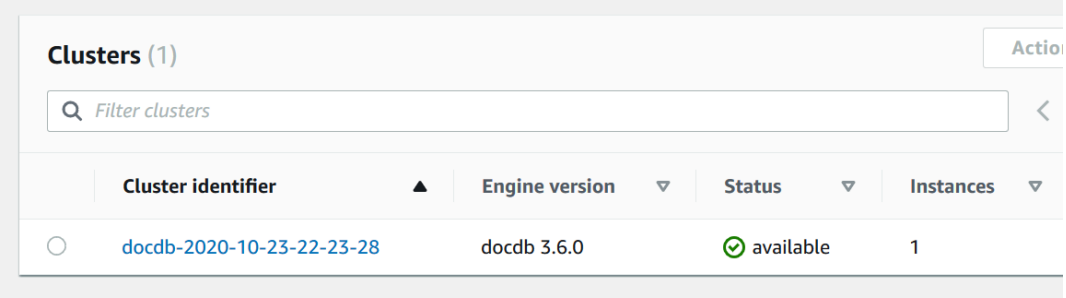
Using the AWS-Managementkonsole

Verwenden Sie das folgende Verfahren, AWS-Managementkonsole um den Status eines Clusters zu ermitteln.

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Klicken Sie im Navigationsbereich auf Cluster.
3. Im Cluster-Navigationsfeld sehen Sie die Spalte Cluster-ID. Ihre Instances werden unter Clustern aufgeführt, ähnlich wie im folgenden Screenshot.



4. Suchen Sie in der Spalte Cluster-ID den Namen der Instance, an der Sie interessiert sind. Um den Status der Instance zu ermitteln, lesen Sie dann über diese Zeile bis zur Spalte Status, wie unten gezeigt.



Using the AWS CLI

Wenn Sie AWS CLI den Status eines Clusters ermitteln möchten, verwenden Sie den `describe-db-clusters` Vorgang. Der folgende Code ermittelt den Status des Clusters `sample-cluster`.

Für Linux, macOS oder Unix:

```
aws docdb describe-db-clusters \
    --db-cluster-identifier sample-cluster  \
    --query 'DBClusters[*].[DBClusterIdentifier,Status]'
```

Für Windows:

```
aws docdb describe-db-clusters ^
    --db-cluster-identifier sample-cluster  ^
    --query 'DBClusters[*].[DBClusterIdentifier,Status]'
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus.

```
[
    [
        "sample-cluster",
        "available"
    ]
]
```

Den Status einer Amazon DocumentDB DocumentDB-Instance überwachen

Amazon DocumentDB bietet Informationen über den aktuellen Zustand jeder konfigurierten Instanz in der Datenbank.

Es gibt drei Statustypen, die Sie für eine Amazon DocumentDB DocumentDB-Instance anzeigen können:

- Instance-Status: Dieser Status wird in der Spalte Status der Cluster-Tabelle im angezeigt AWS-Managementkonsole und zeigt den aktuellen Lebenszykluszustand der Instance an. Die in der Spalte Status angezeigten Werte werden aus dem `Status` Feld der `DescribeDBCluster` API-Antwort abgeleitet.
- Integritätsstatus der Instanz: Dieser Status wird in der Spalte Instanzstatus der Clustertabelle in der angezeigt AWS-Managementkonsole und gibt an, ob die Datenbank-Engine, die Komponente, die für die Verwaltung und das Abrufen von Daten verantwortlich ist, läuft. Die in der Spalte Instance-Zustand angezeigten Werte basieren auf der CloudWatch `EngineUptime` Amazon-Systemmetrik.
- Wartungsstatus: Dieser Status wird in der Spalte Wartung der Cluster-Tabelle im angezeigt AWS-Managementkonsole und gibt den Status aller Wartungsereignisse an, die auf eine Instance angewendet werden müssen. Der Wartungsstatus ist unabhängig vom Status der anderen Instances und wird von der `PendingMaintenanceAction` API abgeleitet. Weitere Informationen zum Wartungsstatus finden Sie unter Wartung von Amazon DocumentDB.

Themen

- Instance-Statuswerte
- Überwachen Sie den Instance-Status mit dem AWS-Managementkonsole oder AWS CLI
- Werte für den Integritätsstatus der Instanz
- Überwachen des Zustands der Instanz mit dem AWS-Managementkonsole

Instance-Statuswerte

Die folgende Tabelle führt die möglichen Statuswerte für Instances auf und gibt an, wie welcher Status berechnet wird. Die Tabelle gibt an, ob Sie für Instance und Speicher, nur für Speicher oder weder für Instance noch Speicher zahlen müssen. Für alle Instance-Status wird immer die Sicherungsnutzung berechnet.

Instance-Status	Berechnet	Description
`available`	Berechnet	Die Instance ist stabil und verfügbar.
`backing-up`	Berechnet	Die Instance wird derzeit gesichert.
`configuring-log-exports`	Berechnet	Das Veröffentlichen von Protokolldateien in Amazon CloudWatch Logs wird für diese Instance aktiviert oder deaktiviert.
`creating`	Nicht berechnet	Die Instance wird gerade erstellt. Während die Instance erstellt wird, kann nicht auf sie zugegriffen werden.
`deleting`	Nicht berechnet	Die Instance wird gerade gelöscht.
`failed`	Nicht berechnet	Die Instance ist ausgefallen und Amazon DocumentDB konnte sie nicht wiederher stellen. Um die Daten wiederherzustellen, führen Sie eine Point-in-Time-Wiederherstel lung auf den letzten wiederherstellbaren Zeitpunkt der Instance durch.
`inaccessible-encryption-cre dentials`	Nicht berechnet	Auf den AWS KMS Schlüssel, der zum Verschlüsseln oder Entschlüsseln der Instance verwendet wird, konnte nicht zugegriffen werden.
`incompatible-network`	Nicht berechnet	Amazon DocumentDB versucht, eine Wiederherstellungsaktion für eine Instance durchzuführen, kann dies jedoch nicht tun, da sich die VPC in einem Zustand befindet, der verhindert, dass die Aktion abgeschlossen werden kann. Dieser Status kann auftreten, wenn beispielsweise alle verfügbaren IP-Adressen in einem Subnetz verwendet wurden und Amazon DocumentD

Instance-Status	Berechnet	Description
		B keine IP-Adresse für die Instance abrufen konnte.
`maintenance`	Berechnet	Amazon DocumentDB wendet ein Wartungsupdate auf die Instance an. Dieser Status wird für Wartungsarbeiten auf Instanzebene verwendet, die Amazon DocumentDB weit im Voraus plant. Wir evaluieren derzeit Möglichkeiten, Kunden über diesen Status auch weitere Wartungsa ktionen kenntlich zu machen.
`modifying`	Berechnet	Die Instance wird aufgrund einer Anforderu ng zur Änderung der Instance geändert.
`rebooting`	Berechnet	Die Instance wird aufgrund einer Anfrage oder eines Amazon DocumentDB DocumentDB-Prozesses, der einen Neustart der Instance erfordert, neu gestartet.
`renaming`	Berechnet	Die Instance wird aufgrund einer Anforderu ng zur Umbenennung umbenannt.
`resetting -master-c redentials`	Berechnet	Die Master-Anmeldeinformationen für die Instance werden aufgrund einer Anforderung zum Zurücksetzen zurückgesetzt.
`restore-error`	Berechnet	Bei dem Versuch, die Instance anhand eines Wiederherstellungszeitpunkts oder eines Snapshots wiederherzustellen, ist ein Fehler aufgetreten.
`starting`	Berechnet für Speicher	Die Instance wird gestartet.
`stopped`	Berechnet für Speicher	Die Instance wird angehalten.
`stopping`	Berechnet für Speicher	Die Instance wird gestoppt.

Instance-Status	Berechnet	Description
`storage-full`	Berechnet	Die Instance hat seine Speicherkapazitäts zuteilung erreicht. Dieser Status ist kritisch und sollte sofort behoben werden. Sie müssen den verfügbaren Speicherplatz hochskalieren, indem Sie die Instance entsprechend ändern. Stellen Sie CloudWatch Amazon-Alarme so ein, dass Sie gewarnt werden, wenn der Speicherplatz knapp wird, damit Sie nicht in diese Situation geraten.

Überwachen Sie den Instance-Status mit dem AWS-Managementkonsole oder AWS CLI

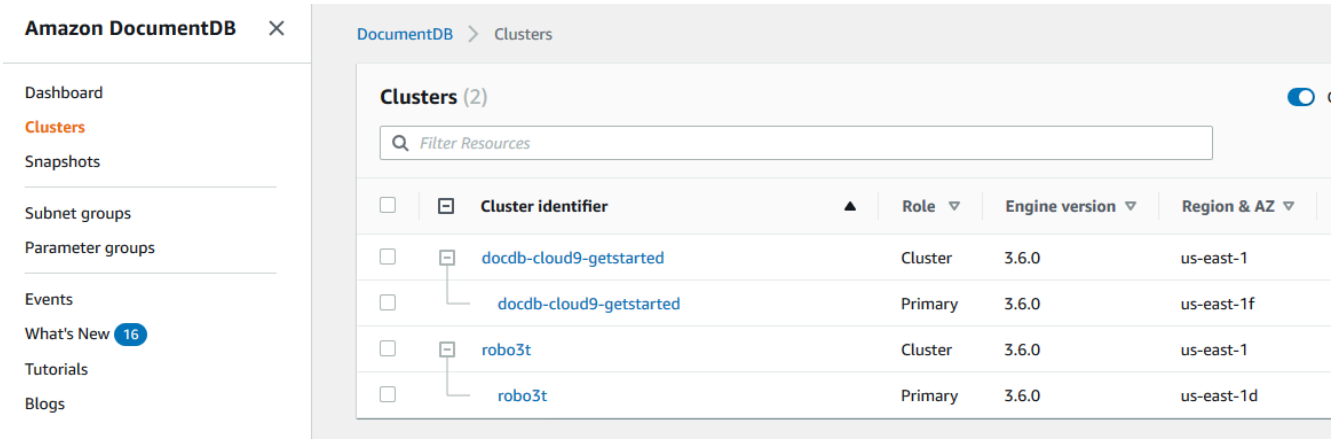
Verwenden Sie das AWS-Managementkonsole oder AWS CLI , um den Status Ihrer Instanz zu überwachen.

Using the AWS-Managementkonsole

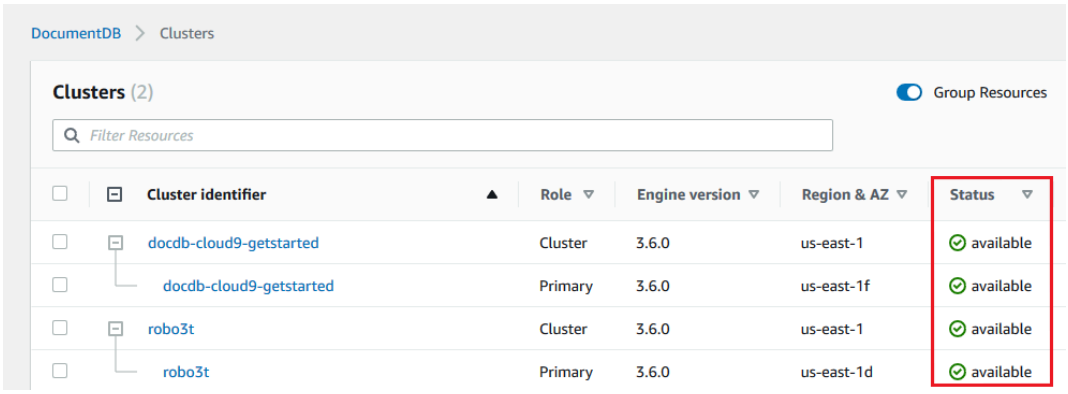
Verwenden Sie das folgende Verfahren, AWS-Managementkonsole um den Status eines Clusters zu ermitteln.

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Klicken Sie im Navigationsbereich auf Cluster.

> **Note**
>
> Beachten Sie, dass im Cluster-Navigationsfeld in der Spalte Cluster-ID sowohl Cluster als auch Instances angezeigt werden. Instances werden unter Clustern aufgeführt, ähnlich wie in der folgenden Abbildung.



3. Suchen Sie den Namen der Instance, an der Sie interessiert sind. Um den Status der Instance zu ermitteln, prüfen Sie die Zeile in die Spalte Status.



Using the AWS CLI

Wenn Sie AWS CLI den Status eines Clusters mithilfe von ermitteln möchten, verwenden Sie den `describe-db-instances` Vorgang. Der folgende Code ermittelt den Status der Instance `sample-cluster-instance-01`.

Für Linux, macOS oder Unix:

```
aws docdb describe-db-instances \
          --db-instance-identifier sample-cluster-instance-01  \
          --query 'DBInstances[*].[DBInstanceIdentifier,DBInstanceStatus]'
```

Für Windows:

```
aws docdb describe-db-instances ^
```

```
          --db-instance-identifier sample-cluster-instance-01  ^
          --query 'DBInstances[*].[DBInstanceIdentifier,DBInstanceStatus]'
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus.

```
[
          [
              "sample-cluster-instance-01",
              "available"
          ]
      ]
```

Werte für den Integritätsstatus der Instanz

In der folgenden Tabelle sind die möglichen Integritätsstatuswerte für Instances aufgeführt. Die Spalte Instanzstatus in der Cluster-Tabelle in der zeigt AWS-Managementkonsole, ob die Datenbank-Engine, die Komponente, die für das Speichern, Verwalten und Abrufen von Daten verantwortlich ist, normal funktioniert. In dieser Spalte wird auch angegeben, ob die `EngineUptime` Systemmetrik CloudWatch, verfügbar in, den Integritätsstatus jeder Instanz anzeigt.

Instance-Zustand	Description
fehlerfrei	Die Datenbank-Engine läuft in der Amazon DocumentDB DocumentDB-Instance.
ungesund	Die Datenbank-Engine läuft nicht oder wurde vor weniger als einer Minute neu gestartet.

Überwachen des Zustands der Instanz mit dem AWS-Managementkonsole

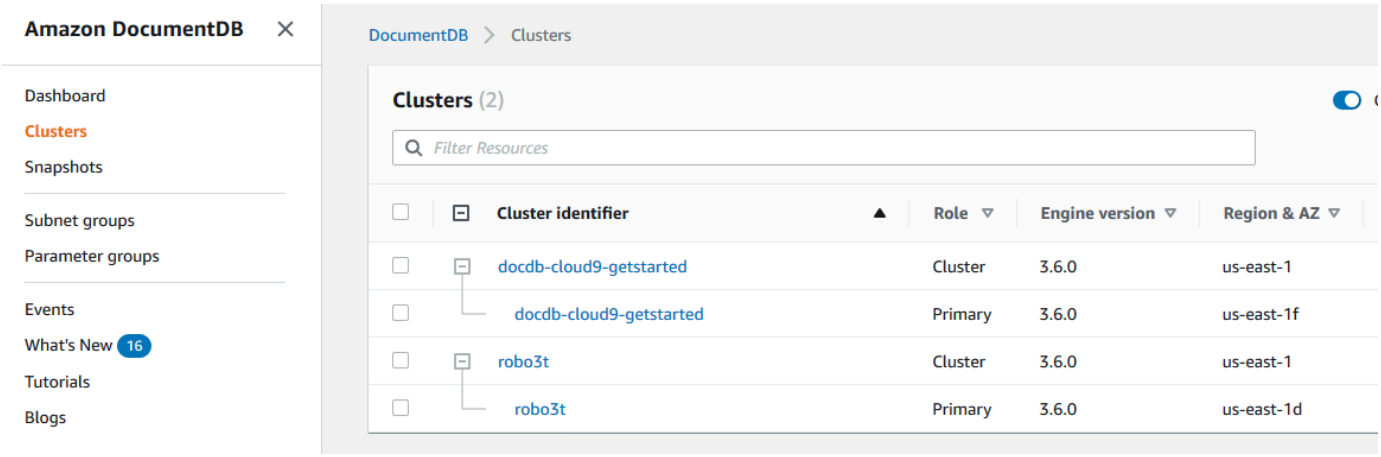
Verwenden Sie den AWS-Managementkonsole , um den Integritätsstatus Ihrer Instance zu überwachen.

Verwenden Sie bei der Verwendung die folgenden Schritte AWS-Managementkonsole, um den Integritätsstatus der Instanz zu verstehen.

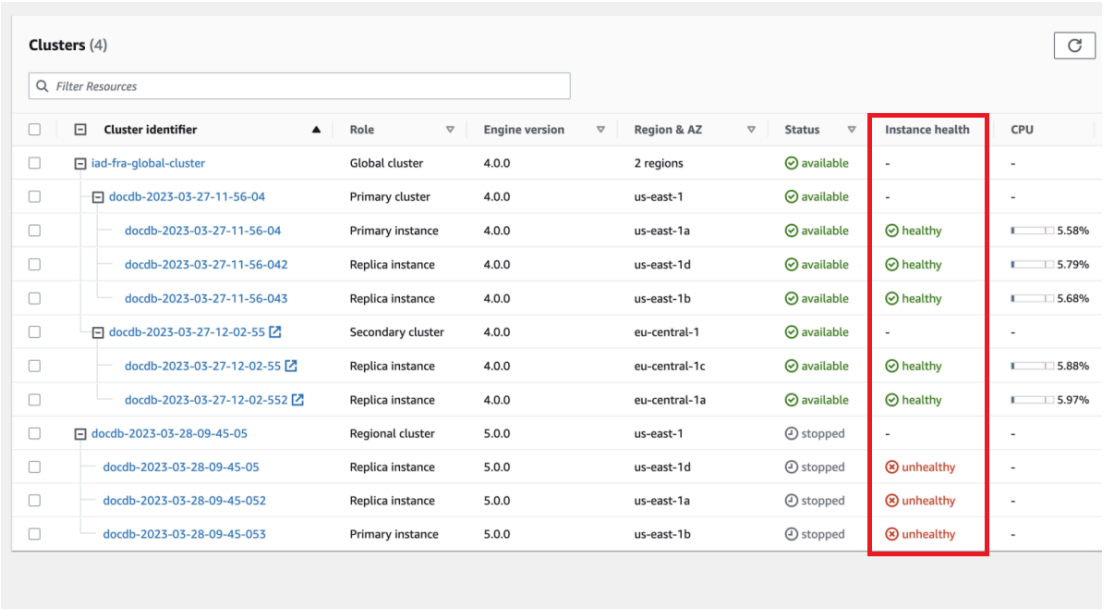
1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.

2. Klicken Sie im Navigationsbereich auf Cluster.

> **Note**
>
> Im Cluster-Navigationsfeld werden in der Spalte Cluster-ID sowohl Cluster als auch Instances angezeigt. Instances werden unter Clustern aufgeführt, ähnlich wie in der folgenden Abbildung.



3. Suchen Sie den Namen der Instance, an der Sie interessiert sind. Um den Status der Instanz zu ermitteln, lesen Sie dann in dieser Zeile bis zur Spalte Instanzstatus nach, wie in der folgenden Abbildung dargestellt:



> **Note**
>
> Die Abfrage des Instance-Integritätsstatus erfolgt alle 60 Sekunden und basiert auf der CloudWatch `EngineUptime` Systemmetrik. Die Werte in der Spalte Instanzstatus werden automatisch aktualisiert.

Amazon DocumentDB DocumentDB-Empfehlungen anzeigen

Amazon DocumentDB bietet eine Liste automatisierter Empfehlungen für Datenbankressourcen wie Instances und Cluster. Diese Empfehlungen dienen als Leitfaden für bewährte Verfahren, indem Sie Ihre Cluster- und Instance-Konfigurationen analysieren.

Ein Beispiel für diese Empfehlungen finden Sie im Folgenden:

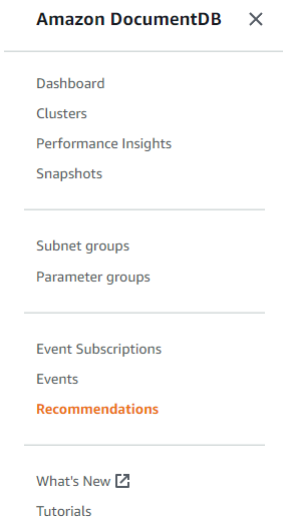
Typ	Beschreibung	Empfehlung	Zusätzliche Informationen
Eine -Instance	Der Cluster enthält nur eine Instanz	Leistung und Verfügbarkeit: Wir empfehlen, eine weitere Instanz mit derselben Instanzklasse in einer anderen Availability Zone hinzuzufügen.	Amazon DocumentDB Hochverfügbarkeit und Replikation

Amazon DocumentDB generiert Empfehlungen für eine Ressource, wenn die Ressource erstellt oder geändert wird. Amazon DocumentDB scannt Ihre Ressourcen auch regelmäßig und generiert Empfehlungen.

Um Empfehlungen von Amazon DocumentDB einzusehen und entsprechende Maßnahmen zu ergreifen

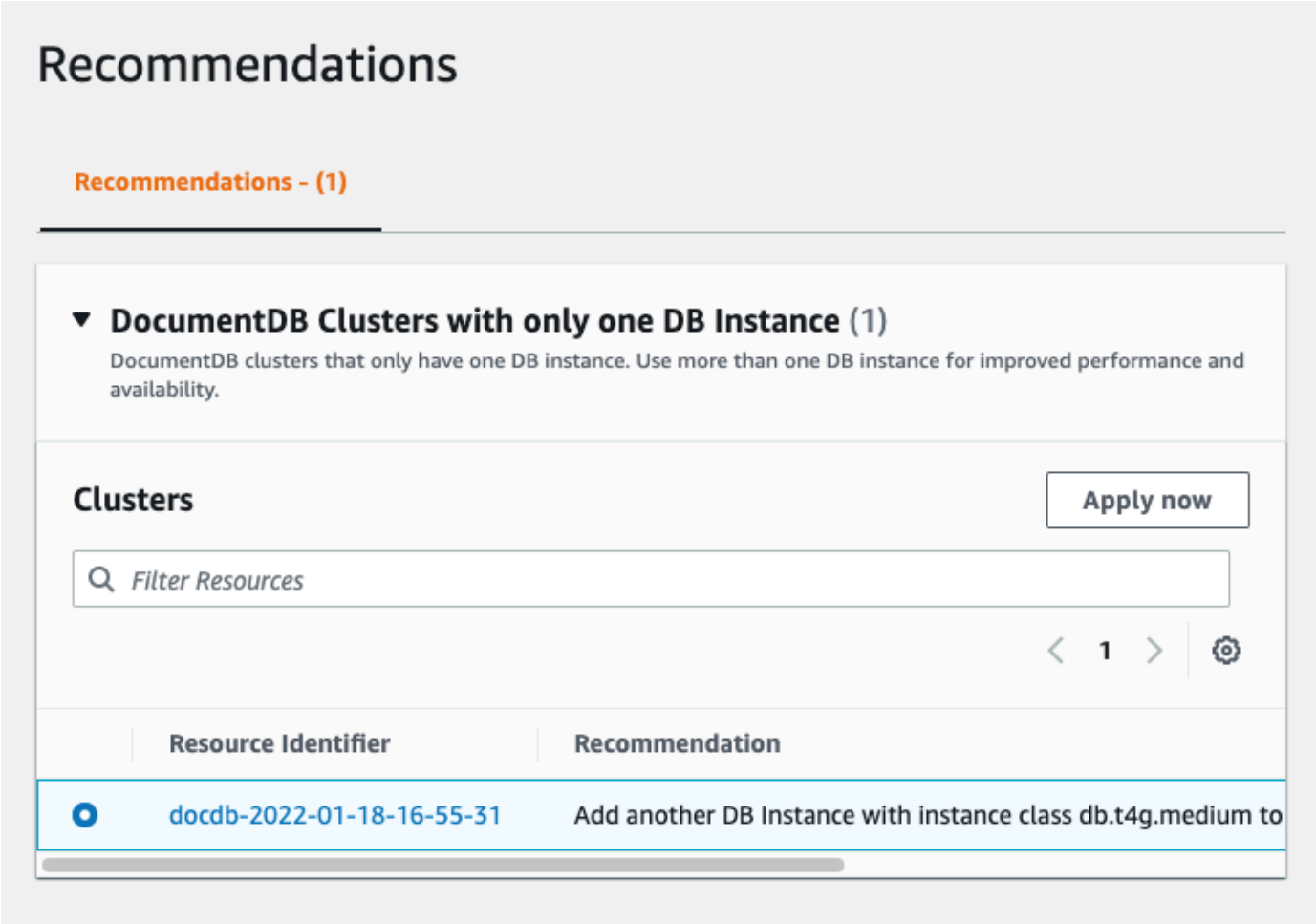
1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.

2. Wählen Sie im Navigationsbereich Empfehlungen aus:



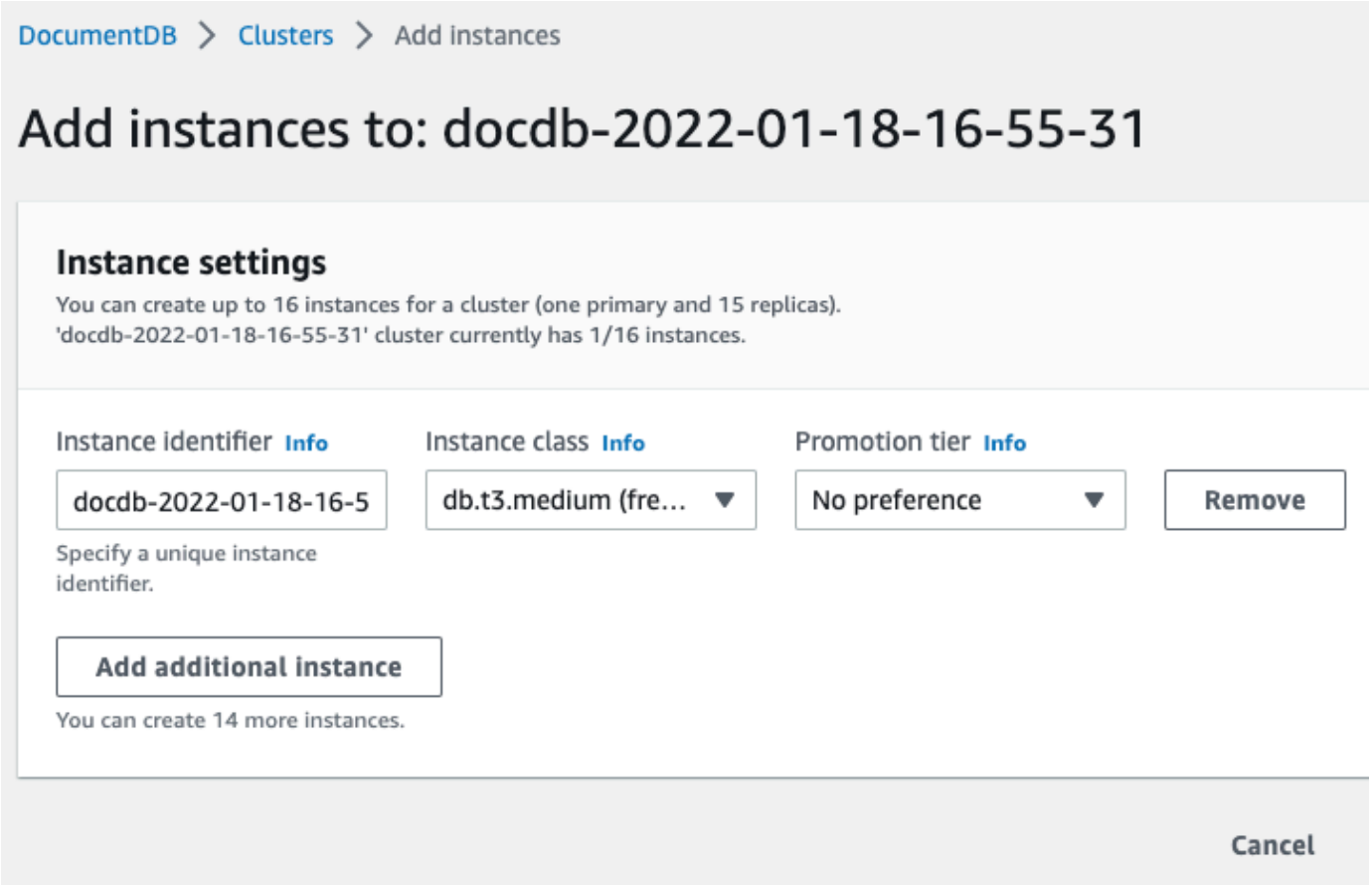
3. Erweitern Sie im Dialogfeld „Empfehlungen“ den gewünschten Bereich und wählen Sie die empfohlene Aufgabe aus.

   Im folgenden Beispiel bezieht sich die empfohlene Aufgabe auf einen Amazon DocumentDB-Cluster mit nur einer Instance. Es wird empfohlen, eine weitere Instance hinzuzufügen, um die Leistung und Verfügbarkeit zu verbessern.



4. Wählen Sie Apply now (Jetzt anwenden) aus.

   In diesem Beispiel wird das Dialogfeld „Instanzen hinzufügen“ angezeigt:



5. Ändern Sie die Einstellungen Ihrer neuen Instanz und wählen Sie Erstellen.

Amazon DocumentDB DocumentDB-Veranstaltungsabonnements verwenden

Amazon DocumentDB verwendet Amazon Simple Notification Service (Amazon SNS), um Benachrichtigungen bereitzustellen, wenn ein Amazon DocumentDB DocumentDB-Ereignis eintritt. Diese Benachrichtigungen können in jeder Form erfolgen, die von Amazon SNS für eine unterstützt wird AWS-Region, z. B. eine E-Mail, eine Textnachricht oder ein Anruf an einen HTTP-Endpunkt.

Amazon DocumentDB gruppiert diese Ereignisse in Kategorien, die Sie abonnieren können, sodass Sie benachrichtigt werden können, wenn ein Ereignis in dieser Kategorie eintritt. Sie können eine Ereigniskategorie für eine Instance, einen Cluster, einen Snapshot, einen Cluster-Snapshot oder eine Parametergruppe abonnieren. Wenn Sie beispielsweise die Backup-Kategorie für eine bestimmte Instanz abonnieren, werden Sie jedes Mal benachrichtigt, wenn ein Backup-bezogenes Ereignis eintritt, das sich auf die Instanz auswirkt. Sie erhalten auch eine Benachrichtigung, wenn sich ein Abonnement für ein Ereignis ändert.

Ereignisse treten sowohl auf Cluster- als auch auf Instanzebene auf, sodass Sie Ereignisse empfangen können, wenn Sie einen Cluster oder eine Instance abonnieren.

Ereignisabonnements werden an die Adressen gesendet, die Sie bei der Erstellung des Abonnements angegeben haben. Möglicherweise möchten Sie mehrere verschiedene Abonnements erstellen, z. B. ein Abonnement, das alle Ereignisbenachrichtigungen empfängt, und ein anderes Abonnement, das nur kritische Ereignisse für Ihre Produktionsinstanzen enthält. Sie können die Benachrichtigungen ganz einfach deaktivieren, ohne ein Abonnement zu löschen. Setzen Sie dazu das Optionsfeld Aktiviert in der Amazon DocumentDB DocumentDB-Konsole auf Nein.

> **Important**
>
> Amazon DocumentDB garantiert nicht die Reihenfolge der Ereignisse, die in einem Event-Stream gesendet werden. Die Reihenfolge der Ereignisse kann sich ändern.

Amazon DocumentDB verwendet den Amazon-Ressourcennamen (ARN) eines Amazon SNS-Themas, um jedes Abonnement zu identifizieren. Die Amazon DocumentDB DocumentDB-Konsole erstellt den ARN für Sie, wenn Sie das Abonnement erstellen.

Die Abrechnung von Amazon DocumentDB DocumentDB-Veranstaltungsabonnements erfolgt über Amazon SNS. Bei Verwendung von Ereignisbenachrichtigungen fallen Amazon-SNS-Gebühren an. Weitere Informationen finden Sie unter Preise für den Amazon Simple Notification Service (SNS). Abgesehen von den Amazon SNS SNS-Gebühren stellt Amazon DocumentDB keine Event-Abonnements in Rechnung.

Themen

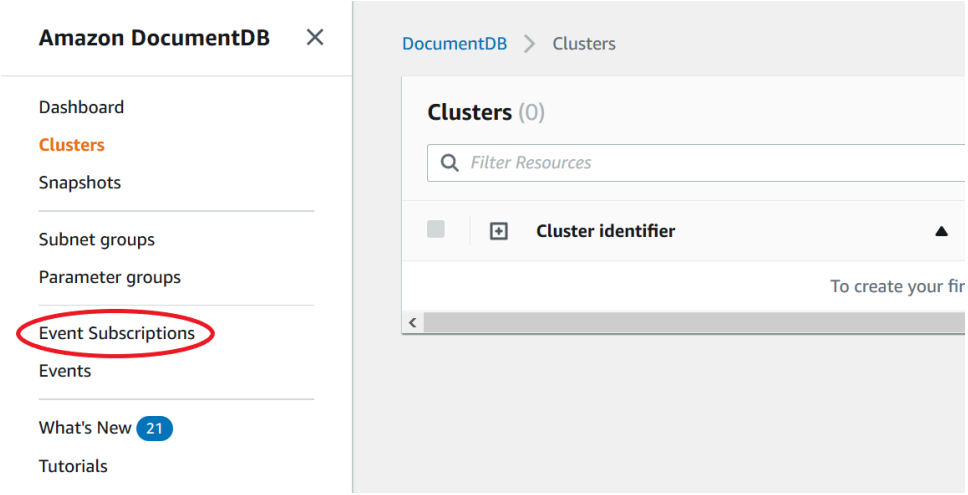
- Amazon DocumentDB DocumentDB-Veranstaltungen abonnieren
- Verwaltung von Abonnements für Amazon DocumentDB DocumentDB-Ereignisbenachrichtigungen
- Amazon DocumentDB DocumentDB-Ereigniskategorien und Meldungen

Amazon DocumentDB DocumentDB-Veranstaltungen abonnieren

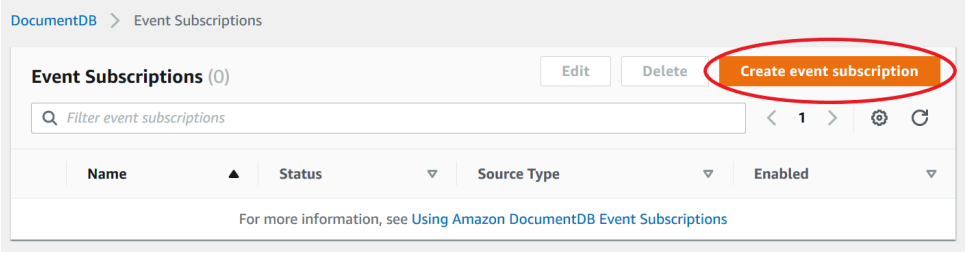
Sie können die Amazon DocumentDB DocumentDB-Konsole verwenden, um Veranstaltungsabonnements wie folgt zu abonnieren:

1. Melden Sie sich AWS-Managementkonsole unter an. https://console.aws.amazon.com/docdb

2. Wählen Sie im Navigationsbereich Ereignisabonnements aus.

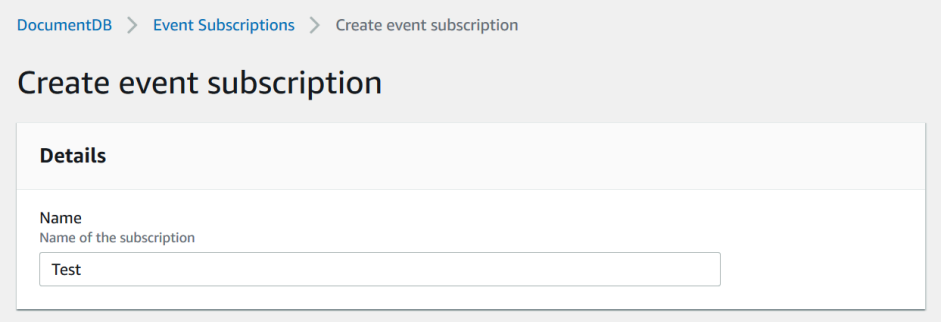


3. Wählen Sie im Bereich Ereignisabonnements Ereignisabonnement erstellen aus.

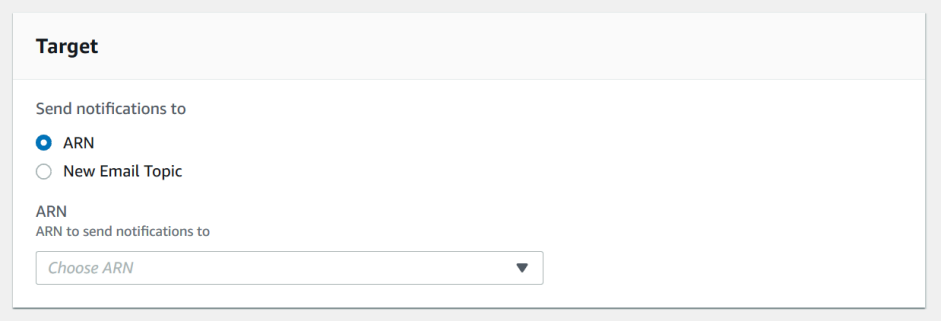


4. Gehen Sie im Dialogfeld Ereignisabonnement erstellen wie folgt vor:

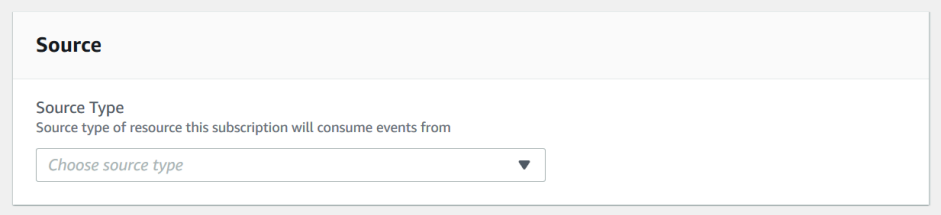
   - Geben Sie unter Name einen Namen für das Abonnement für Ereignisbenachrichtigungen ein.



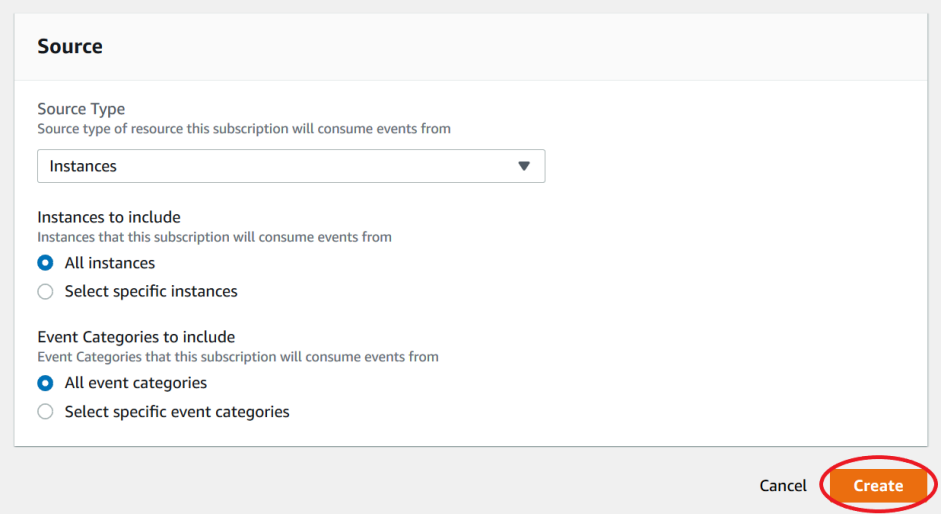
   - Wählen Sie für Target aus, wohin Sie Benachrichtigungen senden möchten. Sie können einen vorhandenen ARN oder Neues E-Mail-Thema wählen, um den Namen eines Themas und eine Empfängerliste einzugeben.



- Wählen Sie für Quelle einen Quelltyp aus. Wählen Sie abhängig vom ausgewähltem Quelltyp die Ereigniskategorien und Quellen aus, für die Sie Ereignisbenachrichtigungen erhalten möchten.



- Wählen Sie Erstellen aus.

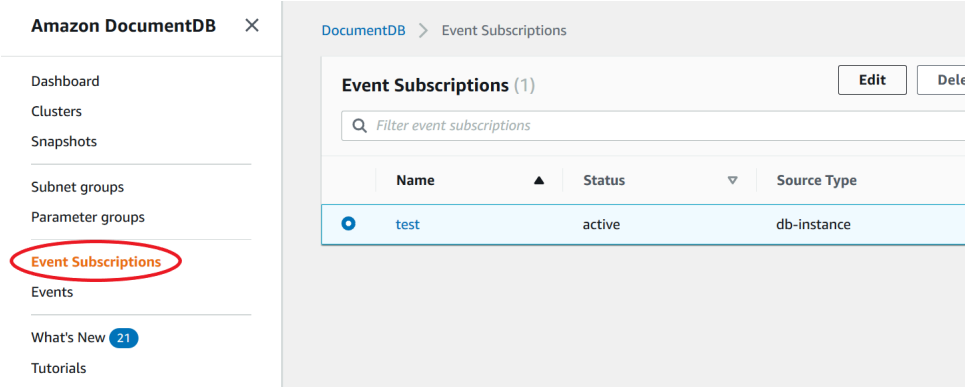


Verwaltung von Abonnements für Amazon DocumentDB DocumentDB-Ereignisbenachrichtigungen

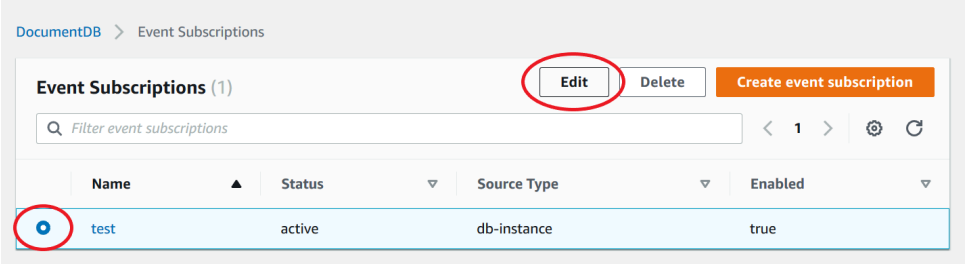
Wenn Sie im Navigationsbereich der Amazon DocumentDB DocumentDB-Konsole Event-Abonnements auswählen, können Sie Abonnementkategorien und eine Liste Ihrer aktuellen Abonnements einsehen. Sie können auch ein bestimmtes Abonnement ändern oder löschen.

So ändern Sie Ihre aktuellen Amazon DocumentDB DocumentDB-Abonnements für Ereignisbenachrichtigungen

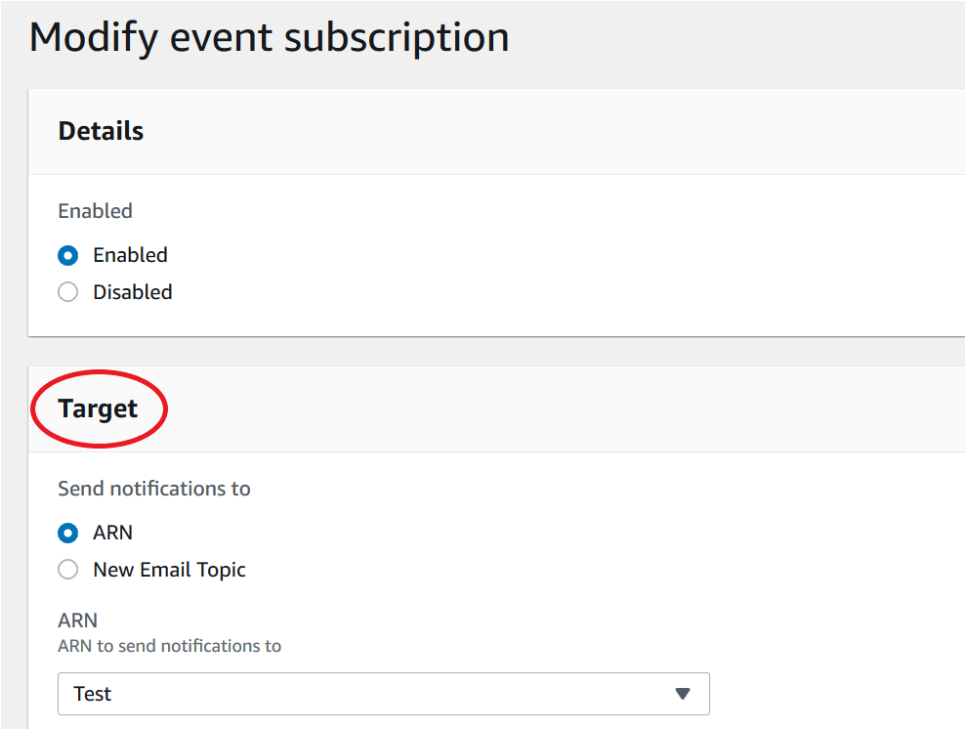
1. Melden Sie sich AWS-Managementkonsole unter an. https://console.aws.amazon.com/docdb
2. Wählen Sie im Navigationsbereich Ereignisabonnements aus. Im Bereich Ereignisabonnements werden all Ihre Abonnements für Ereignisbenachrichtigungen angezeigt.



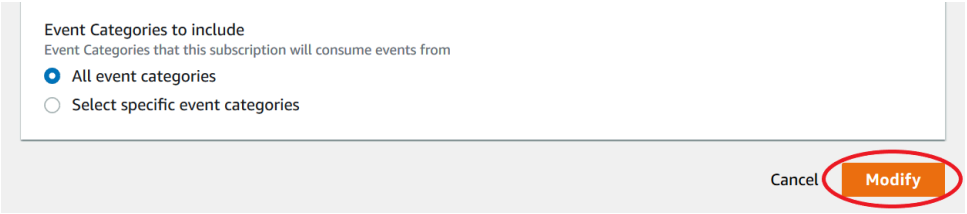
3. Wählen Sie im Bereich Ereignisabonnements das Abonnement, das Sie modifizieren möchten, und klicken Sie auf Bearbeiten.



4. Nehmen Sie Ihre Änderungen am Abonnement im Bereich Ziel oder Quelle vor. Sie können Quell-IDs hinzufügen oder entfernen, indem Sie diese im Bereich Quelle auswählen oder ihre Auswahl aufheben.



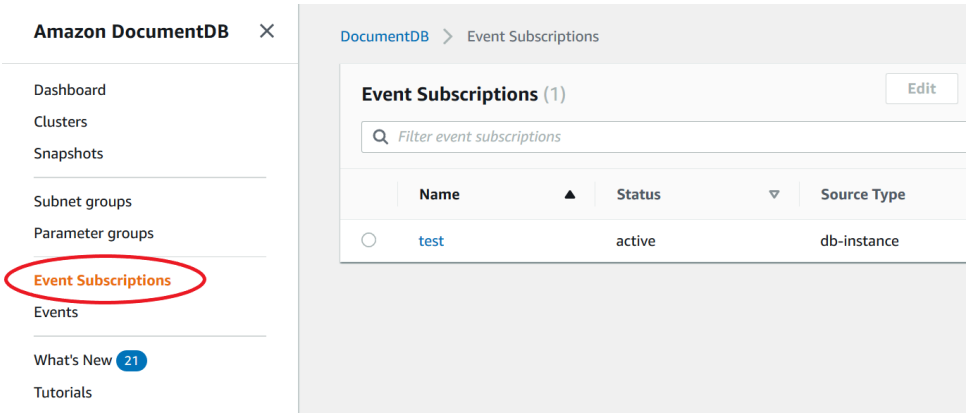
5. Wählen Sie Ändern aus. Die Amazon DocumentDB DocumentDB-Konsole zeigt an, dass das Abonnement geändert wird.



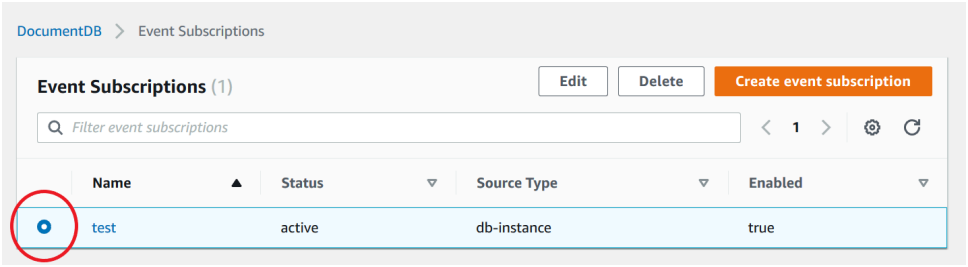
Löschen eines Abonnements für Amazon DocumentDB DocumentDB-Ereignisbenachrichtigungen

Sie können ein Abonnement löschen, wenn Sie es nicht mehr benötigen. Alle Abonnenten des Themas erhalten dann keine weiteren Ereignisbenachrichtigungen, die über dieses Abonnement ausgegeben wurden.

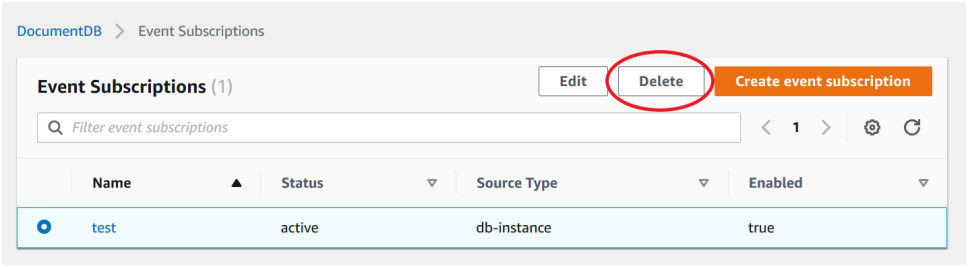
1. Melden Sie sich AWS-Managementkonsole unter an. https://console.aws.amazon.com/docdb
2. Wählen Sie im Navigationsbereich Ereignisabonnements aus.



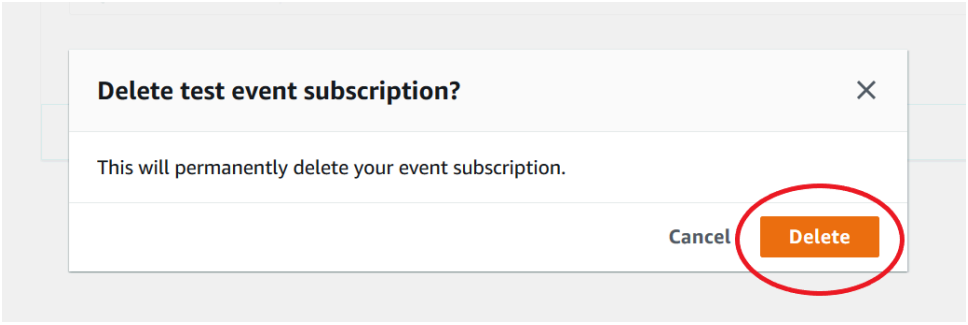
3. Wählen Sie im Bereich Ereignisabonnements das Abonnement aus, das Sie löschen möchten.



4. Wählen Sie Löschen aus.



5. In einem Popup-Fenster werden Sie gefragt, ob Sie diese Benachrichtigung dauerhaft löschen möchten. Wählen Sie Löschen aus.



Amazon DocumentDB DocumentDB-Ereigniskategorien und Meldungen

Amazon DocumentDB generiert eine beträchtliche Anzahl von Ereignissen in Kategorien, die Sie über die Konsole abonnieren können. Jede Kategorie bezieht sich auf einen Quelltyp, bei dem es sich um eine Instance, einen Cluster, einen Snapshot oder eine Parametergruppe handeln kann.

> **Note**
>
> Amazon DocumentDB verwendet bestehende Amazon RDS-Ereignisdefinitionen und -IDs.

Amazon DocumentDB DocumentDB-Ereignisse, die von Instances stammen

Kategorie	Description
Verfügbarkeit	Die Instance wurde neu gestartet.
Verfügbarkeit	Die Instanz wurde heruntergefahren.
Konfigurationsänderung	Änderung auf eine Instanzklasse anwenden.
Konfigurationsänderung	Das Anwenden der Änderung auf eine Instanzklasse wurde abgeschlossen.
Konfigurationsänderung	Setzen Sie die primären Anmeldeinformationen zurück.
Erstellung	Instanz wurde erstellt.
Löschung	Instanz wurde gelöscht
Ausfall	Die Instanz ist aufgrund einer inkompatiblen Konfiguration oder eines zugrunde liegenden Speicherproblems ausgefallen. Starten Sie eine Point-in-Time-Wiederherstellung für die Instanz.
Benachrichtigung	Die Instanz wurde gestoppt.
Benachrichtigung	Instanz wurde gestartet.

Kategorie	Description
Benachrichtigung	Die Instanz wird gestartet, weil sie die maximal zulässige Zeit für das Stoppen überschritten hat.
Wiederherstellung	Die Wiederherstellung der Instanz wurde gestartet. Die Wiederherstellungsdauer variiert je nach zu wiederherstellender Datenmenge.
Wiederherstellung	Die Wiederherstellung der Instanz ist abgeschlossen.
Ausführen von Sicherheits-Patches	Das Betriebssystem-Update ist für Ihre Instance verfügbar. Informationen zum Anwenden von Updates finden Sie unter Wartung von Amazon DocumentDB.

Amazon DocumentDB DocumentDB-Ereignisse, die aus einem Cluster stammen

Kategorie	Description
Erstellung	Cluster wurde erstellt
Löschung	Cluster wurde gelöscht.
Failover	Der vorherige Primärserver wird erneut beworben.
Failover	Der Failover zur Instanz wurde abgeschlossen.
Failover	Der Failover zur DB-Instance wurde gestartet: %s
Failover	Derselbe AZ-Failover zur DB-Instance wurde gestartet: %s

Kategorie	Description
Failover	Cross-AZ-Failover zur DB-Instance gestartet: %s
Wartung	Der Cluster wurde gepatcht.
Wartung	Der Datenbank-Cluster befindet sich in einem Zustand, der nicht aktualisiert werden kann: %s
Benachrichtigung	Der Cluster wurde gestoppt.
Benachrichtigung	Der Cluster wurde gestartet.
Benachrichtigung	Der Clusterstopp ist fehlgeschlagen.
Benachrichtigung	Der Cluster wird gestartet, weil er die maximal zulässige Zeit für das Stoppen überschritten hat.
Benachrichtigung	Der Cluster wurde von %s in %s umbenannt.

Amazon DocumentDB DocumentDB-Ereignisse, die aus einem Cluster-Snapshot stammen

Die folgende Tabelle zeigt die Ereigniskategorie und eine Liste der Ereignisse, wenn ein Amazon DocumentDB-Cluster-Snapshot der Quelltyp ist.

Kategorie	Description
backup	Ein manueller Cluster-Snapshot wird erstellt.
backup	Ein manueller Cluster-Snapshot wurde erstellt.
backup	Erstellen eines automatisierten Cluster-S napshots.
backup	Automatisierter Cluster-Snapshot erstellt.

Amazon DocumentDB DocumentDB-Ereignisse, die aus einer Parametergruppe stammen

Die folgende Tabelle zeigt den Ereignistyp sowie eine Liste der Ereignisse für den Fall, dass der Quelltyp „Parametergruppe“ ist.

Kategorie	Description
Konfigurationsänderung	Der Parameter %s wurde mit der Methode %s auf %s aktualisiert

Überwachen von Amazon DocumentDB mit CloudWatch

Amazon DocumentDB (mit MongoDB-Kompatibilität) ist in Amazon integriert, CloudWatch sodass Sie Betriebsmetriken für Ihre Cluster sammeln und analysieren können. Sie können diese Metriken mit der CloudWatch Konsole, der Amazon DocumentDB DocumentDB-Konsole, der AWS Command Line Interface (AWS CLI) oder der CloudWatch API überwachen.

CloudWatch ermöglicht es Ihnen auch, Alarme einzustellen, sodass Sie benachrichtigt werden können, wenn ein Metrikwert einen von Ihnen angegebenen Schwellenwert überschreitet.
Sie können Amazon CloudWatch Events sogar so einrichten, dass im Falle eines Verstoßes Korrekturmaßnahmen ergriffen werden. Weitere Informationen zur Verwendung CloudWatch und zu Alarmen finden Sie in der CloudWatch Amazon-Dokumentation.

Themen

- Amazon DocumentDB-Metriken
- CloudWatch Daten anzeigen
- Abmessungen von Amazon DocumentDB
- Überwachung von Opcounter-Metriken
- Überwachen von Datenbankverbindungen

Amazon DocumentDB-Metriken

Um den Zustand und die Leistung Ihres Amazon DocumentDB-Clusters und Ihrer Amazon DocumentDB-Instances zu überwachen, können Sie die folgenden Metriken in der Amazon DocumentDB-Konsole einsehen.

> **Note**
>
> Die Metriken in den folgenden Tabellen gelten sowohl für instanzbasierte als auch für elastische Cluster.

Themen

- Metriken zur Ressourcenauslastung
- Latenzmetriken
- NVMe-backed Instanz-Metriken
- Kennzahlen für den Betrieb
- Durchsatzmetriken
- Systemmetriken
- Metriken für T3-Instanzen

Metriken zur Ressourcenauslastung

Metrik	Description	
`BackupRetentionPeriodStorageUsed`	Die Gesamtmenge des Backup-Speichers in Byte, der zur Unterstützung der Point-in-Time-Wiederherstellungsfunktion innerhalb des Aufbewahrungsfensters von Amazon DocumentDB verwendet wird. Ist in dem von der `TotalBackupStorageBilled` -Metrik gemeldeten Gesamtwert enthalten. Wird für jeden Amazon DocumentDB-Cluster separat berechnet.	
`ChangeStreamLogSize`	Die Menge des Speichers , der vom Cluster zum	

Metrik	Description	
	Speichern des Änderungsstream-Protokolls in Megabyte verwendet wird. Dieser Wert ist eine Teilmenge des Gesamtspeichers für den Cluster (`VolumeBytesUsed`) und wirkt sich auf die Kosten des Clusters aus. Informationen zu Speicherpreisen finden Sie auf der Amazon DocumentDB DocumentDB-Produktseite. Die Protokollgröße des Änderungsstreams ist vom Umfang der Änderungen auf Ihrem Cluster und der Aufbewahrungsdauer des Änderungsstream-Protokoll abhängig. Weitere Informationen zu Änderungsstreams finden Sie unter Change-Streams mit Amazon DocumentDB verwenden.	
`CPUUtilization`	Prozentsatz der CPU-Nutzung durch eine Instance.	
`DatabaseConnections`	Die Anzahl der Verbindungen (aktiv und inaktiv), die auf einer Instance im Abstand von 1 Minute geöffnet sind.	

Metrik	Description
DatabaseConnectionsMax	Die maximale Anzahl offener Datenbankverbindungen (aktiv und inaktiv) auf einer Instance in einem Zeitraum von 1 Minute.
DatabaseConnectionsLimit	Die maximale Anzahl gleichzeitiger Datenbankverbindungen (aktiv und inaktiv), die für eine Instance zu einem bestimmten Zeitpunkt zulässig sind.
DatabaseCursors	Die Anzahl der auf einer Instance geöffneten Cursor, die im Abstand von 1 Minute geöffnet werden.
DatabaseCursorsMax	Die maximale Anzahl geöffneter Cursor auf einer Instance in einem Zeitraum von 1 Minute.
DatabaseCursorsLimit	Die maximale Anzahl von Cursorn, die auf einer Instanz zu einem bestimmten Zeitpunkt zulässig sind.
DatabaseCursorsTimedOut	Die Anzahl der Cursor, bei denen innerhalb eines Zeitraums von 1 Minute ein Timeout aufgetreten ist.
FreeableMemory	Die Menge des verfügbaren Arbeitsspeichers (RAM-Speicher) in Bytes.

Metrik	Description
FreeLocalStorage	Diese Metrik gibt die Menge an Speicher an, der für jede Instance für temporäre Tabellen und Protokolle zur Verfügung steht. Dieser Wert hängt von der Instance-Klasse ab. Sie können die Menge an freiem Speicherplatz für eine Instance erhöhen, indem Sie eine größere Instance-Klasse für Ihre Instance auswählen. (Dies gilt nicht für DocumentDB Serverless.)
LowMemThrottleQueueDepth	Die Warteschlangentiefe für Anfragen, die aufgrund von zu wenig verfügbarem Speicherplatz gedrosselt werden und in einer Frequenz von 1 Minute abgerufen werden.
LowMemThrottleMaxQueueDepth	Die maximale Warteschlangentiefe für Anfragen, die aufgrund von zu wenig verfügbarem Speicherplatz in einem Zeitraum von 1 Minute gedrosselt werden.
LowMemNumOperationsThrottled	Die Anzahl der Anfragen, die aufgrund von zu wenig verfügbarem Speicherplatz in einem Zeitraum von 1 Minute gedrosselt werden.

Metrik	Description	
SnapshotStorageUsed	Die Gesamtmenge des Backup-Speichers in Byte, der von allen Snapshots für einen bestimmten Amazon DocumentDB-Cluster außerhalb seines Aufbewahrungsfensters für Backups verbraucht wird. Ist in dem von der TotalBackupStorageBilled -Metrik gemeldeten Gesamtwert enthalten. Wird für jeden Amazon DocumentDB-Cluster separat berechnet.	
SwapUsage	Größe des auf der Instance genutzten Auslagerungsbereichs.	
TotalBackupStorageBilled	Die Gesamtmenge an Backup-Speicher in Byte, die Ihnen für einen bestimmten Amazon DocumentDB-Cluster in Rechnung gestellt wird. Umfasst den Sicherungsspeicher gemessen an den Metriken SnapshotStorageUsed und BackupRetentionPeriodStorageUsed . Wird für jeden Amazon DocumentDB-Cluster separat berechnet.	

Metrik	Description
`TransactionsOpen`	Die Anzahl der offenen Transaktionen auf einer Instance, die im Abstand von 1 Minute ausgeführt wurden.
`TransactionsOpenMax`	Die maximale Anzahl von Transaktionen, die in einem Zeitraum von 1 Minute auf einer Instance geöffnet werden.
`TransactionsOpenLimit`	Die maximale Anzahl gleichzeitiger Transaktionen, die auf einer Instance zu einem bestimmten Zeitpunkt zulässig sind.
`VolumeBytesUsed`	Die Menge des von Ihrem Cluster verwendeten Speicherplatzes in Byte. Dieser Wert wirkt sich auf die Kosten des Clusters aus. Preisinformationen finden Sie auf der Amazon DocumentDB DocumentDB-Produktseite.

Latenzmetriken

Metrik	Description
`DBClusterReplicaLagMaximum`	Die maximale Verzögerung in Millisekunden zwischen der primären Instance und jeder Amazon DocumentD

Metrik	Description
	B DocumentDB-Instance im Cluster.
`DBClusterReplicaLagMinimum`	Die Mindestverzögerung zwischen der Primär-Instance und jeder Replikat-Instance im Cluster, angegeben in Millisekunden.
`DBInstanceReplicaLag`	Die Verzögerung in Millisekunden, wenn Updates von der Primär-Instance an eine Replikat-Instance repliziert werden.
`ReadLatency`	Die durchschnittliche Zeit, die pro Festplattenvorgang benötigt wird. I/O
`WriteLatency`	Die durchschnittliche Zeit, in Millisekunden, die pro Festplattenvorgang benötigt wird. I/O

NVMe-backed Instanz-Metriken

Metrik	Description
`NVMeStorageCacheHitRatio`	Der Prozentsatz der Anfragen, die vom mehrstufigen Cache bedient werden.
`FreeNVMeStorage`	Die Menge des verfügbaren flüchtigen NVMe-Speicherplatzes

Metrik	Description
ReadIOPSNVMeStorage	Die durchschnittliche Anzahl von I/O Festplatten-Lesevorgängen in den ephemeren NVMe-Speicher.
ReadLatencyNVMeStorage	Die durchschnittliche Zeit, die pro Festplattenlesevorgang für Ephemeral I/O NVMe-Speicher benötigt wird.
ReadThroughputNVMeStorage	Die durchschnittliche Anzahl von Bytes, die pro Sekunde von der Festplatte für den flüchtigen NVMe-Speicher gelesen werden.
WriteIOPSNVMeStorage	Die durchschnittliche Anzahl von I/O Schreibvorgängen auf der Festplatte in den ephemeren NVMe-Speicher.
WriteLatencyNVMeStorage	Die durchschnittliche Zeit, die pro I/O Schreibvorgang auf der Festplatte für Ephemeral NVMe-Speicher benötigt wird.
WriteThroughputNVMeStorage	Die durchschnittliche Anzahl von Bytes, die pro Sekunde für den flüchtigen NVMe-Speicher auf die Festplatte geschrieben werden

Kennzahlen für den Betrieb

Metrik	Description	
DocumentsDeleted	Die Anzahl der gelöschten Dokumente in einem Zeitraum von 1 Minute.	
DocumentsInserted	Die Anzahl der eingefügten Dokumente in einem Zeitraum von 1 Minute.	
DocumentsReturned	Die Anzahl der zurückgeg ebenen Dokumente in einem Zeitraum von 1 Minute.	
DocumentsUpdated	Die Anzahl der aktualisierten Dokumente in einem Zeitraum von 1 Minute.	
OpcountersCommand	Die Anzahl der Befehle, die in einem Zeitraum von 1 Minute ausgegeben wurden.	
OpcountersDelete	Die Anzahl der Löschvorg änge, die in einem Zeitraum von 1 Minute ausgeführt wurden.	
OpcountersGetmore	Die Anzahl der innerhalb einer Minute ausgegebenen Getmores.	
OpcountersInsert	Die Anzahl der innerhalb eines Zeitraums von 1 Minute ausgeführten Insert-Op erationen.	

Metrik	Description
`OpcountersQuery`	Die Anzahl der Abfragen, die in einem Zeitraum von 1 Minute ausgegeben wurden.
`OpcountersUpdate`	Die Anzahl der Aktualisierungsvorgänge, die in einem Zeitraum von 1 Minute ausgeführt wurden.
`TransactionsStarted`	Die Anzahl der Transaktionen, die in einem Zeitraum von 1 Minute auf einer Instance gestartet wurden.
`TransactionsCommitted`	Die Anzahl der Transaktionen, die in einem Zeitraum von 1 Minute auf einer Instance festgeschrieben wurden.
`TransactionsAborted`	Die Anzahl der Transaktionen, die auf einer Instance in einem Zeitraum von 1 Minute abgebrochen wurden.
`TTLDeletedDocuments`	Die Anzahl der Dokumente, die von einem TTLMonitor in einem Zeitraum von 1 Minute gelöscht wurden.

Durchsatzmetriken

Metrik	Description
`NetworkReceiveThroughput`	Der von Clients erhaltene Netzwerkdurchsatz für

Metrik	Description	
	jede Instance im Cluster, angegeben in Bytes pro Sekunde. Dieser Durchsatz beinhaltet nicht den Netzwerkdatenverkehr zwischen den Instances im Cluster und dem Cluster-Volume.	
`NetworkThroughput`	Die Menge des Netzwerkdurchsatzes in Byte pro Sekunde, der von jeder Instance im Amazon DocumentDB-Cluster sowohl von Clients empfangen als auch an diese übertragen wird. Dieser Durchsatz beinhaltet nicht den Netzwerkdatenverkehr zwischen den Instances im Cluster und dem Cluster-Volume.	
`NetworkTransmitThroughput`	Der an Clients gesendete Netzwerkdurchsatz für jede Instance im Cluster, angegeben in Bytes pro Sekunde. Dieser Durchsatz beinhaltet nicht den Netzwerkdatenverkehr zwischen den Instances im Cluster und dem Cluster-Volume.	

Metrik	Description
ReadIOPS	Die durchschnittliche Anzahl von I/O Festplatten-Lesevorgängen pro Sekunde. Amazon DocumentDB meldet Lese- und Schreib-IOPS getrennt und in 1-Minuten-Intervallen.
ReadThroughput	Die durchschnittliche Anzahl Byte, die pro Sekunde vom Datenträger gelesen werden.
StorageNetworkReceiveThroughput	Die Menge des Netzwerkdurchsatzes in Byte pro Sekunde, den jede Instance im Cluster vom Amazon DocumentDB-Cluster-Speichervolume empfängt.
StorageNetworkTransmitThroughput	Die Menge an Netzwerkdurchsatz in Byte pro Sekunde, die von jeder Instance im Cluster an das Amazon DocumentDB-Cluster-Speichervolume gesendet wird.

Metrik	Description	
`StorageNetworkThroughput`	Die Menge des Netzwerkdurchsatzes in Byte pro Sekunde, der von jeder Instance im Amazon DocumentDB-Cluster empfangen und an das Amazon DocumentDB-Cluster-Speichervolume gesendet wurde.	

Metrik	Description
`VolumeReadIOPs`	Die durchschnittliche Anzahl von abgerechneten I/O Lesevorgängen auf einem Cluster-Volume, die in 5-Minuten-Intervallen gemeldet werden. In Rechnung gestellte Lesevorgänge werden auf Cluster-Volume-Ebene berechnet, aus allen Instances im Cluster zusammengestellt und dann in fünfminütigen Intervallen gemeldet. Der Wert wird anhand des Werts der Metrik für Leseopera tionen über einen fünfminüt igen Zeitraum berechnet . Sie können die Menge an in Rechnung gestellte n Leseoperationen pro Sekunde bestimmen, indem Sie den Wert der Metrik für in Rechnung gestellte Leseopera tionen durch 300 Sekunden teilen. Wenn der beispielsweise 13.686 `VolumeReadIOPs` zurückgibt, dann sind die fakturierten Lesevorgänge pro Sekunde 45 (13.686/300 = 45,62). In Rechnung gestellte Operationen fallen für Abfragen für nicht im Buffer-

Metrik	Description	
	Cache enthaltene Datenbank seiten an, die erst aus dem Speicher geladen werden müssen. Sie sehen evtl. Spitzenwerte in den in Rechnung gestellten Operationen, da Abfrageergebnisse aus dem Speicher gelesen und anschließend in den Buffer-Cache geladen werden.	

Metrik	Description	
VolumeWriteIOPs	Die durchschnittliche Anzahl von fakturierten I/O Schreibvorgängen auf einem Cluster-Volume, die in 5-Minuten-Intervallen gemeldet wird. In Rechnung gestellte Schreibvorgänge werden auf Cluster-Volume-Ebene berechnet, aus allen Instances im Cluster aggregiert und dann in 5-Minuten-Intervallen gemeldet. Der Wert wird anhand des Werts der Schreiboperationsmetrik über einen Zeitraum von 5 Minuten berechnet. Sie können die Menge der in Rechnung gestellten Schreiboperationen pro Sekunde ermitteln, indem Sie den Wert der Schreiboperations-Abrechnungsmetrik durch 300 Sekunden teilen. Wenn beispielsweise 13.686 VolumeWriteIOPs zurückgegeben wird, beträgt die fakturierte Schreiboperation pro Sekunde 45 (13.686/300 = 45,62). Beachten Sie, dass die VolumeReadIOPs VolumeWriteIOPs Metriken von der DocumentDB-Speicherebene berechnet	

Metrik	Description	
	werden und die von der Primär- und Replikatinstanz ausgeführten IOs einschlie ßen. Die Daten werden alle 20 bis 30 Minuten aggregier t und dann in Intervallen von 5 Minuten gemeldet, sodass in dem Zeitraum derselbe Datenpunkt für die Metrik ausgegeben wird. Wenn Sie nach einer Metrik suchen, die mit Ihren Einfügevo rgängen über ein Intervall von 1 Minute korreliert, können Sie die WriteIOps-Metrik auf Instanzebene verwenden. Die Metrik ist auf der Registerk arte Überwachung Ihrer primären Amazon DocumentD B DocumentDB-Instance verfügbar.	
`WriteIOPS`	Die durchschnittliche Anzahl von I/O Schreibvorgängen auf der Festplatte pro Sekunde. Bei Verwendung auf Clustereb ene `WriteIOPs` werden sie für alle Instanzen im Cluster ausgewertet. Lese- und Schreib-IOPS werden separat und in 1-Minuten-Intervallen angegeben.	

Metrik	Description
`WriteThroughput`	Die durchschnittliche Anzahl von Bytes, die pro Sekunde auf den Datenträger geschrieben werden.

Systemmetriken

Metrik	Description
`AvailableMVCCIds`	Ein Zähler, der die Anzahl der verbleibenden Schreibvorgänge anzeigt, bevor der Wert Null erreicht wird. Wenn dieser Zähler Null erreicht, wechselt Ihr Cluster in den schreibgeschützten Modus, bis IDs zurückgewonnen und recycelt werden. Der Zähler nimmt mit jedem Schreibvorgang ab und steigt, wenn bei der Garbage-Collection alte MVCC-IDs wiederverwendet werden.
`BufferCacheHitRatio`	Der Prozentsatz der vom Buffer-Cache bedienten Anfragen.
`DiskQueueDepth`	Die Anzahl der I/O Operationen, die darauf warten, auf die Festplatte geschrieben oder von der Festplatte gelesen zu werden.

Metrik	Description	
`EngineUptime`	Die Gesamtlaufzeit der Instance in Sekunden.	
`IndexBufferCacheHitRatio`	Der Prozentsatz der Indexanforderungen, die vom Puffercache bedient werden. Möglicherweise stellen Sie unmittelbar nach dem Löschen eines Indexes, einer Sammlung oder einer Datenbank einen Anstieg von mehr als 100 Prozent für die Metrik fest. Dies wird nach 60 Sekunden automatisch korrigiert. Diese Einschränkung wird in einem future Patch-Update behoben.	
`LongestActiveGCRuntime`	Dauer des längsten aktiven Garbage-Collection-Vorgangs in Sekunden. Wird jede Minute aktualisiert und verfolgt nur aktive Vorgänge, ausgenommen Prozesse, die innerhalb des Zeitfensters von einer Minute abgeschlossen werden.	

Metriken für T3-Instanzen

Metrik	Description	
`CPUCreditUsage`	Die Anzahl der CPU-Credits, die während des Messzeitraums ausgegeben wurden.	

Metrik	Description
`CPUCreditBalance`	Die Anzahl der CPU-Credits, die eine Instance gesammelt hat. Dieser Saldo wird während der Steigerung der CPU-Leistung aufgebrau cht, da die CPU-Guthaben schneller verbraucht als erworben werden.
`CPUSurplusCreditBa lance`	Die Anzahl der überschüs sigen CPU-Guthaben, die zur Aufrechterhaltung der CPU-Leistung ausgegeben wurden, wenn der CPUCreditBalance Wert Null ist.
`CPUSurplusCreditsC harged`	Die Anzahl der überschüs sigen CPU-Guthaben, die die maximale Anzahl an CPU-Credits überschre iten, die innerhalb von 24 Stunden verdient werden können, sodass zusätzliche Gebühren anfallen. Weitere Informationen finden Sie unter Überwachen Ihres CPU-Gutha bens.

CloudWatch Daten anzeigen

Sie können CloudWatch Amazon-Daten mit der CloudWatch Konsole, der Amazon DocumentDB-Konsole AWS Command Line Interface (AWS CLI) oder der CloudWatch API anzeigen.

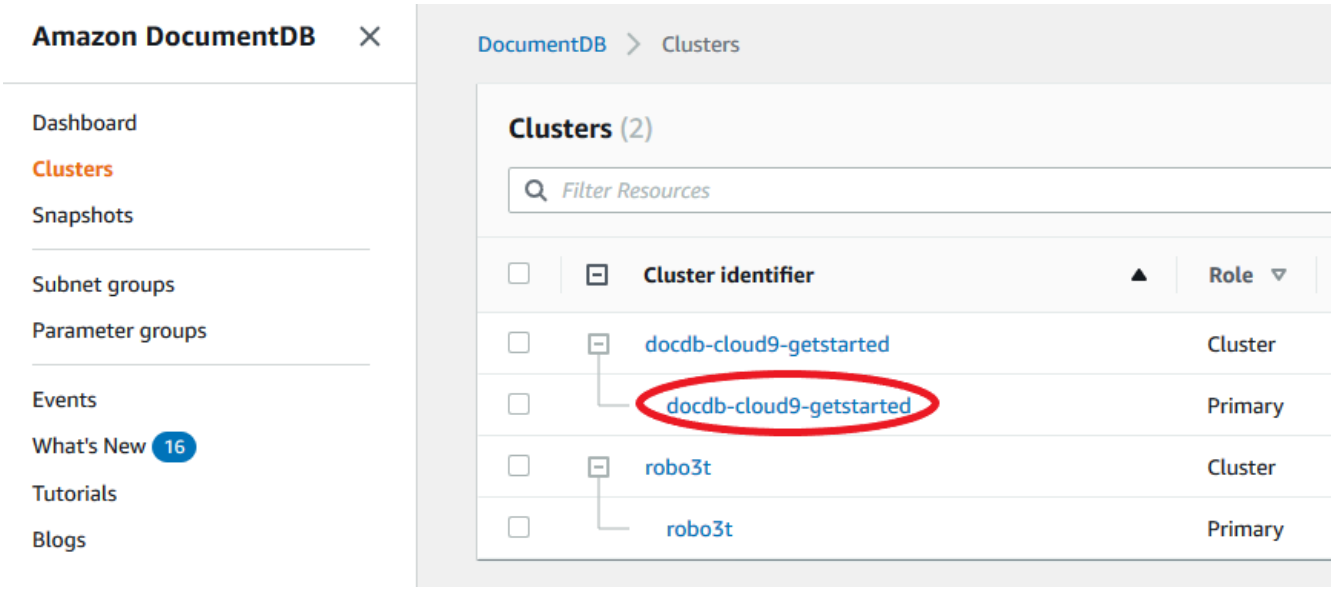
Using the AWS-Managementkonsole

Gehen Sie wie folgt vor, um CloudWatch Metriken mit der Amazon DocumentDB Management Console anzuzeigen.

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Klicken Sie im Navigationsbereich auf Cluster.

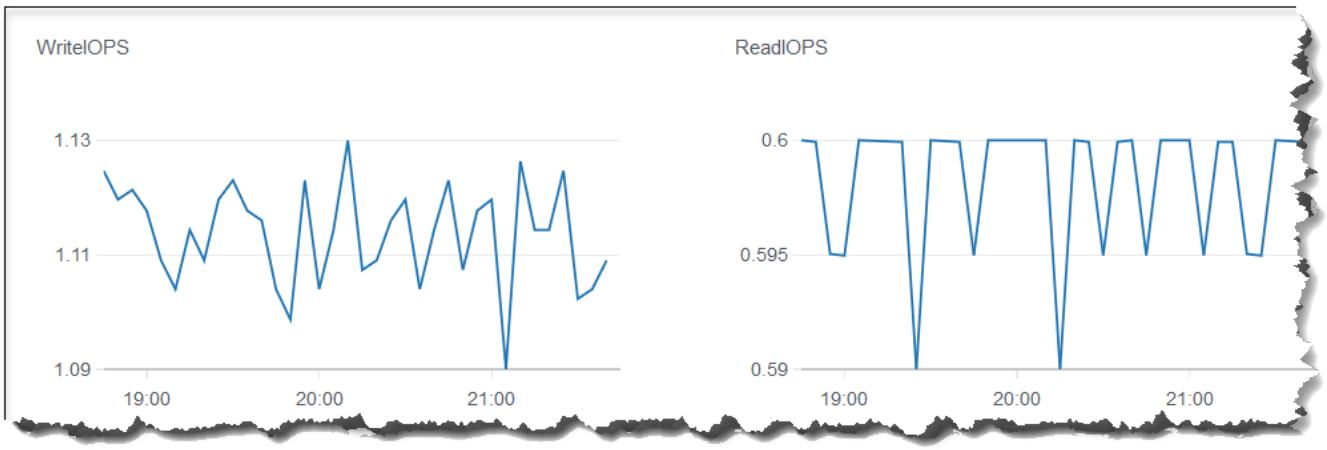
> **Tip**
>
> Wenn der Navigationsbereich auf der linken Seite des Bildschirms nicht angezeigt wird, wählen Sie links oben auf der Seite das Menüsymbol (≡) aus.

3. Im Cluster-Navigationsfeld sehen Sie die Spalte Cluster-ID. Ihre Instances werden unter Clustern aufgeführt, ähnlich wie im folgenden Screenshot.



4. Wählen Sie aus der Liste der Instances den Namen der Instance aus, für die Sie Metriken benötigen.
5. Wählen Sie auf der daraufhin angezeigten Instance-Übersichtsseite den Tab Monitoring, um grafische Darstellungen der Metriken Ihrer Amazon DocumentDB DocumentDB-Instance anzuzeigen. Da für jede Metrik ein Diagramm generiert werden muss, kann es einige Minuten dauern, bis die CloudWatchGrafiken gefüllt sind.

Die folgende Abbildung zeigt die grafische Darstellung von zwei CloudWatch Metriken in der Amazon DocumentDB DocumentDB-Konsole, `WriteIOPS` und`ReadIOPS`.



Using the CloudWatch Management Console

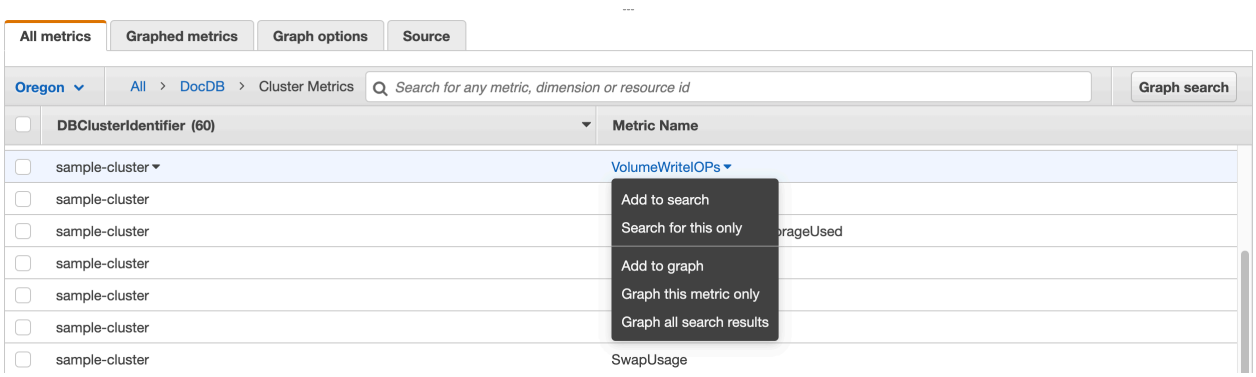
Gehen Sie wie folgt vor, um CloudWatch Metriken mit der CloudWatch Management Console anzuzeigen.

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unterhttps://console.aws.amazon.com/cloudwatch.
2. Wählen Sie im Navigationsbereich Metriken aus. Wählen Sie dann aus der Liste der Dienstnamen DocDB aus.
3. Wählen Sie eine Metrikdimension (z. B. Cluster-Metriken).
4. Auf der Registerkarte Alle Metriken werden alle Metriken für diese Dimension in DocDB angezeigt.

    a. Um die Tabelle sortieren, verwenden Sie die Spaltenüberschrift.

    b. Um eine Metrik grafisch darzustellen, müssen Sie das Kontrollkästchen neben der Metrik aktivieren. Um alle Metriken auszuwählen, aktivieren Sie das Kontrollkästchen in der Kopfzeile der Tabelle.

    c. Um nach Metrik zu filtern, bewegen Sie den Mauszeiger über den Metriknamen und wählen Sie den Dropdown-Pfeil neben dem Metriknamen aus. Wählen Sie dann Zur Suche hinzufügen aus, wie in der folgenden Abbildung gezeigt.



Using the AWS CLI

Verwenden Sie den CloudWatch `get-metric-statistics` Vorgang mit den folgenden Parametern, um CloudWatch Daten für Amazon DocumentDB anzuzeigen.

Parameters

- **`--namespace`** – Erforderlich. Der Service-Namespace, für den Sie CloudWatch -Metriken anzeigen möchten. Für Amazon DocumentDB muss dies der Fall sein. `AWS/DocDB`
- **`--metric-name`** – Erforderlich. Der Name der Metrik, für die Sie Daten benötigen.
- **`--start-time`** – Erforderlich. Der Zeitstempel, der den ersten zurückzugebenden Datenpunkt bestimmt.

  Der angegebene Wert wird eingeschlossen. Die Ergebnisse umfassen Datenpunkte mit dem angegebenen Zeitstempel. Der Zeitstempel muss im UTC-Format ISO 8601 sein (z. B. T23:00:00Z 2016-10-03).
- **`--end-time`** – Erforderlich. Der Zeitstempel, der den letzten zurückzugebenden Datenpunkt bestimmt.

  Der angegebene Wert wird eingeschlossen. Die Ergebnisse umfassen Datenpunkte mit dem angegebenen Zeitstempel. Der Zeitstempel muss im UTC-Format ISO 8601 sein (z. B. 2016-10-03). T23:00:00Z
- **`--period`** – Erforderlich. Die Granularität der zurückgegebenen Datenpunkte in Sekunden. Für Metriken mit regulärer Auflösung kann ein Zeitraum gerade mal eine Minute (60 Sekunden) betragen. Der Wert muss ein Vielfaches von 60 sein. Für hochauflösende Metriken, die in Abständen von weniger als einer Minute erfasst werden, kann der Zeitraum 1, 5, 10, 30, 60 oder ein Vielfaches von 60 betragen.

- **`--dimensions`**— Fakultativ. Wenn die Metrik mehrere Dimensionen enthält, müssen Sie für jede Dimension einen Wert angeben. CloudWatch behandelt jede eindeutige Kombination von Dimensionen als separate Metrik. Wenn eine bestimmte Kombination von Dimensionen nicht veröffentlicht wurde, können Sie keine Metriken dafür abrufen. Sie müssen die gleichen Dimensionen angeben, die bei der Erstellung der Metriken verwendet wurden.
- **`--statistics`**— Fakultativ. Die Metrik-Statistiken abgesehen von den Perzentil-Statistiken. Verwenden Sie für Perzentil-Statistiken `ExtendedStatistics`. Wenn Sie `GetMetricStatistics` aufrufen, müssen Sie `Statistics` oder `ExtendedStatistics` angeben, aber nicht beides.

  Gültige Werte:

  - `SampleCount`
  - `Average`
  - `Sum`
  - `Minimum`
  - `Maximum`
- **`--extended-statistics`**— Fakultativ. Die `percentile`-Statistiken. Geben Sie Werte zwischen p0.0 und p100 an. Wenn Sie `GetMetricStatistics` aufrufen, müssen Sie `Statistics` oder `ExtendedStatistics` angeben, aber nicht beides.
- **`--unit`**— Fakultativ. Die Einheit für eine bestimmte Metrik. Metriken können in mehreren Einheiten angegeben werden. Wenn Sie keine Einheit festlegen, werden alle Einheiten zurückgegeben. Wenn Sie nur eine Einheit angeben, die für die Metrik nicht unterstützt wird, erhalten Sie keine Ergebnisse für den Aufruf.

  Mögliche Werte:

  - `Seconds`
  - `Microseconds`
  - `Milliseconds`
  - `Bytes`
  - `Kilobytes`
  - `Megabytes`
  - `Gigabytes`
  - `Terabytes`

- Bits
- Kilobytes
- Megabits
- Gigabits
- Terabits
- Percent
- Count
- Bytes/Second
- Kilobytes/Second
- Megabytes/Second
- Gigabytes/Second
- Terabytes/Second
- Bits/Second
- Kilobits/Second
- Megabits/Second
- Gigabits/Second
- Terabits/Second
- Count/Second
- None

Example

Im folgenden Beispiel wird die maximale CPUUtilization für einen Zeitraum von 2 Stunden gezeigt, wobei alle 60 Sekunden eine Messung erfolgt.

Für Linux, macOS oder Unix:

```
aws cloudwatch get-metric-statistics \
       --namespace AWS/DocDB \
       --dimensions \
           Name=DBInstanceIdentifier,Value=docdb-2019-01-09-23-55-38 \
       --metric-name CPUUtilization \
       --start-time 2019-02-11T05:00:00Z \
       --end-time 2019-02-11T07:00:00Z \
       --period 60 \
```

```
       --statistics Maximum
```

Für Windows:

```
aws cloudwatch get-metric-statistics ^
       --namespace AWS/DocDB ^
       --dimensions ^
           Name=DBInstanceIdentifier,Value=docdb-2019-01-09-23-55-38 ^
       --metric-name CPUUtilization ^
       --start-time 2019-02-11T05:00:00Z ^
       --end-time 2019-02-11T07:00:00Z ^
       --period 60 ^
       --statistics Maximum
```

Die Ausgabe dieser Operation sieht in etwa wie folgt aus.

```
{
       "Label": "CPUUtilization",
       "Datapoints": [
           {
               "Unit": "Percent",
               "Maximum": 4.49152542374361,
               "Timestamp": "2019-02-11T05:51:00Z"
           },
           {
               "Unit": "Percent",
               "Maximum": 4.25000000000485,
               "Timestamp": "2019-02-11T06:44:00Z"
           },

           ********* some output omitted for brevity *********

           {
               "Unit": "Percent",
               "Maximum": 4.33333333331878,
               "Timestamp": "2019-02-11T06:07:00Z"
           }
       ]
   }
```

Abmessungen von Amazon DocumentDB

Die Metriken für Amazon DocumentDB werden anhand der Werte für das Konto oder den Vorgang qualifiziert. Sie können die CloudWatch Konsole verwenden, um Amazon DocumentDB DocumentDB-Daten abzurufen, die nach einer der Dimensionen in der folgenden Tabelle gefiltert wurden.

Dimension	Description
`DBClusterIdentifier`	Filtert die Daten, die Sie für einen bestimmten Amazon DocumentDB-Cluster anfordern.
`DBClusterIdentifier, Role`	Filtert die Daten, die Sie für einen bestimmte n Amazon DocumentDB-Cluster anfordern, und aggregiert die Metrik nach Instance-Rolle ()WRITER/READER. Sie können beispiels weise Metriken für alle READER-Instances eines Clusters zusammenfassen.
`DBInstanceIdentifier`	Filtert die angeforderten Daten für eine spezifische Datenbank-Instance.

Überwachung von Opcounter-Metriken

Opcounter-Metriken haben einen Wert ungleich Null (normalerweise ~50) für inaktive Cluster. Dies liegt daran, dass Amazon DocumentDB regelmäßige Zustandsprüfungen, interne Abläufe und Aufgaben zur Erfassung von Kennzahlen durchführt.

Überwachen von Datenbankverbindungen

Wenn Sie die Anzahl der Verbindungen mithilfe von Datenbank-Engine-Befehlen wie anzeigen`db.runCommand( { serverStatus: 1 })`, werden Ihnen möglicherweise bis zu 10 Verbindungen mehr angezeigt, als Sie `DatabaseConnections` CloudWatch durchschauen. Dies liegt daran, dass Amazon DocumentDB regelmäßige Zustandsprüfungen und Aufgaben zur Erfassung von Kennzahlen durchführt, die nicht berücksichtigt werden. `DatabaseConnections` `DatabaseConnections`steht nur für vom Kunden initiierte Verbindungen.

Protokollieren Amazon DocumentDB DocumentDB-API-Aufrufen mit AWS CloudTrail

Amazon DocumentDB (mit MongoDB-Kompatibilität) ist in einen Service integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen von Benutzern, Rollen oder einem AWS Service in Amazon DocumentDB (mit MongoDB-Kompatibilität) bereitstellt. CloudTrail erfasst alle AWS CLI API-Aufrufe für Amazon DocumentDB als Ereignisse, einschließlich Aufrufe von der Amazon DocumentDB-Konsole und von Codeaufrufen an das Amazon DocumentDB-SDK. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Übermittlung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für Amazon DocumentDB. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem auf der CloudTrail Konsole im Event-Verlauf einsehen. Anhand der von CloudTrail gesammelten Informationen können Sie die Anfrage an Amazon DocumentDB (mit MongoDB-Kompatibilität), die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde und andere Details ermitteln.

> **Important**
>
> Für bestimmte Verwaltungsfunktionen verwendet Amazon DocumentDB eine Betriebstechnologie, die mit Amazon Relational Database Service (Amazon RDS) gemeinsam genutzt wird. Amazon DocumentDB DocumentDB-Konsolen- und API-Aufrufe werden als Aufrufe der Amazon RDS-API protokolliert. AWS CLI

Weitere Informationen AWS CloudTrail finden Sie im AWS CloudTrail Benutzerhandbuch.

Amazon DocumentDB DocumentDB-Informationen in CloudTrail

CloudTrail ist auf Ihrem aktiviert AWS-Konto , wenn Sie das Konto erstellen. Wenn Aktivitäten in Amazon DocumentDB (mit MongoDB-Kompatibilität) auftreten, wird diese Aktivität zusammen mit anderen AWS Serviceereignissen in der CloudTrail Ereignishistorie in einem Ereignis aufgezeichnet. Sie können aktuelle Ereignisse in Ihrem anzeigen, suchen und herunterladen. AWS-Konto Weitere Informationen finden Sie unter Ereignisse mit CloudTrail Ereignisverlauf anzeigen.

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS-Konto, einschließlich Ereignissen für Amazon DocumentDB (mit MongoDB-Kompatibilität), 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 in der AWS -Partition und stellt die Protokolldateien in dem von Ihnen angegebenen Amazon-S3-Bucket bereit. 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 in folgenden Themen im AWS CloudTrail -Benutzerhandbuch:

- Übersicht zum Erstellen eines Trails
- CloudTrail Unterstützte Dienste und Integrationen
- Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen
- Empfangen von CloudTrail Protokolldateien von mehreren Konten

Jedes Event oder jeder Protokolleintrag enthält Informationen über den Ersteller der Anfrage. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anforderung mit Root- oder -Benutzeranmeldeinformationen 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 Dienst gestellt wurde.

Weitere Informationen finden Sie unter CloudTrail userIdentity-Element.

Profilierung von Amazon DocumentDB DocumentDB-Vorgängen

Sie können den Profiler in Amazon DocumentDB (mit MongoDB-Kompatibilität) verwenden, um die Ausführungszeit und Details der Operationen zu protokollieren, die auf Ihrem Cluster ausgeführt wurden. Profiler ist für die Überwachung der langsamsten Operationen in Ihrem Cluster nützlich. So können Sie die Leistung einzelner Abfragen und die allgemeine Cluster-Leistung verbessern.

Standardmäßig ist die Profiler-Funktion deaktiviert. Wenn diese Option aktiviert ist, protokolliert der Profiler Vorgänge, die länger dauern als ein vom Kunden definierter Schwellenwert (z. B. 100 ms), in Amazon CloudWatch Logs. Zu den protokollierten Details gehören der Befehl, für den das Profil erstellt wird, die Uhrzeit, die Planübersicht und die Client-Metadaten. Nachdem die Vorgänge in CloudWatch Logs protokolliert wurden, können Sie Logs Insights verwenden, um Ihre Amazon DocumentDB CloudWatch DocumentDB-Profilerstellungsdaten zu analysieren, zu überwachen und zu archivieren. Häufige Abfragen sind in Abschnitt Häufig gestellte Fragen zu finden.

Wenn aktiviert, verbraucht der Profiler zusätzliche Ressourcen im Cluster. Sie sollten mit einem hohen Schwellenwert (z. B. 500 ms) beginnen und den Wert allmählich senken, um langsame Operationen zu identifizieren. Ein anfänglicher Schwellenwert von 50 ms kann für Anwendungen mit hohem Durchsatz zu Leistungsproblemen im Cluster führen. Der Profiler ist auf Cluster-Ebene aktiviert und funktioniert auf allen Instances und Datenbanken in einem Cluster. Amazon DocumentDB protokolliert Operationen nach bestem Wissen und Gewissen in Amazon CloudWatch Logs.

Amazon DocumentDB erhebt zwar keine zusätzlichen Gebühren für die Aktivierung des Profilers, Ihnen werden jedoch die Standardtarife für die Nutzung von Logs berechnet. CloudWatch Informationen zu den Preisen für CloudWatch Logs finden Sie unter CloudWatch Amazon-Preise.

Themen

- Unterstützte Vorgänge
- Einschränkungen
- Den Amazon DocumentDB DocumentDB-Profiler aktivieren
- Den Amazon DocumentDB DocumentDB-Profiler deaktivieren
- Export von Profiler-Protokollen deaktivieren
- Zugreifen auf Ihre Amazon DocumentDB DocumentDB-Profiler-Protokolle
- Häufig gestellte Fragen

Unterstützte Vorgänge

Amazon DocumentDB Profiler unterstützt die folgenden Operationen:

- `aggregate`
- `count`
- `delete`
- `distinct`
- `find` (OP_QUERY und Befehl)
- `findAndModify`
- `insert`
- `update`

Einschränkungen

Der Profiler für langsame Abfragen kann Profiler-Protokolle nur ausgeben, wenn die gesamte Ergebnismenge der Abfrage in einen Stapel passt und wenn die Ergebnismenge weniger als 16 MB (maximale BSON-Größe) beträgt. Ergebnissätze, die größer als 16 MB sind, werden automatisch in mehrere Batches aufgeteilt.

Die meisten Treiber oder Shells legen möglicherweise eine kleine Standardstapelgröße fest. Sie können die Batchgröße als Teil Ihrer Abfrage angeben. Für die Erfassung langsamer Abfrageprotokolle empfehlen wir eine Batchgröße, die die Größe Ihrer erwarteten Ergebnismenge übersteigt. Wenn Sie sich bezüglich der Größe der Ergebnismenge nicht sicher sind oder wenn sie variiert, können Sie die Batchgröße auch auf eine große Zahl festlegen (z. B. 100.000).

Die Verwendung einer größeren Batchgröße bedeutet jedoch, dass mehr Ergebnisse aus der Datenbank abgerufen werden müssen, bevor eine Antwort an den Client gesendet wird. Bei einigen Abfragen kann dies zu längeren Verzögerungen führen, bis Sie Ergebnisse erhalten. Wenn Sie nicht vorhaben, die gesamte Ergebnismenge zu verwenden, ist es möglich, dass Sie mehr I/Os für die Verarbeitung der Abfrage ausgeben und das Ergebnis dann verwerfen.

Den Amazon DocumentDB DocumentDB-Profiler aktivieren

Die Aktivierung des Profilers auf einem Cluster erfolgt in drei Schritten. Stellen Sie sicher, dass alle Schritte abgeschlossen sind, da andernfalls keine Profilerstellungsprotokolle an Logs gesendet CloudWatch werden. Profiler wird auf Cluster-Ebene festgelegt und auf allen Datenbanken und Instances des Clusters ausgeführt.

So aktivieren Sie den Profiler in einem Cluster

1. Da Sie eine Standard-Cluster-Parametergruppe nicht ändern können, stellen Sie sicher, dass Sie über eine verfügbare benutzerdefinierte Cluster-Parametergruppe verfügen. Weitere Informationen finden Sie unter Amazon DocumentDB-Cluster-Parametergruppen erstellen.
2. Ändern Sie mithilfe einer verfügbaren benutzerdefinierten Cluster-Parametergruppe die folgenden Parameter: `profiler`, `profiler_threshold_ms` und `profiler_sampling_rate`. Weitere Informationen finden Sie unter Amazon DocumentDB-Cluster-Parametergruppen ändern.
3. Erstellen oder ändern Sie Ihren Cluster, um die benutzerdefinierte Cluster-Parametergruppe zu verwenden und den Export von `profiler` Protokollen in Logs zu CloudWatch ermöglichen.

In den folgenden Abschnitten wird gezeigt, wie Sie diese Schritte mithilfe von AWS-Managementkonsole und AWS Command Line Interface (AWS CLI) implementieren.

Using the AWS-Managementkonsole

1. Bevor Sie beginnen, erstellen Sie einen Amazon DocumentDB-Cluster und eine benutzerdefinierte Cluster-Parametergruppe, falls Sie noch keinen haben. Weitere Informationen erhalten Sie unter Amazon DocumentDB-Cluster-Parametergruppen erstellen und Einen Amazon DocumentDB-Cluster erstellen.
2. Ändern Sie die folgenden Parameter mithilfe einer verfügbaren benutzerdefinierten Cluster-Parametergruppe. Weitere Informationen finden Sie unter Amazon DocumentDB-Cluster-Parametergruppen ändern.

   - `profiler`— Aktiviert oder deaktiviert die Erstellung von Abfrageprofilen. Zugelassene Werte sind `enabled` und `disabled`. Der Standardwert ist `disabled`. Um Profiling zu aktivieren, legen Sie den Wert auf `enabled` fest.
   - `profiler_threshold_ms`— Wenn auf gesetzt `profiler` ist`enabled`, werden alle Befehle protokolliert, die länger dauern als `profiler_threshold_ms` angegeben. CloudWatch Zugelassene Werte sind `[50-INT_MAX]`. Der Standardwert ist `100`.
   - `profiler_sampling_rate`— Der Anteil der langsamen Operationen, für die ein Profil erstellt oder protokolliert werden sollte. Zugelassene Werte sind `[0.0-1.0]`. Der Standardwert ist `1.0`.
3. Ändern Sie Ihren Cluster so, dass er die benutzerdefinierte Cluster-Parametergruppe verwendet, und legen Sie fest, dass die Profiler-Protokollexporte auf Amazon CloudWatch veröffentlicht werden sollen.

   a. Wählen Sie im Navigationsbereich die Option Clusters (Cluster), um die benutzerdefinierte Parametergruppe zu einem Cluster hinzuzufügen.

   b. Wählen Sie die Schaltfläche links neben dem Namen des Clusters, dem Sie die Parametergruppe zuordnen möchten. Wählen Sie Actions (Aktionen) und dann Modify (Ändern) aus, um den Cluster zu ändern.

   c. Wählen Sie unter Cluster options (Cluster-Optionen) die benutzerdefinierte Parametergruppe aus dem obigen Schritt aus, um sie Ihrem Cluster hinzuzufügen.

   d. Wählen Sie unter Protokollexporte die Option Profiler-Protokolle aus, die auf Amazon CloudWatch veröffentlicht werden sollen.

   e. Wählen Sie Continue (Weiter) aus, um eine Übersicht Ihrer Änderungen anzuzeigen.

f. Nachdem Sie Ihre Änderungen überprüft haben, können Sie diese sofort oder während des nächsten Wartungsfensters unter Scheduling of modifications (Planen von Änderungen) anwenden.

g. Wählen Sie Modify cluster (Cluster ändern) aus, um den Cluster mit der neuen Parametergruppe zu aktualisieren.

Using the AWS CLI

Mit dem folgenden Verfahren wird der Profiler für alle unterstützten Operationen für den Cluster `sample-cluster` aktiviert.

1. Bevor Sie beginnen, stellen Sie sicher, dass Sie über eine benutzerdefinierte Clusterparametergruppe verfügen, indem Sie den folgenden Befehl ausführen und die Ausgabe für eine Clusterparametergruppe überprüfen, die nicht `default` im Namen und die Parametergruppenfamilie `docdb3.6` hat. Wenn Sie über keine nicht standardmäßige Clusterparametergruppe verfügen, siehe Amazon DocumentDB-Cluster-Parametergruppen erstellen.

```
aws docdb describe-db-cluster-parameter-groups \
    --query 'DBClusterParameterGroups[*].
[DBClusterParameterGroupName,DBParameterGroupFamily]'
```

In der folgenden Ausgabe erfüllt nur `sample-parameter-group` beide Kriterien.

```
[
       [
           "default.docdb3.6",
           "docdb3.6"
       ],
       [
           "sample-parameter-group",
           "docdb3.6"
       ]
]
```

2. Ändern Sie mithilfe Ihrer benutzerdefinierten Cluster-Parametergruppe die folgenden Parameter:

- `profiler`— Aktiviert oder deaktiviert die Erstellung von Abfrageprofilen. Zugelassene Werte sind `enabled` und `disabled`. Der Standardwert ist `disabled`. Um Profiling zu aktivieren, legen Sie den Wert auf `enabled` fest.
- `profiler_threshold_ms`— Wenn auf gesetzt `profiler` istenabled, dauern alle Befehle länger als protokolliert `profiler_threshold_ms` wurden. CloudWatch Zugelassene Werte sind `[50-INT_MAX]`. Der Standardwert ist `100`.
- `profiler_sampling_rate`— Der Anteil langsamer Operationen, für den ein Profil erstellt oder protokolliert werden sollte. Zugelassene Werte sind `[0.0-1.0]`. Der Standardwert ist `1.0`.

```
aws docdb modify-db-cluster-parameter-group \
    --db-cluster-parameter-group-name sample-parameter-group \
    --parameters
 ParameterName=profiler,ParameterValue=enabled,ApplyMethod=immediate \

 ParameterName=profiler_threshold_ms,ParameterValue=100,ApplyMethod=immediate \

 ParameterName=profiler_sampling_rate,ParameterValue=0.5,ApplyMethod=immediate
```

3. Ändern Sie Ihren Amazon DocumentDB-Cluster so, dass er die `sample-parameter-group` benutzerdefinierte Cluster-Parametergruppe aus dem vorherigen Schritt verwendet und den Parameter `--enable-cloudwatch-logs-exports` auf `profiler` setzt.

   Der folgende Code ändert den Cluster so`sample-cluster`, dass er den `sample-parameter-group` aus dem vorherigen Schritt verwendet, und erweitert `profiler` die aktivierten CloudWatch Logs-Exporte.

```
aws docdb modify-db-cluster \
       --db-cluster-identifier sample-cluster \
       --db-cluster-parameter-group-name sample-parameter-group \
       --cloudwatch-logs-export-configuration '{"EnableLogTypes":["profiler"]}'
```

   Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus.

```
{
    "DBCluster": {
        "AvailabilityZones": [
```

```
            "us-east-1c",
            "us-east-1b",
            "us-east-1a"
        ],
        "BackupRetentionPeriod": 1,
        "DBClusterIdentifier": "sample-cluster",
        "DBClusterParameterGroup": "sample-parameter-group",
        "DBSubnetGroup": "default",
        "Status": "available",
        "EarliestRestorableTime": "2020-04-07T02:05:12.479Z",
        "Endpoint": "sample-cluster.node.us-east-1.docdb.amazonaws.com",
        "ReaderEndpoint": "sample-cluster.node.us-east-1.docdb.amazonaws.com",
        "MultiAZ": false,
        "Engine": "docdb",
        "EngineVersion": "3.6.0",
        "LatestRestorableTime": "2020-04-08T22:08:59.317Z",
        "Port": 27017,
        "MasterUsername": "test",
        "PreferredBackupWindow": "02:00-02:30",
        "PreferredMaintenanceWindow": "tue:09:50-tue:10:20",
        "DBClusterMembers": [
            {
                "DBInstanceIdentifier": "sample-instance-1",
                "IsClusterWriter": true,
                "DBClusterParameterGroupStatus": "in-sync",
                "PromotionTier": 1
            },
            {
                "DBInstanceIdentifier": "sample-instance-2",
                "IsClusterWriter": true,
                "DBClusterParameterGroupStatus": "in-sync",
                "PromotionTier": 1
            }
        ],
        "VpcSecurityGroups": [
            {
                "VpcSecurityGroupId": "sg-abcd0123",
                "Status": "active"
            }
        ],
        "HostedZoneId": "ABCDEFGHIJKLM",
        "StorageEncrypted": true,
        "KmsKeyId": "arn:aws:kms:us-east-1:<accountID>:key/sample-key",
        "DbClusterResourceId": "cluster-ABCDEFGHIJKLMNOPQRSTUVWXYZ",
```

```
        "DBClusterArn": "arn:aws:rds:us-east-1:<accountID>:cluster:sample-
cluster",
        "AssociatedRoles": [],
        "ClusterCreateTime": "2020-01-10T22:13:38.261Z",
        "EnabledCloudwatchLogsExports": [
            "profiler"
        ],
        "DeletionProtection": true
    }
}
```

Den Amazon DocumentDB DocumentDB-Profiler deaktivieren

Um den Profiler zu deaktivieren, deaktivieren Sie sowohl den `profiler` Parameter als auch den Export von `profiler` Protokollen in Logs. CloudWatch

Deaktivieren des Profilers

Sie können den `profiler` Parameter entweder mit AWS-Managementkonsole oder AWS CLI wie folgt deaktivieren.

Using the AWS-Managementkonsole

Das folgende Verfahren verwendet die AWS-Managementkonsole , um Amazon DocumentDB `profiler` zu deaktivieren.

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Wählen Sie im Navigationsbereich Parameter groups (Parametergruppen) aus. Wählen Sie dann den Namen der Cluster-Parametergruppe aus, für die Sie den Profiler deaktivieren möchten.
3. Klicken Sie auf der Seite Cluster parameters (Clusterparameter) auf die Schaltfläche links neben dem `profiler`-Parameter und wählen Sie Edit (Bearbeiten).
4. Wählen Sie im Dialogfeld Modify profiler (Profiler ändern) `disabled` in der Liste aus.
5. Wählen Sie Modify Cluster Parameter (Cluster-Parameter ändern).

Using the AWS CLI

Um `profiler` auf einem Cluster mithilfe der AWS CLI zu deaktivieren, ändern Sie den Cluster wie folgt.

```
aws docdb modify-db-cluster-parameter-group \
    --db-cluster-parameter-group-name sample-parameter-group \
    --parameters
 ParameterName=profiler,ParameterValue=disabled,ApplyMethod=immediate
```

Export von Profiler-Protokollen deaktivieren

Sie können den Export von `profiler` Protokollen in Logs deaktivieren, CloudWatch indem Sie entweder das AWS-Managementkonsole oder verwenden AWS CLI, und zwar wie folgt.

Using the AWS-Managementkonsole

Das folgende Verfahren verwendet die AWS-Managementkonsole , um den Export von Protokollen durch Amazon DocumentDB zu CloudWatch deaktivieren.

1. Öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Klicken Sie im Navigationsbereich auf Cluster. Wählen Sie die Schaltfläche links neben dem Namen des Clusters, für den Sie den Export von Protokollen deaktivieren möchten.
3. Wählen Sie aus dem Menü Actions (Aktionen) die Option Modify (Ändern) aus.
4. Scrollen Sie nach unten zum Abschnitt Log exports (Protokollexporte) und deaktivieren Sie Profiler logs (Profiler-Protokolle).
5. Klicken Sie auf Weiter.
6. Überprüfen Sie Ihre Änderungen und wählen Sie dann aus, wann diese Änderung auf Ihren Cluster angewendet werden soll.
   - Apply during the next scheduled maintenance window (Anwendung während des nächsten geplanten Wartungsfensters)
   - Apply immediately (Sofort anwenden)
7. Wählen Sie Cluster bearbeiten aus.

Using the AWS CLI

Der folgende Code ändert den Cluster `sample-cluster` und deaktiviert CloudWatch Profiler-Logs.

Example

Für Linux, macOS oder Unix:

```
aws docdb modify-db-cluster \
   --db-cluster-identifier sample-cluster \
   --cloudwatch-logs-export-configuration '{"DisableLogTypes":["profiler"]}'
```

Für Windows:

```
aws docdb modify-db-cluster ^
   --db-cluster-identifier sample-cluster ^
   --cloudwatch-logs-export-configuration '{"DisableLogTypes":["profiler"]}'
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus.

```
{
    "DBCluster": {
        "AvailabilityZones": [
            "us-east-1c",
            "us-east-1b",
            "us-east-1a"
        ],
        "BackupRetentionPeriod": 1,
        "DBClusterIdentifier": "sample-cluster",
        "DBClusterParameterGroup": "sample-parameter-group",
        "DBSubnetGroup": "default",
        "Status": "available",
        "EarliestRestorableTime": "2020-04-08T02:05:17.266Z",
        "Endpoint": "sample-cluster.node.us-east-1.docdb.amazonaws.com",
        "ReaderEndpoint": "sample-cluster.node.us-east-1.docdb.amazonaws.com",
        "MultiAZ": false,
        "Engine": "docdb",
        "EngineVersion": "3.6.0",
        "LatestRestorableTime": "2020-04-09T05:14:44.356Z",
        "Port": 27017,
        "MasterUsername": "test",
        "PreferredBackupWindow": "02:00-02:30",
```

```
        "PreferredMaintenanceWindow": "tue:09:50-tue:10:20",
        "DBClusterMembers": [
            {
                "DBInstanceIdentifier": "sample-instance-1",
                "IsClusterWriter": true,
                "DBClusterParameterGroupStatus": "in-sync",
                "PromotionTier": 1
            },
            {
                "DBInstanceIdentifier": "sample-instance-2",
                "IsClusterWriter": true,
                "DBClusterParameterGroupStatus": "in-sync",
                "PromotionTier": 1
            }
        ],
        "VpcSecurityGroups": [
            {
                "VpcSecurityGroupId": "sg-abcd0123",
                "Status": "active"
            }
        ],
        "HostedZoneId": "ABCDEFGHIJKLM",
        "StorageEncrypted": true,
        "KmsKeyId": "arn:aws:kms:us-east-1:<accountID>:key/sample-key",
        "DbClusterResourceId": "cluster-ABCDEFGHIJKLMNOPQRSTUVWXYZ",
        "DBClusterArn": "arn:aws:rds:us-east-1:<accountID>:cluster:sample-cluster",
        "AssociatedRoles": [],
        "ClusterCreateTime": "2020-01-10T22:13:38.261Z",
        "DeletionProtection": true
    }
}
```

Zugreifen auf Ihre Amazon DocumentDB DocumentDB-Profiler-Protokolle

Gehen Sie wie folgt vor, um auf Ihre Profilprotokolle bei Amazon zuzugreifen CloudWatch.

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Stellen Sie sicher, dass Sie sich in derselben Region wie Ihr Amazon DocumentDB-Cluster befinden.
3. Wählen Sie im Navigationsbereich Protokolle aus.

4. Um die Profiler-Protokolle für Ihren Cluster zu finden, wählen Sie in der Liste `/aws/docdb/yourClusterName/profiler` aus.

   Die Profilprotokolle für jede Ihrer Instances sind unter den jeweiligen Instance-Namen verfügbar.

Häufig gestellte Fragen

Im Folgenden finden Sie einige häufige Abfragen, die Sie verwenden können, um Ihre Befehle, für die Profile erstellt wurden, zu analysieren. Weitere Informationen zu CloudWatch Logs Insights finden Sie unter Analysieren von Protokolldaten mit CloudWatch Logs Insights und Beispielabfragen.

Ruft die 10 langsamsten Vorgänge für eine angegebene Sammlung ab

```
filter ns="test.foo" | sort millis desc | limit 10
```

Ruft alle Aktualisierungsvorgänge für eine Sammlung ab, die mehr als 60 ms gedauert haben

```
filter millis > 60 and op = "update"
```

Holen Sie sich die 10 langsamsten Operationen des letzten Monats

```
sort millis desc | limit 10
```

Abrufen aller Abfragen mit einer COLLSCAN-Planübersicht

```
filter planSummary="COLLSCAN"
```

Überwachung mit Performance Insights

Performance Insights erweitert die bestehenden Amazon DocumentDB DocumentDB-Überwachungsfunktionen, um die Leistung Ihres Clusters zu veranschaulichen und Sie bei der Analyse aller Probleme zu unterstützen, die sich darauf auswirken. Mit dem Performance Insights Insights-Dashboard können Sie die Datenbanklast visualisieren und die Last nach Wartezeiten, Abfrageanweisungen, Hosts oder Anwendungen filtern.

> **Note**
>
> Performance Insights ist nur für Amazon DocumentDB 3.6, 4.0, 5.0 und 8.0 instanzbasierte Cluster verfügbar.

Wie ist es nützlich?

- Datenbankleistung visualisieren — Visualisieren Sie die Last, um festzustellen, wann und wo sich die Last in der Datenbank befindet
- Ermitteln Sie, was die Belastung der Datenbank verursacht — Ermitteln Sie, welche Abfragen, Hosts und Anwendungen zur Belastung Ihrer Instance beitragen
- Ermitteln Sie, wann Ihre Datenbank ausgelastet ist — Vergrößern Sie das Performance Insights Insights-Dashboard, um sich auf bestimmte Ereignisse zu konzentrieren, oder zoomen Sie heraus, um Trends über einen längeren Zeitraum zu betrachten
- Warnung beim Laden der Datenbank — Automatischer Zugriff auf neue Datenbank-Lademetriken, von CloudWatch wo aus Sie die DB-Lademetriken zusammen mit anderen Amazon DocumentDB-Metriken überwachen und Warnmeldungen zu diesen einrichten können

Was sind die Einschränkungen von Amazon DocumentDB Performance Insights?

- Performance Insights in den Regionen AWS GovCloud (US-East) und AWS GovCloud (US-West) sind nicht verfügbar
- Performance Insights for Amazon DocumentDB speichert Leistungsdaten für bis zu 7 Tage
- Abfragen, die länger als 1.024 Byte sind, werden in Performance Insights nicht aggregiert

Themen

- Konzepte von Performance Insights
- Aktivieren und Deaktivieren von Performance Insights
- Konfigurieren von Zugriffsrichtlinien für Performance Insights
- Analyse der Metriken mit dem Performance Insights-Dashboard
- Abrufen von Metriken mit der Performance-Insights-API
- CloudWatch Amazon-Metriken für Performance Insights
- Performance Insights für Zählermetriken

Konzepte von Performance Insights

Themen

- Durchschnittliche aktive Sitzungen
- Dimensionen
- Maximale vCPU

Durchschnittliche aktive Sitzungen

Datenbanklast (DB-Last) misst den Aktivitätsgrad in Ihrer Datenbank. Die wichtigste Metrik für Performance Insights ist `DB Load`, die jede Sekunde erfasst wird. Die Einheit für die `DBLoad` Metrik ist der Average Active Sessions (AAS) für eine Amazon DocumentDB DocumentDB-Instance.

Eine aktive Sitzung ist eine Verbindung, die Arbeit an die Amazon DocumentDB DocumentDB-Instance übermittelt hat und auf eine Antwort wartet. Wenn Sie beispielsweise eine Anfrage an eine Amazon DocumentDB DocumentDB-Instance senden, ist die Datenbanksitzung aktiv, während die Instance die Abfrage verarbeitet.

Um die Anzahl der durchschnittlich aktiven Sitzungen AAS zu erhalten, ruft Performance Insights die Anzahl der Sitzungen ab, die gleichzeitig eine Abfrage ausführen. Die AAS ist die Gesamtzahl der Sitzungen geteilt durch die Gesamtzahl der Beispiele. Die folgende Tabelle zeigt fünf aufeinanderfolgende Beispiele einer laufenden Abfrage.

Beispiel	Anzahl der Sitzungen, die eine Abfrage ausführen	AAS	Berechnung
1	2	2	2 Sitzungen/1 Beispiel
2	0	1	2 Sitzungen /2 Beispiele
3	4	2	6 Sitzungen /3 Beispiele
4	0	1.5	6 Sitzungen /4 Beispiele

Beispiel	Anzahl der Sitzungen, die eine Abfrage ausführen	AAS	Berechnung
5	4	2	10 Sitzungen /5 Beispiele

Im vorherigen Beispiel beträgt der DB-Load für das Zeitintervall von 1-5 2 AAS. Eine Erhöhung der DB-Last bedeutet, dass im Durchschnitt mehr Sitzungen für die Datenbank ausgeführt werden.

Dimensionen

Die`DB Load` Metrik unterscheidet sich von den anderen Zeitreihenmetriken, da Sie sie in Unterkomponenten aufteilen können, die als Dimensionen bezeichnet werden. Sie können sich Dimensionen als Kategorien für die verschiedenen Merkmale der `DB Load`-Metrik vorstellen. Bei der Diagnose von Leistungsproblemen sind die Dimensionen Wait States und Top Query am nützlichsten.

Wartezustände

Ein Wartestatus bewirkt, dass eine Abfrageanweisung auf das Eintreten eines bestimmten Ereignisses wartet, bevor sie weiter ausgeführt werden kann. Beispielsweise kann eine Abfrageanweisung warten, bis eine gesperrte Ressource entsperrt ist. Durch die Kombination `DB Load` mit Wartezuständen können Sie sich ein vollständiges Bild vom Sitzungsstatus machen. Hier sind verschiedene Wartezustände von Amazon DocumentDB:

Amazon DocumentDB DocumentDB-Wartestatus	Beschreibung des Wartestatus
Riegeln	Der Latch-Wartestatus tritt auf, wenn die Sitzung darauf wartet, den Pufferpool auszulagern. Häufiges Ein- und Auslagern in den Pufferpool kann häufiger vorkommen, wenn das System häufig umfangreiche Abfragen verarbeitet, Sammlungsscans durchführt oder wenn der Pufferpool zu klein ist, um den Arbeitssatz zu verarbeiten.

Amazon DocumentDB DocumentDB-Wartestatus	Beschreibung des Wartestatus
CPU	Der CPU-Wartestatus tritt auf, wenn die Sitzung auf die CPU wartet.
CollectionLock	Der CollectionLock Wartestatus tritt ein, wenn die Sitzung darauf wartet, eine Sperre für die Sammlung zu erlangen. Diese Ereignisse treten auf, wenn DDL-Operationen für die Sammlung ausgeführt werden.
DocumentLock	Der DocumentLock Wartestatus tritt ein, wenn die Sitzung darauf wartet, ein Dokument zu sperren. Eine hohe Anzahl gleichzeitiger Schreibvorgänge auf dasselbe Dokument führt zu mehr DocumentLock Wartezuständen in diesem Dokument.
SystemLock	Der SystemLock Wartestatus tritt auf, wenn die Sitzung auf dem System wartet. Dies kann der Fall sein, wenn häufig Abfragen mit langer Laufzeit, lang andauernde Transaktionen oder eine hohe Parallelität im System auftreten.
IO	Der IO-Wartestatus tritt auf, wenn die Sitzung auf den Abschluss der IO wartet.
BufferLock	Der BufferLock Wartestatus tritt ein, wenn die Sitzung darauf wartet, eine Sperre für eine gemeinsam genutzte Seite im Puffer zu erlangen. BufferLockWartezustände können verlängert werden, wenn andere Prozesse die Cursor auf den angeforderten Seiten offen halten.

Amazon DocumentDB DocumentDB-Wartestatus	Beschreibung des Wartestatus
LowMemThrottle	Der LowMemThrottle Wartestatus tritt auf, wenn die Sitzung aufgrund einer hohen Speicherauslastung auf der Amazon DocumentDB DocumentDB-Instance wartet. Wenn dieser Status für eine lange Zeit andauert, sollten Sie erwägen, die Instance zu skalieren, um zusätzlichen Speicher bereitzustellen. Weitere Informationen finden Sie unter Resource Governor.
BackgroundActivity	Der BackgroundActivity Wartestatus tritt auf, wenn die Sitzung auf interne Systemprozesse wartet.
Sonstige	Der Wartestatus Andere ist ein interner Wartestatus. Wenn dieser Status über einen längeren Zeitraum andauert, sollten Sie erwägen, diese Abfrage zu beenden. Weitere Informationen finden Sie unter Wie finde und beende ich Abfragen mit langer Laufzeit oder blockierter Ausführung?

Die häufigsten Abfragen

Während bei Wartezuständen Engpässe auftreten, zeigen Abfragen am häufigsten, welche Abfragen am meisten zur Datenbanklast beitragen. Beispielsweise könnten derzeit viele Abfragen gleichzeitig in der Datenbank ausgeführt werden, aber eine einzelne Abfrage könnte 99 % der DB-Last verbrauchen. In diesem Fall könnte die hohe Belastung auf ein Problem mit der Abfrage hinweisen.

Maximale vCPU

Das Diagramm Datenbanklast im Dashboard dient zum Erfassen, Aggregieren und Anzeigen von Sitzungsinformationen. Um zu sehen, ob aktive Sitzungen die maximale CPU überschreiten, sehen Sie sich ihre Beziehung zur Max vCPU-Linie an. Der Max vCPU-Wert wird durch die Anzahl der vCPU-Kerne (virtuelle CPU) für Ihre Amazon DocumentDB DocumentDB-Instance bestimmt.

Wenn die DB-Last häufig über der Max vCPU-Linie liegt und der primäre Wartezustand „CPU“ lautet, ist die CPU überlastet. In diesem Fall möchten Sie möglicherweise die Verbindungen zur Instance drosseln, alle Abfragen mit hoher CPU-Last optimieren oder eine größere Instance-Klasse in Betracht ziehen. Hohe und konsistente Instances von Wartezuständen deuten darauf hin, dass es möglicherweise Engpässe oder Probleme mit Ressourcenkonflikten gibt, die behoben werden müssen. Dies kann auch dann zutreffen, wenn die DB-Last die mit Max vCPU definierte Linie nicht überschreitet.

Aktivieren und Deaktivieren von Performance Insights

Um Performance Insights zu nutzen, aktivieren Sie es auf Ihrer DB-Instance. Sie können sie bei Bedarf später deaktivieren. Das Aktivieren und Deaktivieren von Performance Insights führt nicht zu Ausfallzeiten, einem Neustart oder einem Failover.

Der Performance-Insights-Agent verbraucht eine begrenzte Menge an CPU und Arbeitsspeicher auf dem DB-Host. Wenn die DB-Last hoch ist, begrenzt der Agent die Auswirkungen auf die Leistung, indem Daten seltener erfasst werden.

Aktivieren von Performance Insights beim Erstellen eines Clusters

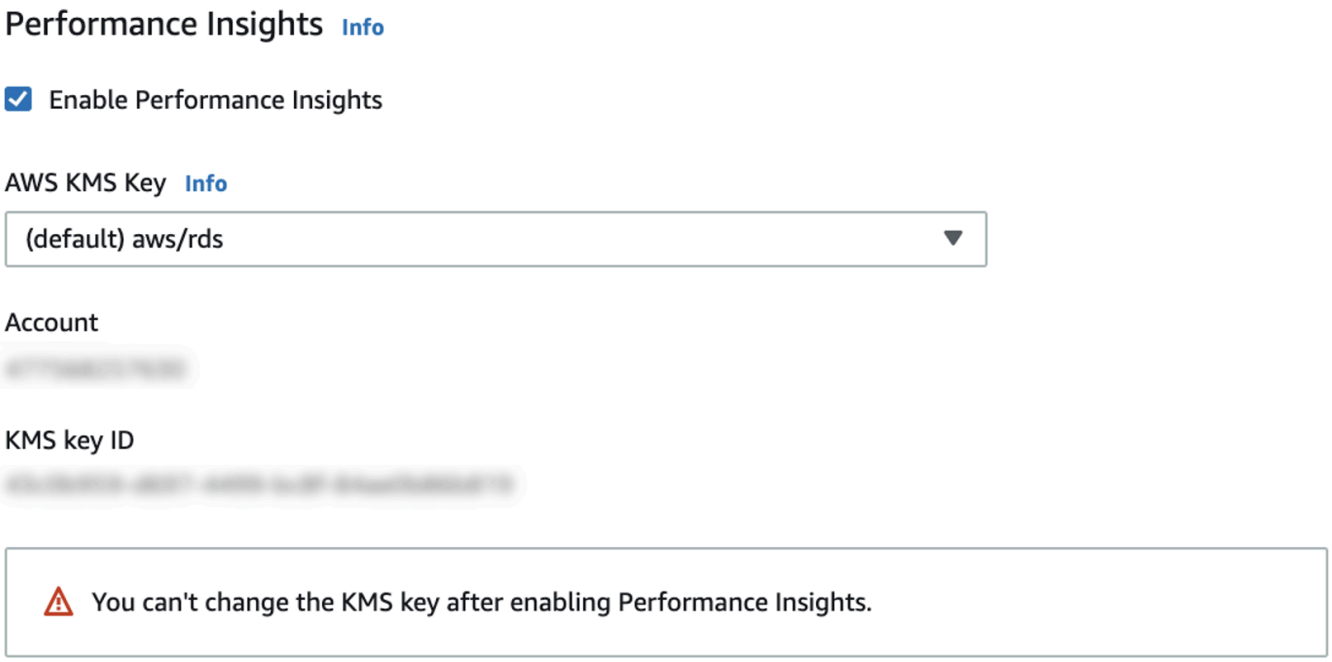
In der Konsole können Sie Performance Insights aktivieren oder deaktivieren, wenn Sie eine neue DB-Instance erstellen oder ändern.

Verwendung der AWS-Managementkonsole

In der Konsole können Sie Performance Insights aktivieren, wenn Sie einen Amazon DocumentDB-Cluster erstellen. Wenn Sie einen neuen Amazon DocumentDB-Cluster erstellen, aktivieren Sie Performance Insights, indem Sie im Abschnitt Performance Insights die Option Performance Insights aktivieren wählen.

Anweisungen für die Konsole

1. Um einen Cluster zu erstellen, folgen Sie den Anweisungen unter Erstellen eines Amazon DocumentDB-Clusters.
2. Wählen Sie im Abschnitt Performance Insights die Option Performance Insights aktivieren aus.



> **Note**
>
> Die Aufbewahrungsfrist für Performance Insights Insights-Daten beträgt sieben Tage.

AWS KMS Schlüssel — Geben Sie Ihren AWS KMS-Schlüssel an. Performance Insights verschlüsselt alle potenziell sensiblen Daten mit Ihrem AWS KMS Schlüssel. Die Daten werden während der Übertragung und im Ruhezustand verschlüsselt. Weitere Informationen finden Sie unter Konfiguration einer AWS AWS KMS Richtlinie für Performance Insights.

Aktivierung und Deaktivierung beim Ändern einer Instanz

Sie können eine DB-Instance ändern, um Performance Insights mithilfe der Konsole oder zu aktivieren oder zu deaktivieren AWS CLI.

Using the AWS-Managementkonsole

Anweisungen für die Konsole

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Klicken Sie auf Cluster.

3. Wählen Sie eine DB-Instance aus und wählen Sie Ändern.
4. Wählen Sie im Abschnitt Performance Insights entweder Performance Insights aktivieren oder Performance Insights deaktivieren aus.

   > **Note**
   >
   > Wenn Sie Enable Performance Insights wählen, können Sie Ihren AWS AWS KMS Schlüssel angeben. Performance Insights verschlüsselt alle potenziell sensiblen Daten mit Ihrem AWS KMS Schlüssel. Die Daten werden während der Übertragung und im Ruhezustand verschlüsselt. Weitere Informationen finden Sie unter Amazon DocumentDB DocumentDB-Daten im Ruhezustand verschlüsseln.

5. Klicken Sie auf Weiter.
6. Wählen Sie für Einplanung von Änderungen die Option Sofort anwenden aus. Wenn Sie während des nächsten geplanten Wartungsfensters Anwenden wählen, ignoriert Ihre Instance diese Einstellung und aktiviert Performance Insights sofort.
7. Wählen Sie Modify instance (Instance ändern).

Using the AWS CLI

Wenn Sie die `modify-db-instance` AWS AWS CLI Befehle `create-db-instance` oder verwenden, können Sie Performance Insights durch Angabe aktivieren oder deaktivieren`--enable-performance-insights`, indem Sie angeben`--no-enable-performance-insights`.

Im folgenden Verfahren wird beschrieben, wie Sie mit der AWS AWS CLI Performance-Insights für eine DB-Instance aktivieren oder deaktivieren.

AWS AWS CLI Anweisungen

Rufen Sie den `modify-db-instance` AWS AWS CLI Befehl auf und geben Sie die folgenden Werte an:

- `--db-instance-identifer`— Der Name der DB-Instance
- `--enable-performance-insights` zum Aktivieren oder `--no-enable-performance-insights` zum Deaktivieren

Example

Das folgende Beispiel aktiviert Performance Insights für`sample-db-instance`:

For Linux, macOS, or Unix:

```
aws docdb modify-db-instance \
    --db-instance-identifier sample-db-instance \
    --enable-performance-insights
```

For Windows:

```
aws docdb modify-db-instance ^
    --db-instance-identifier sample-db-instance ^
    --enable-performance-insights
```

Konfigurieren von Zugriffsrichtlinien für Performance Insights

Um auf Performance Insights zugreifen zu können, müssen Sie über die entsprechenden Berechtigungen von AWS Identity and Access Management (IAM) verfügen. Sie haben folgende Möglichkeiten, Zugriff zu gewähren:

- Fügen Sie die verwaltete Richtlinie `AmazonRDSPerformanceInsightsReadOnly` an einen Berechtigungssatz oder eine Rolle an.
- Erstellen Sie eine benutzerdefinierte IAM-Richtlinie und fügen Sie diese an einen Berechtigungssatz oder eine Rolle an.

Wenn Sie bei der Aktivierung von Performance Insights einen vom Kunden verwalteten Schlüssel angegeben haben, stellen Sie außerdem sicher, dass die Benutzer in Ihrem Konto über die Berechtigungen `kms:Decrypt` und `kms:GenerateDataKey` für den KMS-Schlüssel verfügen.

> **Note**
>
> Für die Verschlüsselung im Ruhezustand mit der Verwaltung von AWS KMS Schlüsseln und Sicherheitsgruppen nutzt Amazon DocumentDB Betriebstechnologie, die mit Amazon RDS gemeinsam genutzt wird.

Anhängen der Richtlinie an einen IAM-Prinzipal AmazonRDSPerformanceInsightsReadOnly

`AmazonRDSPerformanceInsightsReadOnly`ist eine AWS verwaltete Richtlinie, die Zugriff auf alle schreibgeschützten Operationen der Amazon DocumentDB Performance Insights-API gewährt. Derzeit sind alle Operationen in dieser API schreibgeschützt. Wenn Sie `AmazonRDSPerformanceInsightsReadOnly` an einen Berechtigungssatz oder eine Rolle anfügen, kann der Empfänger Performance Insights mit anderen Konsolenfunktionen verwenden.

Erstellen einer benutzerdefinierten IAM-Richtlinie für Performance Insights

Für Benutzer, die nicht über die `AmazonRDSPerformanceInsightsReadOnly`-Richtlinien verfügen, können Sie den Zugriff auf Performance Insights gewähren, indem Sie eine benutzerverwaltete IAM-Richtlinie erstellen oder ändern. Wenn Sie die Richtlinie an einen Berechtigungssatz oder eine Rolle anhängen, kann der Empfänger Performance Insights verwenden.

Erstellen eine benutzerdefinierten Richtlinie

1. Öffnen Sie unter https://console.aws.amazon.com/iam/ die IAM-Konsole.
2. Wählen Sie im Navigationsbereich Richtlinien.
3. Wählen Sie Richtlinie erstellen aus.
4. Wählen Sie auf der Seite Create Policy (Richtlinie erstellen) die Registerkarte „JSON“ aus.
5. Kopieren Sie den folgenden Text und fügen Sie ihn ein. *`us-east-1`* Ersetzen Sie ihn durch den Namen Ihrer AWS Region und *`111122223333`* durch Ihre Kundenkontonummer.

   JSON

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

```
            "Action": "rds:DescribeDBClusters",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "pi:DescribeDimensionKeys",
            "Resource": "arn:aws:pi:us-east-1:111122223333:metrics/rds/*"
        },
        {
            "Effect": "Allow",
            "Action": "pi:GetDimensionKeyDetails",
            "Resource": "arn:aws:pi:us-east-1:111122223333:metrics/rds/*"
        },
        {
            "Effect": "Allow",
            "Action": "pi:GetResourceMetadata",
            "Resource": "arn:aws:pi:us-east-1:111122223333:metrics/rds/*"
        },
        {
            "Effect": "Allow",
            "Action": "pi:GetResourceMetrics",
            "Resource": "arn:aws:pi:us-east-1:111122223333:metrics/rds/*"
        },
        {
            "Effect": "Allow",
            "Action": "pi:ListAvailableResourceDimensions",
            "Resource": "arn:aws:pi:us-east-1:111122223333:metrics/rds/*"
        },
        {
            "Effect": "Allow",
            "Action": "pi:ListAvailableResourceMetrics",
            "Resource": "arn:aws:pi:us-east-1:111122223333:metrics/rds/*"
        }
    ]
}
```

6. Wählen Sie Richtlinie prüfen.
7. Geben Sie einen Namen und optional eine Beschreibung für die Richtlinie an und wählen Sie dann Create policy (Richtlinie erstellen) aus.

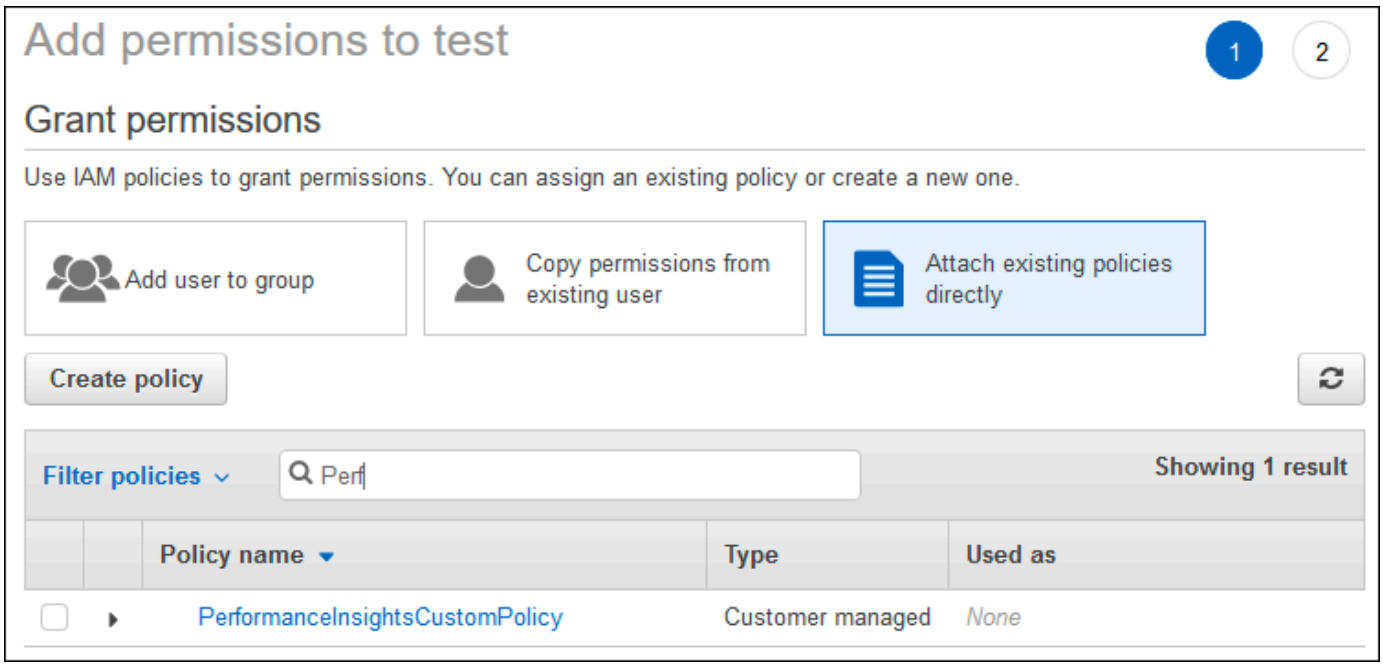
Sie können die Richtlinie nun an einen Berechtigungssatz oder eine Rolle anfügen. Das folgende Verfahren setzt voraus, dass Sie für diesen Zweck bereits einen Benutzer zur Verfügung haben.

So fügen Sie die Richtlinie an einen Benutzer an

1. Öffnen Sie unter https://console.aws.amazon.com/iam/ die IAM-Konsole.
2. Klicken Sie im Navigationsbereich auf Users (Benutzer).
3. Wählen Sie einen vorhandenen Benutzer aus der Liste aus.

> **Important**
>
> Um Performance Insights verwenden zu können, stellen Sie sicher, dass Sie zusätzlich zur benutzerdefinierten Richtlinie Zugriff auf Amazon DocumentDB haben. Die AmazonDocDBReadOnlyAccessvordefinierte Richtlinie bietet beispielsweise Lesezugriff auf Amazon. DocDB.For Weitere Informationen finden Sie unter Zugriff mithilfe von Richtlinien verwalten.

4. Wählen Sie auf der Seite Summary (Übersicht) die Option Add permissions (Berechtigungen hinzufügen) aus.
5. Wählen Sie Attach existing policies directly (Vorhandene Richtlinien direkt zuordnen). Geben Sie in Suche die ersten Zeichen Ihres Richtliniennamens ein, wie nachfolgend gezeigt.



6. Wählen Sie Ihre Richtlinie und wählen Sie anschließend Nächster Schritt: Prüfen.
7. Wählen Sie Add permissions (Berechtigungen hinzufügen) aus.

Konfiguration eines AWS KMS Richtlinie für Performance Insights

Performance Insights verwendet an AWS KMS key , um sensible Daten zu verschlüsseln. Wenn Sie Performance Insights über die API oder die Konsole aktivieren, haben Sie folgende Möglichkeiten:

- Wählen Sie die Standardeinstellung Von AWS verwalteter Schlüssel.

  Amazon DocumentDB verwendet die Von AWS verwalteter Schlüssel für Ihre neue DB-Instance. Amazon DocumentDB erstellt eine Von AWS verwalteter Schlüssel für Ihr AWS Konto. Ihr AWS Konto hat Von AWS verwalteter Schlüssel für Amazon DocumentDB für jede AWS Region ein anderes.
- Wählen Sie einen kundenverwalteten Schlüssel.

  Wenn Sie einen vom Kunden verwalteten Schlüssel angeben, benötigen Benutzer in Ihrem Konto, die die Performance Insights API aufrufen, die Berechtigungen `kms:Decrypt` und `kms:GenerateDataKey` für den KMS-Schlüssel. Sie können diese Berechtigungen über IAM-Richtlinien konfigurieren. Wir empfehlen jedoch, dass Sie diese Berechtigungen über Ihre KMS-Schlüsselrichtlinie verwalten. Weitere Informationen finden Sie unter Verwenden von Schlüsselrichtlinien in AWS -KMS.

Example

Das folgende Beispiel für eine Schlüsselrichtlinie zeigt, wie Sie Ihrer KMS-Schlüsselrichtlinie Anweisungen hinzufügen können. Diese Anweisungen erlaubt den Zugriff auf Performance Insights. Je nachdem, wie Sie das verwenden AWS KMS, möchten Sie möglicherweise einige Einschränkungen ändern. Bevor Sie Ihrer Richtlinie Anweisungen hinzufügen, entfernen Sie alle Kommentare.

Analyse der Metriken mit dem Performance Insights-Dashboard

Das Dashboard von Performance Insights enthält Informationen zur Datenbank-Performance, die Sie bei der Analyse und Behebung von Performance-Problemen unterstützen. Auf der Hauptseite des Dashboards können Sie Informationen zur Datenbanklast (DB-Load) einsehen. Sie können die Datenbanklast nach Dimensionen wie Wartestatus oder Abfrage „aufteilen“.

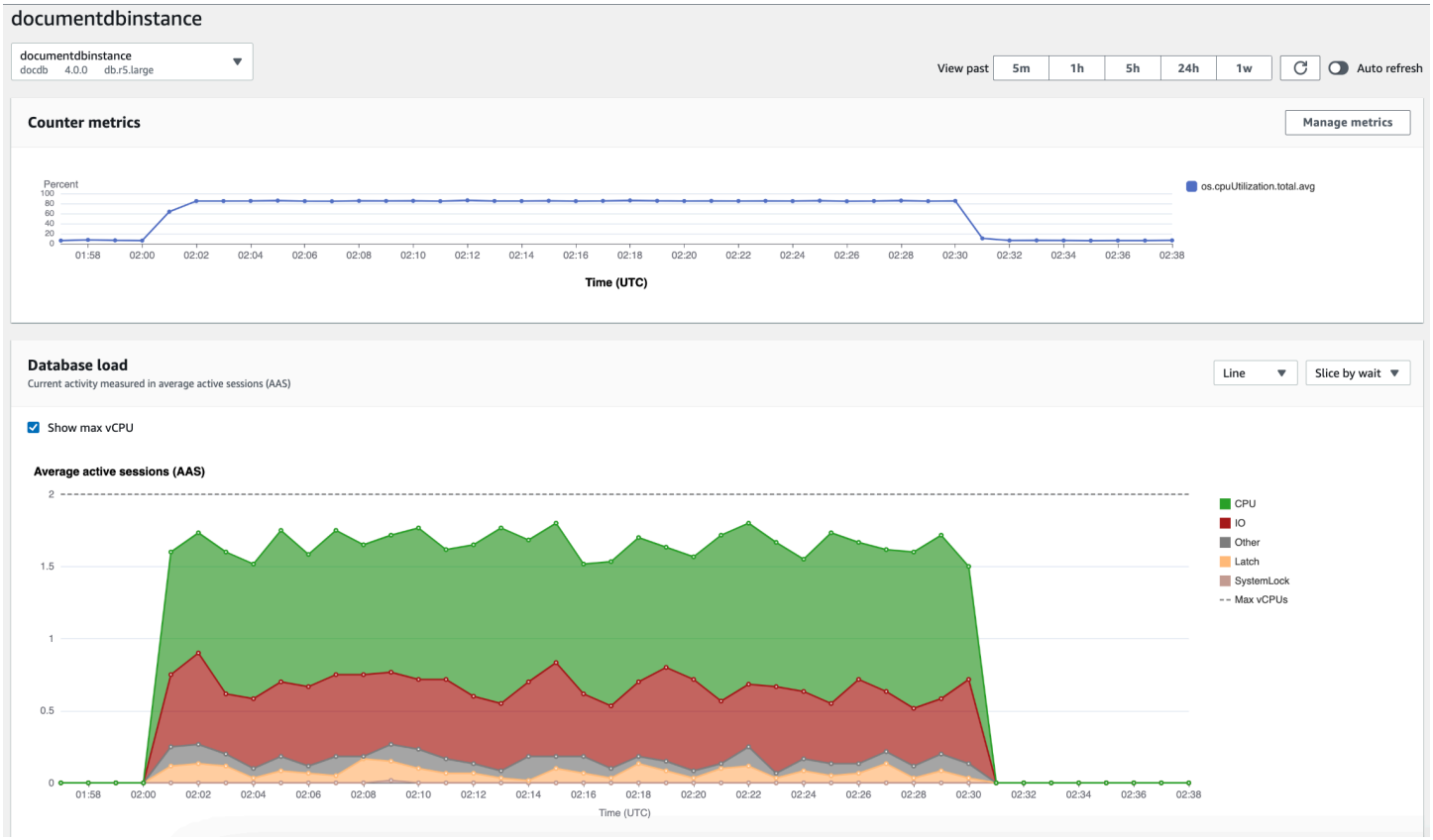
Themen

- Überblick über Performance Insights
- Öffnen des Performance Insights-Dashboards

- Analysieren der Datenbanklast nach Wartezuständen
- Überblick über die Registerkarte „Häufigste Abfragen“
- Das Diagramm zum Laden der Datenbank vergrößern

Überblick über Performance Insights

Das Dashboard ist die einfachste Möglichkeit, mit Performance Insights zu interagieren. Das folgende Beispiel zeigt das Dashboard für eine Amazon DocumentDB DocumentDB-Instance. Standardmäßig zeigt das Dashboard von Performance Insights die Daten der letzten Stunde an.



Das Dashboard ist in folgende Teile gegliedert:

1. Zählermetriken — Zeigt Daten für bestimmte Leistungsindikatormetriken an.
2. Datenbanklast — Zeigt, wie die DB-Last im Vergleich zur DB-Instance-Kapazität abschneidet, wie sie in der Zeile Max vCPU dargestellt wird.
3. Top-Dimensionen — Zeigt die wichtigsten Dimensionen an, die zur DB-Auslastung beitragen. Zu diesen Dimensionen gehören `waitsqueries`,`hosts`,`databases`, und`applications`.

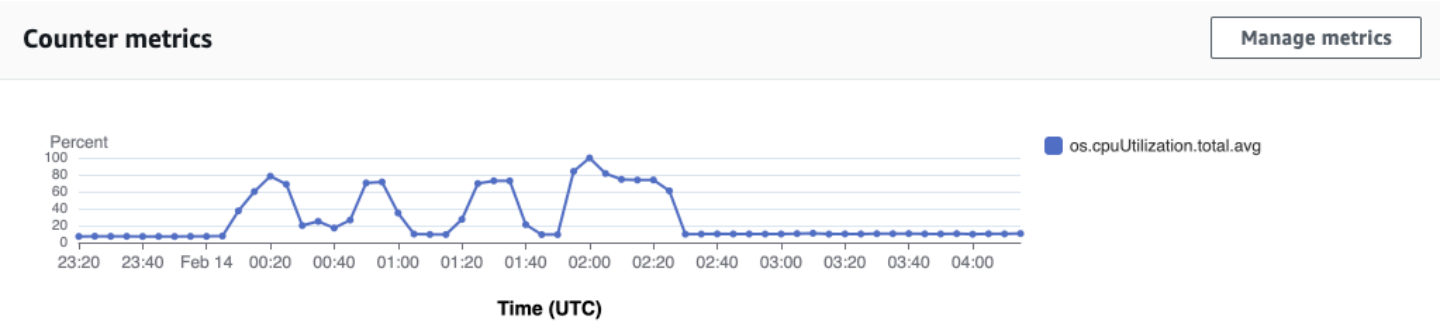
Themen

- Zählermetriken-Diagramm
- Datenbank-Ladediagramm
- Dimensionen pro Tabelle

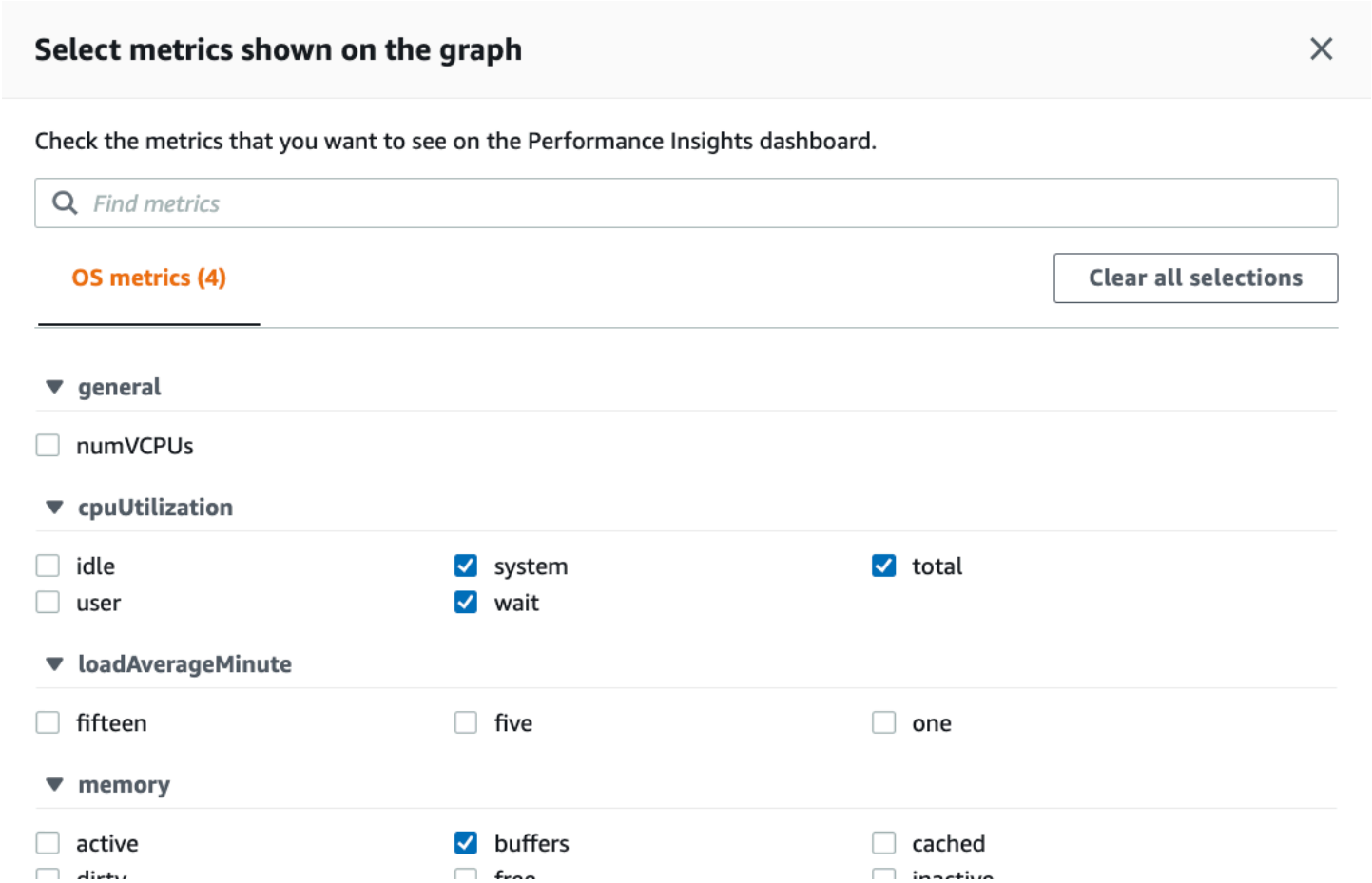
Zählermetriken-Diagramm

Mithilfe von Zählermetriken können Sie das Performance-Insights-Dashboard anpassen und bis zu 10 weitere Diagramme aufnehmen. Diese Grafiken zeigen eine Auswahl von Dutzenden von Betriebssystemmetriken. Diese Informationen können mit der Datenbanklast korreliert werden, um Performance-Probleme zu identifizieren und zu analysieren.

Das Counter Metrics (Zählermetriken)-Diagramm enthält Daten zu Leistungsindikatoren.



Um die Leistungsindikatoren zu ändern, wählen Sie Metriken verwalten aus. Sie können mehrere Betriebssystemmetriken auswählen, wie im folgenden Screenshot gezeigt. Um Details für jede Metrik anzuzeigen, bewegen Sie den Mauszeiger über den Metriknamen.



Datenbank-Ladediagramm

Das Diagramm zum Laden der Datenbank zeigt, wie die Datenbankaktivität im Vergleich zur Instanzkapazität abschneidet, wie sie in der Zeile Max. vCPU dargestellt wird. Standardmäßig stellt das gestapelte Liniendiagramm die DB-Last als durchschnittliche aktive Sitzungen pro Zeiteinheit dar. Die DB-Last wird nach Wartestatus aufgeteilt (gruppiert).

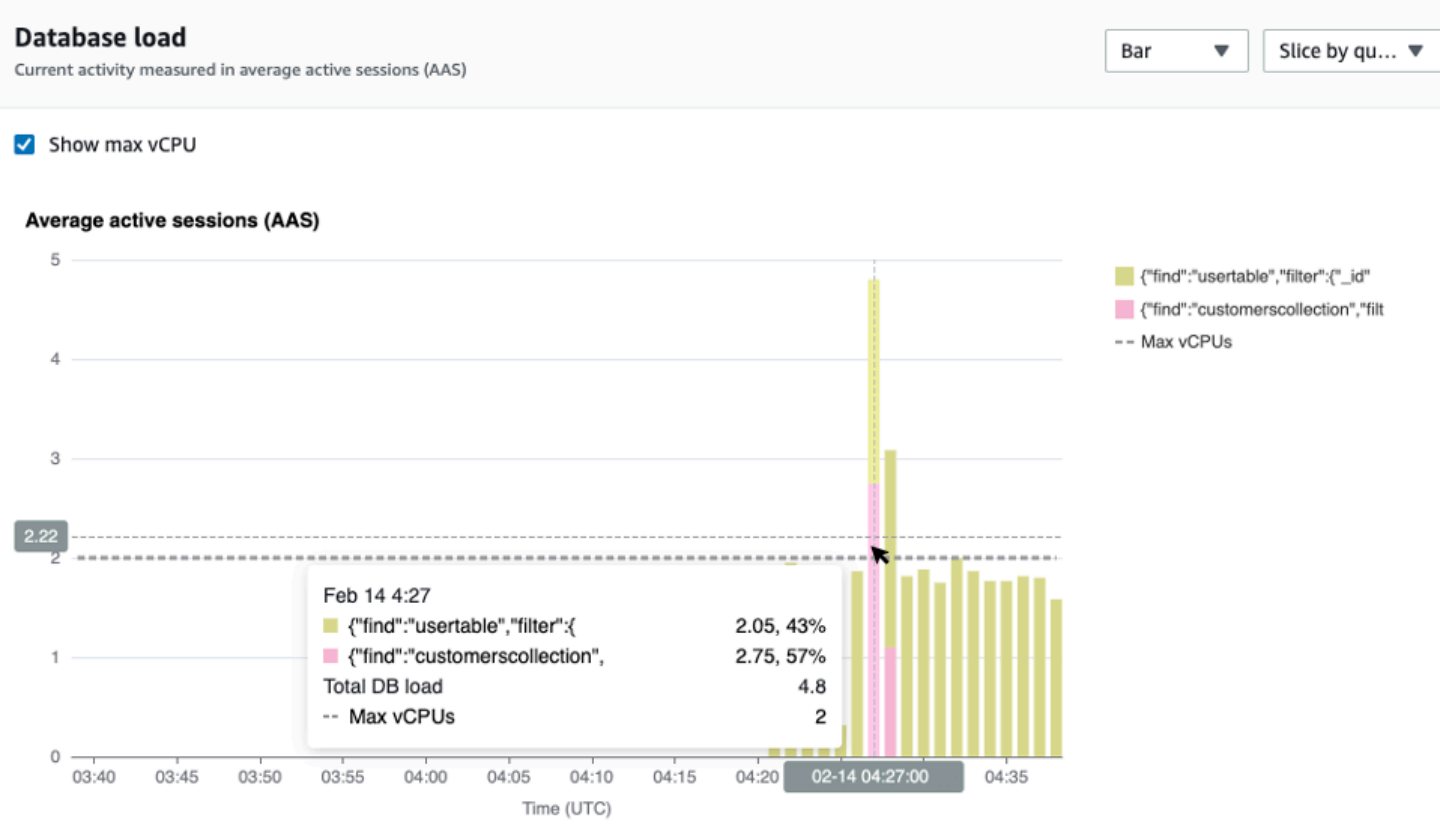
DB-Last aufgeteilt nach Dimensionen

Sie können die Last als aktive Sitzungen anzeigen, die nach unterstützten Dimensionen gruppiert sind. Die folgende Abbildung zeigt die Abmessungen für die Amazon DocumentDB DocumentDB-Instance.

DB-Ladedetails für ein Dimensionselement

Um Details zu einem DB-Lastelement innerhalb einer Dimension anzuzeigen, bewegen Sie den Mauszeiger über den Elementnamen. Die folgende Abbildung zeigt Details für eine Abfrageanweisung.

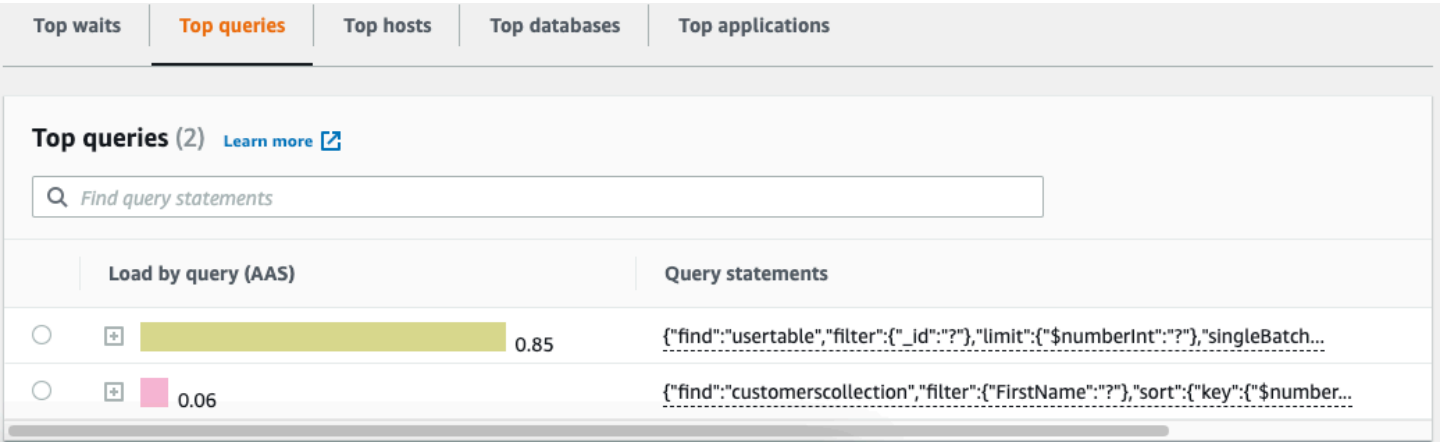
Um Details zu einem Element für den ausgewählten Zeitraum in der Legende anzuzeigen, bewegen Sie den Mauszeiger über dieses Element.



Dimensionen pro Tabelle

In der Tabelle mit den obersten Abmessungen wird die Datenbanklast nach verschiedenen Dimensionen aufgeteilt. Eine Dimension ist eine Kategorie oder „Aufteilung“ für verschiedene Merkmale der DB-Last. Wenn es sich bei der Dimension um eine Abfrage handelt, zeigt die Liste der häufigsten Abfragen die Abfrageanweisungen an, die am meisten zur DB-Auslastung beitragen.

Wählen Sie eine der folgenden Dimensionsregisterkarten.



Die folgende Tabelle enthält eine kurze Beschreibung der einzelnen Registerkarten.

Description
Das Ereignis, auf das der Backend wartet
Die Anweisungen, die derzeit ausgeführt werden
Die Hosts (IP-Adresse)
Der Name der Datenbank (Top-

Description
Datenbanken, mit der der Client verbunden ist
Der Name des Top-Anwendungen, die mit der Datenbank verbunden ist

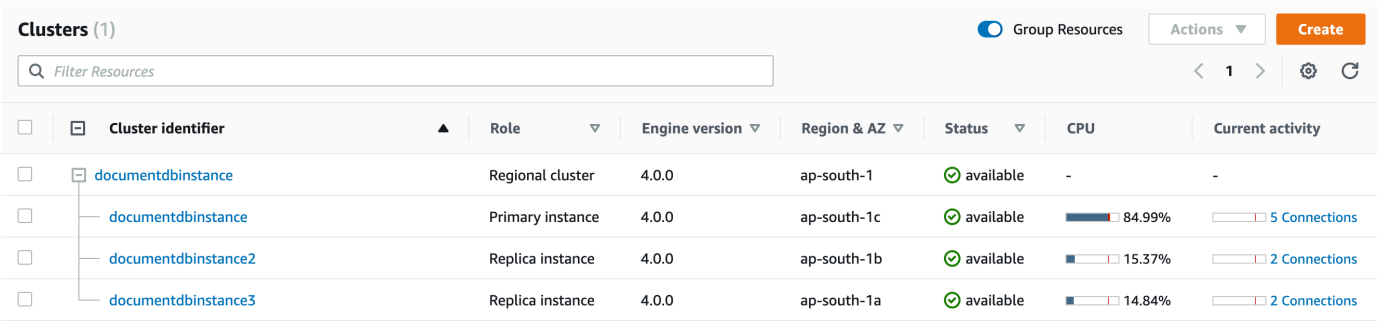
Informationen zum Analysieren von Abfragen mithilfe der Registerkarte „Häufig gestellte Abfragen“ finden Sie unter Überblick über die Registerkarte „Häufigste Abfragen“.

Öffnen des Performance Insights-Dashboards

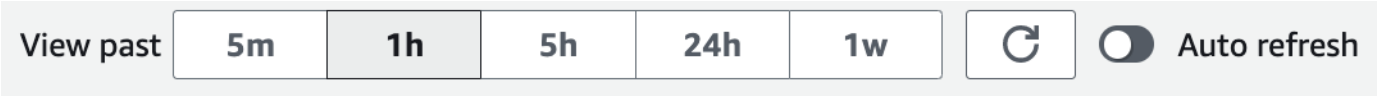
Um das Performance Insights Insights-Dashboard in der AWS Gehen Sie in der Management Console wie folgt vor:

1. Öffnen Sie die Performance Insights Insights-Konsole unter https://console.aws.amazon.com/docdb/.
2. Wählen Sie eine DB-Instance aus. Das Performance Insights Insights-Dashboard wird für diese Amazon DocumentDB DocumentDB-Instance angezeigt.

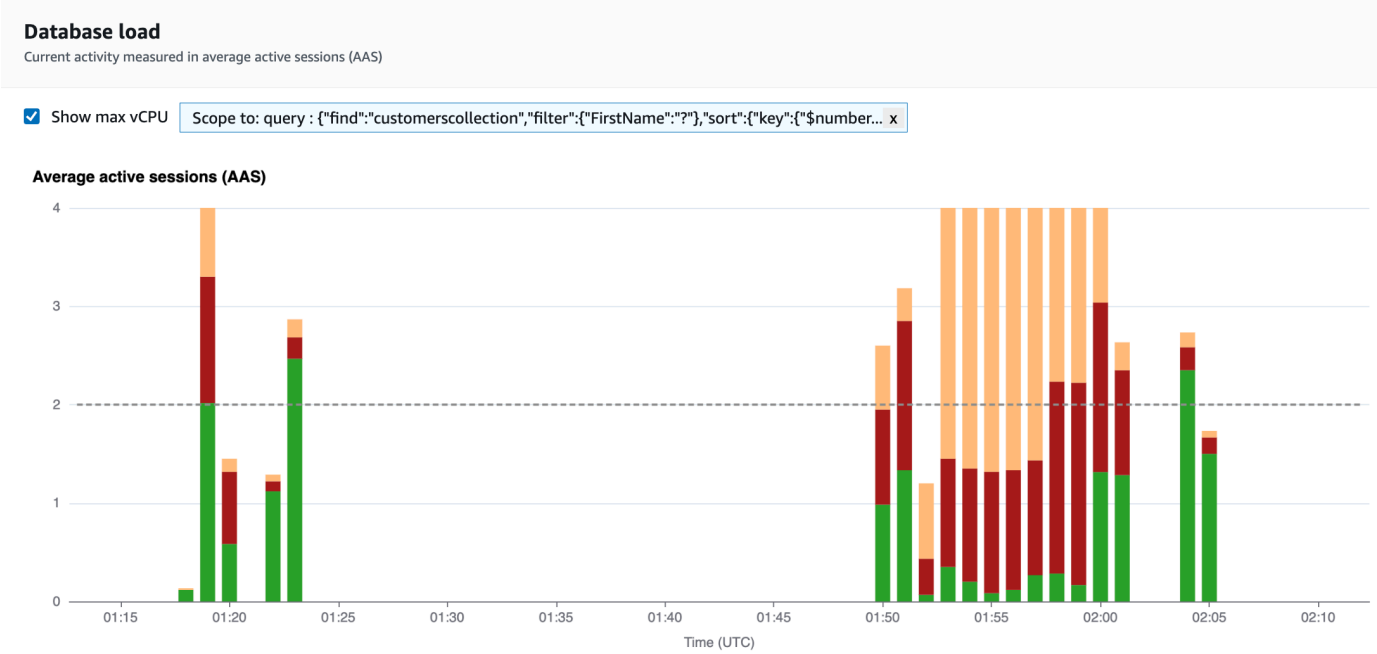
Für Amazon DocumentDB DocumentDB-Instances mit aktiviertem Performance Insights können Sie das Dashboard auch aufrufen, indem Sie in der Liste der Instances den Eintrag Sessions auswählen. Unter Aktuelle Aktivität zeigt das Element Sitzungen die Datenbanklast von durchschnittlichen, aktiven Sitzungen der letzten fünf Minuten an. Der Balken zeigt die Last grafisch an. Wenn die Leiste leer ist, befindet sich die Instance im Leerlauf. Wenn die Last ansteigt, wird der Balken blau ausgefüllt. Wenn die Last die Anzahl der virtuellen CPUs (vCPUs) in der Instance-Klasse überschreitet, färbt sich der Balken rot, was auf einen potenziellen Engpass hinweist.



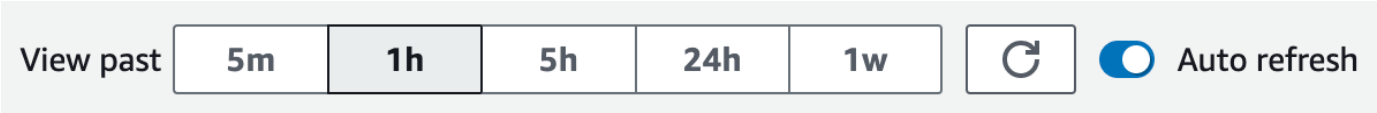
3. (Optional) Wählen Sie über eine der Schaltflächen rechts oben ein anderes Zeitintervall aus. Um das Intervall beispielsweise auf 1 Stunde zu ändern, wählen Sie 1h aus.



Im folgenden Screenshot beträgt das DB-Ladeintervall 1 Stunde.



4. Um Ihre Daten automatisch zu aktualisieren, aktivieren Sie Automatische Aktualisierung.



   Das Performance Insights-Dashboard wird automatisch mit neuen Daten aktualisiert. Die Aktualisierungsrate hängt von der Menge der angezeigten Daten ab:

   - „5 Minuten“ wird alle 5 Sekunden aktualisiert.
   - 1 Stunde, wird jede Minute aktualisiert.
   - 5 Stunden, wird jede Minute aktualisiert.
   - „24 Stunden“ wird alle 5 Minuten aktualisiert.
   - „1 Woche“ wird jede Stunden aktualisiert.

Analysieren der Datenbanklast nach Wartezuständen

Wenn das Diagramm zur Datenbankauslastung (DB-Last) einen Engpass anzeigt, können Sie herausfinden, woher die Last kommt. Betrachten Sie dazu die Tabelle mit den Hauptlastelementen unterhalb des Datenbanklast-Diagramms Wählen Sie ein bestimmtes Element aus, z. B. eine Abfrage oder eine Anwendung, um dieses Element genauer zu untersuchen und Details zu diesem Element anzuzeigen.

Die Datenbanklast, gruppiert nach Waits und Top-Abfragen, bietet in der Regel den besten Einblick in Leistungsprobleme. DB-Last gruppiert nach Wartezeiten zeigt an, ob Ressourcen- oder Parallelitätsengpässe in der Datenbank vorhanden sind. In diesem Fall wird auf der Registerkarte „Häufigste Abfragen“ der Tabelle mit den am häufigsten ausgelasteten Elementen angezeigt, welche Abfragen für diese Auslastung verantwortlich sind.

Ihr typischer Workflow für die Diagnose von Performance-Problemen ist folgendermaßen:

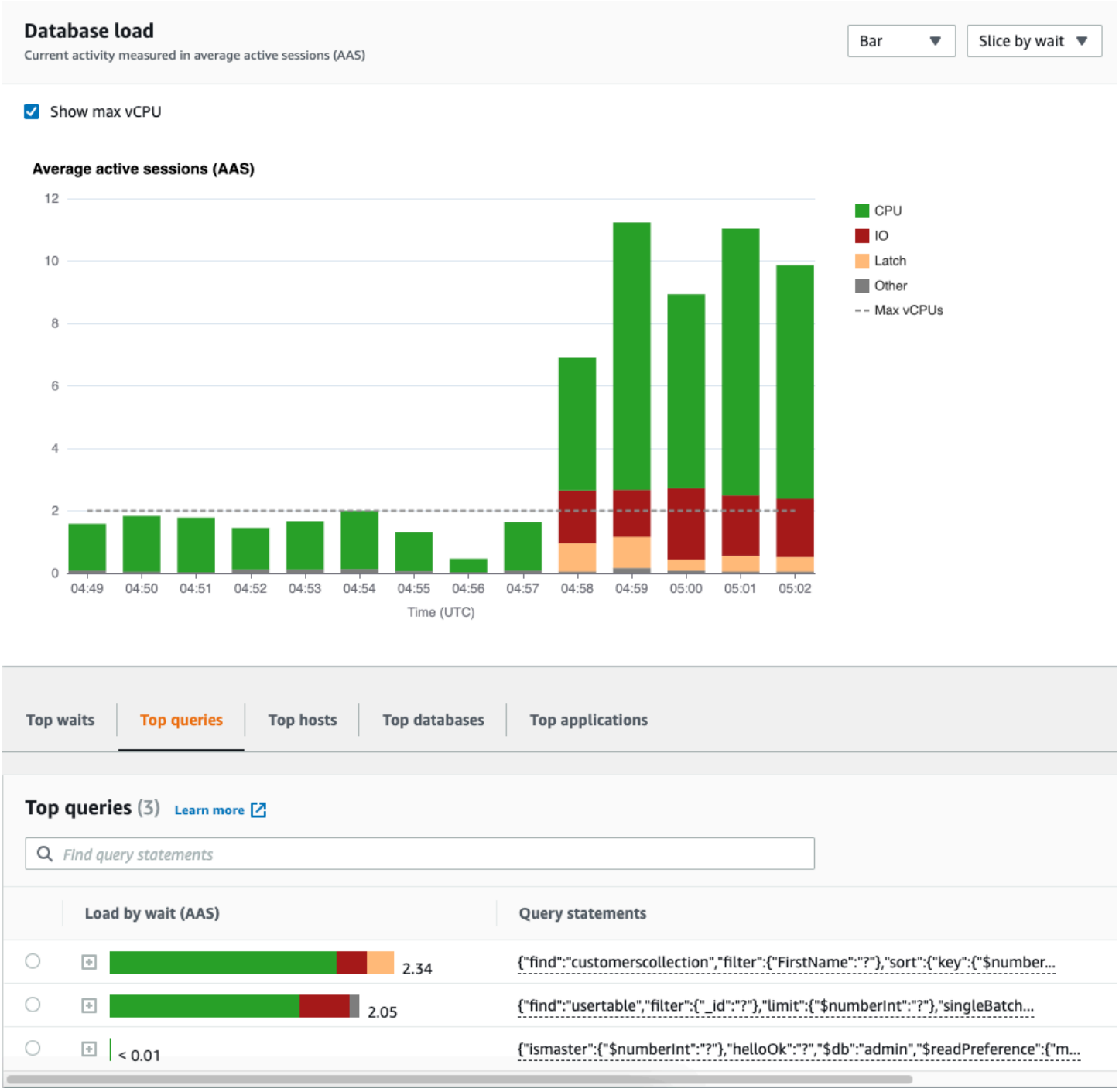
1. Überprüfen Sie das Diagramm der durchschnittlich aktiven Sitzungen auf irgendwelche Ereignisse, in denen die Datenbanklast die Max CPU-Linie übersteigt.
2. Wenn ja, schauen Sie sich das Diagramm der durchschnittlich aktiven Sitzungen an und identifizieren Sie, welcher Wartezustand oder welche Zustände primär dafür verantwortlich sind.
3. Identifizieren Sie die Digest-Abfragen, die die Last verursacht haben, indem Sie sehen, welche der Abfragen auf der Registerkarte „Häufigste Abfragen“ in der Tabelle mit den am häufigsten

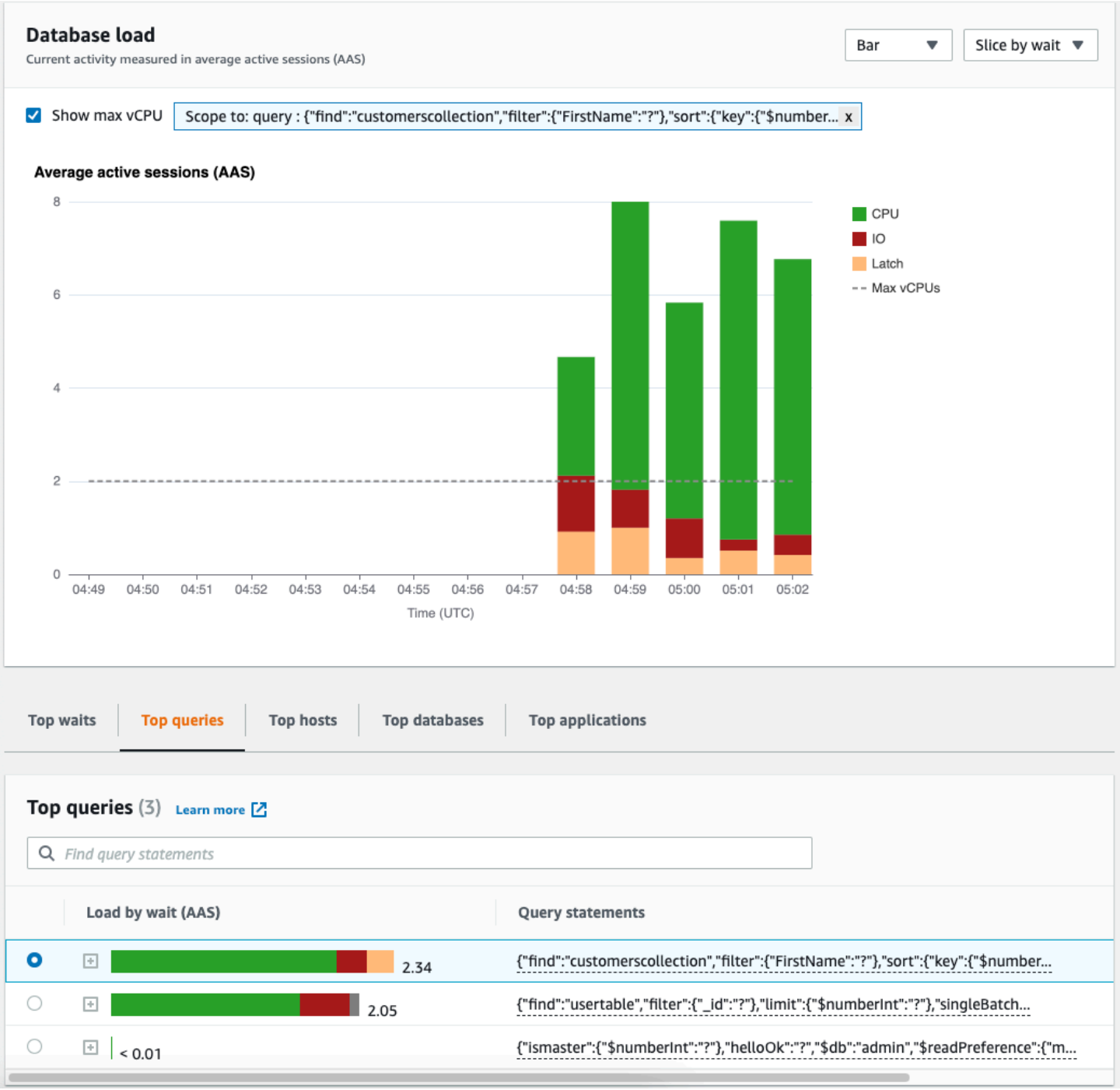
geladenen Elementen am meisten zu diesen Wartezuständen beitragen. Sie können diese anhand der Spalte Load by Wait (AAS) identifizieren.

4. Wählen Sie auf der Registerkarte „Häufig gestellte Abfragen“ eine dieser Digest-Abfragen aus, um sie zu erweitern und die untergeordneten Abfragen zu sehen, aus denen sie besteht.

Sie können auch sehen, welche Hosts oder Anwendungen die meiste Last verursachen, indem Sie jeweils Top-Hosts oder Top-Anwendungen auswählen. Anwendungsnamen werden in der Verbindungszeichenfolge zur Amazon DocumentDB DocumentDB-Instance angegeben. `Unknown`gibt an, dass das Anwendungsfeld nicht angegeben wurde.

Im folgenden Dashboard machen beispielsweise CPU-Wartezeiten den größten Teil der DB-Last aus. Wenn Sie unter Häufigste Abfragen die oberste Abfrage auswählen, wird das Diagramm zur Datenbankauslastung so ausgerichtet, dass der Schwerpunkt auf der höchsten Last liegt, die durch die ausgewählte Abfrage verursacht wird.


Database load
Current activity measured in average active sessions (AAS)
Bar
Slice by wait
Show max vCPU
Average active sessions (AAS)
12
10
8
6
4
2
0
04:49
04:50
04:51
04:52
04:53
04:54
04:55
04:56
04:57
04:58
04:59
05:00
05:01
05:02
Time (UTC)
CPU
IO
Latch
Other
Max vCPUs
Top waits
Top queries
Top hosts
Top databases
Top applications
Top queries (3)
Learn more
Find query statements
Load by wait (AAS)
Query statements
2.34
{"find":"customerscollection","filter":{"FirstName":"?"},"sort":{"key":{"$number...
2.05
{"find":"usertable","filter":{"_id":"?"},"limit":{"$numberInt":"?"},"singleBatch...
< 0.01
{"ismaster":{"$numberInt":"?"},"helloOk":"?","$db":"admin","$readPreference":{"m...



Überblick über die Registerkarte „Häufigste Abfragen“

Standardmäßig werden auf der Registerkarte „Häufigste Abfragen“ die Abfragen angezeigt, die am meisten zur DB-Auslastung beitragen. Sie können den Abfragetext analysieren, um Ihre Abfragen zu optimieren.

Themen

- Zusammenfassungen von Abfragen
- Nach Waits laden (AAS)
- Detaillierte Abfrageinformationen anzeigen
- Zugriff auf den Abfragetext der Anweisung
- Abfragetext für Kontoauszüge anzeigen und herunterladen

Zusammenfassungen von Abfragen

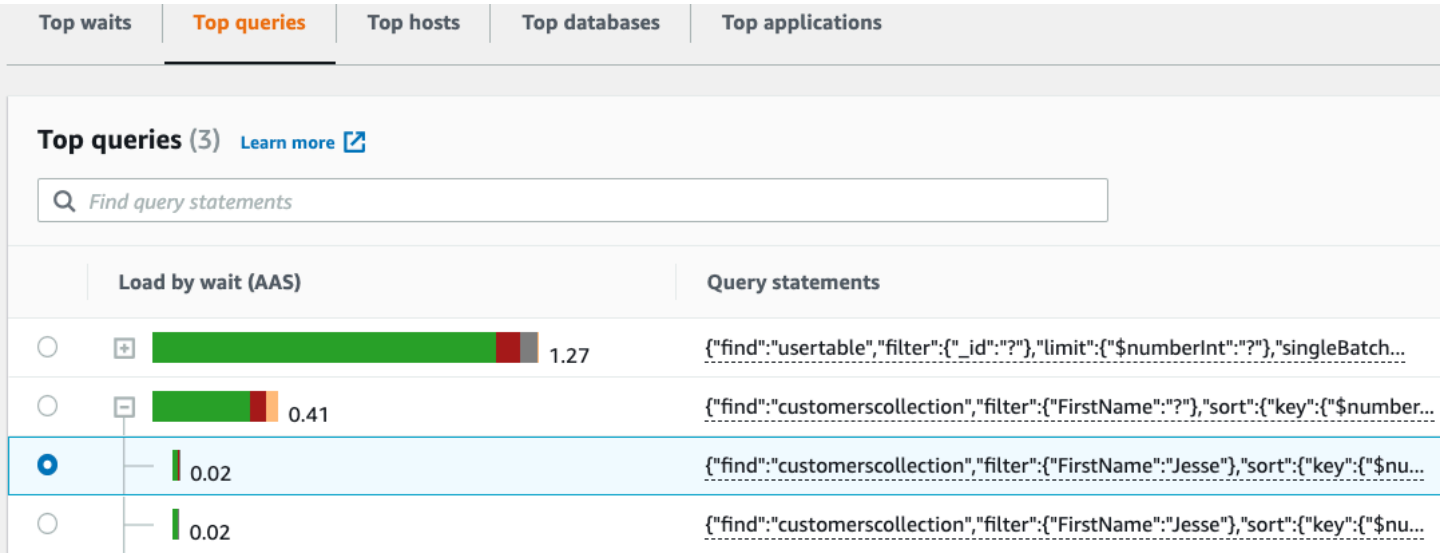
Ein Abfrage-Digest besteht aus mehreren tatsächlichen Abfragen, die sich strukturell ähneln, aber unterschiedliche Literalwerte haben können. Der Digest ersetzt fest codierte Werte durch ein Fragezeichen. Ein Abfrage-Digest könnte beispielsweise so aussehen:

```
{"find":"customerscollection","filter":{"FirstName":"?"},"sort":{"key":
{"$numberInt":"?"}},"limit":{"$numberInt":"?"}}
```

Dieser Digest kann die folgenden untergeordneten Abfragen enthalten:

```
{"find":"customerscollection","filter":{"FirstName":"Karrie"},"sort":{"key":
{"$numberInt":"1"}},"limit":{"$numberInt":"3"}}
{"find":"customerscollection","filter":{"FirstName":"Met"},"sort":{"key":
{"$numberInt":"1"}},"limit":{"$numberInt":"3"}}
{"find":"customerscollection","filter":{"FirstName":"Rashin"},"sort":{"key":
{"$numberInt":"1"}},"limit":{"$numberInt":"3"}}
```

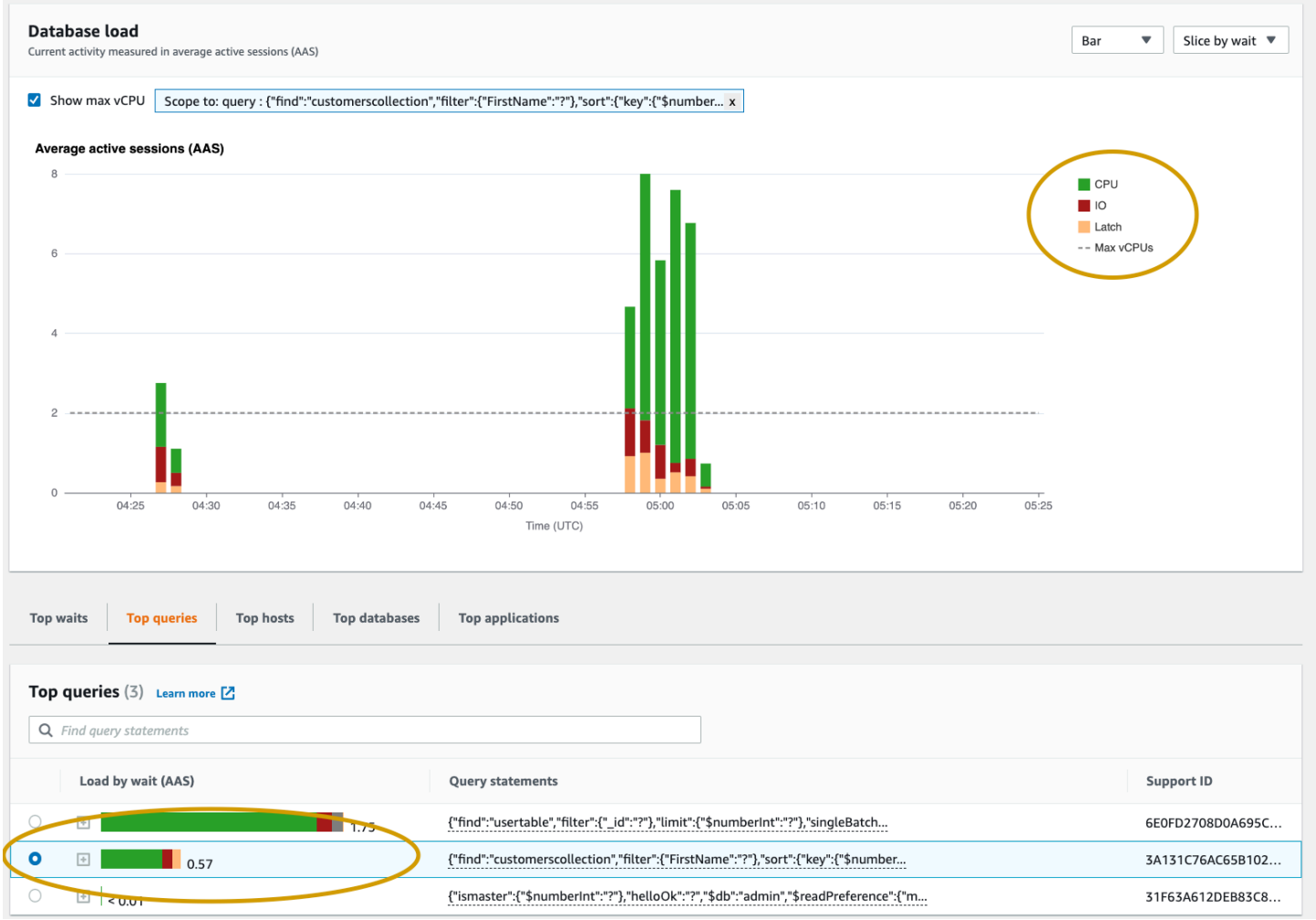
Um die wörtlichen Abfrageanweisungen in einem Digest zu sehen, wählen Sie die Abfrage und dann das Pluszeichen () aus. + Im folgenden Screenshot ist die ausgewählte Abfrage ein Digest.



> **Note**
>
> In einem Abfrage-Digest werden ähnliche Abfrageanweisungen gruppiert, sensible Informationen werden jedoch nicht geschwärzt.

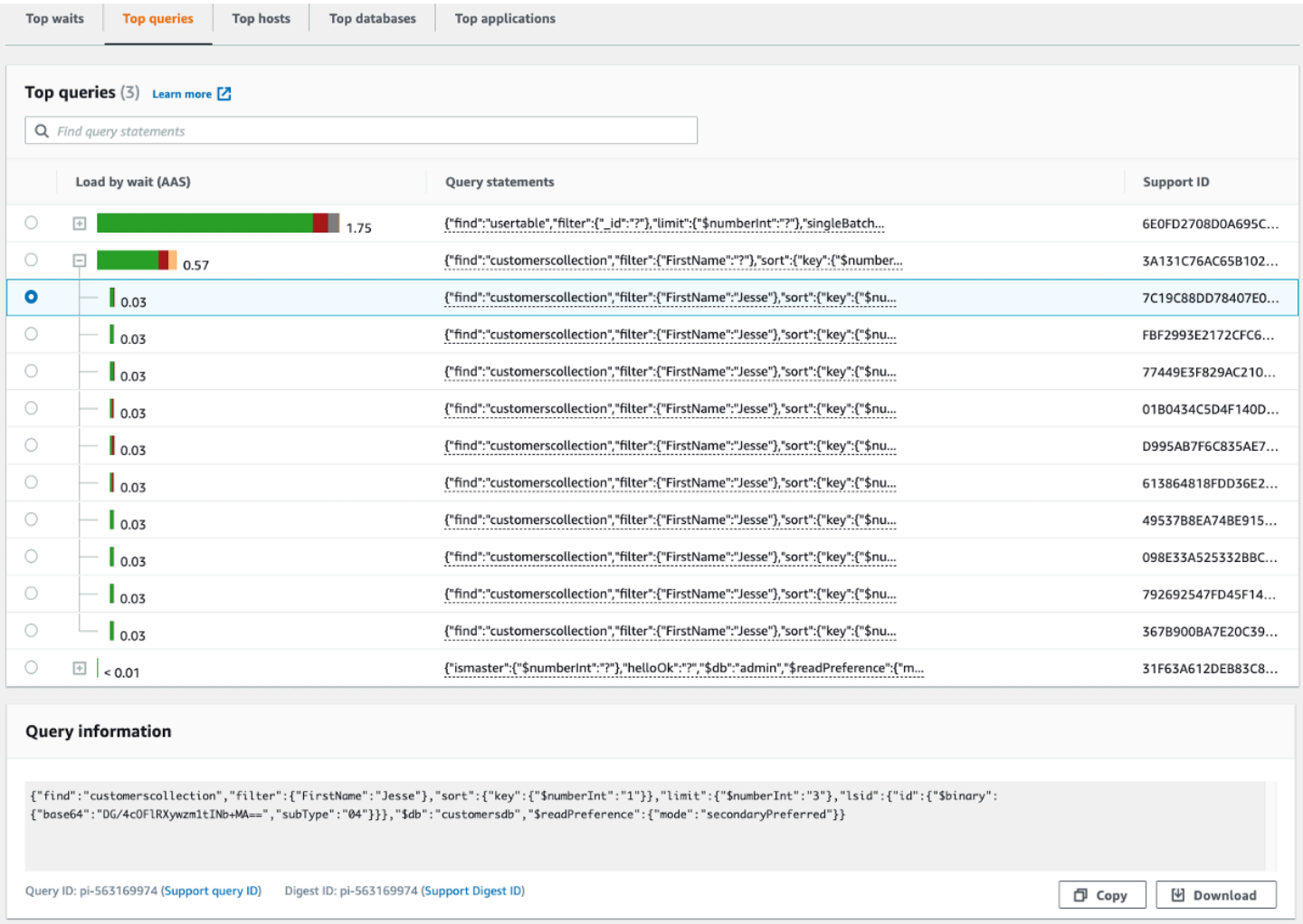
Nach Waits laden (AAS)

In Top-Abfragen zeigt die Spalte Load by Waits (AAS) den Prozentsatz der Datenbanklast, der jedem Top-Load-Element zugeordnet ist. Diese Spalte gibt die Last für dieses Element nach der Gruppierung wieder, die derzeit im DB-Lastdiagramm ausgewählt ist. Beispielsweise können Sie das DB-Last-Diagramm nach Wartezuständen gruppieren. In diesem Fall ist der Balken DB Load by Waits (DB-Last nach Wartezuständen) so groß, segmentiert und farbcodiert, dass angezeigt wird, zu wieviel Prozent diese Abfrage zum betreffenden Wartezustand beiträgt. Es zeigt zudem auf, welche Wartezustände sich auf die ausgewählte Abfrage auswirken.



Detaillierte Abfrageinformationen anzeigen

In der Abfragetabelle „Top“ können Sie eine Digest-Anweisung öffnen, um die zugehörigen Informationen anzuzeigen. Die Informationen werden im unteren Bereich angezeigt.



Die folgenden Typen von Bezeichnern (IDs) sind mit Abfrageanweisungen verknüpft:

1. Support-Abfrage-ID — Ein Hashwert der Abfrage-ID. Dieser Wert dient nur zum Verweisen auf eine Abfrage-ID, wenn Sie mit AWS Support arbeiten. AWS Der Support hat keinen Zugriff auf Ihre tatsächlichen Abfrage-IDs und Ihren Abfragetext.
2. Support-Digest-ID — Ein Hashwert der Digest-ID. Dieser Wert dient nur zum Verweisen auf eine Digest-ID, wenn Sie mit AWS Support zusammenarbeiten. AWS Der Support hat keinen Zugriff auf Ihre tatsächlichen Digest-IDs und den Abfragetext.

Zugriff auf den Abfragetext der Anweisung

Standardmäßig enthält jede Zeile in der Tabelle mit den häufigsten Abfragen 500 Byte Abfragetext für jede Abfrageanweisung. Wenn eine Digest-Anweisung 500 Byte überschreitet, können Sie mehr Text anzeigen, indem Sie die Anweisung im Performance Insights Insights-Dashboard öffnen. In

diesem Fall beträgt die maximale Länge der angezeigten Abfrage 1 KB. Wenn Sie eine vollständige Abfrageanweisung anzeigen, können Sie auch Herunterladen wählen.

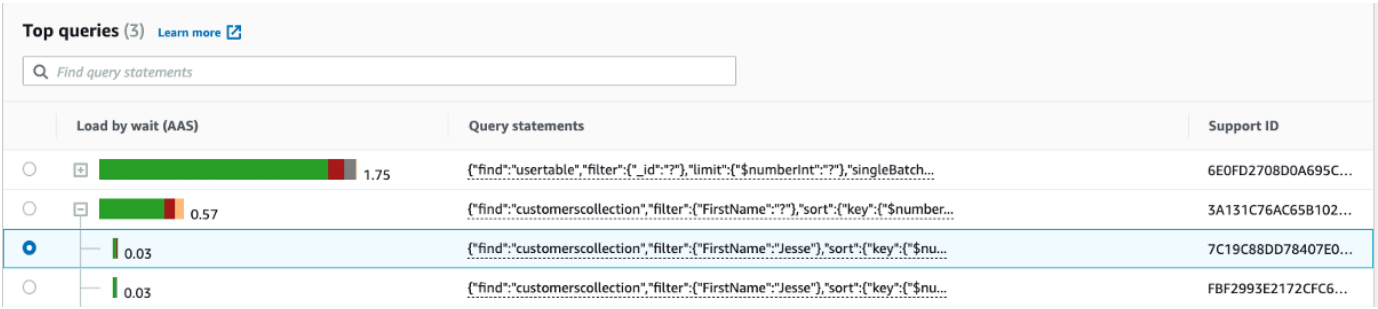
Abfragetext für Kontoauszüge anzeigen und herunterladen

Im Performance Insights Insights-Dashboard können Sie Abfragetext anzeigen oder herunterladen.

So zeigen Sie mehr Abfragetext im Performance Insights Insights-Dashboard an

1. Öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter: https://console.aws.amazon.com/docdb/
2. Wählen Sie im Navigationsbereich Performance-Insights aus.
3. Wählen Sie eine DB-Instance aus. Das Performance Insights-Dashboard wird für diese DB-Instance angezeigt.

   Abfrageanweisungen mit Text, der größer als 500 Byte ist, sehen wie in der folgenden Abbildung aus:



4. Sehen Sie sich den Abschnitt mit den Abfrageinformationen an, um mehr vom Abfragetext zu sehen.

Das Performance Insights Insights-Dashboard kann bis zu 1 KB für jede vollständige Abfrageanweisung anzeigen.

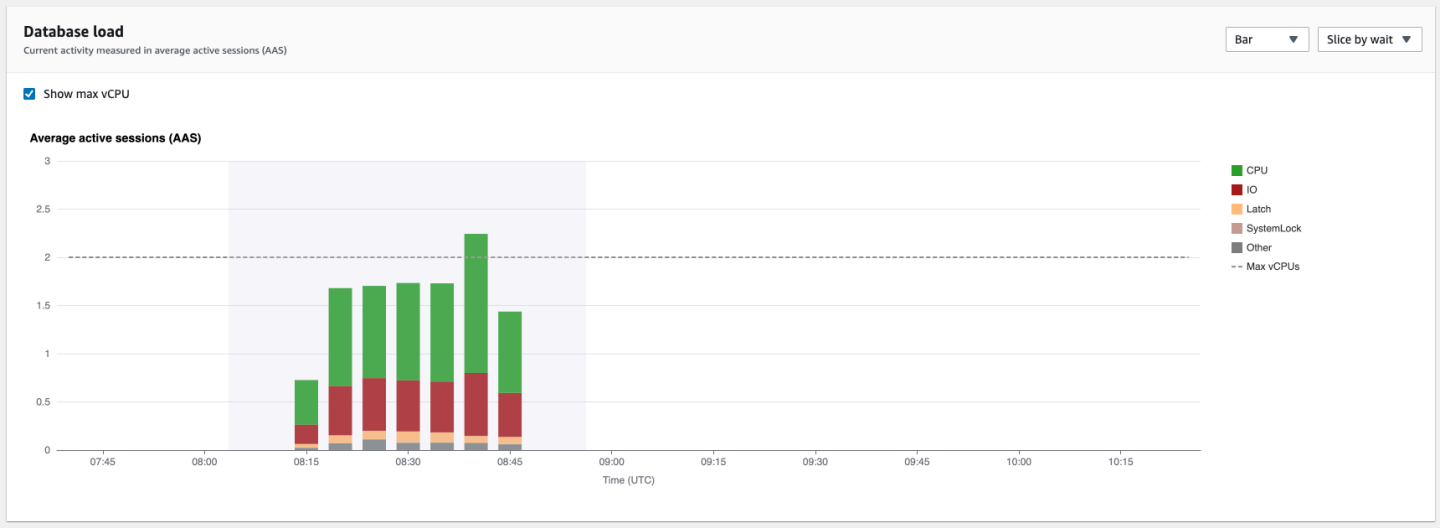
> **Note**
>
> Um die Abfrageanweisung zu kopieren oder herunterzuladen, deaktivieren Sie alle Popup-Blocker.

Das Diagramm zum Laden der Datenbank vergrößern

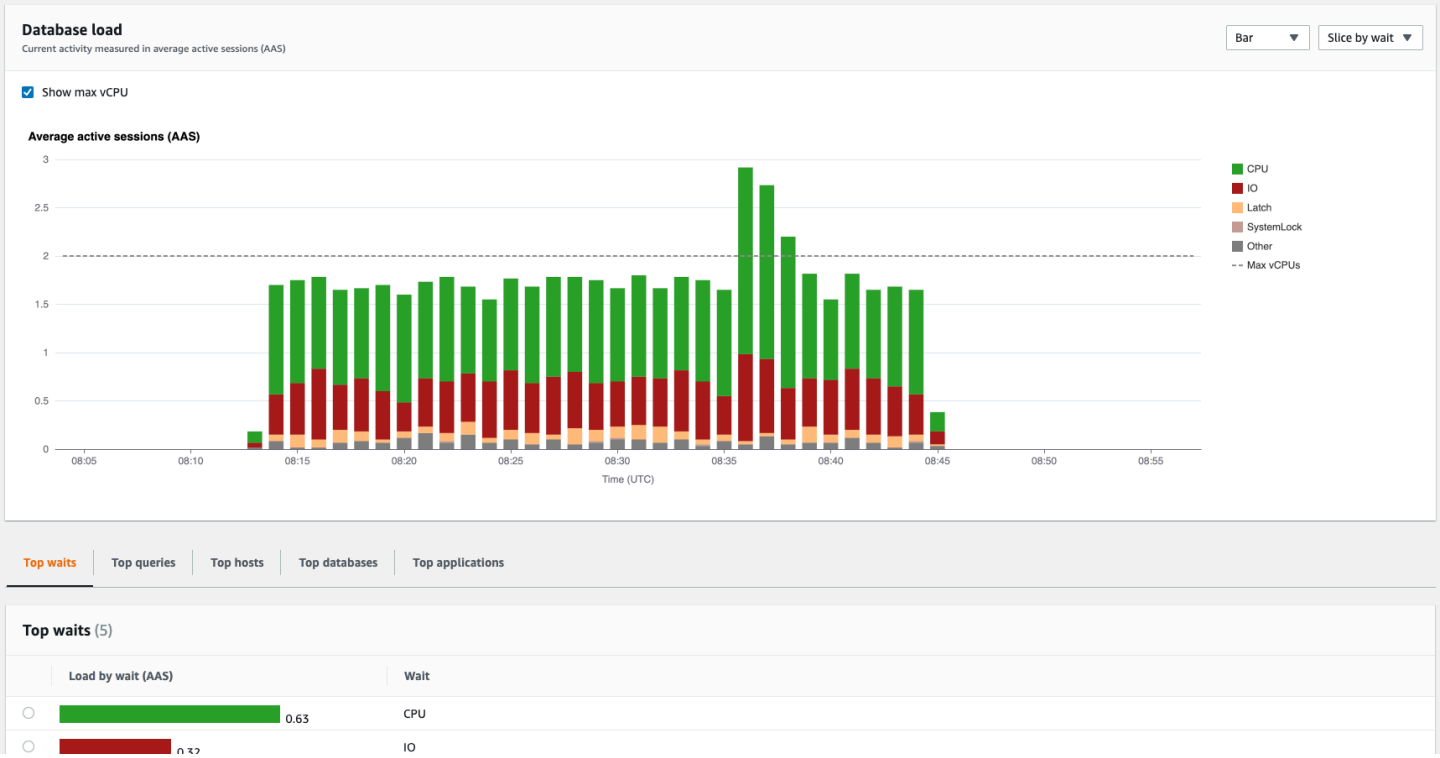
Sie können weitere Funktionen der Benutzeroberfläche von Performance Insights verwenden, um die Performance-Daten zu analysieren.

Click-and-Drag Vergrößern

In der Benutzeroberfläche von Performance Insights können Sie einen kleinen Teil des Lastdiagramms auswählen und die Details vergrößern.



Um einen Teil des Lastdiagramms zu vergrößern, wählen Sie die Startzeit und ziehen Sie mit der Maus an das Ende des gewünschten Zeitraums. Dabei wird der markierte Bereich farblich hervorgehoben. Wenn Sie die Maustaste loslassen, vergrößert das Lastdiagramm den ausgewählten Bereich, und die Tabelle mit den wichtigsten Elementen wird neu berechnet.



Abrufen von Metriken mit der Performance-Insights-API

Wenn Performance Insights aktiviert ist, bietet die API Einblicke in die Instance-Leistung Amazon CloudWatch Logs bietet die maßgebliche Quelle für verkaufte Monitoring-Metriken für AWS Services.

Performance Insights bietet eine domänenspezifische Ansicht der Datenbanklast, gemessen als durchschnittliche aktive Sitzungen (AAS). Diese Metrik erscheint API-Verbrauchern als zweidimensionaler Zeitreihendatensatz. Die Zeitdimension der Daten stellt die Datenbanklastdaten für jeden Zeitpunkt im abgefragten Zeitraum bereit. Für jeden Zeitpunkt wird die Gesamtlast bezogen auf die angeforderten Dimensionen zerlegt, z. B. `Query`, `Wait-state`, `Application` oder `Host`, gemessen zum betreffenden Zeitpunkt.

Amazon DocumentDB Performance Insights überwacht Ihre Amazon DocumentDB-DB-Instance, sodass Sie die Datenbankleistung analysieren und Fehler beheben können. Eine Möglichkeit zum Anzeigen von Performance-Insights-Daten bietet die AWS-Managementkonsole. Performance Insights stellt außerdem eine öffentliche API bereit, sodass Sie Ihre eigenen Daten abfragen können. Sie können die API für Folgendes verwenden:

- Auslagern von Daten in eine Datenbank
- Hinzufügen von Performance-Insights-Daten zu bestehenden Überwachungs-Dashboards
- Entwickeln von Überwachungstools

Um die Performance Insights-API zu verwenden, aktivieren Sie Performance Insights auf einer Ihrer Amazon DocumentDB DocumentDB-Instances. Weitere Informationen zum Aktivieren von Performance Insights finden Sie unter Aktivieren und Deaktivieren von Performance Insights. Weitere Informationen zur Performance Insights-API finden Sie in der Referenz zur Performance Insights-API.

Die Performance-Insights-API bietet die folgenden Operationen.

Performance-Insights-Aktion	AWS CLI Befehl	Description
DescribeDimensionKeys	aws pi describe-dimension-keys	Ruft die Schlüssel der Top N-Dimension für eine Metrik für einen bestimmten Zeitraum ab.
GetDimensionKeyDetails	aws pi get-dimension-key-details	Ruft die Attribute der angegebenen Dimensionsgruppe für eine DB-Instance oder Datenquelle ab. Wenn Sie beispielsweise eine Abfrage-ID angeben und die Dimensionsdetails verfügbar sind, wird der vollständige Text der Dimension `GetDimensionKeyDetails` abgerufen, die dieser ID `db.query.statement` zugeordnet ist. Dieser Vorgang ist nützlich, weil er `GetResourceMetrics` das Abrufen von umfangreichem Text in Abfrageanweisungen `DescribeDimensionKeys` nicht unterstützt.
GetResourceMetadata	aws pi get-resource-metadata	Rufen Sie die Metadaten für verschiedene Funktionen ab. Die Metadaten könnten

Performance-Insights-Aktion	AWS CLI Befehl	Description
		beispielsweise darauf hindeuten, dass eine Funktion für eine bestimmte DB-Instan ce ein- oder ausgeschaltet ist.
GetResourceMetrics	aws pi get-resource-metrics	Ruft Performance-Insights-Metriken für eine Reihe von Datenquellen über einen Zeitraum ab. Sie können spezifische Dimension sgruppen und Dimensionen bereitstellen und Aggregati on und Filterkriterien für jede Gruppe bereitstellen.
ListAvailableResou rceDimensions	aws pi list-avai lable-resource-dim ensions	Rufen Sie die Dimensionen ab, die für jeden angegebenen Metriktyp für eine bestimmte Instance abgefragt werden können.
ListAvailableResou rceMetrics	aws pi list-avai lable-resource-met rics	Rufen Sie alle verfügbaren Metriken der angegeben en Metriktypen ab, die für eine bestimmte DB-Instance abgefragt werden können.

Themen

- AWS CLI für Performance Insights
- Abrufen von Zeitreihenmetriken
- AWS CLI Beispiele für Performance Insights

AWS CLI für Performance Insights

Sie können Performance-Insights-Daten über die anzeige AWS CLI. Hilfe zu den AWS CLI -Befehlen für Performance Insights erhalten Sie durch Eingabe der folgenden Befehle an der Befehlszeile.

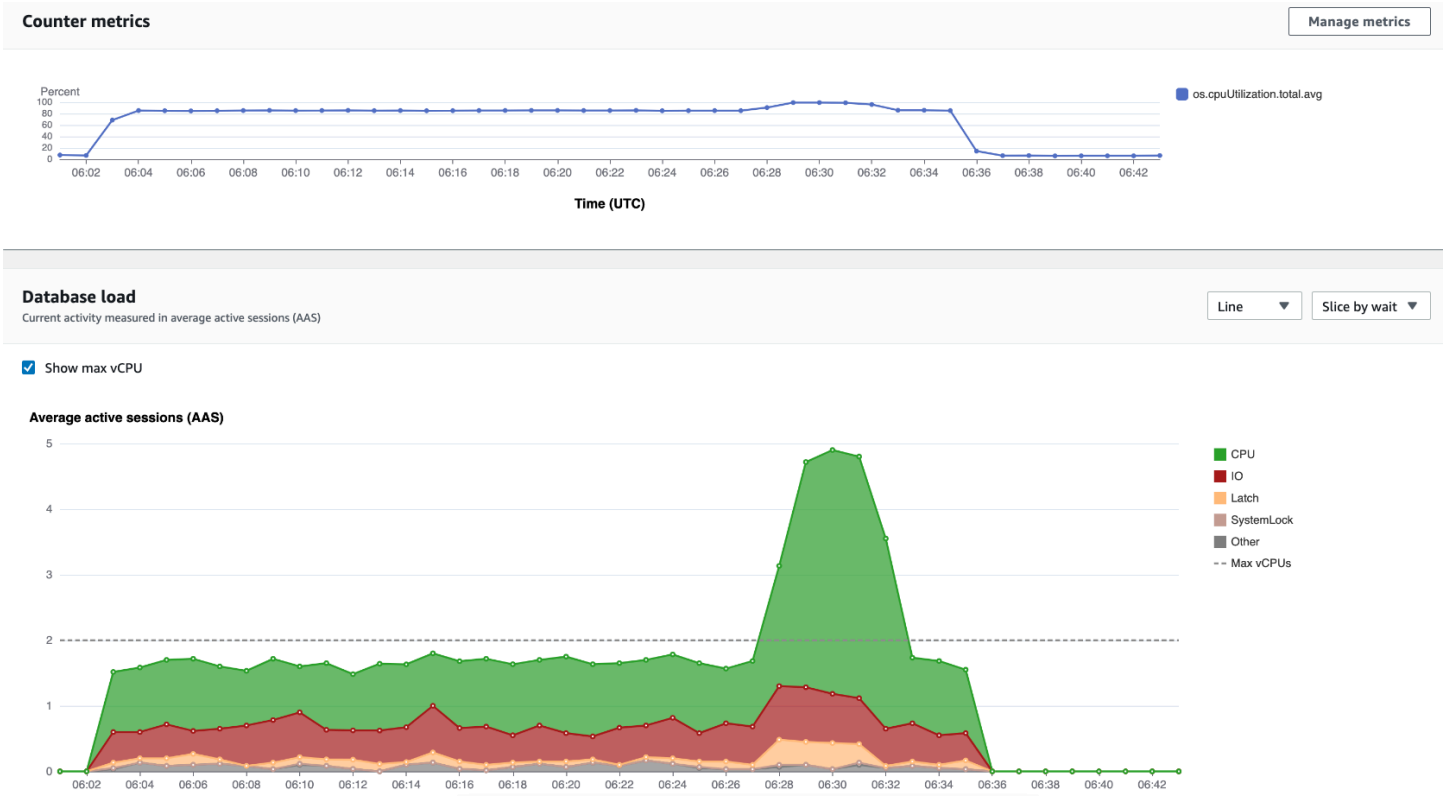
```
aws pi help
```

Falls Sie das nicht AWS CLI installiert haben, finden Sie unter Installation der AWS Befehlszeilenschnittstelle im AWS CLI Benutzerhandbuch weitere Informationen zur Installation.

Abrufen von Zeitreihenmetriken

Mit der `GetResourceMetrics`-Operation werden ein oder mehrere Zeitreihenmetriken aus den Performance Insights-Daten abgerufen. Für `GetResourceMetrics` ist eine Metrik und ein Zeitraum erforderlich, damit eine Antwort mit einer Liste von Datenpunkten zurückgegeben wird.

Zum Beispiel die AWS-Managementkonsole Verwendung, `GetResourceMetrics` um die Diagramme „Counter Metrics“ und „Database Load“ auszufüllen, wie in der folgenden Abbildung dargestellt.



Alle von zurückgegebenen Metriken`GetResourceMetrics` sind Standard-Zeitreihenmetriken, mit Ausnahme von`db.load`. Diese Metrik wird im Diagramm Database Load (Datenbanklast)

angezeigt. Die`db.load` Metrik unterscheidet sich von den anderen Zeitreihenmetriken, da Sie sie in Unterkomponenten aufteilen können, die als Dimensionen bezeichnet werden. In der vorherigen Abbildung wird `db.load` unterteilt und nach Wartezuständen gruppiert, aus denen `db.load` besteht.

> **Note**
>
> `GetResourceMetrics` kann auch die `db.sampleload`-Metrik zurückgeben, aber die `db.load`-Metrik ist in den meisten Fällen angemessen.

Informationen zu den Zählermetriken, die von `GetResourceMetrics` zurückgegeben werden, finden Sie unter Performance Insights für Zählermetriken.

Die folgenden Berechnungen werden für die Metriken unterstützt:

- Durchschnitt – Der durchschnittliche Wert für die Metrik über einen bestimmten Zeitraum. Fügen Sie dem Metriknamen `.avg` an.
- Minimum – Der minimale Wert für die Metrik über einen bestimmten Zeitraum. Fügen Sie dem Metriknamen `.min` an.
- Maximum – Der maximale Wert für die Metrik über einen bestimmten Zeitraum. Fügen Sie dem Metriknamen `.max` an.
- Summe – Die Summe der Metrikwerte über einen bestimmten Zeitraum. Fügen Sie dem Metriknamen `.sum` an.
- Beispielanzahl – Die Anzahl, wie oft die Metrik über einen bestimmten Zeitraum erfasst wurde. Fügen Sie dem Metriknamen `.sample_count` an.

Nehmen wir an, dass eine Metrik beispielsweise 300 Sekunden (5 Minuten) lang erfasst wird und dass die Metrik einmal pro Minute erfasst wird. Die Werte für jede Minute sind 1, 2, 3, 4 und 5. In diesem Fall werden die folgenden Berechnungen zurückgegeben:

- Durchschnitt – 3
- Minimum – 1
- Maximum – 5
- Summe – 15
- Beispielanzahl – 5

Hinweise zur Verwendung des `get-resource-metrics` AWS CLI Befehls finden Sie unter [get-resource-metrics].

Geben Sie für die `--metric-queries`-Option eine oder mehrere Abfragen an, um die entsprechenden Ergebnisse zu erhalten. Jede Abfrage besteht aus einem obligatorischen `Metric`- sowie optionalen `GroupBy`- und `Filter`-Parametern. Es folgt ein Beispiel für eine Spezifikation der `--metric-queries`-Option.

```
{
   "Metric": "string",
   "GroupBy": {
     "Group": "string",
     "Dimensions": ["string", ...],
     "Limit": integer
   },
   "Filter": {"string": "string"
     ...}
```

AWS CLI Beispiele für Performance Insights

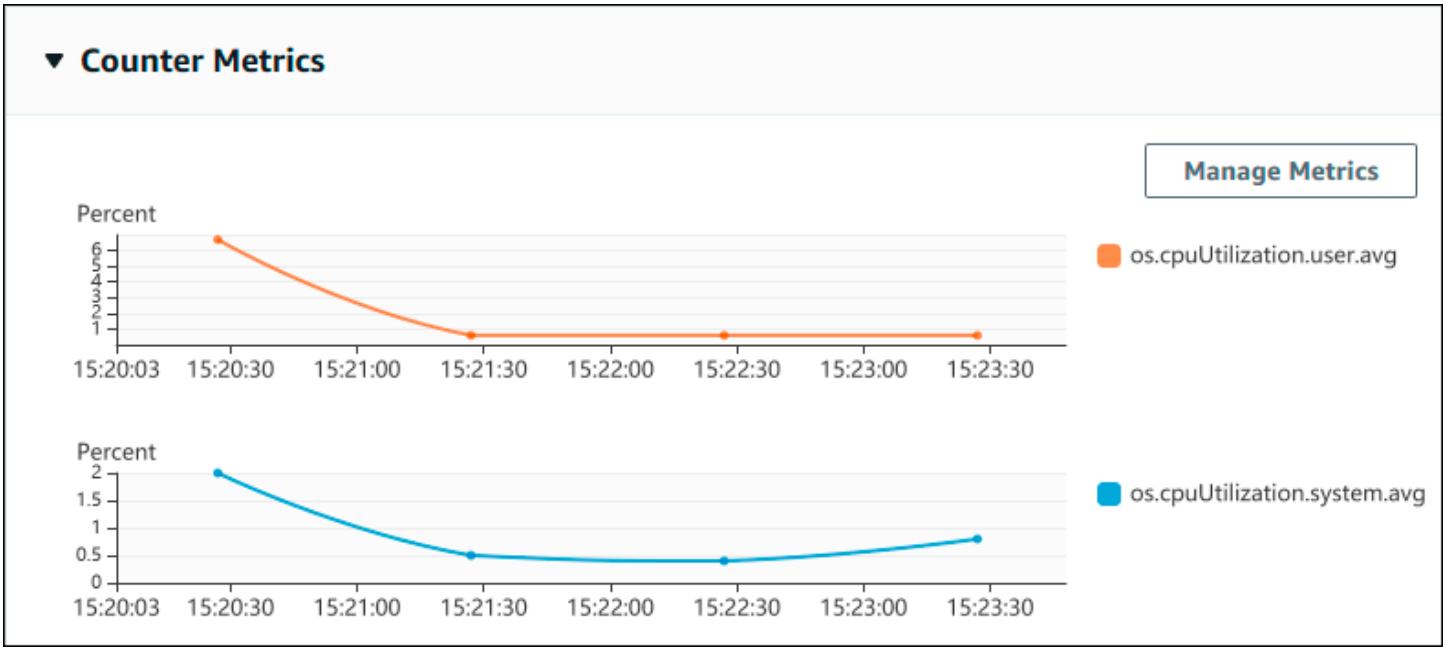
Die folgenden Beispiele zeigen, wie Sie AWS CLI for Performance Insights verwenden können.

Themen

- Abrufen von Zählermetriken
- Der DB-Lastdurchschnitt für die höchsten Wartezeiten wird abgerufen
- Der durchschnittliche DB-Ladestand für die oberste Abfrage wird abgerufen
- Abrufen des nach Query gefilterten DB-Ladedurchschnitts

Abrufen von Zählermetriken

Der folgende Screenshot zeigt zwei Zählermetriken-Diagramme in der AWS-Managementkonsole.



Das folgende Beispiel veranschaulicht, wie die Daten, die die AWS-Managementkonsole zum Erstellen der beiden Zählermetriken-Diagramme verwendet, gesammelt werden.

Für Linux, macOS oder Unix:

```
aws pi get-resource-metrics \
   --service-type DOCDB \
   --identifier db-ID \
   --start-time 2022-03-13T8:00:00Z \
   --end-time   2022-03-13T9:00:00Z \
   --period-in-seconds 60 \
   --metric-queries '[{"Metric": "os.cpuUtilization.user.avg"  },
                      {"Metric": "os.cpuUtilization.idle.avg"}]'
```

Für Windows:

```
aws pi get-resource-metrics ^
   --service-type DOCDB ^
   --identifier db-ID ^
   --start-time 2022-03-13T8:00:00Z ^
   --end-time   2022-03-13T9:00:00Z ^
   --period-in-seconds 60 ^
   --metric-queries '[{"Metric": "os.cpuUtilization.user.avg"  },
                      {"Metric": "os.cpuUtilization.idle.avg"}]'
```

Sie können einen Befehl besser lesbar gestalten, indem Sie eine Datei für die Option `--metrics-query` angeben. Im folgenden Beispiel wird eine Datei namens query.json für die Option verwendet. Die Datei enthält Folgendes.

```
[
    {
        "Metric": "os.cpuUtilization.user.avg"
    },
    {
        "Metric": "os.cpuUtilization.idle.avg"
    }
]
```

Führen Sie den folgenden Befehl aus, um die Datei zu verwenden.

Für Linux, macOS oder Unix:

```
aws pi get-resource-metrics \
   --service-type DOCDB \
   --identifier db-ID \
   --start-time 2022-03-13T8:00:00Z \
   --end-time   2022-03-13T9:00:00Z \
   --period-in-seconds 60 \
   --metric-queries file://query.json
```

Für Windows:

```
aws pi get-resource-metrics ^
   --service-type DOCDB ^
   --identifier db-ID ^
   --start-time 2022-03-13T8:00:00Z ^
   --end-time   2022-03-13T9:00:00Z ^
   --period-in-seconds 60 ^
   --metric-queries file://query.json
```

Das vorige Beispiel gibt die folgenden Werte für die Optionen an:

- `--service-type`— DOCDB für Amazon DocumentDB
- `--identifier` – Die Ressource-ID für die DB-Instance
- `--start-time` und `--end-time` – Die ISO 8601-Werte `DateTime` für den abzufragenden Zeitraum mit mehreren unterstützten Formaten

Der Abfragezeitraum beträgt eine Stunde:

- `--period-in-seconds` – `60` für eine Abfrage pro Minute
- `--metric-queries` – Ein Array mit zwei Abfragen, jeweils für nur eine Metrik.

  Der Metrikname verwendet Punkte, um die Metrik in eine sinnvolle Kategorie einzustufen, wobei das letzte Element eine Funktion ist. Im Beispiel lautet die Funktion `avg` für jede Abfrage. Wie bei Amazon CloudWatch sind die unterstützten Funktionen `min`, `max`, `total`, und `avg`.

Die Antwort sieht in etwa so aus:

```
{
    "AlignedStartTime": "2022-03-13T08:00:00+00:00",
    "AlignedEndTime": "2022-03-13T09:00:00+00:00",
    "Identifier": "db-NQF3TTMFQ3GTOKIMJODMC3KQQ4",
    "MetricList": [
        {
            "Key": {
                "Metric": "os.cpuUtilization.user.avg"
            },
            "DataPoints": [
                {
                    "Timestamp": "2022-03-13T08:01:00+00:00", //Minute1
                    "Value": 3.6
                },
                {
                    "Timestamp": "2022-03-13T08:02:00+00:00", //Minute2
                    "Value": 2.6
                },
                //.... 60 datapoints for the os.cpuUtilization.user.avg metric
        {
            "Key": {
                "Metric": "os.cpuUtilization.idle.avg"
            },
            "DataPoints": [
                {
                    "Timestamp": "2022-03-13T08:01:00+00:00",
                    "Value": 92.7
                },
                {
                    "Timestamp": "2022-03-13T08:02:00+00:00",
                    "Value": 93.7
```

```
                },
                //.... 60 datapoints for the os.cpuUtilization.user.avg metric
            ]
        }
    ] //end of MetricList
} //end of response
```

Die Antwort enthält Werte für `Identifier`, `AlignedStartTime` und `AlignedEndTime`. Bei einem `--period-in-seconds`-Wert von `60` wurden Start- und Endzeiten auf die Minute ausgerichtet. Wenn der `--period-in-seconds`-Wert `3600` lautet, werden Start- und Endzeiten auf die Stunde ausgerichtet.

Die `MetricList` in der Antwort enthält eine Reihe von Einträgen, und zwar jeweils mit einem `Key`- und einem `DataPoints`-Eintrag. Jeder `DataPoint` verfügt über einen `Timestamp` und einen `Value`. Jede `Datapoints`-Liste enthält 60 Datenpunkte, da die Abfragen eine Stunde lang jede Minute Daten abfragen, und zwar mit den Werten `Timestamp1/Minute1`, `Timestamp2/Minute2` usw. bis `Timestamp60/Minute60`.

Da sich die Abfrage auf zwei verschiedene Zählermetriken bezieht, enthält die -Antwort zwei Element `MetricList`.

Der DB-Lastdurchschnitt für die höchsten Wartezeiten wird abgerufen

Das folgende Beispiel ist dieselbe Abfrage, die AWS-Managementkonsole verwendet wird, um ein gestapeltes Flächenliniendiagramm zu generieren. In diesem Beispiel wird der Wert `db.load.avg` für die letzte Stunde abgerufen, wobei die Auslastung nach den sieben höchsten Wartezuständen aufgeteilt wird. Der Befehl ist mit dem Befehl unter identisc Abrufen von Zählermetriken. Die Datei query.json enthält hingegen Folgendes.

```
[
    {
        "Metric": "db.load.avg",
        "GroupBy": { "Group": "db.wait_state", "Limit": 7 }
    }
]
```

Führen Sie den folgenden Befehl aus.

Für Linux, macOS oder Unix:

```
aws pi get-resource-metrics \
```

```
   --service-type DOCDB \
   --identifier db-ID \
   --start-time 2022-03-13T8:00:00Z \
   --end-time   2022-03-13T9:00:00Z \
   --period-in-seconds 60 \
   --metric-queries file://query.json
```

Für Windows:

```
aws pi get-resource-metrics ^
   --service-type DOCDB ^
   --identifier db-ID ^
   --start-time 2022-03-13T8:00:00Z ^
   --end-time   2022-03-13T9:00:00Z ^
   --period-in-seconds 60 ^
   --metric-queries file://query.json
```

Das Beispiel gibt die Metrik für `db.load.avg` und a `GroupBy` der sieben wichtigsten Wartezustände an. Einzelheiten zu gültigen Werten für dieses Beispiel finden Sie DimensionGroupin der Performance Insights API-Referenz.

Die Antwort sieht in etwa so aus:

```
{
    "AlignedStartTime": "2022-04-04T06:00:00+00:00",
    "AlignedEndTime": "2022-04-04T06:15:00+00:00",
    "Identifier": "db-NQF3TTMFQ3GTOKIMJODMC3KQQ4",
    "MetricList": [
        {//A list of key/datapoints
            "Key": {
                //A Metric with no dimensions. This is the total db.load.avg
                "Metric": "db.load.avg"
            },
            "DataPoints": [
                //Each list of datapoints has the same timestamps and same number of
 items
                {
                    "Timestamp": "2022-04-04T06:01:00+00:00",//Minute1
                    "Value": 0.0
                },
                {
                    "Timestamp": "2022-04-04T06:02:00+00:00",//Minute2
```

```
                    "Value": 0.0
                },
                //... 60 datapoints for the total db.load.avg key
                ]
        },
        {
            "Key": {
                //Another key. This is db.load.avg broken down by CPU
                "Metric": "db.load.avg",
                "Dimensions": {
                    "db.wait_state.name": "CPU"
                }
            },
            "DataPoints": [
                {
                    "Timestamp": "2022-04-04T06:01:00+00:00",//Minute1
                    "Value": 0.0
                },
                {
                    "Timestamp": "2022-04-04T06:02:00+00:00",//Minute2
                    "Value": 0.0
                },
                //... 60 datapoints for the CPU key
            ]
        },//... In total we have 3 key/datapoints entries, 1) total, 2-3) Top Wait
 States
    ] //end of MetricList
} //end of response
```

In dieser Antwort gibt es drei Einträge in der`MetricList`. Es gibt einen Eintrag für die Gesamtzahl `db.load.avg` und jeweils drei Einträge für die `db.load.avg` Aufteilung nach einem der drei höchsten Wartezustände. Da es eine Gruppierungsdimension gab (im Gegensatz zum ersten Beispiel), muss es für jede Gruppierung der Metrik einen Schlüssel geben. Für jede Metrik kann nicht nur ein Schlüssel vorhanden sein, wie im Anwendungsfall der Basiszählermetrik.

Der durchschnittliche DB-Ladestand für die oberste Abfrage wird abgerufen

Das folgende Beispiel `db.wait_state` gruppiert nach den 10 wichtigsten Abfrageanweisungen. Es gibt zwei verschiedene Gruppen für Abfrageanweisungen:

- `db.query`— Die vollständige Abfrageanweisung, wie `{"find":"customers","filter": {"FirstName":"Jesse"},"sort":{"key":{"$numberInt":"1"}}}`

- `db.query_tokenized`— Die tokenisierte Abfrageanweisung, z. B. `{"find":"customers","filter":{"FirstName":"?"},"sort":{"key": {"$numberInt":"?"}},"limit":{"$numberInt":"?"}}`

Bei der Analyse der Datenbankleistung kann es nützlich sein, Abfrageanweisungen, die sich nur durch ihre Parameter unterscheiden, als ein Logikelement zu betrachten. In diesem Fall können Sie `db.query_tokenized` beim Abfragen verwenden. Vor allem, wenn Sie daran interessiert sind`explain()`, ist es manchmal sinnvoller, vollständige Abfrageanweisungen mit Parametern zu untersuchen. Es besteht eine Beziehung zwischen tokenisierten und vollständigen Abfragen, wobei mehrere vollständige Abfragen (untergeordnete Abfragen) unter derselben tokenisierten Abfrage (übergeordnete Abfrage) gruppiert sind.

Der Befehl in diesem Beispiel ähnelt dem Befehl unter Der DB-Lastdurchschnitt für die höchsten Wartezeiten wird abgerufen. Die Datei query.json enthält hingegen Folgendes.

```
[
    {
        "Metric": "db.load.avg",
        "GroupBy": { "Group": "db.query_tokenized", "Limit": 10 }
    }
]
```

Im folgenden Beispiel wird verwende `db.query_tokenized`.

Für Linux, macOS oder Unix:

```
aws pi get-resource-metrics \
   --service-type DOCDB \
   --identifier db-ID \
   --start-time 2022-03-13T8:00:00Z \
   --end-time   2022-03-13T9:00:00Z \
   --period-in-seconds 3600 \
   --metric-queries file://query.json
```

Für Windows:

```
aws pi get-resource-metrics ^
   --service-type DOCDB ^
   --identifier db-ID ^
```

```
    --start-time 2022-03-13T8:00:00Z ^
    --end-time   2022-03-13T9:00:00Z  ^
    --period-in-seconds 3600 ^
    --metric-queries file://query.json
```

In diesem Beispiel werden Abfragen über eine Stunde mit einem Zeitraum von einer Minute in Sekunden abgefragt.

Das Beispiel gibt die Metrik für `db.load.avg` und einen `GroupBy` der sieben höchsten Wartezustände an. Einzelheiten zu gültigen Werten für dieses Beispiel finden Sie DimensionGroupin der Performance Insights API-Referenz.

Die Antwort sieht in etwa so aus:

```
{
    "AlignedStartTime": "2022-04-04T06:00:00+00:00",
    "AlignedEndTime": "2022-04-04T06:15:00+00:00",
    "Identifier": "db-NQF3TTMFQ3GTOKIMJODMC3KQQ4",
    "MetricList": [
        {//A list of key/datapoints
            "Key": {
                "Metric": "db.load.avg"
            },
            "DataPoints": [
                //... 60 datapoints for the total db.load.avg key
                ]
        },
               {
            "Key": {//Next key are the top tokenized queries
                "Metric": "db.load.avg",
                "Dimensions": {
                    "db.query_tokenized.db_id": "pi-1064184600",
                    "db.query_tokenized.id": "77DE8364594EXAMPLE",
                    "db.query_tokenized.statement": "{\"find\":\"customers\",\"filter
\":{\"FirstName\":\"?\"},\"sort\":{\"key\":{\"$numberInt\":\"?\"}},\"limit\"
:{\"$numberInt\":\"?\"},\"$db\":\"myDB\",\"$readPreference\":{\"mode\":\"primary\"}}"
                }
            },
            "DataPoints": [
            //... 60 datapoints
            ]
        },
        // In total 11 entries, 10 Keys of top tokenized queries, 1 total key
```

```
    ] //End of MetricList
} //End of response
```

Diese Antwort enthält 11 Einträge in der Abfrage `MetricList` (insgesamt 1, 10 am häufigsten tokenisierte Abfragen), wobei jeder Eintrag 24 Einträge pro Stunde enthält. `DataPoints`

Bei tokenisierten Abfragen gibt es drei Einträge in jeder Dimensionsliste:

- `db.query_tokenized.statement`— Die tokenisierte Abfrageanweisung.
- `db.query_tokenized.db_id` — Die synthetische ID, die Performance Insights für Sie generiert. In diesem Beispiel wird die synthetische ID `pi-1064184600` zurückgegeben.
- `db.query_tokenized.id` – Die ID der Abfrage innerhalb von Performance-Insights.

  In der AWS-Managementkonsole wird diese ID als Support-ID bezeichnet. Es trägt diesen Namen, weil es sich bei der ID um Daten handelt, die der AWS Support untersuchen kann, um Ihnen bei der Behebung eines Problems mit Ihrer Datenbank zu helfen. AWS nimmt die Sicherheit und den Schutz Ihrer Daten sehr ernst, und fast alle Daten werden verschlüsselt zusammen mit Ihren gespeichert AWS KMS key. Daher AWS kann niemand im Inneren diese Daten einsehen. Im vorherigen Beispiel wird sowohl `tokenized.statement` als auch `tokenized.db_id` verschlüsselt gespeichert. Wenn Sie ein Problem mit Ihrer Datenbank haben, kann Ihnen der AWS Support unter Angabe der Support-ID weiterhelfen.

Beim Abfragen empfiehlt es sich ggf., eine `Group` in `GroupBy` anzugeben. Für eine präzisere Kontrolle der Daten, die zurückgegeben werden, sollten Sie allerdings die Dimensionsliste angeben. Wenn z. B. lediglich eine `db.query_tokenized.statement` erforderlich ist, kann der query.json-Datei ein `Dimensions`-Attribut hinzugefügt werden.

```
[
    {
        "Metric": "db.load.avg",
        "GroupBy": {
            "Group": "db.query_tokenized",
            "Dimensions":["db.query_tokenized.statement"],
            "Limit": 10
        }
    }
]
```

Abrufen des nach Query gefilterten DB-Ladedurchschnitts

Die entsprechende API-Abfrage in diesem Beispiel ähnelt dem Befehl unter Der durchschnittliche DB-Ladestand für die oberste Abfrage wird abgerufen. Die Datei query.json enthält hingegen Folgendes.

```
[
 {
        "Metric": "db.load.avg",
        "GroupBy": { "Group": "db.wait_state", "Limit": 5  },
        "Filter": { "db.query_tokenized.id": "AKIAIOSFODNN7EXAMPLE" }
    }
]
```

In dieser Antwort werden alle Werte entsprechend dem Beitrag der tokenisierten Abfrage AKIAIOSFODNN7EXAMPLE gefiltert, die in der Datei query.json angegeben ist. Die Schlüssel haben möglicherweise auch eine andere Reihenfolge als eine Abfrage ohne Filter, da sich die gefilterte Abfrage auf die fünf Wartezustände mit der höchsten Wartezeit ausgewirkt hat.

CloudWatch Amazon-Metriken für Performance Insights

Performance Insights veröffentlicht automatisch Metriken auf Amazon CloudWatch. Dieselben Daten können von Performance Insights abgefragt werden, aber wenn die Metriken vorhanden sind, ist es einfach, Alarme hinzuzufügen CloudWatch . CloudWatch Die Metriken können auch leicht zu vorhandenen CloudWatch-Dashboards hinzugefügt werden.

Metrik	Beschreibung
DBLoad	Die Anzahl der aktiven Sitzungen für Amazon DocumentDB. In der Regel sind Sie an den Daten für die durchschnittliche Anzahl der aktiven Sitzungen interessiert. Diese Daten werden in Performance Insights als `db.load.avg` abgefragt.
DBLoadCPU	Die Anzahl der aktiven Sitzungen, bei denen der Wartestatustyp CPU ist. In Performan ce Insights werden diese Daten abgefragt alsdb.load.avg , gefiltert nach dem Wartestatustyp. CPU

Metrik	Beschreibung
DBLoadNonCPU	Die Anzahl der aktiven Sitzungen, bei denen der Wartestatustyp nicht CPU ist.

> **Note**
>
> Diese Metriken werden CloudWatch nur veröffentlicht, wenn die DB-Instance ausgelastet ist.

Sie können diese Metriken mithilfe der CloudWatch Konsole AWS CLI, der oder der CloudWatch API untersuchen.

Um beispielsweise die statistischen Daten zur Metrik `DBLoad` anzuzeigen, führen Sie den Befehl get-metric-statistics aus.

```
aws cloudwatch get-metric-statistics \
    --region ap-south-1 \
    --namespace AWS/DocDB \
    --metric-name DBLoad  \
    --period 360 \
    --statistics Average \
    --start-time 2022-03-14T8:00:00Z \
    --end-time 2022-03-14T9:00:00Z \
    --dimensions Name=DBInstanceIdentifier,Value=documentdbinstance
```

Dieses Beispiel generiert eine Ausgabe wie die folgende.

```
{
    "Datapoints": [
        {
            "Timestamp": "2022-03-14T08:42:00Z",
            "Average": 1.0,
            "Unit": "None"
        },
        {
            "Timestamp": "2022-03-14T08:24:00Z",
            "Average": 2.0,
            "Unit": "None"
        },
```

```
        {
            "Timestamp": "2022-03-14T08:54:00Z",
            "Average": 6.0,
            "Unit": "None"
        },
        {
            "Timestamp": "2022-03-14T08:36:00Z",
            "Average": 5.7,
            "Unit": "None"
        },
        {
            "Timestamp": "2022-03-14T08:06:00Z",
            "Average": 4.0,
            "Unit": "None"
        },
        {
            "Timestamp": "2022-03-14T08:00:00Z",
            "Average": 5.2,
            "Unit": "None"
        }
    ],
    "Label": "DBLoad"
}
```


Sie können die mathematische `DB_PERF_INSIGHTS` Metrikfunktion in der CloudWatch Konsole verwenden, um Zählermetriken von Amazon DocumentDB Performance Insights abzufragen. Die `DB_PERF_INSIGHTS` Funktion beinhaltet auch die `DBLoad` Metrik in Intervallen unter einer Minute. Sie können CloudWatch Alarme für diese Messwerte einrichten. Weitere Informationen zum Erstellen eines Alarms finden Sie unter Erstellen eines Alarms für Performance Insights Insights-Zählermetriken aus einer AWS Datenbank.

Weitere Informationen zu CloudWatch finden Sie unter Was ist Amazon CloudWatch? im CloudWatch Amazon-Benutzerhandbuch.

Performance Insights für Zählermetriken

Zählermetriken sind Betriebssystemmetriken im Performance Insights Insights-Dashboard. Um Leistungsprobleme zu identifizieren und zu analysieren, können Sie Zählermetriken mit der DB-Last korrelieren.

Performance-Insights-Betriebssystemzähler

Die folgenden Betriebssystemindikatoren sind mit Amazon DocumentDB Performance Insights verfügbar.

Zähler	Typ	Metrik
Aktiv	memory	os.memory.active
buffers	memory	os.memory.buffers
cached	memory	os.memory.cached
dirty	memory	os.memory.dirty
free	memory	os.memory.free
inactive	memory	os.memory.inactive
mapped	memory	os.memory.mapped
pageTables	memory	os.memory.pageTables
slab	memory	os.memory.slab
total	memory	os.memory.total
writeback	memory	os.memory.writeback
idle	cpuUtilization	os.cpu Utilization.idle
system	cpuUtilization	os.cpu Utilization.system
total	cpuUtilization	os.cpu Utilization.total
user	cpuUtilization	os.cpu Utilization.user
wait	cpuUtilization	os.cpu Utilization.wait
one	laden AverageMinute	os.load AverageMinute.one
fifteen	laden AverageMinute	os.load AverageMinute.fifteen

Zähler	Typ	Metrik
fünf	laden AverageMinute	os.load AverageMinute.five
cached	swap	os.swap.cached
free	swap	os.swap.free
in	swap	os.swap.in
out	swap	os.swap.out
total	swap	os.swap.total
rx	network	os.network.rx
tx	network	os.network.tx
numVCPUs	general	os.general.numVCPUs

Zero-ETL Integration mit Amazon OpenSearch Service

Topics

- Amazon OpenSearch Service als Ziel
- Einschränkungen

Amazon OpenSearch Service als Ziel

OpenSearch Die Serviceintegration mit Amazon DocumentDB ermöglicht es Ihnen, Volllast- und Änderungsdatenereignisse an OpenSearch Domains zu streamen. Die Aufnahmeinfrastruktur wird als OpenSearch Ingestion-Pipelines gehostet und bietet einen hochskalierten Mechanismus mit geringer Latenz, um kontinuierlich Daten aus Amazon DocumentDB-Sammlungen zu streamen.

Bei Volllast extrahiert die Zero-ETL-Integration zunächst historische Volllastdaten, um sie mithilfe einer Aufnahme-Pipeline zu extrahieren. OpenSearch Sobald die Volllastdaten aufgenommen wurden, beginnen die OpenSearch Aufnahme-Pipelines mit dem Lesen von Daten aus Amazon DocumentDB-Change-Streams und catch schließlich auf, um die Datenkonsistenz zwischen Amazon DocumentDB und nahezu in Echtzeit aufrechtzuerhalten. OpenSearch OpenSearch speichert Dokumente in Indizes. Eingehende Daten aus Amazon DocumentDB-Sammlungen können entweder an einen Index gesendet oder in verschiedene Indizes partitioniert werden. Ingestion-Pipelines synchronisieren alle Erstellungs-, Aktualisierungs- und Löschereignisse in einer Amazon DocumentDB-Sammlung als entsprechendes Erstellen, Aktualisieren und Löschen von OpenSearch Dokumenten, um beide Datensysteme synchron zu halten. Erfassungspipelines können so konfiguriert werden, dass sie Daten aus einer Sammlung lesen und in einen Index schreiben oder Daten aus einer Sammlung lesen und bedingt an mehrere Indizes weiterleiten.

Ingestion-Pipelines können so konfiguriert werden, dass sie Daten von Amazon DocumentDB zu Amazon Service streamen, indem Sie: OpenSearch

- Nur Volllast
- Stream-Change-Stream-Ereignisse von Amazon DocumentDB ohne Volllast streamen
- Volllast, gefolgt von Change-Streams aus Amazon DocumentDB

Gehen Sie wie folgt vor, um Ihre Aufnahme-Pipeline einzurichten:

Schritt 1: Amazon OpenSearch Service-Domain oder OpenSearch serverlose Sammlung erstellen

Eine Amazon OpenSearch Service-Erfassung mit entsprechenden Berechtigungen zum Lesen von Daten ist erforderlich. Informationen zum Erstellen einer Sammlung finden Sie unter Erste Schritte mit Amazon OpenSearch Service oder Erste Schritte mit Amazon OpenSearch Serverless im Amazon OpenSearch Service Developer Guide. Informationen zum Erstellen einer OpenSearch AIM-Rolle mit den richtigen Berechtigungen für den Zugriff auf Schreibdaten für die Sammlung oder Domain finden Sie unter Amazon Ingestion im Amazon OpenSearch Service Developer Guide.

Schritt 2: Change-Streams auf dem Amazon DocumentDB-Cluster aktivieren

Stellen Sie sicher, dass Change-Streams für die erforderlichen Sammlungen im Amazon DocumentDB-Cluster aktiviert sind. Weitere Informationen finden Sie unter Change-Streams mit Amazon DocumentDB verwenden.

Schritt 3: Richten Sie die Pipeline-Rolle mit Schreibberechtigungen für den Amazon S3 S3-Bucket und die Zieldomäne oder Sammlung ein

Nachdem Sie Ihre Amazon DocumentDB-Sammlung erstellt und den Change-Stream aktiviert haben, richten Sie die Pipeline-Rolle ein, die Sie in Ihrer Pipeline-Konfiguration verwenden möchten, und fügen Sie der Rolle die folgenden Berechtigungen hinzu:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "allowReadAndWriteToS3ForExport",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:AbortMultipartUpload",
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Resource": [
```

```
                "arn:aws:s3:::my-bucket/export/*"
            ]
        }
    ]
}
```

Damit eine OpenSearch Pipeline Daten in eine Domain schreiben kann, muss die OpenSearch Domain 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::{your-account-id}:role/{pipeline-role}"
      },
      "Action": ["es:DescribeDomain", "es:ESHttp*"],
      "Resource": "arn:aws:es:{region}:{your-account-id}:domain/{domain-name}/*"
    }
  ]
}
```

Schritt 4: Fügen Sie die Berechtigungen hinzu, die für die zu erstellende Pipeline-Rolle erforderlich sind X-ENI

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:*:420497401461:network-interface/*",
                "arn:aws:ec2:*:420497401461:subnet/*",
                "arn:aws:ec2:*:420497401461: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" }
            }
        }
    ]
}
```

Schritt 5: Erstellen Sie die Pipeline

Konfigurieren Sie eine OpenSearch Aufnahme-Pipeline mit Amazon DocumentDB als Quelle. Bei dieser Beispiel-Pipeline-Konfiguration wird davon ausgegangen, dass ein Mechanismus zum Abrufen von Change-Streams verwendet wird. Weitere Informationen finden Sie unter Verwenden einer OpenSearch Ingestion-Pipeline mit Amazon DocumentDB im Amazon OpenSearch Service Developer Guide.

Einschränkungen

Die folgenden Einschränkungen gelten für die Amazon DocumentDB OpenSearch DocumentDB-Integration:

- Pro Pipeline wird nur eine Amazon DocumentDB-Sammlung als Quelle unterstützt.
- Cross-region Die Datenaufnahme wird nicht unterstützt. Ihr Amazon DocumentDB-Cluster und Ihre OpenSearch Domain müssen sich in derselben AWS Region befinden.
- Cross-account Die Datenaufnahme wird nicht unterstützt. Ihr Amazon DocumentDB-Cluster und Ihre OpenSearch Ingestion-Pipeline müssen sich im selben Konto befinden. AWS
- Elastische Amazon DocumentDB-Cluster werden nicht unterstützt. Es werden nur auf Amazon DocumentDB DocumentDB-Instanzen basierende Cluster unterstützt.
- Stellen Sie sicher, dass für den Amazon DocumentDB-Cluster die Authentifizierung mithilfe von AWS Geheimnissen aktiviert ist. AWS Geheimnisse sind der einzige unterstützte Authentifizierungsmechanismus.
- Die bestehende Pipeline-Konfiguration kann nicht aktualisiert werden, um Daten aus einer anderen Datenbank oder and/or einer anderen Sammlung aufzunehmen. Um den Namen der and/or Datenbanksammlung einer Pipeline zu aktualisieren, müssen Sie eine neue Pipeline erstellen.

Serverloses Verwenden von Amazon DocumentDB

Amazon DocumentDB serverless ist eine On-Demand-Konfiguration mit auto Skalierung, die die Prozesse der dynamischen Anpassung der Kapazität Ihrer Amazon DocumentDB DocumentDB-Datenbank an die Anwendungsnachfrage automatisiert. Ihnen werden nur die Ressourcen in Rechnung gestellt, die Ihre Cluster verbrauchen. Somit kann DocumentDB serverless Ihnen helfen, Ihr Budget einzuhalten und zu vermeiden, für Computerressourcen zu bezahlen, die Sie nicht nutzen.

Diese Art der Automatisierung ist besonders nützlich für Umgebungen mit sehr variablen und unvorhersehbaren Workloads, wie z. B. Mehrmandantendatenbanken, verteilte Datenbanken sowie Entwicklungs- und Testsysteme.

Topics

- Anwendungsfälle für serverlose DocumentDB
- Vorteile von Amazon DocumentDB serverlos
- So funktioniert Amazon DocumentDB serverless
- Anforderungen und Einschränkungen für DocumentDB serverless
- Einen Cluster erstellen, der Amazon DocumentDB serverless verwendet
- Migration zu Amazon DocumentDB serverlos
- Serverlose Verwaltung von Amazon DocumentDB
- Beschränkungen für serverlose Amazon DocumentDB DocumentDB-Instances
- Serverlose Skalierungskonfiguration von Amazon DocumentDB
- Serverlose Überwachung von Amazon DocumentDB

Anwendungsfälle für serverlose DocumentDB

Sowohl von Amazon DocumentDB bereitgestellte Cluster als auch DocumentDB serverless unterstützen viele Arten von Datenbank-Workloads, von Entwicklungs- und Testumgebungen bis hin zu den anspruchsvollsten, geschäftskritischen Anwendungen, die eine hohe Skalierbarkeit und Verfügbarkeit erfordern. DocumentDB serverless erweitert die Workloads der Kunden jedoch um eine weitere Dimension, nämlich die Fähigkeit, Websites und Anwendungen mit unvorhersehbaren Workloads zu unterstützen.

DocumentDB serverless ist besonders nützlich für die folgenden Anwendungsfälle:

- Variable Workloads — Sie führen Workloads aus, bei denen die Aktivität plötzlich und unvorhersehbar zunimmt. Ein Beispiel dafür ist eine Verkehrs-Website, für die Aktivitätsspitzen entstehen, wenn es zu regnen beginnt. Eine andere ist eine E-Commerce-Website mit erhöhtem Datenverkehr, wenn Sie Verkaufs- oder Sonderaktionen anbieten. Mit DocumentDB serverless skaliert Ihre Datenbank automatisch die Kapazität, um den Anforderungen der Spitzenlast der Anwendung gerecht zu werden, und wird wieder herunterskaliert, wenn der Aktivitätsschub vorbei ist. Mit DocumentDB serverless müssen Sie keine Spitzen- oder Durchschnittskapazitäten mehr bereitstellen. Sie können eine obere Kapazitätsgrenze angeben, um die schlimmste Situation zu bewältigen. Diese Kapazität wird nur genutzt, wenn sie benötigt wird.
  - Die Granularität der Skalierung in DocumentDB serverless hilft Ihnen dabei, die Kapazität genau an die Anforderungen Ihrer Datenbank anzupassen. Für einen bereitgestellten Cluster erfordert die Skalierung das Hinzufügen einer ganz neuen Instanz. DocumentDB serverless kann eine halbe DCU hinzufügen, wenn nur etwas mehr Kapazität benötigt wird. Je nach der zusätzlichen Kapazität, die zur Bewältigung einer erhöhten Arbeitslast erforderlich ist, können 0,5, 1, 1,5, 2 oder weitere halbe DCUs hinzugefügt werden. Außerdem können 0,5, 1, 1,5, 2 oder weitere halbe DCUs entfernt werden, wenn die Arbeitslast sinkt und diese Kapazität nicht mehr benötigt wird.
- Multi-tenant Anwendungen — Mit DocumentDB serverless müssen Sie die Datenbankkapazität nicht für jede Anwendung in Ihrer Flotte einzeln verwalten. DocumentDB serverless verwaltet individuelle Datenbankkapazitäten für Sie.
  - Sie können einen Cluster für jeden Mandanten erstellen. Auf diese Weise können Sie Funktionen wie Klonen und Snapshot-Wiederherstellung verwenden, um die Hochverfügbarkeit und die Notfallwiederherstellung für jeden Mandanten entsprechend zu verbessern.
  - Jeder Mandant kann je nach Tageszeit, Jahreszeit, Werbeveranstaltungen usw. bestimmte Perioden mit hoher und geringer Aktivität haben. Jeder Cluster kann einen großen Kapazitätsbereich aufweisen. Auf diese Weise fallen für Cluster mit geringer Aktivität nur minimale Instanzgebühren an. Jeder Cluster kann schnell hochskaliert werden, um Perioden mit hoher Aktivität zu bewältigen.
- Neue Anwendungen — Sie stellen eine neue Anwendung bereit und sind sich nicht sicher, welche Instance-Größe Sie benötigen. Wenn Sie DocumentDB serverless verwenden, können Sie einen Cluster mit einer oder mehreren Instanzen einrichten und die Datenbank automatisch an die Kapazitätsanforderungen Ihrer Anwendung anpassen lassen.
- Mixed-use Anwendungen — Nehmen wir an, Sie haben eine OLTP-Anwendung (Online Transaction Processing), aber Sie erleben regelmäßig Spitzenwerte im Abfrageverkehr. Indem Sie Upgrade-Stufen für die serverlosen DocumentDB-Instances in einem Cluster angeben, können

Sie Ihren Cluster so konfigurieren, dass die Reader-Instances unabhängig von der Writer-Instanz skaliert werden können, um die zusätzliche Last zu bewältigen. Wenn der Nutzungsanstieg nachlässt, werden die Reader-Instances wieder herunterskaliert, um sie an die Kapazität der Writer-Instanz anzupassen.

- Kapazitätsplanung — Nehmen wir an, dass Sie in der Regel Ihre Datenbankkapazität anpassen oder die optimale Datenbankkapazität für Ihre Arbeitslast überprüfen, indem Sie die Instance-Klassen aller Instances in einem Cluster ändern. Mit DocumentDB serverless können Sie diesen administrativen Aufwand vermeiden. Sie können die entsprechende Mindest- und Höchstkapazität ermitteln, indem Sie den Workload ausführen und überprüfen, wie stark die Instanzen tatsächlich skalieren.
  - Sie können bestehende Instanzen von bereitgestellt zu DocumentDB serverlos oder von DocumentDB serverlos zu bereitgestellt ändern. In solchen Fällen müssen Sie keinen neuen Cluster oder eine neue Instanz erstellen.
- Entwicklung und Testen — Neben der Ausführung Ihrer anspruchsvollsten Anwendungen können Sie DocumentDB auch serverlos für Entwicklungs- und Testumgebungen verwenden. Mit DocumentDB serverless können Sie Instanzen mit einer niedrigen Mindestkapazität erstellen, anstatt burstable db.t*-Instanzklassen zu verwenden. Sie können die maximale Kapazität so hoch festlegen, dass diese Instanzen trotzdem umfangreiche Workloads ausführen können, ohne dass der Arbeitsspeicher knapp wird. Wenn die Datenbank nicht verwendet wird, werden alle Instanzen herunterskaliert, um unnötige Gebühren zu vermeiden.

Serverlose Nutzung von Amazon DocumentDB für bestehende bereitgestellte Workloads

Angenommen, Sie haben bereits eine DocumentDB-Anwendung, die auf einem bereitgestellten Cluster ausgeführt wird. Sie können überprüfen, wie die Anwendung mit DocumentDB serverless funktionieren würde, indem Sie dem vorhandenen Cluster eine oder mehrere serverlose DocumentDB-Instanzen als Reader-Instanzen hinzufügen. Sie können überprüfen, wie oft die Reader-Instanzen nach oben oder unten skaliert werden. Sie können den DocumentDB-Failover-Mechanismus verwenden, um eine serverlose DocumentDB-Instanz zum Autor hochzustufen und zu überprüfen, wie sie mit der Arbeitslast umgeht. read/write Auf diese Weise können Sie mit minimalen Ausfallzeiten und ohne Ändern des Endpunkts, den Ihre Clientanwendungen verwenden, umstellen. Einzelheiten zum Verfahren zur Konvertierung vorhandener Cluster in serverlose DocumentDB-Cluster finden Sie unter. Migration zu Amazon DocumentDB serverlos

Vorteile von Amazon DocumentDB serverlos

DocumentDB serverless ist für variable oder „stachelige“ Workloads vorgesehen. Bei solch unvorhersehbaren Workloads haben Sie möglicherweise Schwierigkeiten zu planen, wann Ihre Datenbankkapazität geändert werden soll. Möglicherweise haben Sie auch Probleme, Kapazitätsänderungen schnell genug vorzunehmen, indem Sie die bekannten Mechanismen wie das Hinzufügen von Instanzen oder das Ändern von Instanzklassen verwenden. DocumentDB serverless bietet die folgenden Vorteile, um bei solchen Anwendungsfällen zu helfen:

- Einfacheres Kapazitätsmanagement als bereitgestellt — DocumentDB serverless reduziert den Aufwand für die Planung der Instanzgrößen und die Größenänderung von Instanzen, wenn sich die Arbeitslast ändert. Es reduziert auch den Aufwand für die Aufrechterhaltung einer konsistenten Kapazität für alle Instanzen in einem Cluster.

- Schnellere und einfachere Skalierung in Zeiten hoher Aktivität — DocumentDB serverless skaliert die Rechen- und Speicherkapazität nach Bedarf, ohne dass die Kundentransaktionen oder Ihre gesamte Arbeitslast unterbrochen werden. Die Möglichkeit, Reader-Instanzen mit DocumentDB serverless zu verwenden, hilft Ihnen, zusätzlich zur vertikalen Skalierung auch die Vorteile der horizontalen Skalierung zu nutzen. Die Möglichkeit, globale DocumentDB-Cluster zu verwenden, bedeutet, dass Sie Ihren serverlosen DocumentDB-Lese-Workload auf mehrere verteilen können. AWS-Regionen Diese Fähigkeit ist bequemer als die Skalierungsmechanismen für bereitgestellte Cluster.

- Cost-effective in Zeiten geringer Aktivität — DocumentDB serverless hilft Ihnen, eine Überprovisionierung Ihrer Instanzen zu vermeiden. DocumentDB serverless fügt Ressourcen in granulierten Schritten hinzu, wenn Instanzen skaliert werden. Sie zahlen nur für die Datenbankressourcen, die Sie verbrauchen. Die Nutzung serverloser DocumentDB-Ressourcen wird pro Sekunde gemessen. Auf diese Weise wird die reduzierte Ressourcennutzung sofort registriert, wenn eine Instanz herunterskaliert wird.

- Funktionsparität mit bereitgestellten Funktionen — Sie können alle DocumentDB-Funktionen mit DocumentDB serverless verwenden. Mit DocumentDB serverless können Sie beispielsweise Reader-Instanzen, AWS Identity and Access Management (IAM) -Datenbankauthentifizierung und Performance Insights verwenden.

Insbesondere mit DocumentDB serverless können Sie die folgenden Funktionen von bereitgestellten Clustern nutzen:

- Reader-Instanzen — DocumentDB serverless kann Reader-Instanzen nutzen, um horizontal zu skalieren. Wenn ein Cluster eine oder mehrere Reader-Instanzen enthält, kann der Cluster bei Problemen mit der Writer-Instanz sofort ein Failover durchführen.
- Multi-AZ Cluster — Sie können die serverlosen DocumentDB-Instanzen eines Clusters auf mehrere Availability Zones (AZs) verteilen. Die Einrichtung eines Multi-AZ Clusters trägt dazu bei, die Geschäftskontinuität auch in den seltenen Fällen sicherzustellen, dass Probleme auftreten, die eine gesamte AZ betreffen.
- Globale Cluster — Sie können DocumentDB serverless in Kombination mit globalen DocumentDB-Clustern verwenden, um für Disaster Recovery-Zwecke zusätzliche schreibgeschützte Kopien Ihres Clusters in anderen AWS-Regionen zu erstellen.

So funktioniert Amazon DocumentDB serverless

Topics

- -Übersicht
- Konfigurationen für Amazon DocumentDB-Cluster
- Serverlose Skalierungskapazität von Amazon DocumentDB
- Serverlose Skalierung von Amazon DocumentDB
- Ruhezustand (0,5 DCUs)

-Übersicht

Amazon DocumentDB serverless eignet sich für die anspruchsvollsten, sehr variablen Workloads. Zum Beispiel könnte Ihre Datenbanknutzung für einen kurzen Zeitraum sehr hoch sein, gefolgt von langen Zeiträumen mit nur leichter oder gar keiner Aktivität. Beispiele hierfür sind Einzelhandels-Websites, Spiele oder Sportveranstaltungen mit regelmäßigen Werbeveranstaltungen sowie Datenbanken, die nach Bedarf Berichte erstellen. Andere Beispiele sind Entwicklungs- und Testumgebungen sowie neue Anwendungen, in denen die Nutzung schnell ansteigen könnte. In Fällen wie diesen und vielen anderen ist es mit dem bereitgestellten Modell nicht immer möglich, die Kapazität vorab korrekt zu konfigurieren. Es können auch höhere Kosten entstehen, wenn Sie zu viel Kapazität bereitstellen, die Sie dann nicht benötigen.

Im Gegensatz dazu eignen sich von DocumentDB bereitgestellte Cluster für stetige Workloads. Bei bereitgestellten Clustern wählen Sie eine Instanzklasse aus, die über eine vordefinierte Menge an Arbeitsspeicher, CPU-Leistung, I/O Bandbreite usw. verfügt. Wenn sich Ihre Workload ändert, ändern Sie die Instance-Klasse Ihres Writers und Ihrer Readers manuell. Das bereitgestellte Modell funktioniert gut, wenn Sie die Kapazität im Vorfeld der erwarteten Verbrauchsmustern anpassen können. Es ist akzeptabel, dass kurze Ausfälle auftreten, während Sie die Instance-Klasse des Writers und der Reader in Ihrem Cluster ändern.

DocumentDB Serverless wurde von Grund auf so konzipiert, dass es serverlose Cluster unterstützt, die sofort skalierbar sind. DocumentDB serverless wurde so konzipiert, dass es das gleiche Maß an Sicherheit und Isolierung bietet wie bereitgestellte Writer und Reader. Diese Aspekte sind in serverlosen Cloud-Umgebungen mit mehreren Mandanten entscheidend. Der dynamische Skalierungsmechanismus umfasst sehr wenig Aufwand, sodass er schnell auf Änderungen der Datenbank-Workload reagieren kann. Er bietet auch genügend Leistung, um einen drastischen Anstieg beim Bedarf nach Rechenleistung zu meistern.

Wenn Sie DocumentDB serverless verwenden, können Sie einen DocumentDB-Cluster erstellen, ohne an eine bestimmte Datenbankkapazität für jeden Writer und Reader gebunden zu sein. Sie geben den minimalen und maximalen Bereich für die Kapazität an. DocumentDB skaliert jeden serverlosen DocumentDB-Writer oder -Leser im Cluster innerhalb dieses Kapazitätsbereichs. Durch die Verwendung eines Multi-AZ Clusters, in dem jeder Writer oder Reader dynamisch skalieren kann, können Sie die Vorteile der dynamischen Skalierung und der hohen Verfügbarkeit nutzen.

DocumentDB serverless skaliert die Datenbankressourcen automatisch auf der Grundlage Ihrer Mindest- und Höchstkapazitätsspezifikationen. Die Skalierung ist schnell, da die meisten Skalierungsereignisoperationen den Writer oder Reader auf demselben Host halten. In den seltenen Fällen, in denen ein serverloser DocumentDB-Writer oder -Leser von einem Host auf einen anderen verschoben wird, verwaltet DocumentDB serverless die Verbindungen automatisch. Sie müssen Ihren Datenbank-Client-Anwendungscode oder Ihre Datenbank-Verbindungszeichenfolgen nicht ändern.

Bei DocumentDB Serverless sind, wie bei bereitgestellten Clustern, Speicherkapazität und Rechenkapazität getrennt. Wenn wir von serverloser Kapazität und Skalierung von DocumentDB sprechen, ist es immer die Rechenkapazität, die zunimmt oder sinkt. Somit kann Ihr Cluster viele Terabyte an Daten enthalten, auch wenn die CPU und Speicherkapazität auf ein niedriges Niveau herunterskalieren.

Anstelle der Bereitstellung und Verwaltung von Datenbankservern geben Sie die Datenbankkapazität an. Die tatsächliche Kapazität der serverlosen DocumentDB-Writer oder -Lesegeräte variiert je nach

Arbeitslast im Laufe der Zeit. Details zu diesem Mechanismus finden Sie unter Serverlose Skalierung von Amazon DocumentDB.

Konfigurationen für Amazon DocumentDB-Cluster

Für jeden Ihrer Amazon DocumentDB-Cluster können Sie eine beliebige Kombination aus serverloser DocumentDB-Kapazität, bereitgestellter Kapazität oder beidem wählen.

Sie können einen Cluster einrichten, der sowohl serverlose als auch bereitgestellte DocumentDB-Kapazität enthält, was als Cluster mit gemischter Konfiguration bezeichnet wird. Nehmen wir beispielsweise an, dass Sie mehr read/write Kapazität benötigen, als für einen serverlosen DocumentDB-Writer verfügbar ist. In diesem Fall können Sie den Cluster mit einem sehr großen bereitgestellten Writer einrichten. Dann können Sie DocumentDB weiterhin serverlos für die Leser verwenden. Oder nehmen Sie an, dass die Schreib-Workload für Ihren Cluster variiert, die Lese-Workload jedoch stabil ist. In diesem Fall können Sie Ihren Cluster mit einem serverlosen DocumentDB-Writer und einem oder mehreren bereitgestellten Lesegeräten einrichten.

Sie können auch einen Cluster einrichten, in dem die gesamte Kapazität von DocumentDB serverless verwaltet wird. Dazu können Sie einen neuen Cluster erstellen und DocumentDB von Anfang an serverless verwenden. Oder Sie können die gesamte bereitgestellte Kapazität in einem vorhandenen Cluster durch DocumentDB serverless ersetzen. Die Verfahren zum Erstellen eines neuen Clusters mit DocumentDB serverless oder zum Umstellen eines vorhandenen Clusters auf DocumentDB serverless finden Sie unter und. Einen Cluster erstellen, der Amazon DocumentDB serverless verwendet Migration zu Amazon DocumentDB serverlos

Wenn Sie DocumentDB in einem Cluster überhaupt nicht serverlos verwenden, werden alle Writer und Reader im Cluster bereitgestellt. Dies ist der häufigste Clustertyp, mit dem die meisten Benutzer vertraut sind. Die bereitgestellte Kapazität ist konstant. Die Gebühren sind relativ einfach zu prognostizieren. Sie müssen jedoch im Vorfeld prognostizieren, wie viel Kapazität Sie benötigen. In einigen Fällen sind Ihre Prognosen möglicherweise ungenau oder Ihr Kapazitätsbedarf kann sich ändern. In diesen Fällen kann Ihr Cluster unterprovisioniert (langsamer als gewünscht) oder überprovisioniert (teurer als gewünscht) werden.

Serverlose Skalierungskapazität von Amazon DocumentDB

Die Maßeinheit für Amazon DocumentDB serverless ist die DocumentDB Capacity Unit (DCU). Die serverlose Skalierungskapazität von DocumentDB ist nicht an die Instanzklassen gebunden, die Sie für bereitgestellte Cluster verwenden.

Jede DCU ist eine Kombination aus ungefähr 2 Gibibyte (GiB) Arbeitsspeicher, entsprechender CPU und Netzwerk. Mit dieser Maßeinheit geben Sie den Kapazitätsbereich der Datenbank an. Die Metriken `ServerlessDatabaseCapacity` und `DCUUtilization` CloudWatch helfen Ihnen festzustellen, wie viel Kapazität Ihre Datenbank tatsächlich nutzt und wo diese Kapazität innerhalb des angegebenen Bereichs liegt.

Jeder serverlose DocumentDB-Writer oder -Leser verfügt zu jedem Zeitpunkt über eine Kapazität. Die Kapazität ist eine Gleitkommazahl, die DCUs darstellt. Die Kapazität steigt oder nimmt ab, sobald der Writer oder Reader skaliert. Dieser Wert wird jede Sekunde gemessen. Für jeden Cluster, in dem Sie DocumentDB serverless verwenden möchten, definieren Sie einen Kapazitätsbereich: die minimalen und maximalen Kapazitätswerte, zwischen denen jeder serverlose DocumentDB-Writer oder -Leser skalieren kann. Der Kapazitätsbereich ist für jeden serverlosen DocumentDB-Writer oder -Leser in einem Cluster derselbe. Jeder serverlose DocumentDB-Writer oder -Leser hat seine eigene Kapazität, die irgendwo in diesem Bereich liegt.

DocumentDB serverless wird auf DocumentDB 5.0 und 8.0 mit einem Kapazitätsbereich von 0,5 bis 256 DCUs unterstützt.

Die kleinste serverlose DocumentDB-Kapazität, die Sie definieren können, beträgt 0,5 DCUs. Sie können eine höhere Zahl angeben, wenn sie kleiner oder gleich dem Wert für die maximal unterstützte Kapazität ist. Wenn Sie die Mindestkapazität auf einen kleinen Wert festlegen, verbrauchen leicht ausgelastete Cluster nur minimale Rechenressourcen. Gleichzeitig bleiben sie bereit, Verbindungen sofort anzunehmen und hochzuskalieren, wenn ihre Aktivität ansteigt.

Wir empfehlen, den Mindestwert auf einen Wert festzulegen, der es jedem Autor oder Leser ermöglicht, den Arbeitssatz der Anwendung im Pufferpool zu speichern. Auf diese Weise wird der Inhalt des Pufferpools in Zeiten geringer Aktivität nicht verworfen. Alle Überlegungen zur Auswahl des Skalierungskapazitätsbereichs finden Sie unterAuswahl des Skalierungskapazitätsbereichs für einen serverlosen DocumentDB-Cluster.

Je nachdem, wie Sie die Lesegeräte in einer Multi-AZ Bereitstellung konfigurieren, können ihre Kapazitäten an die Kapazität des Schreibers gebunden oder unabhängig voneinander genutzt werden. Weitere Informationen zur Vorgehensweise finden Sie unter Die Promotion-Stufe für serverlose Lesegeräte anzeigen und ändern.

Bei der serverlosen Überwachung von DocumentDB werden die Kapazitätswerte für den Writer und die Reader in Ihrem Cluster im Laufe der Zeit gemessen. Wenn Ihre Datenbank nicht auf die Mindestkapazität herunterskaliert, können Sie Maßnahmen ergreifen, z. B. den minimalen Wert anpassen und Ihre Datenbankanwendung optimieren. Wenn Ihre Datenbank ihre maximale Kapazität

konsequent erreicht, können Sie Maßnahmen wie die Erhöhung des maximalen Werts ergreifen. Sie können auch Ihre Datenbankanwendung optimieren und die Abfragelast auf mehr Reader verteilen.

Die Gebühren für die serverlose Kapazität von DocumentDB werden in folgenden Werten gemessen: DCU-hours Informationen zur Berechnung der Gebühren für serverlose DocumentDB-Dienste finden Sie unter Amazon DocumentDB DocumentDB-Preise. Nehmen wir an, dass die Gesamtzahl der Writer und Reader in Ihrem Cluster n beträgt. In diesem Fall verbraucht der Cluster mindestens n x DCUs, wenn Sie keine Datenbankoperationen ausführen. Amazon DocumentDB selbst führt möglicherweise Überwachungs- oder Wartungsvorgänge durch, die eine geringe Belastung verursachen. Dieser Cluster verbraucht maximal n x DCUs, wenn die Datenbank mit voller Kapazität läuft.

Weitere Informationen zur Auswahl geeigneter minimaler und maximaler DCU-Werte finden Sie unter. Auswahl des Skalierungskapazitätsbereichs für einen serverlosen DocumentDB-Cluster Die von Ihnen angegebenen minimalen und maximalen DCU-Werte wirken sich auch auf einige Amazon DocumentDB DocumentDB-Instance-Limits aus. Einzelheiten zur Interaktion zwischen dem Kapazitätsbereich und den Instance-Limits finden Sie unter. Beschränkungen für serverlose Amazon DocumentDB DocumentDB-Instances

Serverlose Skalierung von Amazon DocumentDB

Für jeden serverlosen DocumentDB-Writer oder -Leser verfolgt Amazon DocumentDB kontinuierlich die Nutzung von Ressourcen wie CPU, Arbeitsspeicher und Netzwerk. Diese Messungen werden zusammen als Last bezeichnet. Die Last umfasst die von Ihrer Anwendung ausgeführten Datenbankoperationen. Es umfasst auch die Hintergrundverarbeitung für den Datenbankserver und Verwaltungsaufgaben von Amazon DocumentDB. Wenn die Kapazität durch einen dieser Faktoren eingeschränkt wird, wird DocumentDB serverless skaliert. DocumentDB serverless skaliert auch, wenn es Leistungsprobleme erkennt, die es auf diese Weise lösen kann. Sie können die Ressourcennutzung und ihre Auswirkungen auf die serverlose Skalierung von DocumentDB überwachen, indem Sie die Verfahren unter verwenden. Serverlose Überwachung von Amazon DocumentDB

Die Auslastung kann je nach Writer und Reader in Ihrem Cluster variieren. Der Writer verarbeitet Schreibvorgänge und führt alle Datenänderungen am Cluster-Volume durch. Leser können Anfragen nur mit Leserechten bearbeiten.

Skalierung ist der Vorgang, mit dem die serverlose Kapazität von DocumentDB für Ihre Datenbank erhöht oder verringert wird. Mit DocumentDB serverless hat jeder Writer und Reader seinen

eigenen aktuellen Kapazitätswert, gemessen in DCUs. DocumentDB serverless skaliert einen Writer oder Reader auf eine höhere Kapazität, wenn die aktuelle Kapazität zu gering ist, um die Last zu bewältigen. Der Writer oder Reader wird auf eine geringere Kapazität skaliert, wenn seine aktuelle Kapazität höher als erforderlich ist.

DocumentDB serverless kann die Kapazität schrittweise erhöhen. Wenn Ihr Workload-Bedarf die aktuelle Datenbankkapazität eines Schreibers oder Lesegeräts erreicht, erhöht DocumentDB serverless die Anzahl der DCUs für diesen Writer oder Reader. DocumentDB serverless skaliert die Kapazität in den Schritten, die erforderlich sind, um die beste Leistung für die verbrauchten Ressourcen zu erzielen. Die Skalierung erfolgt in Schritten von nur 0,5 DCUs. Je größer die aktuelle Kapazität, desto größer ist das Skalierungsinkrement und desto schneller kann die Skalierung erfolgen.

Da die serverlose Skalierung von DocumentDB so häufig, detailliert und unterbrechungsfrei erfolgt, verursacht sie keine diskreten Ereignisse in der. AWS-Managementkonsole Stattdessen können Sie die CloudWatch Amazon-Metriken wie `serverlessDatabaseCapacity` und messen und `DCUUtilization` deren Mindest-, Höchst- und Durchschnittswerte im Zeitverlauf verfolgen. Weitere Informationen zur serverlosen Überwachung von DocumentDB finden Sie unter. Serverlose Überwachung von Amazon DocumentDB

Das Hoch- oder Herunterskalieren kann folgende Ursachen haben:

- Speichernutzung
- CPU-Auslastung
- Netzwerkauslastung
- Speichernutzung

Sie können diese Ursachen der Skalierung up/down auf serverlosen DocumentDB-Instanzen überwachen. Weitere Informationen finden Sie unter Serverlose Überwachung von Amazon DocumentDB.

Sie können wählen, ob ein Reader gleichzeitig mit dem zugehörigen Writer oder unabhängig vom Writer skalieren soll. Dazu geben Sie die Hochstufungsstufe für diesen Reader an.

- Serverlose DocumentDB-Lesegeräte der Promotion-Stufen 0 und 1 skalieren zur gleichen Zeit wie der Writer. Dieses Skalierungsverhalten macht Reader in den Prioritätsstufen 0 und 1 ideal verfügbar. Das liegt daran, dass sie immer auf die richtige Kapazität dimensioniert sind, um die Workload des Writers im Falle eines Failovers zu übernehmen.

- Reader der Hochstufungsstufen 2 bis 15 skalieren unabhängig vom Writer. Jeder Leser bleibt innerhalb der minimalen und maximalen DCU-Werte, die Sie für Ihren Cluster angegeben haben. Wenn ein Reader unabhängig von der zugehörigen Writer-DB skaliert, kann er inaktiv werden und herunterskalieren, während der Writer weiterhin ein hohes Transaktionsvolumen verarbeitet. Er ist nach wie vor als Failover-Ziel verfügbar, wenn keine anderen Reader in niedrigeren Hochstufungsstufen zur Verfügung stehen. Wenn der Reader jedoch zum Writer hochgestuft wird, muss er möglicherweise hochskalieren, um die volle Workload des Writers zu bewältigen.

Weitere Informationen zum Anzeigen und Ändern von Promotion-Stufen für serverlose Instances finden Sie unter. Die Promotion-Stufe für serverlose Lesegeräte anzeigen und ändern

Die serverlose Skalierung von DocumentDB kann erfolgen, während Datenbankverbindungen geöffnet sind, während Transaktionen ausgeführt werden usw. DocumentDB serverless wartet nicht auf einen ruhigen Punkt, um mit der Skalierung zu beginnen. Die Skalierung unterbricht keine laufenden Datenbankoperationen.

Wenn Ihr Workload mehr Lesekapazität benötigt, als mit einem einzelnen Writer und einem einzelnen Reader verfügbar ist, können Sie dem Cluster mehrere serverlose DocumentDB-Reader hinzufügen. Jeder serverlose DocumentDB-Reader kann innerhalb des Bereichs der minimalen und maximalen Kapazitätswerte skaliert werden, die Sie für Ihren Cluster angegeben haben. Sie können den Reader-Endpunkt des Clusters verwenden, um schreibgeschützte Sitzungen an die Reader zu leiten und die Last des Writers zu reduzieren.

Ob DocumentDB serverless die Skalierung durchführt und wie schnell die Skalierung nach dem Start erfolgt, hängt auch von den minimalen und maximalen DCU-Einstellungen für den Cluster ab. Darüber hinaus hängt es davon ab, ob ein Reader so konfiguriert ist, dass er zusammen mit dem Writer oder unabhängig davon skaliert wird. Einzelheiten zur Skalierungskonfiguration finden Sie unter. Serverlose Skalierungskonfiguration von Amazon DocumentDB

Ruhezustand (0,5 DCUs)

Wenn serverlose Amazon DocumentDB DocumentDB-Writer oder -Lesegeräte inaktiv sind, unterstützen serverlose DocumentDB-Instances das Herunterskalieren auf einen Leerlaufstatus von 0,5 DCUs, wenn der Cluster auf 0,5 konfiguriert MinCapacity ist.

Im Ruhezustand verfügen die serverlosen DocumentDB-Instanzen nicht über genügend CPU-Rechenkapazität, um die meisten Produktionsworkloads zu unterstützen, können aber schnell hochskaliert werden, um eine neue Arbeitslast zu unterstützen. In einem Zustand ohne Leerlauf

benötigen serverlose DocumentDB-Instanzen in der Regel mindestens 1,0 bis 2,5 DCUs. Wenn serverlose DocumentDB-Instanzen von einem Ruhezustand in einen Zustand ohne Leerlauf hochskaliert werden, werden sie daher direkt auf 1,0 bis 2,5 DCUs (oder den Wert von, MaxCapacity falls dieser niedriger ist) hochskaliert.

Um das Herunterskalieren auf 0,5 DCUs im Leerlauf zu unterstützen, werden die Instance-Limits begrenzt, wenn sie so konfiguriert sind, dass sie kleiner oder gleich 1,0 DCUs sind. MinCapacity Weitere Informationen darüber, wie sich die MinCapacity Konfiguration auf die Grenzwerte auswirkt, finden Sie unter. Beschränkungen für serverlose Amazon DocumentDB DocumentDB-Instances

Anforderungen und Einschränkungen für DocumentDB serverless

Anforderungen an die Funktionen

Verfügbarkeit in Regionen

Der serverlose Instance-Typ Amazon DocumentDB ist in den folgenden Regionen verfügbar:

Der folgende AWS CLI Befehl kann verwendet werden, um die genauen Optionen für serverlose DocumentDB-Instanzen zu überprüfen, die in einer bestimmten Region angeboten werden:

```
aws docdb describe-orderable-db-instance-options \
        --region my_region \
        --db-instance-class db.serverless \
        --engine docdb
```

Verfügbarkeit der Engine-Version

DocumentDB serverless wird von den Engine-Versionen 5.0 und 8.0 von Amazon DocumentDB unterstützt. Sie ist in den Engine-Versionen 3.6 oder 4.0 nicht verfügbar.

> **Note**
>
> DocumentDB serverless wird nur auf neueren Patch-Versionen von 5.0.0 unterstützt. Stellen Sie sicher, dass Ihr Cluster auf eine aktuelle Engine-Patch-Version aktualisiert wurde. Weitere Informationen zur Verwaltung von Amazon DocumentDB-Clustern finden Sie unter Wartung von Amazon DocumentDB

Cluster-Konfiguration

Bevor Sie serverlose Amazon DocumentDB-Instances zu einem Amazon DocumentDB-Cluster hinzufügen, muss für den Cluster auch der `ServerlessV2ScalingConfiguration` Parameter festgelegt sein. Dies definiert den Kapazitätsbereich der serverlosen DocumentDB-Instanzen im Cluster. Weitere Informationen zur Skalierungskonfiguration finden Sie unter. Serverlose Skalierungskonfiguration von Amazon DocumentDB

Einstellungen für den minimalen Skalierungskapazitätsbereich für bestimmte Amazon DocumentDB DocumentDB-Funktionen

Einige Amazon DocumentDB DocumentDB-Funktionen funktionieren mit DocumentDB serverlos, können jedoch Probleme verursachen, wenn Ihr Kapazitätsbereich für die Speicheranforderungen für diese Funktionen mit Ihrer spezifischen Arbeitslast geringer ist als erforderlich. In diesem Fall funktioniert Ihre Datenbank möglicherweise nicht so gut wie gewohnt oder es kann zu Fehlern wegen zu wenig Speicherplatz kommen.

Die folgenden Funktionen erfordern für einen optimalen Betrieb eine Konfiguration mit einem höheren `MinCapacity` and/or `MaxCapacity` Wert:

- Performance Insights
- Globale Cluster (gilt nur für die primären AWS-Region)
- Serverlose Instanzerstellung auf einem Cluster mit einem großen Datenvolumen

  Dies beinhaltet die serverlose Instanzerstellung im Rahmen einer Cluster-Wiederherstellung.

Empfehlungen zur Einstellung des geeigneten Kapazitätsbereichs (falls Sie diese Funktion verwenden) finden Sie unterAuswahl des Skalierungskapazitätsbereichs für einen serverlosen DocumentDB-Cluster. Informationen zur Fehlerbehebung, wenn für Ihre Datenbank aufgrund eines falsch konfigurierten Kapazitätsbereichs Fehler wegen zu wenig Speicherplatz auftreten, finden Sie unter Vermeiden von Fehlern aufgrund von zu wenig Speicher.

Einen Cluster erstellen, der Amazon DocumentDB serverless verwendet

Einen serverlosen Amazon DocumentDB-Cluster erstellen

Mit Amazon DocumentDB serverlos sind Ihre Cluster mit bereitgestellten Clustern austauschbar. Sie können Cluster einrichten, in denen einige Instances serverless verwenden und einige Instances bereitgestellt werden.

Stellen Sie sicher, dass Ihre gewünschte Region und Engine-Version DocumentDB serverless unterstützen. Siehe Anforderungen und Einschränkungen für DocumentDB serverless.

Um einen Amazon DocumentDB-Cluster zu erstellen, in dem Sie serverlose Instances hinzufügen können, gehen Sie genauso vor wie unter. Einen Amazon DocumentDB-Cluster erstellen Der einzige Unterschied besteht darin, dass das `ServerlessV2ScalingConfiguration` Argument ebenfalls angegeben werden muss.

Das `ServerlessV2ScalingConfiguration` Argument gibt den Skalierungskapazitätsbereich Ihrer serverlosen DocumentDB-Instances an. Sie besteht aus den minimalen und maximalen DCU (DocumentDB Capacity Unit) -Werten, die für alle serverlosen DocumentDB-Instanzen im Cluster gelten:

- Der `MinCapacity` Wert gibt die minimale Skalierungskapazität an.
- Der `MaxCapacity` Wert gibt die maximale Skalierungskapazität an.

Weitere Informationen zur Skalierung finden Sie unter Serverlose Skalierungskonfiguration von Amazon DocumentDB.

Using the AWS-Managementkonsole

Das folgende AWS-Managementkonsole Konfigurationsbeispiel zeigt, wie ein serverloser DocumentDB-Cluster erstellt wird.

1. Melden Sie sich bei der Amazon DocumentDB DocumentDB-Konsole an AWS-Managementkonsoleund öffnen Sie sie.
2. Klicken Sie im Navigationsbereich auf Cluster.

> **Tip**
>
> Wenn der Navigationsbereich auf der linken Seite des Bildschirms nicht angezeigt wird, wählen Sie links oben auf der Seite das Menüsymbol (≡) aus.

Die Cluster-Tabelle wird angezeigt.

3. Wählen Sie Erstellen aus.

   Die Seite Amazon DocumentDB-Cluster erstellen wird angezeigt.

4. Wählen Sie auf der Seite Amazon DocumentDB-Cluster erstellen im Abschnitt Clustertyp die Option Instance-based Cluster aus (dies ist die Standardoption).

5. Gehen Sie im Abschnitt Cluster-Konfiguration wie folgt vor:

   a. Geben Sie als Cluster-ID einen eindeutigen Namen ein, z. B. **`myserverlesscluster`**. Beachten Sie, dass die Konsole alle Clusternamen unabhängig von der Art der Eingabe in Kleinbuchstaben ändert.

   b. Wählen Sie für Engine-Version 5.0.0 aus (dies ist die Standardoption).

6. Wählen Sie im Abschnitt Cluster-Speicherkonfiguration Amazon DocumentDB Standard (dies ist die Standardoption).

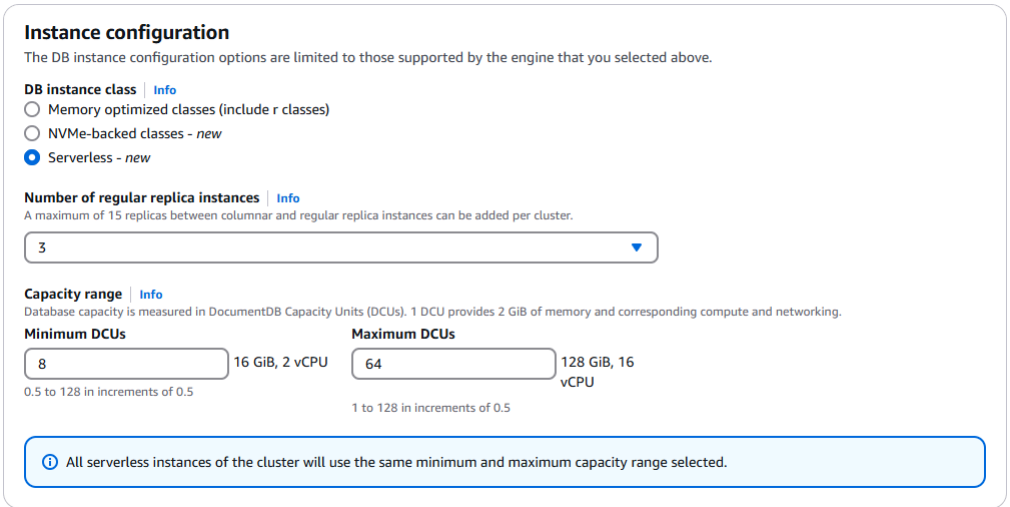
> **Note**
>
> Die andere Option in dieser Kategorie ist Amazon DocumentDB I/O-Optimized. Weitere Informationen zu den beiden Optionen finden Sie unter Amazon DocumentDB-Cluster-Speicherkonfigurationen

7. Im Abschnitt Instanzkonfiguration:

   a. Wählen Sie die DB-Instance-Klasse Serverless aus.

   b. Wählen Sie für Anzahl der regulären Replikatinstanzen die Option 3 aus (dies ist die Standardoption).

   c. Behalten Sie im Abschnitt Kapazitätsbereich die Standardwerte für Minimum DCUs und Maximum DCUs bei. Informationen zum Einstellen dieser Parameter finden Sie unter. Beschränkungen für serverlose Amazon DocumentDB DocumentDB-Instances



8. Behalten Sie im Abschnitt Konnektivität die Standardeinstellung „Keine Verbindung zu einer EC2-Rechenressource herstellen“ bei.
9. Geben Sie im Abschnitt Authentifizierung einen Benutzernamen für den Hauptbenutzer ein und wählen Sie dann Selbstverwaltet aus. Geben Sie ein Passwort ein und bestätigen Sie es.

   Wenn Sie stattdessen Verwaltet in wählen AWS Secrets Manager, finden Sie Passwortverwaltung mit Amazon DocumentDB und AWS Secrets Manager weitere Informationen unter.
10. Behalten Sie alle anderen Optionen als Standard bei und wählen Sie Cluster erstellen aus.

Using the AWS CLI

Ersetzen Sie im folgenden Beispiel jede *`user input placeholder`* durch Ihre eigenen Informationen oder Konfigurationsparameter.

Informationen zum Erstellen eines Clusters, das mit serverlosen DocumentDB-Instanzen kompatibel ist AWS CLI, finden Sie unter. Erstellen eines Clusters mit dem AWS CLI

Nehmen Sie die folgenden zusätzlichen Parameter in Ihren `create-db-cluster` Befehl auf:

```
--serverless-v2-scaling-configuration
     MinCapacity=minimum_capacity,MaxCapacity=maximum_capacity
```

Beispiel:

```
aws docdb create-db-cluster \
```

```
    --db-cluster-identifier sample-cluster \
    --engine docdb \
    --engine-version 5.0.0 \
    --serverless-v2-scaling-configuration MinCapacity=0.5,MaxCapacity=16 \
    --master-username user-name \
    --master-user-password password
```

Hinzufügen einer serverlosen Amazon DocumentDB DocumentDB-Instance

Um eine serverlose DocumentDB-Instanz hinzuzufügen, gehen Sie genauso vor wie unter und achten Sie daraufHinzufügen einer Amazon DocumentDB DocumentDB-Instance zu einem Cluster, db.serverless als Instanzklasse anzugeben.

Hinzufügen einer serverlosen Instanz mithilfe der AWS-Managementkonsole.

Informationen zum Hinzufügen serverloser DocumentDB-Instanzen mithilfe der Konsole finden Hinzufügen einer Amazon DocumentDB DocumentDB-Instance zu einem Cluster Sie unter Verwenden der AWS-Managementkonsole Registerkarte Verwenden.

Hinzufügen einer serverlosen Instanz mithilfe der AWS CLI

Informationen zum Hinzufügen serverloser DocumentDB-Instanzen mithilfe von finden Hinzufügen einer Amazon DocumentDB DocumentDB-Instance zu einem Cluster Sie unter Verwenden der AWS CLI Registerkarte. AWS CLI

Verwenden Sie das folgende CLI-Argument für die Instanzklasse:

```
--db-instance-class db.serverless
```

Beispiel:

```
aws docdb create-db-instance \
      --db-cluster-identifier sample-cluster \
      --db-instance-identifier sample-instance \
      --db-instance-class db.serverless \
      --engine docdb
```

Migration zu Amazon DocumentDB serverlos

Topics

- Migration vorhandener DocumentDB-Cluster auf Serverless
- Migration von MongoDB zu DocumentDB serverlos

Migration vorhandener DocumentDB-Cluster auf Serverless

Aktualisierung der Engine-Version eines Clusters

Wenn auf Ihrem bereitgestellten Cluster eine niedrigere Engine-Version ausgeführt wird, die DocumentDB serverless nicht unterstützt, müssen Sie den Cluster zunächst auf eine unterstützte Engine-Version aktualisieren. Weitere Informationen finden Sie unter Direktes Upgrade der Hauptversion von Amazon DocumentDB.

Migration eines bereitgestellten Clusters zu DocumentDB serverless

Gehen Sie wie folgt vor, um einen bereitgestellten Cluster auf die serverlose Verwendung von DocumentDB umzustellen:

1. Prüfen Sie, ob die Engine-Version des bereitgestellten Clusters aktualisiert werden muss, damit sie mit DocumentDB serverless verwendet werden kann. Siehe Anforderungen und Einschränkungen für DocumentDB serverless.

   > **Note**
   >
   > Wenn auf dem bereitgestellten Cluster eine Engine-Version ausgeführt wird, die für DocumentDB serverless nicht verfügbar ist, aktualisieren Sie die Engine-Version des Clusters. Siehe Direktes Upgrade der Hauptversion von Amazon DocumentDB.

2. Konfigurieren Sie die Skalierungskonfiguration für den Cluster. Einzelheiten zur Auswahl der Skalierungskonfiguration finden Sie unter. Auswahl des Skalierungskapazitätsbereichs für einen serverlosen DocumentDB-Cluster Informationen zum Ändern der Skalierungskonfiguration für einen Cluster finden Sie unterDie Konfiguration des Skalierungskapazitätsbereichs eines Clusters anzeigen und ändern.
3. Konfigurieren Sie alle anderen Clustereigenschaften, um die serverlosen Anforderungen und Einschränkungen von DocumentDB zu berücksichtigen. Anforderungen und Einschränkungen für DocumentDB serverless
4. Fügen Sie dem Cluster eine oder mehrere serverlose DocumentDB-Instanzen hinzu. Folgen Sie dem Verfahren unter Hinzufügen einer serverlosen Amazon DocumentDB DocumentDB-Instance.

> **Note**
>
> In einigen Fällen verfügen Sie möglicherweise bereits über eine oder mehrere bereitgestellte Reader-Instanzen im Cluster. In diesem Fall können Sie einen der Reader in eine serverlose DocumentDB-Instanz konvertieren, anstatt eine neue Instanz zu erstellen. Eine Schritt-für-Schritt-Anleitung hierzu finden Sie unter Die Klasse einer Instance ändern.

5. (Optional) Führen Sie einen Failover-Vorgang durch, um eine serverlose DocumentDB-Instance zum Cluster-Writer zu machen. Siehe Amazon DocumentDB-Failover.
6. (Optional) Konvertieren Sie alle verbleibenden bereitgestellten Amazon DocumentDB DocumentDB-Instances in serverlose DocumentDB-Instances (siheDie Klasse einer Instance ändern) oder entfernen Sie sie aus dem Cluster (siehe). Löschen einer Amazon DocumentDB DocumentDB-Instance

Using the AWS-Managementkonsole

Das folgende AWS-Managementkonsole Konfigurationsbeispiel zeigt den Migrationsprozess mithilfe eines von Amazon DocumentDB bereitgestellten Clusters, auf dem Amazon DocumentDB 5.0.0 ausgeführt wird. Für den Start der serverlosen Nutzung von DocumentDB ist kein Upgrade der Engine-Version erforderlich. Der Cluster hat einen Namen und beginnt mit drei bereitgestellten Instances namens`sample`, und. `sample` `sample2` `sample3` In diesem Beispiel werden diese drei Instanzen durch drei serverlose Instanzen ersetzt.

1. Melden Sie sich bei der Amazon DocumentDB DocumentDB-Konsole an AWS-Managementkonsoleund öffnen Sie sie.
2. Klicken Sie im Navigationsbereich auf Cluster.

> **Tip**
>
> Wenn der Navigationsbereich auf der linken Seite des Bildschirms nicht angezeigt wird, wählen Sie links oben auf der Seite das Menüsymbol (≡) aus.

Die Cluster-Tabelle wird angezeigt.

3. Aktivieren Sie in der Cluster-Tabelle das Kontrollkästchen des Clusters, dem Sie eine serverlose Instance hinzufügen möchten.
4. Wählen Sie Actions (Aktionen) und dann Add instances (Instances hinzufügen) aus.
5. Wählen Sie im Dialogfeld „Instanzen hinzufügen“ im Abschnitt DB-Instance-Klasse für jede neue serverlose Instance, die Sie erstellen möchten, die Option Serverless aus.
6. Für Einstellungen zur serverlosen Kapazität legen Sie die Skalierungskonfiguration auf der Grundlage der Kapazitätsbeschreibung im Dialogfeld fest.
7. (Optional) Um eine weitere Instanz hinzuzufügen, wählen Sie Instanz hinzufügen. Fügen Sie weitere Instanzen hinzu, bis Sie die gewünschte Anzahl neuer Instanzen erreicht haben.

   In diesem Beispiel werden drei neue serverlose Instanzen erstellt.
8. Wählen Sie Erstellen aus.

   Es dauert einige Minuten, bis eine Instance erstellt ist. Sie können die Konsole oder die verwenden AWS CLI , um den Status der Instanz einzusehen. Weitere Informationen finden Sie unter Überwachen des Status eines Amazon DocumentDB-Clusters.
9. Kehren Sie zur Cluster-Tabelle zurück und aktivieren Sie die Kontrollkästchen aller drei ursprünglich bereitgestellten Instances.
10. Wählen Sie Aktionen und anschließend Löschen aus.

Während des Löschvorgangs wird automatisch ein Failover durchgeführt, um eine der verbleibenden Instances zum Writer hochzustufen. Nach einigen Minuten ist der Löschvorgang abgeschlossen. Der bestehende Cluster enthält jetzt drei serverlose DocumentDB-Instanzen (wie in der Spalte Größe definiert).

Using the AWS CLI

Das folgende AWS CLI Konfigurationsbeispiel zeigt den Migrationsprozess mithilfe eines von Amazon DocumentDB bereitgestellten Clusters, auf dem Amazon DocumentDB 5.0.0 ausgeführt wird. Für den Start der serverlosen Nutzung von DocumentDB ist kein Upgrade der Engine-Version erforderlich. Der Cluster hat einen Namen und beginnt mit drei bereitgestellten Instances namens`sample`, und. `sample` `sample2` `sample3` In diesem Beispiel werden diese drei Instanzen durch drei serverlose Instanzen ersetzt. Der Cluster hat einen Namen `sample-cluster` und beginnt mit zwei bereitgestellten Instanzen namens `sample-provisioned-instance-1` und`sample-provisioned-instance-2`, einer Writer-Instanz und einer Reader-Instanz.

Ersetzen Sie im folgenden Beispiel jede *user input placeholder* durch Ihre eigenen Informationen oder Konfigurationsparameter.

Verwenden Sie den `aws docdb describe-db-clusters` Vorgang, um den Status eines Clusters zu ermitteln. Der folgende Code ermittelt den Status des Clusters `sample-cluster` und gibt die Ergebnisse in einer Tabelle aus:

```
aws docdb describe-db-clusters \
    --db-cluster-identifier sample-cluster \
    --query 'DBClusters[*].DBClusterMembers' \
    --output table
```

```
----------------------------------------------------------------------------------------------
|                                          DescribeDBClusters
                  |
+---------------------------------+---------------------------------
+------------------+----------------+
|  DBClusterParameterGroupStatus |      DBInstanceIdentifier       | IsClusterWriter
  | PromotionTier  |
+---------------------------------+---------------------------------
+------------------+----------------+
|  in-sync                       |  sample-provisioned-instance-2  |  False
  |  1             |
|  in-sync                       |  sample-provisioned-instance-1  |  True
  |  1             |
+---------------------------------+---------------------------------
+------------------+----------------+
```

Fügen Sie die Skalierungskonfiguration für den Cluster hinzu:

```
aws docdb modify-db-cluster \
    --db-cluster-identifier sample-cluster \
    --serverless-v2-scaling-configuration MinCapacity=0.5,MaxCapacity=16
```

Fügen Sie die serverlosen Instanzen hinzu. In diesem Beispiel werden neue serverlose Instanzen benannt `sample-serverless-instance-1` und hinzugefügt`sample-serverless-instance-2`:

```
aws docdb create-db-instance \
    --db-cluster-identifier sample-cluster \
```

```
    --db-instance-identifier sample-serverless-instance-1 \
    --db-instance-class db.serverless \
    --engine docdb

aws docdb create-db-instance \
    --db-cluster-identifier sample-cluster \
    --db-instance-identifier sample-serverless-instance-2 \
    --db-instance-class db.serverless \
    --engine docdb
```

Geben Sie Folgendes ein, um zu warten, bis die serverlosen Instanzen verfügbar sind, bevor Sie fortfahren:

```
aws docdb wait db-instance-available \
    --db-instance-identifier sample-serverless-instance-1

aws docdb wait db-instance-available \
    --db-instance-identifier sample-serverless-instance-2
```

Führen Sie einen Failover durch, um die neue `sample-serverless-instance-1` Instanz zum Cluster-Writer zu machen:

```
aws docdb failover-db-cluster \
    --db-cluster-identifier sample-cluster \
    --target-db-instance-identifier sample-serverless-instance-1
```

Es dauert einige Sekunden, bis der Failover abgeschlossen ist. Danach wird sample-serverless-instance-1 zum Cluster-Writer. Überprüfen Sie dies mit der folgenden Eingabe:

```
aws docdb describe-db-clusters \
    --db-cluster-identifier sample-cluster \
    --query 'DBClusters[*].DBClusterMembers' \
    --output table
```

```
-------------------------------------------------------------------------------------------
|                                        DescribeDBClusters
                  |
+---------------------------------+---------------------------------
+------------------+----------------+
|  DBClusterParameterGroupStatus |      DBInstanceIdentifier       | IsClusterWriter
  | PromotionTier  |
```

```
+--------------------------------+--------------------------------
+------------------+----------------+
|  in-sync                       |  sample-provisioned-instance-2  |  False
  |  1             |
|  in-sync                       |  sample-provisioned-instance-1  |  False
  |  1             |
|  in-sync                       |  sample-serverless-instance-2   |  False
  |  1             |
|  in-sync                       |  sample-serverless-instance-1   |  True
  |  1             |
+--------------------------------+--------------------------------
+------------------+----------------+
```

Löschen Sie abschließend die ursprünglich bereitgestellten Instanzen:

```
aws docdb delete-db-instance \
    --db-instance-identifier sample-provisioned-instance-1

aws docdb delete-db-instance \
    --db-instance-identifier sample-provisioned-instance-2
```

Migration von MongoDB zu DocumentDB serverlos

Sie können Ihre MongoDB-Datenbanken zu DocumentDB serverless migrieren, genau wie bei der bereitgestellten Amazon DocumentDB. Weitere Informationen finden Sie unter Migration zu Amazon DocumentDB.

Serverlose Verwaltung von Amazon DocumentDB

Die Konfiguration des Skalierungskapazitätsbereichs eines Clusters anzeigen und ändern

Das `ServerlessV2ScalingConfiguration` Argument gibt den Skalierungskapazitätsbereich Ihrer serverlosen DocumentDB-Instances an. Sie besteht aus den minimalen und maximalen DCU (DocumentDB Capacity Unit) -Werten, die für alle serverlosen DocumentDB-Instanzen im Cluster gelten.

- **`MinCapacity`**— Die minimale Skalierungskapazität aller serverlosen DocumentDB-Instanzen im Cluster.

- **`MaxCapacity`**— Die maximale Skalierungskapazität aller serverlosen DocumentDB-Instanzen im Cluster.

> **Note**
>
> Die folgenden Änderungen an der Skalierungskonfiguration erfordern einen Neustart der Instanz, um die neuen Werte `MinCapacity` und `MaxCapacity` widerzuspiegeln:
>
> - Jegliche Änderungen am `MaxCapacity` Wert
> - Änderung des `MinCapacity` Werts von einem höheren Wert auf 1,0 oder niedriger
> - Änderung des `MinCapacity` Werts von einem niedrigeren Wert auf einen Wert über 1,0

Weitere Informationen zur Skalierungskonfiguration und zur Auswahl geeigneter Skalierungskapazitätsgrenzen finden Sie unterServerlose Skalierungskonfiguration von Amazon DocumentDB.

Using the AWS-Managementkonsole

Das folgende AWS-Managementkonsole Konfigurationsbeispiel zeigt, wie die Skalierungskonfigurationseinstellungen eines serverlosen DocumentDB-Clusters angezeigt und bearbeitet werden.

1. Melden Sie sich bei der Amazon DocumentDB DocumentDB-Konsole an AWS-Managementkonsoleund öffnen Sie sie.
2. Klicken Sie im Navigationsbereich auf Cluster.

   > **Tip**
   >
   > Wenn der Navigationsbereich auf der linken Seite des Bildschirms nicht angezeigt wird, wählen Sie links oben auf der Seite das Menüsymbol (≡) aus.

   Die Cluster-Tabelle wird angezeigt.
3. Aktivieren Sie in der Cluster-Tabelle das Kontrollkästchen des Clusters, für den Sie die Skalierungskapazität ändern möchten.

4. Wählen Sie Actions (Aktionen) und dann Modify (Ändern) aus.

   Das Dialogfeld „Cluster ändern“ wird angezeigt.

5. Suchen Sie den Abschnitt „Einstellung der Kapazität ohne Server“ und legen Sie die Skalierungskonfiguration (Kapazitätsbereich) auf der Grundlage der Kapazitätsbeschreibung im Dialogfeld fest.

   Weitere Informationen zur Skalierung und zu Kapazitätsbereichen finden Sie unterServerlose Skalierungskonfiguration von Amazon DocumentDB.

6. Klicken Sie auf Weiter.
7. Wählen Sie für Scheduling of modifications (Einplanung von Änderungen) die Option Apply immediately (Sofort anwenden) aus.
8. Wählen Sie Cluster bearbeiten aus.
9. Sobald die Änderung abgeschlossen ist, sollte jede serverlose Instanz neu gestartet werden. Um die Nichtverfügbarkeit des Writers zu minimieren, führen Sie die folgende Abfolge von Vorgängen aus:

   a. Starten Sie jede serverlose Reader-Instanz neu.

      i. Wählen Sie die Reader-Instanz aus, klicken Sie auf Aktionen und anschließend auf Neustart.

      ii. Warten Sie, bis der Instanzstatus wieder verfügbar ist.

   b. Führen Sie einen Failover auf eine neu gestartete serverlose Instanz durch.

      i. Wählen Sie den Cluster aus, klicken Sie auf Aktionen und dann auf Failover.

      ii. Warten Sie, bis der Failover-Vorgang abgeschlossen ist.

   c. Starten Sie die verbleibende serverlose Instanz neu.

      i. Wählen Sie die verbleibende Instanz aus, klicken Sie auf Aktionen und anschließend auf Neustart.

      ii. Warten Sie, bis der Instanzstatus wieder verfügbar ist.

Using the AWS CLI

Das folgende AWS CLI Konfigurationsbeispiel zeigt die aktuelle Skalierungskonfiguration.

Ersetzen Sie im folgenden Beispiel jede *user input placeholder* durch Ihre eigenen Informationen oder Konfigurationsparameter.

Die aktuelle Skalierungskonfiguration des Clusters kann mit dem `describe-db-clusters` AWS CLI folgenden Befehl angezeigt werden:

```
aws docdb describe-db-clusters \
    --db-cluster-identifier sample-cluster \
    --query 'DBClusters[0].ServerlessV2ScalingConfiguration'
```

Die Ausgabe dieses Befehls ist wie folgt:

```
{
    "MinCapacity": 0.5,
    "MaxCapacity": 16.0
}
```

Die Skalierungskonfiguration des Clusters kann mit dem `modify-db-cluster` folgenden Befehl geändert werden:

```
aws docdb modify-db-cluster \
    --db-cluster-identifier sample-cluster \
    --serverless-v2-scaling-configuration MinCapacity=0.5,MaxCapacity=32
```

Sobald der Vorgang abgeschlossen ist, sollte jede serverlose Instanz neu gestartet werden. Um die Nichtverfügbarkeit des Writers zu minimieren, können wir die folgende Abfolge von Vorgängen ausführen:

```
aws docdb reboot-db-instance \
    --db-instance-identifier sample-serverless-instance-reader

aws docdb wait db-instance-available \
    --db-instance-identifier sample-serverless-instance-reader

aws docdb failover-db-cluster \
   --db-cluster-identifier sample-cluster \
   --target-db-instance-identifier sample-serverless-instance-reader

aws docdb reboot-db-instance \
    --db-instance-identifier sample-serverless-instance-writer
```

```
aws docdb wait db-instance-available \
    --db-instance-identifier sample-serverless-instance-writer

aws docdb failover-db-cluster \
   --db-cluster-identifier sample-cluster \
   --target-db-instance-identifier sample-serverless-instance-writer
```

Die Promotion-Stufe für serverlose Lesegeräte anzeigen und ändern

Achten Sie bei Clustern, die mehrere serverlose DocumentDB-Instanzen oder eine Mischung aus bereitgestellten und serverlosen Instanzen enthalten, auf die Einstellung der Promotion-Stufe für jede serverlose Instanz. Diese Einstellung steuert mehr Verhalten für serverlose Instanzen als für bereitgestellte Instanzen.

Bei bereitgestellten Instances bestimmt die Wahl der Stufen 0—15 nur die Reihenfolge, in der Amazon DocumentDB auswählt, welche Reader-Instance während eines Failover-Vorgangs zum Writer hochgestuft werden soll. Bei serverlosen Instances bestimmt die Tier-Nummer jedoch auch, ob die Instance entsprechend der Kapazität der Writer-Instance skaliert oder unabhängig von ihrer eigenen Arbeitslast skaliert wird. Serverlose Reader-Instanzen der Stufe 0 oder 1 verfügen über eine Mindestkapazität, die mindestens so hoch ist wie die der Writer-Instance. Auf diese Weise sind sie bereit, im Falle eines Failovers die Writer-Instanz zu übernehmen. Wenn es sich bei der Writer-Instance um eine bereitgestellte Instance handelt, schätzt Amazon DocumentDB die entsprechende serverlose DocumentDB-Kapazität. Es verwendet diese Schätzung als Mindestkapazität für die serverlose Reader-Instance.

Für serverlose DocumentDB-Reader-Instanzen der Stufen 2—15 gelten nicht dieselben Einschränkungen in Bezug auf ihre Mindestkapazität. Wenn sie inaktiv sind, können sie auf den Mindestwert der DocumentDB-Kapazitätseinheit (DCU) herunterskaliert werden, der im Kapazitätsbereich des Clusters angegeben ist.

Using the AWS-Managementkonsole

Das folgende AWS-Managementkonsole Konfigurationsbeispiel zeigt, wie Sie die Promotion-Tarif-Einstellungen eines serverlosen DocumentDB-Instance-Readers anzeigen und ändern können.

1. Melden Sie sich bei der Amazon DocumentDB DocumentDB-Konsole an AWS-Managementkonsoleund öffnen Sie sie.

Die Promotion-Stufen jeder Instance werden in der Spalte Promotion-Stufe im AWS-Managementkonsole angezeigt.

2. Klicken Sie im Navigationsbereich auf Cluster.

> **Tip**
>
> Wenn der Navigationsbereich auf der linken Seite des Bildschirms nicht angezeigt wird, wählen Sie links oben auf der Seite das Menüsymbol (≡) aus.

Die Cluster-Tabelle wird angezeigt.

3. Aktivieren Sie in der Cluster-Tabelle das Kontrollkästchen der Instance, für die Sie die Promotion-Stufe ändern möchten.
4. Wählen Sie Actions (Aktionen) und dann Modify (Ändern) aus.

Das Dialogfeld „Instanz ändern“ wird angezeigt.

5. Suchen Sie den Abschnitt Failover und stellen Sie die Stufe Promotion auf die gewünschte Stufe ein.
6. Klicken Sie auf Weiter.
7. Wählen Sie für Scheduling of modifications (Einplanung von Änderungen) die Option Apply immediately (Sofort anwenden) aus.
8. Wählen Sie Modify instance (Instance ändern).

Using the AWS CLI

Das folgende AWS CLI Konfigurationsbeispiel zeigt die aktuelle Skalierungskonfiguration.

Ersetzen Sie im folgenden Beispiel jede *user input placeholder* durch Ihre eigenen Informationen oder Konfigurationsparameter.

Die Promotion-Stufen aller Instances in einem Cluster können mit dem `describe-db-clusters` AWS CLI folgenden Befehl angezeigt werden:

```
aws docdb describe-db-clusters \
    --db-cluster-identifier sample-cluster \
```

```
    --query 'DBClusters[0].DBClusterMembers' \
    --output table
```

Die Ausgabe dieses Befehls ist wie folgt:

```
----------------------------------------------------------------------------------------------------
|                                          DescribeDBClusters
                  |
+---------------------------------+---------------------------------
+------------------+----------------+
|  DBClusterParameterGroupStatus |      DBInstanceIdentifier       | IsClusterWriter
  | PromotionTier  |
+---------------------------------+---------------------------------
+------------------+----------------+
|  in-sync                       |  sample-serverless-instance-2   |  False
  |  1             |
|  in-sync                       |  sample-serverless-instance-1   |  True
  |  1             |
+---------------------------------+---------------------------------
+------------------+----------------+
```

Die Aufstiegsstufe einer bestimmten Instanz kann mit dem `modify-db-instance` folgenden Befehl geändert werden:

```
aws docdb modify-db-instance \
    --db-instance-identifier sample-serverless-instance-2 \
    --promotion-tier 3
```

Beschränkungen für serverlose Amazon DocumentDB DocumentDB-Instances

Für serverlose DocumentDB-Instances hängen die folgenden Grenzwerte pro Instanz von der aktuellen Skalierungskapazität der Instanz ab:

- Instanzspeicher (GiB)
- Verbindungen (alle)
- Cursor-Limit
- Transaktionen öffnen

- Verbindungen (aktiv)

In den folgenden Tabellen wird beschrieben, wie die Grenzwerte für serverlose Instances pro Instanz im Verhältnis zur aktuellen Skalierungskapazität der Instance skaliert werden.

Beachten Sie, dass die Grenzwerte unterschiedlich sind, je nachdem, ob die `MinCapacity` Skalierungskonfiguration des Clusters auf mehr als zwei (2) festgelegt wurde. Wenn auf weniger als oder gleich 2 gesetzt `MinCapacity` ist, sind die Grenzwerte für Cursorlimit, offene Transaktionen und Verbindungen (aktiv) auf einen niedrigeren Maximalwert begrenzt. (Der technische Grund für die Obergrenze besteht darin, das Herunterskalieren in einen „inaktiven“ Zustand zu unterstützen. Weitere Informationen finden Sie unter Ruhezustand (0,5 DCUs).

db.serverless-Instanzlimits bei ≤1 MinCapacity

Aktuelle Kapazität (DCU)	Instanzspeicher (GiB)	Verbindungen (alle)	Cursor-Limit	Transaktionen öffnen	Verbindungen (aktiv)
0.5	1	250	6	12	39
1	2	500	12	24	79
2	4	1000	24	48	173
4	8	2000	48	96	416
8	16	4000	96	192	1071
16	32	8000	132	264	1550
32	64	16000	132	264	1550
64	128	32000	132	264	1550
128	256	60000	132	264	1550
256	512	60000	132	264	1550

db.serverless-Instanzlimits, wenn >1 MinCapacity

Aktuelle Kapazität (DCU)	Instanzspeicher (GiB)	Verbindungen (alle)	Cursor-Limit	Transaktionen öffnen	Verbindungen (aktiv)
1.5	3	7250	18	36	124
2	4	1000	24	48	173
4	8	2000	48	96	416
8	16	4000	96	192	1071
16	32	8000	192	384	2709
32	64	16000	384	768	4500
64	128	32000	768	1536	4500
128	256	60000	1536	3072	4500
256	512	60000	3072	6144	4500

Mithilfe der folgenden CloudWatch Messwerte können Sie die Limits pro Instanz überwachen und Alarme ausgeben. Weitere Informationen zu Amazon CloudWatch DocumentDB-Metriken finden Sie unterÜberwachen von Amazon DocumentDB mit CloudWatch.

Ressource	CloudWatch Metrik einschränken	CloudWatch Nutzungsmetrik (max. 1 Minute)	CloudWatch Nutzungsmetrik
Instanzspeicher	-	-	FreeableMemory
Verbindungen (alle)	DatabaseConnectionsLimit	DatabaseConnectionsMax	DatabaseConnections
Cursor	DatabaseCursorsLimit	DatabaseCursorsMax	DatabaseCursors
Transaktionen	TransactionsOpenLimit	TransactionsOpenMax	TransactionsOpen

Serverlose Skalierungskonfiguration von Amazon DocumentDB

Topics

- Auswahl des Skalierungskapazitätsbereichs für einen serverlosen DocumentDB-Cluster
- MinCapacityEinstellung für einen serverlosen DocumentDB-Cluster auswählen
- MaxCapacityEinstellung für einen serverlosen DocumentDB-Cluster auswählen
- Vermeiden von Fehlern aufgrund von zu wenig Speicher
- Warum wird meine serverlose Instance nicht herunterskaliert?

Auswahl des Skalierungskapazitätsbereichs für einen serverlosen DocumentDB-Cluster

Bevor Sie serverlose DocumentDB-Instances zu einem Amazon DocumentDB-Cluster hinzufügen, muss für den Cluster auch der `ServerlessV2ScalingConfiguration` Parameter festgelegt sein.

Der `ServerlessV2ScalingConfiguration` Parameter besteht aus zwei Werten, die den Kapazitätsbereich für die serverlose Skalierung jeder serverlosen Instance im Cluster definieren:

- **`MinCapacity`**— Die minimale Skalierungskapazität aller serverlosen DocumentDB-Instanzen im Cluster.
- **`MaxCapacity`**— Die maximale Skalierungskapazität aller serverlosen DocumentDB-Instanzen im Cluster.

`MinCapacity`Einstellung für einen serverlosen DocumentDB-Cluster auswählen

Es ist verlockend, immer 0,5 für zu wählen. `MinCapacity` Dieser Wert ermöglicht es der Instance, auf die kleinste Kapazität herunterzuskalieren, wenn sie vollständig inaktiv ist, und gleichzeitig aktiv bleibt. Je nachdem, wie Sie diesen Cluster verwenden und wie die anderen Einstellungen konfiguriert sind, ist jedoch eine andere Mindestkapazität ggf. am effektivsten. Berücksichtigen Sie bei der Auswahl der Mindestkapazitätseinstellung die folgenden Faktoren:

- Die Skalierungsrate für eine serverlose DocumentDB-Instanz hängt von ihrer aktuellen Kapazität ab. Je höher die aktuelle Kapazität, desto schneller kann sie hochskalieren. Wenn Sie möchten,

dass die Instance schnell auf eine sehr hohe Kapazität hochskaliert wird, sollten Sie die Mindestkapazität auf einen Wert festlegen, bei dem die Skalierungsrate Ihren Anforderungen entspricht.

- Wenn Sie in der Regel die Instanzklasse Ihrer Instances in Erwartung einer besonders hohen oder niedrigen Arbeitslast ändern, können Sie diese Erfahrung nutzen, um eine grobe Schätzung des entsprechenden serverlosen Kapazitätsbereichs von DocumentDB vorzunehmen. Informationen zur Bestimmung der Speichergröße eines bereitgestellten Amazon DocumentDB DocumentDB-Instance-Typs finden Sie unter. Instance-Limits

  Nehmen wir beispielsweise an, Sie verwenden die `db.r6g.xlarge` Instance-Klasse, wenn Ihr Cluster eine geringe Arbeitslast hat. Diese Instanzklasse hat 32 GiB Speicher. Sie können also einen Wert `MinCapacity` von 16 angeben, um eine serverlose Instanz einzurichten, die auf ungefähr dieselbe Kapazität herunterskaliert werden kann. Das liegt daran, dass jede DCU ungefähr 2 GiB Speicher entspricht. Sie können einen etwas niedrigeren Wert angeben, um die Instance weiter herunterskalieren zu lassen, falls Ihre `db.r6g.xlarge` Instance manchmal nicht ausgelastet war.
- Wenn Ihre Anwendung am effizientesten arbeitet, wenn die Instances über eine bestimmte Datenmenge im Puffercache verfügen, sollten Sie eine DCU-Mindesteinstellung angeben, bei der der Speicher groß genug ist, um die häufig aufgerufenen Daten aufzunehmen. Andernfalls werden einige Daten aus dem Puffercache entfernt, wenn die serverlosen Instanzen auf eine geringere Speichergröße herunterskaliert werden. Wenn die Instanzen dann wieder hochskaliert werden, werden die Informationen im Laufe der Zeit wieder in den Puffer-Cache eingelesen. Wenn die Menge, mit der I/O die Daten wieder in den Puffer-Cache zurückgebracht werden sollen, beträchtlich ist, ist es möglicherweise effektiver, einen höheren DCU-Mindestwert zu wählen. Weitere Informationen finden Sie unter Dimensionierung der Instanzen.
- Wenn Ihre serverlosen DocumentDB-Instanzen die meiste Zeit mit einer bestimmten Kapazität ausgeführt werden, sollten Sie erwägen, eine Mindestkapazitätseinstellung anzugeben, die niedriger als diese Grundeinstellung, aber nicht zu viel niedriger ist. Serverlose Instances können am effektivsten abschätzen, wie viel und wie schnell eine Skalierung erforderlich ist, wenn die aktuelle Kapazität nicht drastisch unter der erforderlichen Kapazität liegt.
- Wenn Ihr bereitgestellter Workload Speicheranforderungen hat, die für kleine Instance-Klassen wie T3 oder T4g zu hoch sind, wählen Sie eine DCU-Mindesteinstellung, die Speicherplatz bietet, der mit einer R5- oder R6g-Instance vergleichbar ist.
- Insbesondere empfehlen wir die folgenden Mindestanforderungen `MinCapacity` für die Verwendung mit den angegebenen Funktionen (diese Empfehlungen können sich ändern):
  - Performance Insights — 2 DCUs

  - Globale Cluster — 8 DCUs (gilt nur für die primären) AWS-Region
- In Amazon DocumentDB erfolgt die Replikation auf der Speicherebene, sodass sich die Lesekapazität nicht direkt auf die Replikation auswirkt. Stellen Sie bei serverlosen DocumentDB-Reader-Instances, die unabhängig skaliert werden, jedoch sicher, dass die Mindestkapazität ausreicht, um Workloads in schreibintensiven Zeiten zu bewältigen, um Abfragelatenz zu vermeiden. Wenn bei Reader-Instances der Promotion-Stufen 2—15 Leistungsprobleme auftreten, sollten Sie eine Erhöhung der Mindestkapazität des Clusters in Betracht ziehen. Einzelheiten dazu, wie Sie ändern können, ob Reader-Instances zusammen mit dem Autor oder unabhängig voneinander skaliert werden, finden Sie unterDie Promotion-Stufe für serverlose Lesegeräte anzeigen und ändern.

  Wenn Sie einen Cluster mit serverlosen DocumentDB-Reader-Instances haben, skalieren die Reader nicht zusammen mit der Writer-Instanz, wenn die Promotion-Stufe der Reader nicht 0 oder 1 ist. In diesem Fall kann das Festlegen einer geringen Mindestkapazität zu einer übermäßigen Replikationsverzögerung führen. Das liegt daran, dass die Reader möglicherweise nicht genug Kapazität haben, um Änderungen vom Writer zu übernehmen, wenn die Datenbank ausgelastet ist. Es wird empfohlen, die Mindestkapazität auf einen Wert festzulegen, der einer mit der Writer-Instanz vergleichbaren Speicher- und CPU-Menge entspricht.
- Die Zeit, die eine serverlose DocumentDB-Instanz benötigt, um von ihrer minimalen Kapazität zur maximalen Kapazität zu skalieren, hängt von der Differenz zwischen ihren minimalen und maximalen DCU-Werten ab. Wenn die aktuelle Kapazität der Instanz groß ist, wird DocumentDB serverless in größeren Schritten skaliert, als wenn die Instanz mit einer kleinen Kapazität gestartet wird. Wenn Sie also eine relativ große maximale Kapazität angeben und die Instance die meiste Zeit in der Nähe dieser Kapazität verbringt, sollten Sie erwägen, die minimale DCU-Einstellung zu erhöhen. Auf diese Weise kann eine Instance im Leerlauf schneller wieder auf die maximale Kapazität hochskaliert werden.
- Bestimmte Instance-Limits werden durch die aktuelle Kapazität der serverlosen Instance bestimmt, z. B. Verbindungslimit, Cursorlimit und Limit für offene Transaktionen. Wenn die aktuelle Kapazität der Instance gering ist, sind auch die Grenzwerte entsprechend gering. Wenn diese Grenzwerte ein Problem darstellen, wenn Ihre serverlose Instance auf ihren `MinCapacity` Wert herunterskaliert wird, sollten Sie eine Erhöhung `MinCapacity` auf einen höheren Wert in Betracht ziehen. Weitere Informationen finden Sie unter Beschränkungen für serverlose Amazon DocumentDB DocumentDB-Instances.
- Darüber hinaus gelten für bestimmte Instance-Limits ein niedrigerer Höchstwert, wenn dieser auf weniger als oder gleich 1,0 DCUs festgelegt `MinCapacity` ist, wie z. B. das Limit für aktive Verbindungen, das Cursorlimit und das Limit für offene Transaktionen. Wenn diese Obergrenzen

für Ihre Arbeitslast nicht ausreichen, verwenden Sie einen `MinCapacity` Wert von mindestens 1,5 DCUs. Weitere Informationen finden Sie unter Beschränkungen für serverlose Amazon DocumentDB DocumentDB-Instances.

Anweisungen zum Ändern der Skalierungskonfiguration eines Clusters finden Sie unter. Serverlose Verwaltung von Amazon DocumentDB

`MaxCapacity`Einstellung für einen serverlosen DocumentDB-Cluster auswählen

Es ist verlockend, immer einen hohen Wert für die maximale serverlose Kapazität von DocumentDB zu wählen. Eine große maximale Kapazität ermöglicht es der Instanz, am stärksten zu skalieren, wenn sie eine intensive Arbeitslast ausführt. Mit einem niedrigen Wert entfällt die Möglichkeit unerwarteter Gebühren. Je nachdem, wie Sie diesen Cluster verwenden und die anderen Einstellungen konfigurieren, kann der effektivste Wert höher oder niedriger sein, als Sie ursprünglich dachten. Berücksichtigen Sie bei der Auswahl der maximalen Kapazitätseinstellung die folgenden Faktoren:

- Die maximale Kapazität muss mindestens so hoch sein wie die Mindestkapazität. Sie können die minimale und maximale Kapazität auf den gleichen Wert festlegen. In diesem Fall skaliert sich die Kapazität jedoch niemals hoch oder herunter. Daher ist die Verwendung identischer Werte für die minimale und maximale Kapazität außerhalb von Testsituationen nicht geeignet.
- Die maximale Kapazität muss mindestens 1,0 DCUs und darf höchstens 256 DCUs betragen.
- Wir empfehlen, die Skalierung und die Ressourcennutzung Ihrer serverlosen Instances zu überwachen. Wenn Ihre serverlose Instance häufig auf maximale Kapazität skaliert und dabei auf Ressourcenbeschränkungen stößt (z. B. wenn die `DCUUtilization` Metrik bei 100,0 liegt), empfehlen wir, einen höheren Wert auszuwählen. `MaxCapacity` Weitere Informationen finden Sie unter Serverlose Überwachung von Amazon DocumentDB.
- Wenn Sie in der Regel die Instanzklasse Ihrer bereitgestellten Instanzen in Erwartung einer besonders hohen oder niedrigen Arbeitslast ändern, können Sie diese Erfahrung nutzen, um den entsprechenden serverlosen Kapazitätsbereich von DocumentDB abzuschätzen. Informationen zur Bestimmung der Speichergröße der bereitgestellten Amazon DocumentDB DocumentDB-Instances finden Sie unter. Instance-Limits

  Nehmen wir beispielsweise an, Sie verwenden die `db.r6g.4xlarge` Instance-Klasse, wenn Ihr Cluster eine hohe Arbeitslast hat. Diese Instanzklasse hat 128 GiB Arbeitsspeicher. Daher können

Sie eine maximale DCU-Einstellung von 64 angeben, um eine serverlose Instanz einzurichten, die auf ungefähr dieselbe Kapazität skaliert werden kann. Das liegt daran, dass jede DCU ungefähr 2 GiB Speicher entspricht. Sie können einen etwas höheren Wert angeben, damit die Instance weiter skaliert werden kann, falls Ihre `db.r6g.4xlarge` Instance manchmal nicht über genügend Kapazität verfügt, um die Arbeitslast effektiv zu bewältigen.

- Wenn Sie eine Budgetobergrenze für Ihre Datenbanknutzung haben, wählen Sie einen Wert, der innerhalb dieser Obergrenze bleibt, auch wenn all Ihre serverlosen Instances ständig mit maximaler Kapazität laufen. Denken Sie daran, dass, wenn Sie n serverlose Instances in Ihrem Cluster haben, die theoretische maximale serverlose Kapazität, die der Cluster zu einem beliebigen Zeitpunkt verbrauchen kann, das n-fache der maximalen DCU-Einstellung für den Cluster beträgt. (Der tatsächlich verbrauchte Betrag ist möglicherweise geringer, wenn beispielsweise einige Reader unabhängig vom Writer skalieren.)
- Wenn Sie serverlose Reader-Instances verwenden, um einen Teil der schreibgeschützten Arbeitslast von der Writer-Instanz auszulagern, können Sie möglicherweise eine niedrigere Einstellung für die maximale Kapazität wählen. Sie tun dies, um zu berücksichtigen, dass nicht jede Reader-Instanz so hoch skaliert werden muss, als ob der Cluster nur eine einzige Instanz enthält.
- Angenommen, Sie möchten sich vor übermäßiger Auslastung aufgrund falsch konfigurierter Datenbankparameter oder ineffizienter Abfragen in Ihrer Anwendung schützen. In diesem Fall können Sie eine versehentliche Überbeanspruchung vermeiden, indem Sie eine maximale Kapazitätseinstellung wählen, die niedriger ist als die absolut höchste, die Sie festlegen können.
- Wenn Spitzen aufgrund realer Benutzeraktivitäten zwar selten sind, aber dennoch auftreten, können Sie diese Situationen bei der Auswahl der maximalen Kapazitätseinstellung berücksichtigen. Wenn die Priorität darin besteht, dass die Anwendung weiterhin mit voller Leistung und Skalierbarkeit ausgeführt wird, können Sie eine maximale Kapazitätseinstellung angeben, die höher ist, als Sie bei normaler Auslastung beobachten. Wenn es akzeptabel ist, dass die Anwendung bei sehr extremen Aktivitätsspitzen mit reduziertem Durchsatz ausgeführt wird, können Sie eine etwas niedrigere maximale Kapazitätseinstellung wählen. Stellen Sie sicher, dass Sie eine Einstellung auswählen, die immer noch über genügend Speicher- und CPU-Ressourcen verfügt, damit die Anwendung weiterhin ausgeführt wird.
- Wenn Sie Einstellungen in Ihrem Cluster aktivieren, die die Speichernutzung für jede Instanz erhöhen, berücksichtigen Sie diesen Speicher, wenn Sie den maximalen DCU-Wert festlegen. Zu diesen Einstellungen gehören die Einstellungen für Performance Insights und globale Cluster. Stellen Sie sicher, dass der maximale DCU-Wert es den serverlosen Instances ermöglicht, so weit zu skalieren, dass sie die Arbeitslast bewältigen können, wenn diese Funktionen verwendet werden. Informationen zur Behebung von Problemen, die durch die Kombination einer niedrigen

maximalen DCU-Einstellung und Amazon DocumentDB DocumentDB-Funktionen verursacht werden, die einen Speicheraufwand verursachen, finden Sie unter Vermeiden von Fehlern aufgrund von zu wenig Speicher (unten).

- Insbesondere empfehlen wir die folgenden Mindestanforderungen `MaxCapacity` für die Verwendung mit den angegebenen Funktionen (diese Empfehlungen können sich ändern):
  - Serverlose Instanzerstellung auf einem Cluster mit einem großen Datenvolumen — 2 DCUs (dazu gehört auch die serverlose Instanzerstellung im Rahmen einer Cluster-Wiederherstellung.)
- Bestimmte Instanzlimits werden durch die aktuelle Kapazität der Instanz bestimmt, z. B. das Verbindungslimit, das Cursorlimit und das Limit für offene Transaktionen. Achten Sie bei der Auswahl des `MaxCapacity` Werts für Ihren Workload darauf, diese Instance-Limits zu berücksichtigen, um zu vermeiden, dass Sie durch eines dieser Limits einen Engpass bekommen. Weitere Informationen finden Sie unter Beschränkungen für serverlose Amazon DocumentDB DocumentDB-Instances.

Anweisungen zum Ändern der Skalierungskonfiguration eines Clusters finden Sie unter. Serverlose Verwaltung von Amazon DocumentDB

Vermeiden von Fehlern aufgrund von zu wenig Speicher

Wenn eine Ihrer serverlosen DocumentDB-Instances ständig die Grenze ihrer maximalen Kapazität erreicht, weist Amazon DocumentDB auf diesen Zustand hin, indem die Instance auf den Status inkompatibler Parameter gesetzt wird. Die Instance hat zwar den Status inkompatibler Parameter, aber einige Operationen sind blockiert. Beispielsweise können Sie die Engine-Version nicht aktualisieren. Weitere Informationen zum Status einer Amazon DocumentDB DocumentDB-Instance finden Sie unter Überwachen des Status einer Amazon DocumentDB DocumentDB-Instance.

In der Regel nimmt Ihre Instance diesen Status an, wenn sie aufgrund von Fehlern aufgrund von Speichermangel häufig neu gestartet wird. Amazon DocumentDB zeichnet ein Ereignis auf, wenn diese Art von Neustart stattfindet. Informationen zum Anzeigen von Ressourcenereignissen finden Sie unterAmazon DocumentDB DocumentDB-Ereignisse anzeigen. Ein ungewöhnlich hoher Speicherverbrauch kann aufgrund des Mehraufwands beim Aktivieren von Einstellungen wie Performance Insights auftreten. Dies kann auch auf eine hohe Arbeitslast auf Ihrer Instanz oder auf die Verwaltung der Metadaten zurückzuführen sein, die mit einer großen Anzahl von Schemaobjekten verknüpft sind.

Wenn der Speicherdruck geringer wird, sodass die Instance ihre maximale Kapazität nicht sehr oft erreicht, ändert Amazon DocumentDB den Instance-Status automatisch wieder auf verfügbar.

Zur Wiederherstellung nach diesem Zustand können Sie einige oder alle der folgenden Aktionen ausführen:

- Erhöhen Sie die untere Kapazitätsgrenze für serverlose Instances, indem Sie den Mindestwert der DocumentDB-Kapazitätseinheit (DCU) für den Cluster ändern. Dadurch werden Probleme vermieden, bei denen eine inaktive Datenbank auf eine Kapazität mit weniger Speicher herunterskaliert wird, als für die in Ihrem Cluster aktivierten Funktionen benötigt wird. Nachdem Sie die DCU-Einstellungen für den Cluster geändert haben, starten Sie die serverlose Instanz neu. Dadurch wird geprüft, ob Amazon DocumentDB den Status wieder auf verfügbar zurücksetzen kann.
- Erhöhen Sie die Kapazitätsobergrenze für serverlose Instances, indem Sie den maximalen DCU-Wert für den Cluster ändern. Auf diese Weise werden Probleme vermieden, bei denen eine ausgelastete Datenbank nicht auf eine Kapazität mit genügend Speicher für die in Ihrem Cluster aktivierten Funktionen und die Datenbank-Workload hochskaliert werden kann. Nachdem Sie die DCU-Einstellungen für den Cluster geändert haben, starten Sie die serverlose Instanz neu. Dadurch wird geprüft, ob Amazon DocumentDB den Status wieder auf verfügbar zurücksetzen kann.
- Deaktivieren Sie Konfigurationseinstellungen, die Speicher-Overhead erfordern. Nehmen wir zum Beispiel an, Sie haben eine Funktion wie Performance Insights aktiviert, verwenden sie aber nicht. Wenn ja, können Sie sie ausschalten. Oder Sie können die Mindest- und Höchstkapazitätswerte für den Cluster höher anpassen, um dem von diesen Funktionstypen verwendeten Speicher Rechnung zu tragen. Richtlinien zur Auswahl der minimalen und maximalen Kapazitätseinstellungen finden Sie unter Auswahl des Skalierungskapazitätsbereichs für einen serverlosen DocumentDB-Cluster.
- Reduzieren Sie die Arbeitslast auf der Instanz. Sie können dem Cluster beispielsweise Reader-Instances hinzufügen, um die Last aus schreibgeschützten Abfragen auf mehrere Instanzen zu verteilen.

Warum wird meine serverlose Instance nicht herunterskaliert?

In einigen Fällen lässt sich DocumentDB serverless nicht auf die Mindestkapazität herunterskalieren, selbst wenn die Datenbank nicht belastet wird. Dies kann aus einem der folgenden Gründe geschehen:

- Performance Insights kann die Ressourcennutzung erhöhen und verhindern, dass die Datenbank auf die Mindestkapazität herunterskaliert wird. Nachstehend sind einige dieser Features aufgeführt:

- Wenn eine Reader-Instance nicht auf das Minimum herunterskaliert wird und dieselbe oder eine höhere Kapazität als die Writer-Instance hat, überprüfen Sie die Prioritätsstufe der Reader-Instance. Serverlose DocumentDB-Reader-Instanzen der Stufe 0 oder 1 verfügen über eine Mindestkapazität, die mindestens so hoch ist wie die der Writer-Instanz. Ändern Sie die Prioritätsstufe der Reader-Instance in 2 oder höher, sodass sie unabhängig von der Writer-Instance hoch- und herunterskaliert wird. Weitere Informationen finden Sie unter Serverlose Skalierung von Amazon DocumentDB.
- Hohe Datenbank-Workloads können die Ressourcennutzung erhöhen.
- Große Datenbank-Volumes können die Ressourcennutzung erhöhen. Amazon DocumentDB verwendet Speicher- und CPU-Ressourcen für die Clusterverwaltung. Amazon DocumentDB benötigt mehr CPU und Arbeitsspeicher, um Cluster mit größeren Datenbankvolumen zu verwalten. Wenn die Mindestkapazität Ihres Clusters unter der für die Clusterverwaltung erforderlichen Mindestkapazität liegt, skaliert Ihr Cluster nicht auf die Mindestkapazität herunter.
- Wartungsaktivitäten im Hintergrund können die Ressourcennutzung regelmäßig erhöhen.

Wenn die Datenbank immer noch nicht auf die konfigurierte Mindestkapazität herunterskaliert wird, beenden Sie die Datenbank und starten Sie sie neu, um alle Speicherfragmente zurückzugewinnen, die sich im Laufe der Zeit angesammelt haben könnten. Das Stoppen und Starten einer Datenbank führt zu Ausfallzeiten, daher empfehlen wir, achtsam vorzugehen.

Serverlose Überwachung von Amazon DocumentDB

Weitere Informationen zur Überwachung in Amazon DocumentDB finden Sie unterAmazon DocumentDB überwachen.

Topics

- Nicht genügend Arbeitsspeicher: Status inkompatibler Parameter
- CloudWatch Amazon-Metriken für DocumentDB serverlos
- Überwachung der serverlosen Leistung von DocumentDB mit Performance Insights

Nicht genügend Arbeitsspeicher: Status inkompatibler Parameter

Wenn eine Ihrer serverlosen Instances ständig die Grenze ihrer maximalen Kapazität erreicht, weist Amazon DocumentDB auf diesen Zustand hin, indem die Instance auf den Status inkompatibler

Parameter gesetzt wird. Weitere Informationen finden Sie unter Vermeiden von Fehlern aufgrund von zu wenig Speicher.

CloudWatch Amazon-Metriken für DocumentDB serverlos

Weitere Informationen zur Verwendung CloudWatch mit Amazon DocumentDB finden Sie unterÜberwachen von Amazon DocumentDB mit CloudWatch.

Sie können Ihre serverlosen Instances unter anzeigen CloudWatch , um die von jeder Instance verbrauchte Kapazität anhand der `ServerlessDatabaseCapacity` Metrik zu überwachen. Sie können auch alle CloudWatch Standardmetriken von DocumentDB überwachen, z. B. `DatabaseConnections` Abfragen. Die vollständige Liste der CloudWatch Metriken, die Sie für Amazon DocumentDB überwachen können, finden Sie unterÜberwachen von Amazon DocumentDB mit CloudWatch. Es ist wichtig, die folgenden Metriken CloudWatch auf Instanzebene zu überwachen, damit Sie verstehen, wie Ihre serverlosen DocumentDB-Instances nach oben und unten skalieren. Alle diese Metriken werden jede Sekunde berechnet. Auf diese Weise können Sie den aktuellen Status Ihrer serverlosen Instances überwachen. Sie können Alarme einrichten, sodass Sie benachrichtigt werden, wenn sich eine serverlose Instance einem Schwellenwert für Kapazitätsmetriken nähert. Sie können feststellen, ob die minimalen und maximalen Kapazitätseinstellungen angemessen sind oder ob Sie sie anpassen müssen. Sie können bestimmen, worauf Sie sich konzentrieren müssen, um die Effizienz Ihrer Datenbank zu optimieren.

- **`ServerlessDatabaseCapacity`**— Als Metrik auf Instanzebene gibt sie die Anzahl der DCUs an, die durch die aktuelle Instanzkapazität repräsentiert wird. Als Metrik auf Clusterebene stellt sie den Durchschnitt der `ServerlessDatabaseCapacity` Werte aller serverlosen DocumentDB-Instances im Cluster dar.
- **`DCUUtilization.`**— Diese Metrik ist neu in DocumentDB serverless. Dieser Wert wird als Prozentsatz dargestellt. Sie wird berechnet als der Wert der `ServerlessDatabaseCapacity` Metrik geteilt durch den maximalen DCU-Wert des Clusters. Beachten Sie die folgenden Richtlinien, um diese Metrik zu interpretieren und Maßnahmen zu ergreifen:
  - Wenn sich diese Metrik einem Wert von nähert`100.0`, wurde die Instance so weit wie möglich hochskaliert. Erwägen Sie, die maximale DCU-Einstellung für den Cluster zu erhöhen. Auf diese Weise können sowohl Writer- als auch Reader-Instances auf eine höhere Kapazität skaliert werden.
  - Nehmen wir an, dass sich eine Reader-Instance aufgrund eines Nur-Lese-Workloads einem Wert `DCUUtilization` von `100.0` annähert, während die Writer-Instanz nicht annähernd ihre maximale Kapazität erreicht. In diesem Fall sollten Sie erwägen, dem Cluster zusätzliche

Reader-Instanzen hinzuzufügen. Auf diese Weise können Sie den schreibgeschützten Teil der Arbeitslast auf mehrere Instanzen verteilen und so die Belastung der einzelnen Reader-Instances reduzieren.

- Angenommen, Sie führen eine Produktionsanwendung aus, bei der Leistung und Skalierbarkeit die Hauptüberlegungen sind. In diesem Fall können Sie den maximalen DCU-Wert für den Cluster auf einen hohen Wert festlegen. Ihr Ziel ist es, dass die `DCUUtilization` Metrik immer unter 100,0 liegt. Bei einem hohen maximalen DCU-Wert können Sie sicher sein, dass genügend Spielraum für den Fall vorhanden ist, dass unerwartete Spitzen bei der Datenbankaktivität auftreten. Berechnet wird Ihnen nur die tatsächlich verbrauchte Datenbankkapazität.

- **`CPUUtilization`**— Diese Metrik wird in DocumentDB serverless anders interpretiert als in bereitgestellten Instanzen. Für DocumentDB serverless ist dieser Wert ein Prozentsatz, der als die Menge der aktuell verwendeten CPU geteilt durch die CPU-Kapazität berechnet wird, die unter dem maximalen DCU-Wert des Clusters verfügbar ist. Amazon DocumentDB überwacht diesen Wert automatisch und skaliert Ihre serverlose Instance, wenn die Instance durchweg einen hohen Anteil ihrer CPU-Kapazität nutzt.

  Wenn sich diese Metrik einem Wert von nähert`100.0`, hat die Instance ihre maximale CPU-Kapazität erreicht. Erwägen Sie, die maximale DCU-Einstellung für den Cluster zu erhöhen. Wenn sich diese Metrik einem Wert von `100.0` auf einer Reader-Instance nähert, sollten Sie erwägen, dem Cluster weitere Reader-Instances hinzuzufügen. Auf diese Weise können Sie den schreibgeschützten Teil der Arbeitslast auf mehrere Instances verteilen und so die Belastung der einzelnen Reader-Instances reduzieren.

- **`FreeableMemory`**— Dieser Wert stellt die Menge an ungenutztem Speicher dar, der verfügbar ist, wenn die serverlose DocumentDB-Instanz auf ihre maximale Kapazität skaliert wird. Für jede DCU, bei der die aktuelle Kapazität unter der maximalen Kapazität liegt, erhöht sich dieser Wert um etwa 2 GiB. Somit nähert sich diese Metrik erst Null, wenn die Instance so weit wie möglich hochskaliert wurde.

  Wenn sich diese Metrik einem Wert von Null nähert, hat die Instance so weit wie möglich hochskaliert und nähert sich der Grenze ihres verfügbaren Speichers. Erwägen Sie, die maximale DCU-Einstellung für den Cluster zu erhöhen. Wenn sich diese Metrik auf einer Reader-Instance einem Wert von Null nähert, sollten Sie erwägen, dem Cluster weitere Reader-Instances hinzuzufügen. Auf diese Weise kann der schreibgeschützte Teil der Arbeitslast auf mehrere Instanzen verteilt werden, wodurch der Speicherverbrauch auf jeder Reader-Instance reduziert wird.

- **`TempStorageIops`**— Die Anzahl der IOPS, die auf dem mit der Instanz verbundenen lokalen Speicher ausgeführt wurden. Dabei sind IOPS für Lese- und Schreibvorgänge enthalten. Diese Metrik stellt eine Zählung dar und wird einmal pro Sekunde gemessen. Dies ist eine neue Metrik für DocumentDB serverless. Details hierzu finden Sie unter Überwachen von Amazon DocumentDB mit CloudWatch.
- **`TempStorageThroughput`**— Die Datenmenge, die zum und vom lokalen Speicher übertragen wird, der der Instanz zugeordnet ist. Diese Metrik wird in Byte angegeben und einmal pro Sekunde gemessen. Dies ist eine neue Metrik für DocumentDB serverless. Details hierzu finden Sie unter Überwachen von Amazon DocumentDB mit CloudWatch.

In der Regel werden die meisten Skalierungen für serverlose DocumentDB-Instanzen durch Speichernutzung und CPU-Aktivität verursacht. Mithilfe der `TempStorageThroughput` Metriken `TempStorageIops` und können Sie die seltenen Fälle diagnostizieren, in denen Netzwerkaktivitäten für Übertragungen zwischen Ihrer Instance und lokalen Speichergeräten für unerwartete Kapazitätssteigerungen verantwortlich sind. Wenn Sie andere Netzwerkaktivitäten überwachen möchten, können Sie diese vorhandenen Metriken verwenden:

- `NetworkReceiveThroughput`
- `NetworkThroughput`
- `NetworkTransmitThroughput`
- `StorageNetworkReceiveThroughput`
- `StorageNetworkThroughput`
- `StorageNetworkTransmitThroughput`

So wirken sich serverlose CloudWatch DocumentDB-Metriken auf Ihre AWS Rechnung

Die Gebühren für serverloses DocumentDB auf Ihrer AWS Rechnung werden auf der Grundlage derselben `ServerlessDatabaseCapacity` Metrik berechnet, die Sie überwachen können. In Fällen, in denen Sie die serverlose Kapazität von DocumentDB nur für einen Teil einer Stunde nutzen, kann der Abrechnungsmechanismus vom berechneten CloudWatch Durchschnitt für diese Metrik abweichen. Es kann auch anders sein, wenn Systemprobleme dazu führen, dass die CloudWatch Metrik für kurze Zeit nicht verfügbar ist. Daher wird DCU-hours auf Ihrer Rechnung möglicherweise ein etwas anderer Wert von angezeigt, als wenn Sie die Zahl selbst anhand des `ServerlessDatabaseCapacity` Durchschnittswerts berechnen würden.

Beispiele für Amazon CloudWatch CLI-Befehle für serverlose DocumentDB-Metriken

Die folgenden AWS CLI Beispiele zeigen, wie Sie die wichtigsten CloudWatch Metriken im Zusammenhang mit DocumentDB serverless überwachen können. Ersetzen Sie in jedem Fall die `Value=` Zeichenfolge für den `--dimensions` Parameter durch den Bezeichner Ihrer eigenen serverlosen DocumentDB-Instanz.

Das folgende Linux-Beispiel zeigt die minimalen, maximalen und durchschnittlichen Kapazitätswerte für eine Instanz, gemessen alle 10 Minuten über eine Stunde. Die Linux-Datumsbefehle geben die Start- und Endzeit relativ zum aktuellen Datum und zur aktuellen Uhrzeit an. Die `sort_by`-Funktion im `--query`-Parameter sortiert die Ergebnisse chronologisch basierend auf dem Feld `Timestamp`.

```
aws cloudwatch get-metric-statistics \
    --metric-name "ServerlessDatabaseCapacity" \
    --start-time "$(date -d '1 hour ago')" \
    --end-time "$(date -d 'now')" \
    --period 600 \
    --namespace "AWS/DocDB" \
    --statistics Minimum Maximum Average \
    --dimensions Name=DBInstanceIdentifier,Value=my_instance \
    --query 'sort_by(Datapoints[*].
{min:Minimum,max:Maximum,avg:Average,ts:Timestamp},&ts)' \
    --output table
```

Das folgende Linux-Beispiel zeigt die Überwachung der Kapazität einer Instanz in einem Cluster. Es misst die minimale, maximale und durchschnittliche Kapazitätsauslastung einer Instanz. Die Messungen werden einmal pro Stunde über einen Zeitraum von drei Stunden durchgeführt. In diesen Beispielen wird die `DCUUtilization` Metrik verwendet, die einen Prozentsatz der Obergrenze für DCUs `ServerlessDatabaseCapacity` darstellt, anstatt eine feste Anzahl von DCUs darzustellen. Auf diese Weise müssen Sie die tatsächlichen Zahlen für die minimalen und maximalen DCU-Werte im Kapazitätsbereich nicht kennen. Sie können Prozentsätze zwischen 0 und 100 sehen.

```
aws cloudwatch get-metric-statistics \
    --metric-name "DCUUtilization" \
    --start-time "$(date -d '3 hours ago')" \
    --end-time "$(date -d 'now')" \
    --period 3600 \
    --namespace "AWS/DocDB" \
    --statistics Minimum Maximum Average \
    --dimensions Name=DBInstanceIdentifier,Value=my_instance \
```

```
    --query 'sort_by(Datapoints[*].
{min:Minimum,max:Maximum,avg:Average,ts:Timestamp},&ts)' \
    --output table
```

Im folgenden Linux-Beispiel werden ähnliche Messungen wie die vorherigen ausgeführt. In diesem Fall gelten die Messungen für die `CPUUtilization`-Metrik Die Messungen werden alle zehn Minuten über einen Zeitraum von einer Stunde durchgeführt. Die Zahlen stellen den Prozentsatz der verfügbaren CPU-Auslastung dar, basierend auf den CPU-Ressourcen, die bei der Einstellung für die maximale Kapazität für die Instanz verfügbar sind.

```
aws cloudwatch get-metric-statistics \
    --metric-name "CPUUtilization" \
    --start-time "$(date -d '1 hour ago')" \
    --end-time "$(date -d 'now')" \
    --period 600 \
    --namespace "AWS/DocDB" \
    --statistics Minimum Maximum Average \
    --dimensions Name=DBInstanceIdentifier,Value=my_instance \
    --query 'sort_by(Datapoints[*].
{min:Minimum,max:Maximum,avg:Average,ts:Timestamp},&ts)' \
    --output table
```

Im folgenden Linux-Beispiel werden ähnliche Messungen wie die vorherigen ausgeführt. In diesem Fall gelten die Messungen für die `FreeableMemory`-Metrik Die Messungen werden alle zehn Minuten über einen Zeitraum von einer Stunde durchgeführt.

```
aws cloudwatch get-metric-statistics \
    --metric-name "FreeableMemory" \
    --start-time "$(date -d '1 hour ago')" \
    --end-time "$(date -d 'now')" \
    --period 600 \
    --namespace "AWS/DocDB" \
    --statistics Minimum Maximum Average \
    --dimensions Name=DBInstanceIdentifier,Value=my_instance \
    --query 'sort_by(Datapoints[*].
{min:Minimum,max:Maximum,avg:Average,ts:Timestamp},&ts)' \
    --output table
```

Überwachung der serverlosen Leistung von DocumentDB mit Performance Insights

Sie können Performance Insights verwenden, um die Leistung von serverlosen DocumentDB-Instanzen zu überwachen. Informationen zu Performance-Insights-Verfahren finden Sie unter Überwachung mit Performance Insights.

Die folgenden neuen Performance Insights Insights-Zähler gelten für serverlose DocumentDB-Instanzen:

- **`os.general.serverlessDBCapacity`**— Die aktuelle Kapazität der Instanz in DCUs. Der Wert entspricht der `ServerlessDatabaseCapacity` CloudWatch Metrik für die Instance.
- **`os.general.dcuUtilization`**— Der prozentuale Anteil der aktuellen Kapazität an der konfigurierten Maximalkapazität. Der Wert entspricht der `DCUUtilization` CloudWatch Metrik für die Instance.
- **`os.general.maxConfiguredDcu`**— Die maximale Kapazität, die Sie für diese serverlose DocumentDB-Instanz konfiguriert haben. Sie wird in DCUs gemessen.
- **`os.general.minConfiguredDcu`**— Die Mindestkapazität, die Sie für diese serverlose DocumentDB-Instanz konfiguriert haben. Sie wird in DCUs gemessen.

Eine vollständige Liste der Performance-Insights-Zähler finden Sie unter Performance Insights für Zählermetriken.

Wenn vCPU-Werte für eine serverlose DocumentDB-Instance in Performance Insights angezeigt werden, stellen diese Werte Schätzungen dar, die auf dem DCU-Wert für die Instanz basieren. Im Standardintervall von einer Minute werden alle fraktionierten vCPU-Werte auf die nächste ganze Zahl aufgerundet. Für längere Intervalle ist der angezeigte vCPU-Wert der Durchschnitt der ganzzahligen vCPU-Werte für jede Minute.

Entwickeln mit Amazon DocumentDB

In diesen Abschnitten wird die Entwicklung mit Amazon DocumentDB behandelt.

Themen

- Connect zu Amazon DocumentDB her
- Programm mit Amazon DocumentDB

Connect zu Amazon DocumentDB her

Amazon DocumentDB bietet mehrere Verbindungsoptionen, darunter programmatische Verbindungen mithilfe von MongoDB-Treibern, Verbindungen von außerhalb einer VPC über SSH-Tunneling oder AWS VPN sowie beliebte Tools wie Studio 3T und. DataGrip Der Service unterstützt Verbindungen mit Replikatgruppen für hohe Verfügbarkeit. Für Analysen und Berichte können Sie mithilfe von JDBC- oder ODBC-Treibern eine Verbindung herstellen. EC2-Instances in derselben VPC können sich direkt mit DocumentDB-Clustern verbinden. Alle Verbindungen erfordern TLS und sind ordnungsgemäß. AWS credentials/authentication

Themen

- Programmgesteuertes Herstellen einer Verbindung zu Amazon DocumentDB
- Von außerhalb einer Amazon VPC eine Verbindung zu einem Amazon DocumentDB-Cluster herstellen
- Als Replikatsatz eine Verbindung zu Amazon DocumentDB herstellen
- Von Studio 3T aus eine Verbindung zu einem Amazon DocumentDB-Cluster herstellen
- Connect zu Amazon DocumentDB her mit DataGrip
- Stellen Sie mithilfe von Amazon EC2 eine Verbindung her
- Stellen Sie mithilfe des Amazon DocumentDB DocumentDB-JDBC-Treibers eine Verbindung her
- Stellen Sie mithilfe des Amazon DocumentDB DocumentDB-ODBC-Treibers eine Verbindung her

Programmgesteuertes Herstellen einer Verbindung zu Amazon DocumentDB

Dieser Abschnitt enthält Codebeispiele, die zeigen, wie Sie mithilfe verschiedener Sprachen eine Verbindung zu Amazon DocumentDB (mit MongoDB-Kompatibilität) herstellen können. Die Beispiele

sind in zwei Abschnitte unterteilt: Verbindung mit einem Cluster mit und ohne aktiviertem TLS (Transport Layer Security). Standardmäßig ist TLS auf Amazon DocumentDB-Clustern aktiviert. Sie können TLS jedoch bei Bedarf deaktivieren. Weitere Informationen finden Sie unter Verschlüsseln von Daten während der Übertragung.

Wenn Sie versuchen, von außerhalb der VPC, in der sich Ihr Cluster befindet, eine Verbindung zu Ihrer Amazon DocumentDB herzustellen, finden Sie weitere Informationen unter. Von außerhalb einer Amazon VPC eine Verbindung zu einem Amazon DocumentDB-Cluster herstellen

Bevor Sie sich mit Ihrem Cluster verbinden, müssen Sie wissen, ob TLS auf dem Cluster aktiviert ist. Der nächste Abschnitt zeigt Ihnen, wie Sie den Wert des Parameters `tls` Ihres Clusters mit der AWS-Managementkonsole oder der AWS CLI bestimmen können. Danach können Sie fortfahren, indem Sie das entsprechende Codebeispiel anwenden.

Themen

- Ermitteln Sie den Wert Ihres tls-Parameters
- Verbindung bei aktiviertem TLS herstellen
- Verbindung bei deaktiviertem TLS herstellen

Ermitteln Sie den Wert Ihres tls-Parameters

Die Feststellung, ob TLS in Ihrem Cluster aktiviert ist, ist ein zweistufiger Prozess, den Sie entweder mit AWS-Managementkonsole oder AWS CLI durchführen können.

1. Bestimmen Sie, welche Parametergruppe Ihren Cluster steuert.

   Using the AWS-Managementkonsole

   1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
   2. Wählen Sie im linken Navigationsbereich Cluster aus.
   3. Wählen Sie in der Liste der Cluster den Namen des Clusters aus.
   4. Auf der anschließend angezeigten Seite werden die Details des von Ihnen ausgewählten Clusters angezeigt. Wählen Sie die Registerkarte Configuration aus. Suchen Sie im Abschnitt Konfigurationen und Status den Namen der Parametergruppe unter Cluster-Parametergruppe.

Using the AWS CLI

Der folgende AWS CLI Code bestimmt, welcher Parameter Ihren Cluster steuert. Ersetzen Sie *sample-cluster* durch den Namen Ihres Clusters.

```
aws docdb describe-db-clusters \
    --db-cluster-identifier sample-cluster \
    --query 'DBClusters[*].[DBClusterIdentifier,DBClusterParameterGroup]'
```

Die Ausgabe dieser Operation sieht in etwa wie folgt aus:

```
[
       [
           "sample-cluster",
           "sample-parameter-group"
       ]
]
```

2. Bestimmen Sie den Wert des Parameters **`tls`** in der Parametergruppe Ihres Clusters.

Using the AWS-Managementkonsole

1. Wählen Sie im Navigationsbereich Parameter groups (Parametergruppen) aus.
2. Wählen Sie im Fenster Cluster-Parametergruppen den Namen Ihrer Cluster-Parametergruppe aus Schritt 1d aus.
3. Auf der Ergebnisseite werden die Parameter der Cluster-Parametergruppe angezeigt. Hier können Sie den Wert des `tls`-Parameters sehen. Informationen zum Ändern dieses Parameters finden Sie unter Amazon DocumentDB-Cluster-Parametergruppen ändern.

Using the AWS CLI

Sie können den `describe-db-cluster-parameters` AWS CLI Befehl verwenden, um die Details der Parameter in Ihrer Cluster-Parametergruppe anzuzeigen.

- **`--describe-db-cluster-parameters`**— Um alle Parameter innerhalb einer Parametergruppe und ihre Werte aufzulisten.
  - **`--db-cluster-parameter-group name`** – Erforderlich. Der Name Ihrer Cluster-Parametergruppe.

Ersetzen Sie in den folgenden Beispielen jeden *user input placeholder* durch die Informationen Ihres Clusters.

```
aws docdb describe-db-cluster-parameters \
    --db-cluster-parameter-group-name sample-parameter-group
```

Die Ausgabe dieser Operation sieht in etwa wie folgt aus:

```
{
        "Parameters": [
            {
                "ParameterName": "profiler_threshold_ms",
                "ParameterValue": "100",
                "Description": "Operations longer than profiler_threshold_ms
 will be logged",
                "Source": "system",
                "ApplyType": "dynamic",
                "DataType": "integer",
                "AllowedValues": "50-2147483646",
                "IsModifiable": true,
                "ApplyMethod": "pending-reboot"
            },
            {
                "ParameterName": "tls",
                "ParameterValue": "disabled",
                "Description": "Config to enable/disable TLS",
                "Source": "user",
                "ApplyType": "static",
                "DataType": "string",
                "AllowedValues": "disabled,enabled,fips-140-3",
                "IsModifiable": true,
                "ApplyMethod": "pending-reboot"
            }
        ]
}
```

> **Note**
>
> Amazon DocumentDB unterstützt FIPS 140-3-Endpunkte, beginnend mit Amazon DocumentDB 5.0-Clustern (Engine-Version 3.0.3727) in diesen Regionen: ca-central-1, us-west-2, us-east-1, us-east-2, us-gov-east-1, us-gov-west-1.

Nachdem Sie den Wert des `tls`-Parameters bestimmt haben, fahren Sie mit dem Herstellen einer Verbindung zu Ihrem Cluster fort, indem Sie eines der Codebeispiele in den folgenden Abschnitten verwenden.

- Verbindung bei aktiviertem TLS herstellen
- Verbindung bei deaktiviertem TLS herstellen

Verbindung bei aktiviertem TLS herstellen

Um ein Codebeispiel für die programmgesteuerte Verbindung zu einem TLS-enabled Amazon DocumentDB-Cluster anzuzeigen, wählen Sie die entsprechende Registerkarte für die Sprache, die Sie verwenden möchten.

Um Daten während der Übertragung zu verschlüsseln, laden Sie den öffentlichen Schlüssel für Amazon DocumentDB `global-bundle.pem` mit dem folgenden Vorgang herunter.

```
wget https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem
```

Wenn sich Ihre Anwendung auf Microsoft Windows befindet und eine PKCS7-Datei benötigt, können Sie das PKCS7-Zertifikat-Bundle herunterladen. Dieses Paket enthält sowohl das Zwischen- als auch das Stammzertifikat unter. https://truststore.pki.rds.amazonaws.com/global/global-bundle.p7b

Python

Der folgende Code zeigt, wie Sie mit Python eine Verbindung zu Amazon DocumentDB herstellen, wenn TLS aktiviert ist.

Ersetzen Sie im folgenden Beispiel jede *`user input placeholder`* durch die Informationen Ihres Clusters.

```
import pymongo
```

```
import sys

##Create a MongoDB client, open a connection to Amazon DocumentDB as a replica set
 and specify the read preference as secondary preferred
client = pymongo.MongoClient('mongodb://sample-user:password@sample-
cluster.node.us-east-1.docdb.amazonaws.com:27017/?tls=true&tlsCAFile=global-
bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')

##Specify the database to be used
db = client.sample_database

##Specify the collection to be used
col = db.sample_collection

##Insert a single document
col.insert_one({'hello':'Amazon DocumentDB'})

##Find the document that was previously written
x = col.find_one({'hello':'Amazon DocumentDB'})

##Print the result to the screen
print(x)

##Close the connection
client.close()
```

Node.js

Der folgende Code zeigt, wie Sie eine Verbindung zu Amazon DocumentDB herstellen Node.js , wenn TLS aktiviert ist.

> **Important**
>
> Es gibt eine bekannte Einschränkung bei Node.js Treibern, die älter als Version 6.13.1 sind und derzeit nicht von der IAM-Identitätsauthentifizierung für Amazon DocumentDB unterstützt werden. Node.js Treiber und Tools, die Node.js Treiber verwenden (z. B. Mongosh), müssen aktualisiert werden, sodass sie die Node.js Treiberversion 6.13.1 oder höher verwenden.

Ersetzen Sie im folgenden Beispiel jede durch die Informationen *user input placeholder* Ihres Clusters.

```
var MongoClient = require('mongodb').MongoClient

//Create a MongoDB client, open a connection to DocDB; as a replica set,
//  and specify the read preference as secondary preferred

var client = MongoClient.connect(
'mongodb://sample-user:password@sample-cluster.node.us-
east-1.docdb.amazonaws.com:27017/sample-database?
tls=true&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false',
{
  tlsCAFile: `global-bundle.pem` //Specify the DocDB; cert
},
function(err, client) {
    if(err)
        throw err;

    //Specify the database to be used
    db = client.db('sample-database');

    //Specify the collection to be used
    col = db.collection('sample-collection');

    //Insert a single document
    col.insertOne({'hello':'Amazon DocumentDB'}, function(err, result){
      //Find the document that was previously written
      col.findOne({'hello':'Amazon DocumentDB'}, function(err, result){
        //Print the result to the screen
        console.log(result);

        //Close the connection
        client.close()
      });
   });
});
```

PHP

Der folgende Code zeigt, wie Sie mit PHP eine Verbindung zu Amazon DocumentDB herstellen, wenn TLS aktiviert ist.

Im folgenden Beispiel ersetzen Sie jeden *user input placeholder* durch die Informationen Ihres Clusters.

```
<?php
//Include Composer's autoloader
require 'vendor/autoload.php';

$TLS_DIR = "/home/ubuntu/global-bundle.pem";

//Create a MongoDB client and open connection to Amazon DocumentDB
$client = new MongoDB\Client("mongodb://sample-user:password@sample-cluster.node.us-
east-1.docdb.amazonaws.com:27017/?retryWrites=false", ["tls" => "true", "tlsCAFile"
 => $TLS_DIR ]);

//Specify the database and collection to be used
$col = $client->sampledatabase->samplecollection;

//Insert a single document
$result = $col->insertOne( [ 'hello' => 'Amazon DocumentDB'] );

//Find the document that was previously written
$result = $col->findOne(array('hello' => 'Amazon DocumentDB'));

//Print the result to the screen
print_r($result);
?>
```

Go

Der folgende Code zeigt, wie Sie mit Go eine Verbindung zu Amazon DocumentDB herstellen, wenn TLS aktiviert ist.

> **Note**
>
> Ab Version 1.2.1 verwendet der MongoDB Go Driver nur das erste CA-Serverzertifikat, das in `sslcertificateauthorityfile` gefunden wurde. Der folgende Beispielcode behebt diese Einschränkung, indem alle in `sslcertificateauthorityfile` gefundenen Serverzertifikate manuell an eine benutzerdefinierte TLS-Konfiguration angehängt werden, die während der Client-Erstellung verwendet wird.

Ersetzen Sie in den folgenden Beispielen jedes Beispiel *`user input placeholder`* durch die Informationen Ihres Clusters.

```
package main

import (
 "context"
 "fmt"
 "log"
 "time"

 "go.mongodb.org/mongo-driver/bson"
 "go.mongodb.org/mongo-driver/mongo"
 "go.mongodb.org/mongo-driver/mongo/options"

 "io/ioutil"
 "crypto/tls"
 "crypto/x509"
 "errors"
)

const (
 // Path to the AWS CA file
 caFilePath = "global-bundle.pem"

 // Timeout operations after N seconds
 connectTimeout  = 5
 queryTimeout    = 30
 username        = "sample-user"
 password        = "password"
 clusterEndpoint = "sample-cluster.node.us-east-1.docdb.amazonaws.com:27017"

 // Which instances to read from
 readPreference = "secondaryPreferred"

 connectionStringTemplate = "mongodb://%s:%s@%s/sample-database?
tls=true&replicaSet=rs0&readpreference=%s"
)

func main() {

 connectionURI := fmt.Sprintf(connectionStringTemplate, username, password,
 clusterEndpoint, readPreference)

 tlsConfig, err := getCustomTLSConfig(caFilePath)
 if err != nil {
```

```
 log.Fatalf("Failed getting TLS configuration: %v", err)
}

client, err :=
mongo.NewClient(options.Client().ApplyURI(connectionURI).SetTLSConfig(tlsConfig))
if err != nil {
 log.Fatalf("Failed to create client: %v", err)
}

ctx, cancel := context.WithTimeout(context.Background(),
connectTimeout*time.Second)
defer cancel()

err = client.Connect(ctx)
if err != nil {
 log.Fatalf("Failed to connect to cluster: %v", err)
}

// Force a connection to verify our connection string
err = client.Ping(ctx, nil)
if err != nil {
 log.Fatalf("Failed to ping cluster: %v", err)
}

fmt.Println("Connected to DocumentDB!")

collection := client.Database("sample-database").Collection("sample-collection")

ctx, cancel = context.WithTimeout(context.Background(), queryTimeout*time.Second)
defer cancel()

res, err := collection.InsertOne(ctx, bson.M{"name": "pi", "value": 3.14159})
if err != nil {
 log.Fatalf("Failed to insert document: %v", err)
}

id := res.InsertedID
log.Printf("Inserted document ID: %s", id)

ctx, cancel = context.WithTimeout(context.Background(), queryTimeout*time.Second)
defer cancel()

cur, err := collection.Find(ctx, bson.D{})
```

```
 if err != nil {
  log.Fatalf("Failed to run find query: %v", err)
 }
 defer cur.Close(ctx)

 for cur.Next(ctx) {
  var result bson.M
  err := cur.Decode(&result)
  log.Printf("Returned: %v", result)

  if err != nil {
   log.Fatal(err)
  }
 }

 if err := cur.Err(); err != nil {
  log.Fatal(err)
 }

}

func getCustomTLSConfig(caFile string) (*tls.Config, error) {
 tlsConfig := new(tls.Config)
 certs, err := ioutil.ReadFile(caFile)

 if err != nil {
  return tlsConfig, err
 }

 tlsConfig.RootCAs = x509.NewCertPool()
 ok := tlsConfig.RootCAs.AppendCertsFromPEM(certs)

 if !ok {
  return tlsConfig, errors.New("Failed parsing pem file")
 }

 return tlsConfig, nil
```

Java

Wenn Sie von einer Java-Anwendung aus eine Verbindung zu einem TLS-enabled Amazon DocumentDB-Cluster herstellen, muss Ihr Programm die AWS bereitgestellte Zertifizierungsstelle

(CA) -Datei verwenden, um die Verbindung zu validieren. Gehen Sie wie folgt vor, um das Amazon RDS-CA-Zertifikat zu verwenden:

1. Laden Sie die Amazon RDS-CA-Datei von herunter https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem.
2. Erstellen Sie einen Vertrauensspeicher mit dem in der Datei enthaltenen CA-Zertifikat, indem Sie die folgenden Befehle ausführen. Stellen Sie sicher, dass Sie das *truststore-password* in etwas anderes ändern. Wenn Sie auf einen Vertrauensspeicher zugreifen, der sowohl das alte CA-Zertifikat (`rds-ca-2015-root.pem`) als auch das neue CA-Zertifikat (`rds-ca-2019-root.pem`) enthält, können Sie das Zertifikat-Bundle in den Vertrauensspeicher importieren.

   Nachfolgend finden Sie ein Beispiel-Shell-Skript, das das Zertifikatpaket in einen Trust Store auf einem Linux-Betriebssystem importiert. Ersetzen Sie in den folgenden Beispielen jedes *user input placeholder* durch Ihre eigenen Informationen. Insbesondere gilt: Wo immer sich das Beispielverzeichnis *mydir* "" im Skript befindet, ersetzen Sie es durch ein Verzeichnis, das Sie für diese Aufgabe erstellt haben.

```
mydir=/tmp/certs
truststore=${mydir}/rds-truststore.jks
storepassword=truststore-password

curl -sS "https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem" >
 ${mydir}/global-bundle.pem
awk 'split_after == 1 {n++;split_after=0} /-----END CERTIFICATE-----/
 {split_after=1}{print > "rds-ca-" n ".pem"}' < ${mydir}/global-bundle.pem

for CERT in rds-ca-*; do
  alias=$(openssl x509 -noout -text -in $CERT | perl -ne 'next unless /
Subject:/; s/.*(CN=|CN = )//; print')
  echo "Importing $alias"
  keytool -import -file ${CERT} -alias "${alias}" -storepass ${storepassword} -
keystore ${truststore} -noprompt
  rm $CERT
done

rm ${mydir}/global-bundle.pem

echo "Trust store content is: "
```

```
keytool -list -v -keystore "$truststore" -storepass ${storepassword} | grep
 Alias | cut -d " " -f3- | while read alias
do
   expiry=`keytool -list -v -keystore "$truststore" -storepass ${storepassword}
 -alias "${alias}" | grep Valid | perl -ne 'if(/until: (.*?)\n/) { print
 "$1\n"; }'`
   echo " Certificate ${alias} expires in '$expiry'"
done
```

Es folgt ein Beispiel für ein Shell-Skript, das das Zertifikatspaket in einen Vertrauensspeicher unter macOS importiert.

```
mydir=/tmp/certs
truststore=${mydir}/rds-truststore.jks
storepassword=truststore-password

curl -sS "https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem" >
 ${mydir}/global-bundle.pem
split -p "-----BEGIN CERTIFICATE-----" ${mydir}/global-bundle.pem rds-ca-

for CERT in rds-ca-*; do
  alias=$(openssl x509 -noout -text -in $CERT | perl -ne 'next unless /
Subject:/; s/.*(CN=|CN = )//; print')
  echo "Importing $alias"
  keytool -import -file ${CERT} -alias "${alias}" -storepass ${storepassword} -
keystore ${truststore} -noprompt
  rm $CERT
done

rm ${mydir}/global-bundle.pem

echo "Trust store content is: "

keytool -list -v -keystore "$truststore" -storepass ${storepassword} | grep
 Alias | cut -d " " -f3- | while read alias
do
   expiry=`keytool -list -v -keystore "$truststore" -storepass ${storepassword}
 -alias "${alias}" | grep Valid | perl -ne 'if(/until: (.*?)\n/) { print
 "$1\n"; }'`
   echo " Certificate ${alias} expires in '$expiry'"
done
```

3. Verwenden Sie das `keystore` in Ihrem Programm, indem Sie die folgenden Systemeigenschaften in Ihrer Anwendung festlegen, bevor Sie eine Verbindung zum Amazon DocumentDB-Cluster herstellen.

```
javax.net.ssl.trustStore: truststore
javax.net.ssl.trustStorePassword: truststore-password;
```

4. Der folgende Code zeigt, wie Sie mit Java eine Verbindung zu Amazon DocumentDB herstellen, wenn TLS aktiviert ist.

   Ersetzen Sie im folgenden Beispiel jede *`user input placeholder`* durch die Informationen Ihres Clusters.

```
package com.example.documentdb;

import com.mongodb.client.*;
import org.bson.Document;

public final class Test {
    private Test() {
    }
    public static void main(String[] args) {

        String template = "mongodb://%s:%s@%s/sample-database?
ssl=true&replicaSet=rs0&readpreference=%s";
        String username = "sample-user";
        String password = "password";
        String clusterEndpoint = "sample-cluster.node.us-
east-1.docdb.amazonaws.com:27017";
        String readPreference = "secondaryPreferred";
        String connectionString = String.format(template, username, password,
 clusterEndpoint, readPreference);

        String truststore = "truststore";
        String truststorePassword = "truststore-password";

        System.setProperty("javax.net.ssl.trustStore", truststore);
        System.setProperty("javax.net.ssl.trustStorePassword",
 truststorePassword);

        MongoClient mongoClient = MongoClients.create(connectionString);
```

```
        MongoDatabase testDB = mongoClient.getDatabase("sample-database");
        MongoCollection<Document> numbersCollection =
 testDB.getCollection("sample-collection");

        Document doc = new Document("name", "pi").append("value", 3.14159);
        numbersCollection.insertOne(doc);

        MongoCursor<Document> cursor = numbersCollection.find().iterator();
        try {
            while (cursor.hasNext()) {
                System.out.println(cursor.next().toJson());
            }
        } finally {
            cursor.close();
        }

    }
}
```

C# / .NET

Der folgende Code zeigt, wie Sie mit C# /.NET eine Verbindung zu Amazon DocumentDB herstellen, wenn TLS aktiviert ist.

Im folgenden Beispiel ersetzen Sie jeden *`user input placeholder`* durch die Informationen Ihres Clusters.

```
using System;
using System.Text;
using System.Linq;
using System.Collections.Generic;
using System.Security.Cryptography;
using System.Security.Cryptography.X509Certificates;
using System.Net.Security;
using MongoDB.Driver;
using MongoDB.Bson;

namespace DocDB
{
    class Program
    {
        static void Main(string[] args)
```

```
        {
            string template = "mongodb://{0}:{1}@{2}/sampledatabase?
tls=true&replicaSet=rs0&readpreference={3}";
            string username = "sample-user";
            string password = "password";
            string readPreference = "secondaryPreferred";
            string clusterEndpoint="sample-cluster.node.us-
east-1.docdb.amazonaws.com:27017";
            string connectionString = String.Format(template, username, password,
 clusterEndpoint, readPreference);

            string pathToCAFile = "<PATH/global-bundle.p7b_file>";

            // ADD CA certificate to local trust store
            // DO this once - Maybe when your service starts
            X509Store localTrustStore = new X509Store(StoreName.Root);
            X509Certificate2Collection certificateCollection = new
 X509Certificate2Collection();
            certificateCollection.Import(pathToCAFile);
            try
            {
                localTrustStore.Open(OpenFlags.ReadWrite);
                localTrustStore.AddRange(certificateCollection);
            }
            catch (Exception ex)
            {
                Console.WriteLine("Root certificate import failed: " + ex.Message);
                throw;
            }
            finally
            {
                localTrustStore.Close();
            }

            var settings = MongoClientSettings.FromUrl(new
 MongoUrl(connectionString));
            var client = new MongoClient(settings);

            var database = client.GetDatabase("sampledatabase");
            var collection =
 database.GetCollection<BsonDocument>("samplecollection");
            var docToInsert = new BsonDocument { { "pi", 3.14159 } };
            collection.InsertOne(docToInsert);
        }
```

```
    }
}
```

MongoDB Shell

Der folgende Code zeigt, wie Sie mit der neuesten Version, Mongosh, oder der vorherigen Mongo-Shell-Version eine Verbindung zu Amazon DocumentDB herstellen und diese abfragen, wenn TLS aktiviert ist.

Stellen Sie mit Mongosh eine Connect zu Amazon DocumentDB her

> **Important**
>
> Es gibt eine bekannte Einschränkung bei Node.js Treibern, die älter als Version 6.13.1 sind und derzeit nicht von der IAM-Identitätsauthentifizierung für Amazon DocumentDB unterstützt werden. Node.js Treiber und Tools, die Node.js Treiber verwenden (z. B. Mongosh), müssen aktualisiert werden, sodass sie die Node.js Treiberversion 6.13.1 oder höher verwenden.

Ersetzen Sie in den folgenden Beispielen jeweils die Informationen *user input placeholder* Ihres Clusters.

```
mongosh --tls --host cluster-end-point:27017 --tlsCAFile  global-bundle.pem --
username sample-user --password password --retryWrites false
```

Stellen Sie mit der vorherigen Mongo-Shell-Version eine Connect zu Amazon DocumentDB her

Wenn Sie IAM verwenden, müssen Sie eine frühere Version von Mongo Shell verwenden. Geben Sie eine der folgenden Befehlsoptionen ein:

```
mongo --ssl --host cluster-end-point:27017 --sslCAFile global-bundle.pem --
username sample-user --password password
```

Wenn Sie eine Version gleich oder höher als 4.2 verwenden, verwenden Sie den folgenden Code, um eine Verbindung herzustellen. Wiederholbare Schreibvorgänge werden in Amazon DocumentDB nicht unterstützt. Wenn Sie eine ältere Mongo-Shell (nicht Mongosh) verwenden, nehmen Sie den `retryWrites=false` Befehl nicht in eine Codezeichenfolge auf.

Standardmäßig sind wiederholbare Schreibvorgänge deaktiviert. `retryWrites=false`Das Einschließen kann zu einem Fehler bei normalen Lesebefehlen führen.

```
mongo --tls --host cluster-end-point:27017 --tlsCAFile global-bundle.pem --
username sample-user --password password
```

Testen Sie die Verbindung

1. Fügen Sie ein einzelnes Dokument ein.

   ```
   db.myTestCollection.insertOne({'hello':'Amazon DocumentDB'})
   ```

2. Suchen Sie das Dokument, das zuvor eingefügt wurde.

   ```
   db.myTestCollection.find({'hello':'Amazon DocumentDB'})
   ```

R

Der folgende Code zeigt, wie Sie mit R mithilfe von mongolite (https://jeroen.github.io/mongolite/) eine Verbindung zu Amazon DocumentDB herstellen, wenn TLS aktiviert ist.

Ersetzen Sie im folgenden Beispiel jede durch die Informationen *user input placeholder* Ihres Clusters.

```
#Include the mongolite library.
library(mongolite)

mongourl <- paste("mongodb://sample-user:password@sample-cluster.node.us-
east-1.docdb.amazonaws.com:27017/test2?ssl=true&",
          "readPreference=secondaryPreferred&replicaSet=rs0", sep="")

#Create a MongoDB client, open a connection to Amazon DocumentDB as a replica
#   set and specify the read preference as secondary preferred
client <-  mongo(url = mongourl, options = ssl_options(weak_cert_validation = F, ca
 ="<PATH/global-bundle.pem>"))

#Insert a single document
str <- c('{"hello" : "Amazon DocumentDB"}')
client$insert(str)
```

```
#Find the document that was previously written
client$find()
```

Ruby

Der folgende Code zeigt, wie Sie mit Ruby eine Verbindung zu Amazon DocumentDB herstellen, wenn TLS aktiviert ist.

Ersetzen Sie im folgenden Beispiel jede *`user input placeholder`* durch die Informationen Ihres Clusters.

```
require 'mongo'
require 'neatjson'
require 'json'
client_host = 'mongodb://sample-cluster.node.us-east-1.docdb.amazonaws.com:27017'
client_options = {
   database: 'test',
   replica_set: 'rs0',
   read: {:secondary_preferred => 1},
   user: 'sample-user',
   password: 'password',
   ssl: true,
   ssl_verify: true,
   ssl_ca_cert: 'PATH/global-bundle.pem',
   retry_writes: false
}


begin
   ##Create a MongoDB client, open a connection to Amazon DocumentDB as a
   ##   replica set and specify the read preference as secondary preferred
   client = Mongo::Client.new(client_host, client_options)

   ##Insert a single document
   x = client[:test].insert_one({"hello":"Amazon DocumentDB"})

   ##Find the document that was previously written
   result = client[:test].find()

   #Print the document
   result.each do |document|
      puts JSON.neat_generate(document)
   end
```

```
end

#Close the connection
client.close
```

Verbindung bei deaktiviertem TLS herstellen

Um ein Codebeispiel für die programmgesteuerte Verbindung zu einem TLS-disabled Amazon DocumentDB-Cluster anzuzeigen, wählen Sie die Registerkarte für die Sprache, die Sie verwenden möchten.

Python

Der folgende Code zeigt, wie Sie mithilfe von Python eine Verbindung zu Amazon DocumentDB herstellen, wenn TLS deaktiviert ist.

Ersetzen Sie im folgenden Beispiel jede *user input placeholder* durch die Informationen Ihres Clusters.

```
## Create a MongoDB client, open a connection to Amazon DocumentDB as a replica set
 and specify the read preference as secondary preferred

import pymongo
import sys

client = pymongo.MongoClient('mongodb://sample-user:password@sample-cluster.node.us-
east-1.docdb.amazonaws.com:27017/?
replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false')

##Specify the database to be used
db = client.sample_database

##Specify the collection to be used
col = db.sample_collection

##Insert a single document
col.insert_one({'hello':'Amazon DocumentDB'})

##Find the document that was previously written
x = col.find_one({'hello':'Amazon DocumentDB'})

##Print the result to the screen
```

```
print(x)

##Close the connection
client.close()
```

Node.js

Der folgende Code zeigt, wie Sie eine Verbindung zu Amazon DocumentDB herstellen Node.js , wenn TLS deaktiviert ist.

> **Important**
>
> Es gibt eine bekannte Einschränkung bei Node.js Treibern, die älter als Version 6.13.1 sind und derzeit nicht von der IAM-Identitätsauthentifizierung für Amazon DocumentDB unterstützt werden. Node.js Treiber und Tools, die Node.js Treiber verwenden (z. B. Mongosh), müssen aktualisiert werden, sodass sie die Node.js Treiberversion 6.13.1 oder höher verwenden.

Ersetzen Sie im folgenden Beispiel jede durch die Informationen *user input placeholder* Ihres Clusters.

```
var MongoClient = require('mongodb').MongoClient;

//Create a MongoDB client, open a connection to Amazon DocumentDB as a replica set,
//  and specify the read preference as secondary preferred
var client = MongoClient.connect(
'mongodb://sample-user:password@sample-cluster.node.us-
east-1.docdb.amazonaws.com:27017/sample-database?
replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false',
{
  useNewUrlParser: true
},

function(err, client) {
    if(err)
        throw err;
    //Specify the database to be used
    db = client.db('sample-database');

    //Specify the collection to be used
```

```
    col = db.collection('sample-collection');

    //Insert a single document
    col.insertOne({'hello':'Amazon DocumentDB'}, function(err, result){
      //Find the document that was previously written
      col.findOne({'hello':'Amazon DocumentDB'}, function(err, result){
        //Print the result to the screen
        console.log(result);

        //Close the connection
        client.close()
      });
   });
});
```

PHP

Der folgende Code zeigt, wie Sie mit PHP eine Verbindung zu Amazon DocumentDB herstellen, wenn TLS deaktiviert ist.

Ersetzen Sie im folgenden Beispiel jede *user input placeholder* durch die Informationen Ihres Clusters.

```
<?php
//Include Composer's autoloader
require 'vendor/autoload.php';

//Create a MongoDB client and open connection to Amazon DocumentDB
$client = new MongoDB\Client("mongodb://sample-user:password@sample-cluster.node.us-
east-1.docdb.amazonaws.com:27017/?retryWrites=false");

//Specify the database and collection to be used
$col = $client->sampledatabase->samplecollection;

//Insert a single document
$result = $col->insertOne( [ 'hello' => 'Amazon DocumentDB'] );

//Find the document that was previously written
$result = $col->findOne(array('hello' => 'Amazon DocumentDB'));

//Print the result to the screen
print_r($result);
?>
```

Go

Der folgende Code zeigt, wie Sie mit Go eine Verbindung zu Amazon DocumentDB herstellen, wenn TLS deaktiviert ist.

Ersetzen Sie im folgenden Beispiel beide *user input placeholder* durch die Informationen Ihres Clusters.

```
package main

import (
 "context"
 "fmt"
 "log"
 "time"

 "go.mongodb.org/mongo-driver/bson"
 "go.mongodb.org/mongo-driver/mongo"
 "go.mongodb.org/mongo-driver/mongo/options"
)

const (
 // Timeout operations after N seconds
 connectTimeout  = 5
 queryTimeout    = 30
 username        = "sample-user"
 password        = "password"
 clusterEndpoint = "sample-cluster.node.us-east-1.docdb.amazonaws.com:27017"

 // Which instances to read from
 readPreference           = "secondaryPreferred"
 connectionStringTemplate = "mongodb://%s:%s@%s/sample-database?
replicaSet=rs0&readpreference=%s"
)

func main() {

 connectionURI := fmt.Sprintf(connectionStringTemplate, username, password,
 clusterEndpoint, readPreference)

 client, err := mongo.NewClient(options.Client().ApplyURI(connectionURI))
 if err != nil {
  log.Fatalf("Failed to create client: %v", err)
```

```
}

ctx, cancel := context.WithTimeout(context.Background(),
connectTimeout*time.Second)
defer cancel()

err = client.Connect(ctx)
if err != nil {
 log.Fatalf("Failed to connect to cluster: %v", err)
}

// Force a connection to verify our connection string
err = client.Ping(ctx, nil)
if err != nil {
 log.Fatalf("Failed to ping cluster: %v", err)
}

fmt.Println("Connected to DocumentDB!")

collection := client.Database("sample-database").Collection("sample-collection")

ctx, cancel = context.WithTimeout(context.Background(), queryTimeout*time.Second)
defer cancel()

res, err := collection.InsertOne(ctx, bson.M{"name": "pi", "value": 3.14159})
if err != nil {
 log.Fatalf("Failed to insert document: %v", err)
}

id := res.InsertedID
log.Printf("Inserted document ID: %s", id)

ctx, cancel = context.WithTimeout(context.Background(), queryTimeout*time.Second)
defer cancel()

cur, err := collection.Find(ctx, bson.D{})

if err != nil {
 log.Fatalf("Failed to run find query: %v", err)
}
defer cur.Close(ctx)

for cur.Next(ctx) {
 var result bson.M
```

```
  err := cur.Decode(&result)
  log.Printf("Returned: %v", result)

  if err != nil {
   log.Fatal(err)
  }
 }

 if err := cur.Err(); err != nil {
  log.Fatal(err)
 }

}
```

Java

Der folgende Code zeigt, wie Sie mit Java eine Verbindung zu Amazon DocumentDB herstellen, wenn TLS deaktiviert ist.

Ersetzen Sie im folgenden Beispiel jede *user input placeholder* durch die Informationen Ihres Clusters.

```
package com.example.documentdb;

import com.mongodb.MongoClient;
import com.mongodb.MongoClientURI;
import com.mongodb.ServerAddress;
import com.mongodb.MongoException;
import com.mongodb.client.MongoCursor;
import com.mongodb.client.MongoDatabase;
import com.mongodb.client.MongoCollection;
import org.bson.Document;


public final class Main {
    private Main() {
    }
    public static void main(String[] args) {

        String template = "mongodb://%s:%s@%s/sample-database?
replicaSet=rs0&readpreference=%s";
        String username = "sample-user";
        String password = "password";
```

```
        String clusterEndpoint = "sample-cluster.node.us-
east-1.docdb.amazonaws.com:27017";
        String readPreference = "secondaryPreferred";
        String connectionString = String.format(template, username, password,
 clusterEndpoint, readPreference);

        MongoClientURI clientURI = new MongoClientURI(connectionString);
        MongoClient mongoClient = new MongoClient(clientURI);

        MongoDatabase testDB = mongoClient.getDatabase("sample-database");
        MongoCollection<Document> numbersCollection = testDB.getCollection("sample-
collection");

        Document doc = new Document("name", "pi").append("value", 3.14159);
        numbersCollection.insertOne(doc);

        MongoCursor<Document> cursor = numbersCollection.find().iterator();
        try {
            while (cursor.hasNext()) {
                System.out.println(cursor.next().toJson());
            }
        } finally {
            cursor.close();
        }

    }
}
```

C# / .NET

Der folgende Code zeigt, wie Sie mit C# /.NET eine Verbindung zu Amazon DocumentDB herstellen, wenn TLS deaktiviert ist.

Ersetzen Sie im folgenden Beispiel jede *user input placeholder* durch die Informationen Ihres Clusters.

```
using System;
using System.Text;
using System.Linq;
using System.Collections.Generic;
using System.Security.Cryptography;
using System.Security.Cryptography.X509Certificates;
using System.Net.Security;
```

```
using MongoDB.Driver;
using MongoDB.Bson;

namespace CSharpSample
{
   class Program
    {
       static void Main(string[] args)
        {
           string template = "mongodb://{0}:{1}@{2}/sampledatabase?
replicaSet=rs0&readpreference={3}";
           string username = "sample-user";
           string password = "password";
           string clusterEndpoint = "sample-cluster.node.us-
east-1.docdb.amazonaws.com:27017";
           string readPreference = "secondaryPreferred";
           string connectionString = String.Format(template, username, password,
 clusterEndpoint, readPreference);

           var settings = MongoClientSettings.FromUrl(new
 MongoUrl(connectionString));
           var client = new MongoClient(settings);

           var database = client.GetDatabase("sampledatabase");
           var collection =
 database.GetCollection<BsonDocument>("samplecollection");
           var docToInsert = new BsonDocument { { "pi", 3.14159 } };
            collection.InsertOne(docToInsert);
        }
    }
}
```

MongoDB Shell

Der folgende Code zeigt, wie Sie mit der neuesten Version, Mongosh, oder der vorherigen Mongo-Shell-Version eine Verbindung zu Amazon DocumentDB herstellen und diese abfragen, wenn TLS deaktiviert ist.

Stellen Sie mit Mongosh eine Connect zu Amazon DocumentDB her

> **Important**
>
> Es gibt eine bekannte Einschränkung bei Node.js Treibern, die älter als Version 6.13.1 sind und derzeit nicht von der IAM-Identitätsauthentifizierung für Amazon DocumentDB unterstützt werden. Node.js Treiber und Tools, die Node.js Treiber verwenden (z. B. Mongosh), müssen aktualisiert werden, sodass sie die Node.js Treiberversion 6.13.1 oder höher verwenden.

Ersetzen Sie in den folgenden Beispielen jeweils die Informationen *user input placeholder* Ihres Clusters.

```
mongosh --host cluster-end-point:27017 --username sample-user --password password --
retryWrites false
```

Stellen Sie mit der vorherigen Mongo-Shell-Version eine Connect zu Amazon DocumentDB her

Wenn Sie IAM verwenden, müssen Sie eine frühere Version von Mongo Shell verwenden. Geben Sie eine der folgenden Befehlsoptionen ein:

```
mongo --host cluster-end-point:27017 --username sample-user --password password
```

Wenn Sie eine Version gleich oder höher als 4.2 verwenden, verwenden Sie den folgenden Code, um eine Verbindung herzustellen. Wiederholbare Schreibvorgänge werden in Amazon DocumentDB nicht unterstützt. Wenn Sie eine ältere Mongo-Shell (nicht Mongosh) verwenden, nehmen Sie den `retryWrites=false` Befehl nicht in eine Codezeichenfolge auf. Standardmäßig sind wiederholbare Schreibvorgänge deaktiviert. `retryWrites=false`Das Einschließen kann zu einem Fehler bei normalen Lesebefehlen führen.

```
mongo --host cluster-end-point:27017 --username sample-user --password password
```

Testen Sie die Verbindung

1. Fügen Sie ein einzelnes Dokument ein.

   ```
   db.myTestCollection.insertOne({'hello':'Amazon DocumentDB'})
   ```

2. Suchen Sie das Dokument, das zuvor eingefügt wurde.

```
db.myTestCollection.find({'hello':'Amazon DocumentDB'})
```

R

Der folgende Code zeigt, wie Sie mit R mithilfe von mongolite (https://jeroen.github.io/mongolite/) eine Verbindung zu Amazon DocumentDB herstellen, wenn TLS deaktiviert ist.

Ersetzen Sie im folgenden Beispiel jede durch die Informationen *user input placeholder* Ihres Clusters.

```
#Include the mongolite library.
library(mongolite)

#Create a MongoDB client, open a connection to Amazon DocumentDB as a replica
#   set and specify the read preference as secondary preferred
client <- mongo(url = "mongodb://sample-user:password@sample-
cluster.node.us-east-1.docdb.amazonaws.com:27017/sample-database?
readPreference=secondaryPreferred&replicaSet=rs0")

##Insert a single document
str <- c('{"hello" : "Amazon DocumentDB"}')
client$insert(str)

##Find the document that was previously written
client$find()
```

Ruby

Der folgende Code zeigt, wie Sie mit Ruby eine Verbindung zu Amazon DocumentDB herstellen, wenn TLS deaktiviert ist.

Ersetzen Sie im folgenden Beispiel jede *user input placeholder* durch die Informationen Ihres Clusters.

```
require 'mongo'
require 'neatjson'
require 'json'
client_host = 'mongodb://sample-cluster.node.us-east-1.docdb.amazonaws.com:27017'
client_options = {
   database: 'test',
   replica_set: 'rs0',
```

```
   read: {:secondary_preferred => 1},
   user: 'sample-user',
   password: 'password',
   retry_writes: false
}

begin
   ##Create a MongoDB client, open a connection to Amazon DocumentDB as a
   ##   replica set and specify the read preference as secondary preferred
   client = Mongo::Client.new(client_host, client_options)

   ##Insert a single document
   x = client[:test].insert_one({"hello":"Amazon DocumentDB"})

   ##Find the document that was previously written
   result = client[:test].find()

   #Print the document
   result.each do |document|
      puts JSON.neat_generate(document)
   end
end

#Close the connection
client.close
```

Von außerhalb einer Amazon VPC eine Verbindung zu einem Amazon DocumentDB-Cluster herstellen

Amazon DocumentDB-Cluster (mit MongoDB-Kompatibilität) werden in einer Amazon Virtual Private Cloud (Amazon VPC) bereitgestellt. Auf sie kann direkt von Amazon EC2 EC2-Instances oder anderen AWS Services zugegriffen werden, die in derselben Amazon VPC bereitgestellt werden. Darüber hinaus kann Amazon DocumentDB von EC2-Instances oder anderen AWS Services in verschiedenen VPCs in derselben AWS-Region oder anderen Regionen über VPC-Peering aufgerufen werden.

Nehmen wir jedoch an, dass Ihr Anwendungsfall erfordert, dass Sie (oder Ihre Anwendung) von außerhalb der VPC des Clusters auf Ihre Amazon DocumentDB DocumentDB-Ressourcen zugreifen. In diesem Fall können Sie SSH-Tunneling (auch bekannt als Portweiterleitung) verwenden, um auf Ihre Amazon DocumentDB DocumentDB-Ressourcen zuzugreifen.

Die eingehende Diskussion zum Thema SSH-Tunneling geht über den Rahmen dieses Themas hinaus. Weitere Informationen zum SSH-Tunneling finden Sie in den folgenden Ressourcen:

- SSH-Tunnel
- Beispiel zum SSH-Port-Forwarding, insbesondere der Abschnitt Lokales Forwarding.

Um einen SSH-Tunnel zu erstellen, benötigen Sie eine Amazon EC2 EC2-Instance, die in derselben Amazon VPC wie Ihr Amazon DocumentDB-Cluster läuft. Sie können entweder eine vorhandene EC2-Instance in derselben VPC wie Ihr Cluster verwenden oder eine erstellen. Weitere Informationen finden Sie im entsprechenden Thema für Ihr Betriebssystem:

- Erste Schritte mit Amazon EC2 EC2-Linux-Instances
- Erste Schritte mit Amazon EC2 EC2-Windows-Instances

Normalerweise verwenden Sie vermutlich den folgenden Befehl, um sich mit einer EC2-Instance zu verbinden:

```
ssh -i "ec2Access.pem" ubuntu@ec2-34-229-221-164.compute-1.amazonaws.com
```

Falls ja, können Sie einen SSH-Tunnel zum Amazon DocumentDB-Cluster einrichten, `sample-cluster.node.us-east-1.docdb.amazonaws.com` indem Sie den folgenden Befehl auf Ihrem lokalen Computer ausführen. Das `-L`-Flag dient zur Weiterleitung eines lokalen Ports. Wenn Sie einen SSH-Tunnel verwenden, empfehlen wir, dass Sie über den Clusterendpunkt eine Verbindung mit Ihrem Cluster herstellen und nicht versuchen, eine Verbindung im Replikatsatzmodus herzustellen (d. h. `replicaSet=rs0` in der Verbindungszeichenfolge anzugeben), da dies zu einem Fehler führt.

```
ssh -i "ec2Access.pem" -L 27017:sample-cluster.node.us-east-1.docdb.amazonaws.com:27017
 ubuntu@ec2-34-229-221-164.compute-1.amazonaws.com -N
```

Nachdem der SSH-Tunnel erstellt wurde, werden alle Befehle, an die Sie ausgeben, an den Amazon DocumentDB-Cluster weitergeleitet, der in der Amazon `sample-cluster` VPC ausgeführt wird. `localhost:27017` Wenn Transport Layer Security (TLS) auf Ihrem Amazon DocumentDB-Cluster aktiviert ist, müssen Sie den öffentlichen Schlüssel für Amazon DocumentDB von herunterladen. https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem Der folgende Vorgang lädt diese Datei herunter:

```
wget https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem
```

> **Note**
>
> TLS ist standardmäßig für neue Amazon DocumentDB-Cluster aktiviert. Eine Deaktivierung ist jedoch möglich. Weitere Informationen finden Sie unter TLS-Einstellungen für Amazon DocumentDB-Cluster verwalten.

Verwenden Sie den folgenden Befehl, um von außerhalb der Amazon VPC eine Verbindung zu Ihrem Amazon DocumentDB-Cluster herzustellen.

```
mongo --sslAllowInvalidHostnames --ssl --sslCAFile global-bundle.pem --username
 <yourUsername> --password <yourPassword>
```

Als Replikatsatz eine Verbindung zu Amazon DocumentDB herstellen

Wenn Sie mit Amazon DocumentDB (mit MongoDB-Kompatibilität) entwickeln, empfehlen wir, dass Sie eine Verbindung zu Ihrem Cluster als Replikatsatz herstellen und Lesevorgänge mithilfe der integrierten Leseeinstellungen Ihres Treibers an Replikatinstanzen verteilen. In diesem Abschnitt wird genauer beschrieben, was das bedeutet, und es wird beschrieben, wie Sie am Beispiel des SDK für Python eine Verbindung zu Ihrem Amazon DocumentDB-Cluster als Replikatsatz herstellen können.

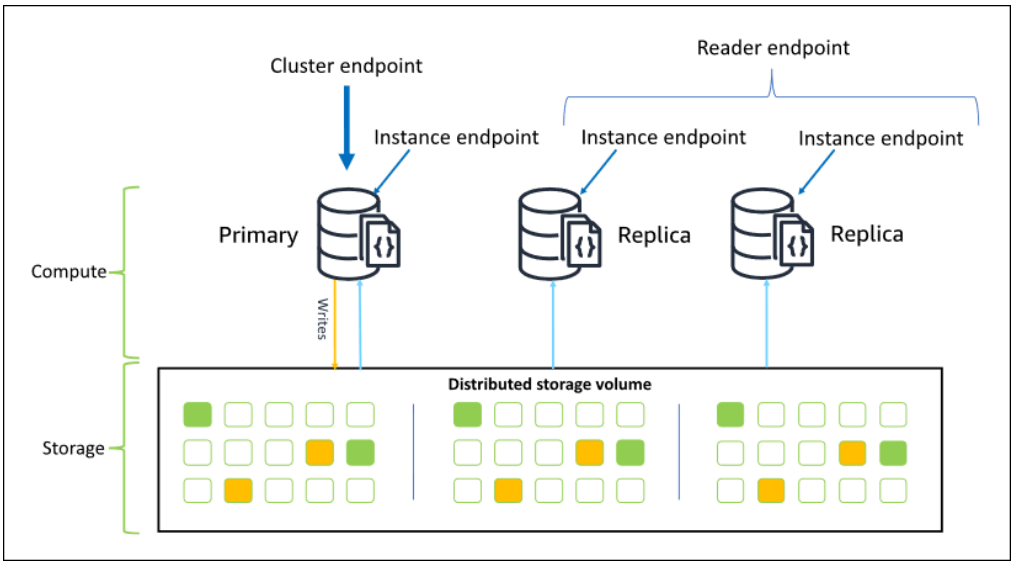
Amazon DocumentDB hat drei Endpunkte, über die Sie eine Verbindung zu Ihrem Cluster herstellen können:

- Cluster-Endpunkt
- Leser-Endpunkt
- Instance-Endpunkte

In den meisten Fällen, wenn Sie eine Verbindung zu Amazon DocumentDB herstellen, empfehlen wir, den Cluster-Endpunkt zu verwenden. Dies ist ein CNAME, der auf die primäre Instance in Ihrem Cluster verweist wie im folgenden Diagramm gezeigt.

Wenn Sie einen SSH-Tunnel verwenden, empfehlen wir, dass Sie über den Clusterendpunkt eine Verbindung mit Ihrem Cluster herstellen und nicht versuchen, eine Verbindung im Replikatsatzmodus herzustellen (d. h. `replicaSet=rs0` in der Verbindungszeichenfolge anzugeben), da dies zu einem Fehler führt.

> **Note**
>
> Weitere Informationen zu Amazon DocumentDB DocumentDB-Endpunkten finden Sie unter. Amazon DocumentDB DocumentDB-Endpunkte



Mithilfe des Cluster-Endpunkts können Sie im Replikatsatzmodus eine Verbindung zu Ihrem Cluster herstellen. Anschließend können Sie die integrierten Treiberfunktionen für Leseeinstellungen verwenden. Im folgenden Beispiel signalisiert die Angabe von `/?replicaSet=rs0` dem SDK, das Sie eine Verbindung als Replikatsatz herstellen möchten. Wenn Sie `/?replicaSet=rs0'` auslassen, leitet der Client alle Anfragen an den Cluster-Endpunkt weiter, d. h. Ihre primäre Instance.

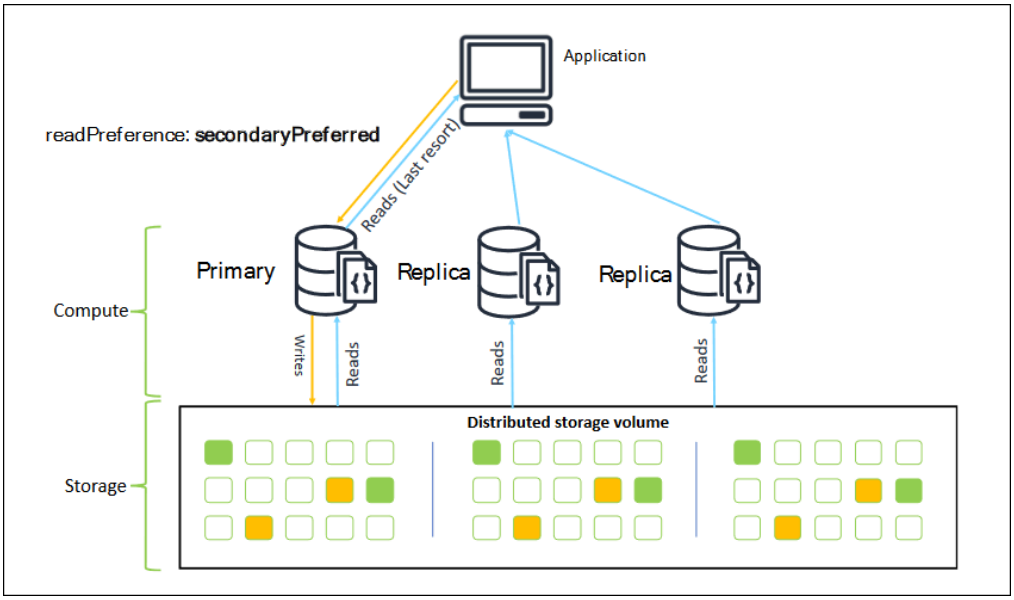
```
## Create a MongoDB client, open a connection to Amazon DocumentDB as a
   ## replica set and specify the read preference as secondary preferred
   client = pymongo.MongoClient('mongodb://<user-name>:<password>@mycluster.node.us-
east-1.docdb.amazonaws.com:27017/?replicaSet=rs0')
```

Der Vorteil der Verbindung als Replikatsatz besteht darin, dass Ihr SDK die Cluster-Topographie automatisch erkennt, auch wenn Instances dem Cluster hinzugefügt oder aus dem Cluster entfernt werden. Anschließend können Sie den Cluster effizienter nutzen, indem Sie Leseanforderungen an Ihre Replikat-Instances weiterleiten.

Wenn Sie eine Verbindung als Replikatsatz herstellen, können Sie die `readPreference` für die Verbindung angeben. Wenn Sie die Leseeinstellung `secondaryPreferred` angeben, leitet der Client Leseabfragen an Ihre Replikate und Schreibabfragen an Ihre primäre Instance weiter (wie

im folgenden Diagramm gezeigt). Damit werden Ihre Cluster-Ressourcen besser genutzt. Weitere Informationen finden Sie unter Lesen Sie die Einstellungsoptionen.

```
## Create a MongoDB client, open a connection to Amazon DocumentDB as a
   ##   replica set and specify the read preference as secondary preferred
client = pymongo.MongoClient('mongodb://<user-name>:<password>@mycluster.node.us-
east-1.docdb.amazonaws.com:27017/?replicaSet=rs0&readPreference=secondaryPreferred')
```



Lesevorgänge von Amazon DocumentDB DocumentDB-Replikaten sind letztendlich konsistent. Sie geben die Daten in der gleichen Reihenfolge zurück, in der sie auf dem primären Knoten geschrieben wurden. Die Replikationsverzögerung beträgt häufig weniger als 50 ms. Sie können die Replikatverzögerung für Ihren Cluster mithilfe der CloudWatch Amazon-Metriken `DBInstanceReplicaLag` und `DBClusterReplicaLagMaximum` überwachen. Weitere Informationen finden Sie unter Überwachen von Amazon DocumentDB mit CloudWatch.

Im Gegensatz zur herkömmlichen monolithischen Datenbankarchitektur trennt Amazon DocumentDB Speicher und Datenverarbeitung. Aufgrund dieser modernen Architektur sollten Sie Lesevorgänge auf Replikat-Instances skalieren. Lesevorgänge auf Replikat-Instances blockieren keine Schreibvorgänge, die von der primären Instance repliziert werden. Sie können einem Cluster bis zu 15 Read-Reaplica-Instances hinzufügen und auf Millionen von Lesevorgängen pro Sekunde skalieren.

Der Hauptvorteil der Verbindung als Replikatsatz und der Verteilung von Lesevorgängen an Replikate besteht darin, dass dies die Gesamtzahl der Ressourcen im Cluster erhöht, die für Ihre Anwendung

verfügbar sind. Wir empfehlen die Verbindung als Replikatsatz als bewährte Methode. Darüber hinaus empfehlen wir diesen Ansatz besonders für die folgenden Szenarien:

- Sie nutzen nahezu 100 Prozent der CPU-Leistung auf Ihrer primären Instance.
- Das Puffer-Cache-Treffer-Verhältnis ist beinahe Null.
- Sie erreichen die Verbindungs- oder Cursor-Limits für eine einzelne Instance.

Die Aufwärtsskalierung einer Cluster-Instance-Größe ist eine Option und kann in einigen Fällen die beste Möglichkeit für die Skalierung des Clusters darstellen. Sie sollten jedoch auch überlegen, wie Sie die Replikate, die in Ihrem Cluster bereits vorhanden sind, besser nutzen können. So können Sie die Skalierung erhöhen, ohne dass für Sie höhere Kosten für die Verwendung eines größeren Instance-Typs anfallen. Wir empfehlen außerdem, diese Grenzwerte (d. h., und`BufferCacheHitRatio`) mithilfe von CloudWatch Alarmen zu überwachen und Warnmeldungen zu erstellen `CPUUtilization`, `DatabaseConnections`, damit Sie wissen, wenn eine Ressource stark beansprucht wird.

Weitere Informationen finden Sie unter den folgenden Themen:

- Bewährte Methoden für Amazon DocumentDB
- Amazon DocumentDB Kontingente und Beschränkungen

Verwenden von Clusterverbindungen

Betrachten Sie ein Szenario, in dem alle Verbindungen in Ihrem Cluster genutzt werden. Beispielsweise hat eine `r5.2xlarge`-Instance ein Limit von 4.500 Verbindungen (und 450 offenen Cursors). Wenn Sie einen Amazon DocumentDB-Cluster mit drei Instanzen erstellen und nur über den Cluster-Endpunkt eine Verbindung zur primären Instance herstellen, liegen Ihre Cluster-Grenzwerte für offene Verbindungen und Cursor bei 4.500 bzw. 450. Sie können diese Limits erreichen, wenn Sie Anwendungen mit zahlreichen Workern verwenden, die in Containern gestartet werden. Die Container öffnen mehrere Verbindungen gleichzeitig und sättigen den Cluster.

Stattdessen könnten Sie sich als Replikatsatz mit dem Amazon DocumentDB-Cluster verbinden und Ihre Lesevorgänge an die Replikatinstanzen verteilen. Anschließend könnten Sie die Anzahl der verfügbaren Verbindungen und Cursors im Cluster effektiv auf 13.500 bzw. 1.350 verdreifachen. Das Hinzufügen weiterer Instances zum Cluster erhöht lediglich die Anzahl der Verbindungen und Cursors für Lese-Workloads. Wenn Sie die Anzahl der Verbindungen für Schreibvorgänge in Ihrem Cluster erhöhen müssen, sollten Sie die Instance-Größe erhöhen.

> **Note**
>
> Die Anzahl der Verbindungen für `large`, `xlarge`, und `2xlarge` Instances erhöht sich mit der Instance-Größe bis zu 4.500. Die maximale Anzahl von Verbindungen pro Instance für `4xlarge` Instances oder größer beträgt 4.500. Weitere Hinweise zu Beschränkungen nach Instance-Typ finden Sie unter Instance-Limits.

In der Regel empfehlen wir das Herstellen von Verbindungen mit Ihrem Cluster unter Verwendung der Leseeinstellung `secondary` nicht. Der Grund hierfür ist, dass die Lesevorgänge fehlschlagen, wenn es keine Replikat-Instances im Cluster gibt. Nehmen wir zum Beispiel an, Sie haben einen Amazon DocumentDB-Cluster mit zwei Instanzen, einem primären und einem Replikat. Wenn die Replikat-Instance ein Problem aufweist, schlagen Leseanforderungen aus einem als `secondary` festgelegten Verbindungspool fehl. Der Vorteil von `secondaryPreferred` besteht darin, dass der Client für Lesevorgänge auf den primären Knoten zurückgreift, wenn er keine geeignete Replikat-Instance für die Verbindung finden kann.

Mehrere Verbindungspools

In einigen Szenarien müssen Lesevorgänge in einer Anwendung eine Lese-nach-Schreib-Konsistenz aufweisen, die nur von der primären Instance in Amazon DocumentDB bedient werden kann. In diesen Szenarien könnten Sie zwei Client-Verbindungspools erstellen: einen für Schreibvorgänge und einen für Lesevorgänge, die „Read after Write Consistency“ benötigen. Ihr Code würde in diesem Fall ungefähr wie folgt aussehen.

```
## Create a MongoDB client,
##    open a connection to Amazon DocumentDB as a replica set and specify the
 readPreference as primary
clientPrimary = pymongo.MongoClient('mongodb://<user-
name>:<password>@mycluster.node.us-east-1.docdb.amazonaws.com:27017/?
replicaSet=rs0&readPreference=primary')

## Create a MongoDB client,
##    open a connection to Amazon DocumentDB as a replica set and specify the
 readPreference as secondaryPreferred
secondaryPreferred = pymongo.MongoClient('mongodb://<user-
name>:<password>@mycluster.node.us-east-1.docdb.amazonaws.com:27017/?
replicaSet=rs0&readPreference=secondaryPreferred')
```

Eine weitere Möglichkeit besteht darin, einen einzelnen Verbindungspool zu erstellen und die Leseeinstellung für eine bestimmte Sammlung zu überschreiben.

```
##Specify the collection and set the read preference level for that collection
col = db.review.with_options(read_preference=ReadPreference.SECONDARY_PREFERRED)
```

Zusammenfassung

Um die Ressourcen im Cluster besser zu nutzen, sollten Sie Verbindungen mit dem Cluster über den Replikatsatzmodus herstellen. Sie können die Zahl der Lesevorgänge für Ihre Anwendung skalieren, indem Sie Ihre Lesevorgänge an die Replikat-Instances verteilen, wenn dies für Ihre Anwendung geeignet ist.

Von Studio 3T aus eine Verbindung zu einem Amazon DocumentDB-Cluster herstellen

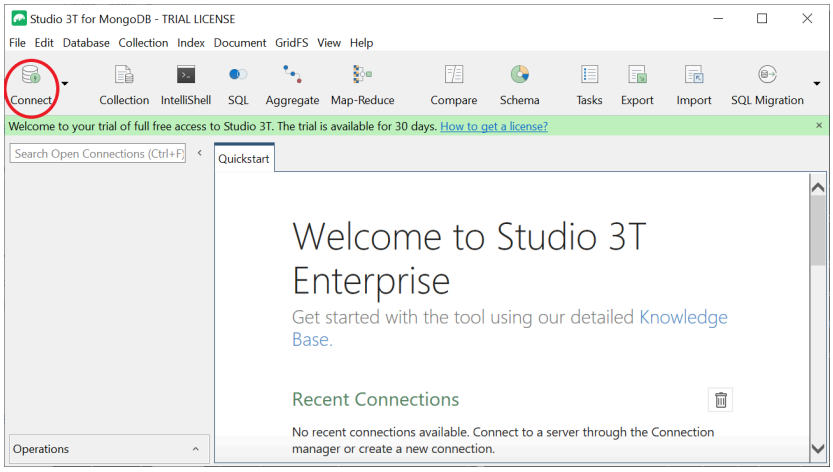
Studio 3T ist eine beliebte GUI und IDE für Entwickler und Dateningenieure, die mit MongoDB arbeiten. Es bietet mehrere leistungsstarke Funktionen Baum-, Tabellen- und JSON-Ansichten Ihrer Daten, einfach import/export in CSV, JSON, SQL und flexible Abfrageoptionen BSON/mongodump, eine visuelle Drag-and-Drop-Benutzeroberfläche, eine integrierte Mongo-Shell mit automatischer Vervollständigung, einen Aggregationspipeline-Editor und SQL-Abfrageunterstützung.

Voraussetzungen

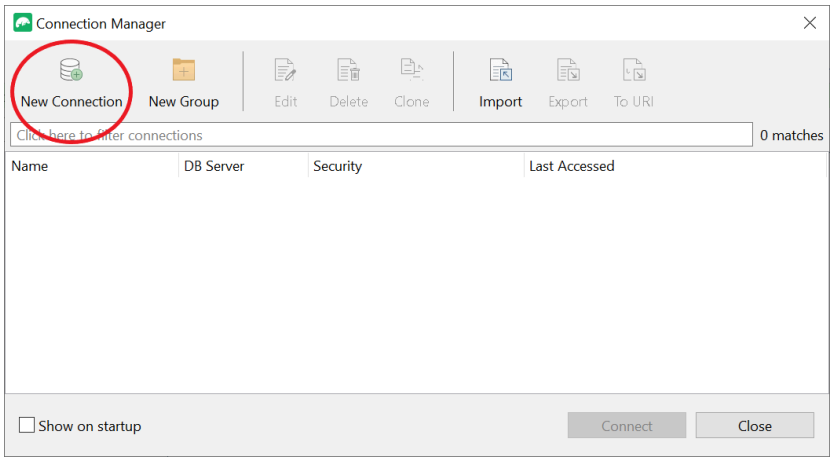
- Wenn Sie noch keinen Amazon DocumentDB-Cluster haben, der Amazon EC2 als bastion/jump Host verwendet, folgen Sie den Anweisungen zur Connect mit Amazon EC2.
- Wenn Sie Studio 3T nicht haben, laden Sie es herunter und installieren Sie es.

Connect zu Studio 3T her

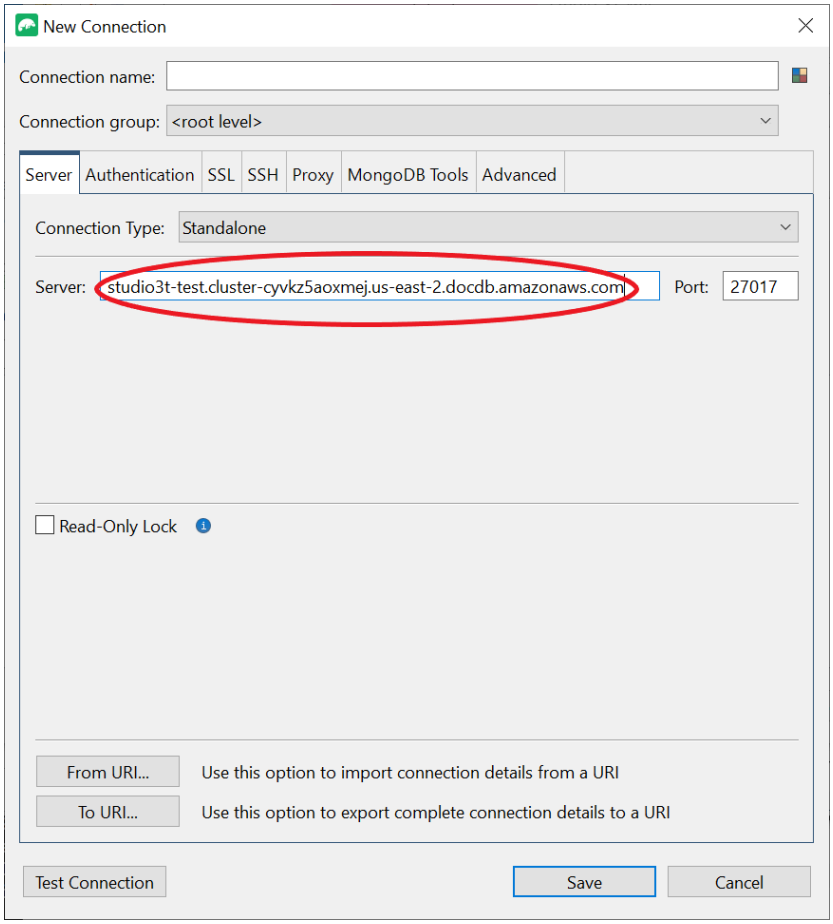
1. Wählen Sie in der oberen linken Ecke der Werkzeugleiste Connect.



2. Wählen Sie in der oberen linken Ecke der Werkzeugleiste die Option Neue Verbindung.

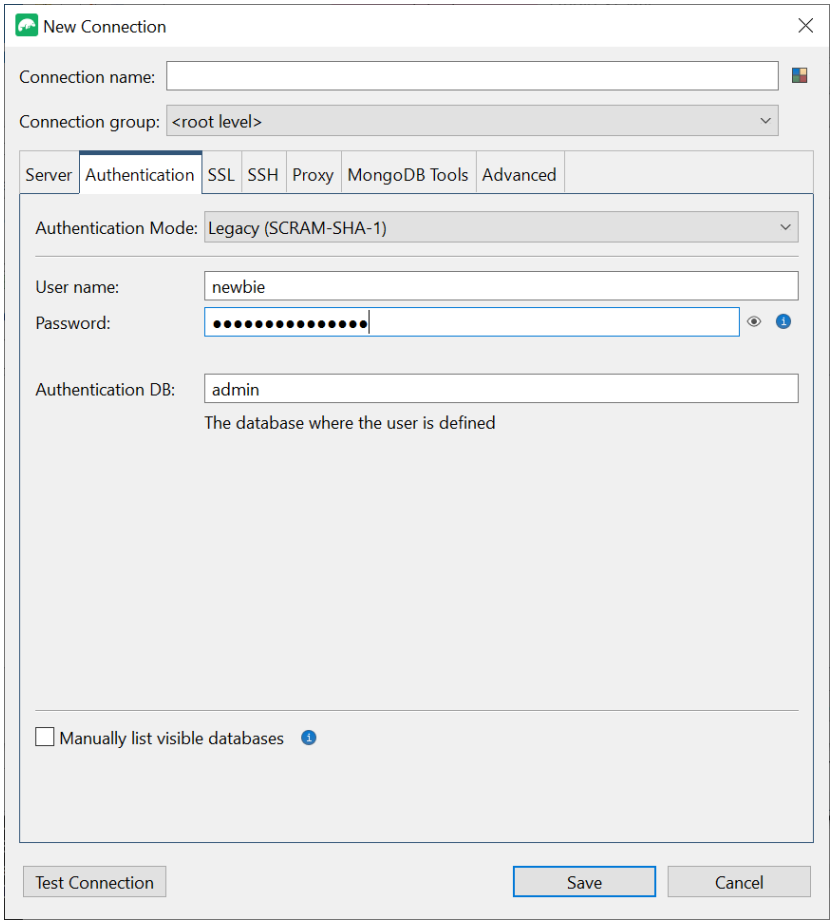


3. Geben Sie auf der Registerkarte Server im Feld Server die Informationen zum Cluster-Endpunkt ein.

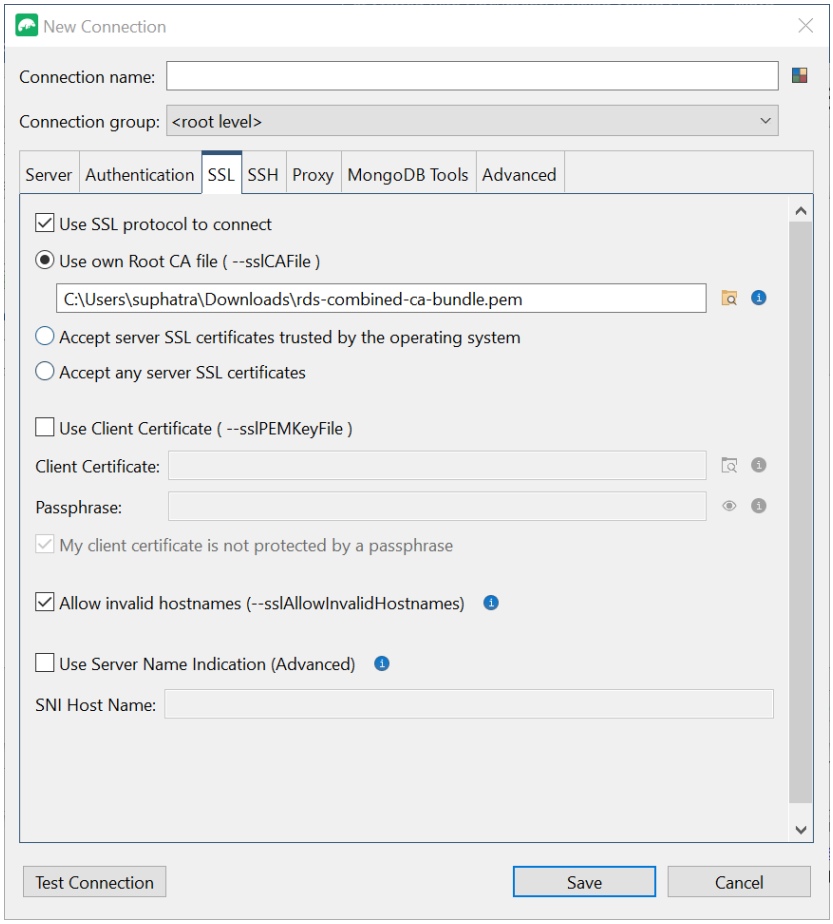


> **Note**
>
> Sie können Ihren Cluster-Endpunkt nicht finden? Folgen Sie einfach den Schritten hier.

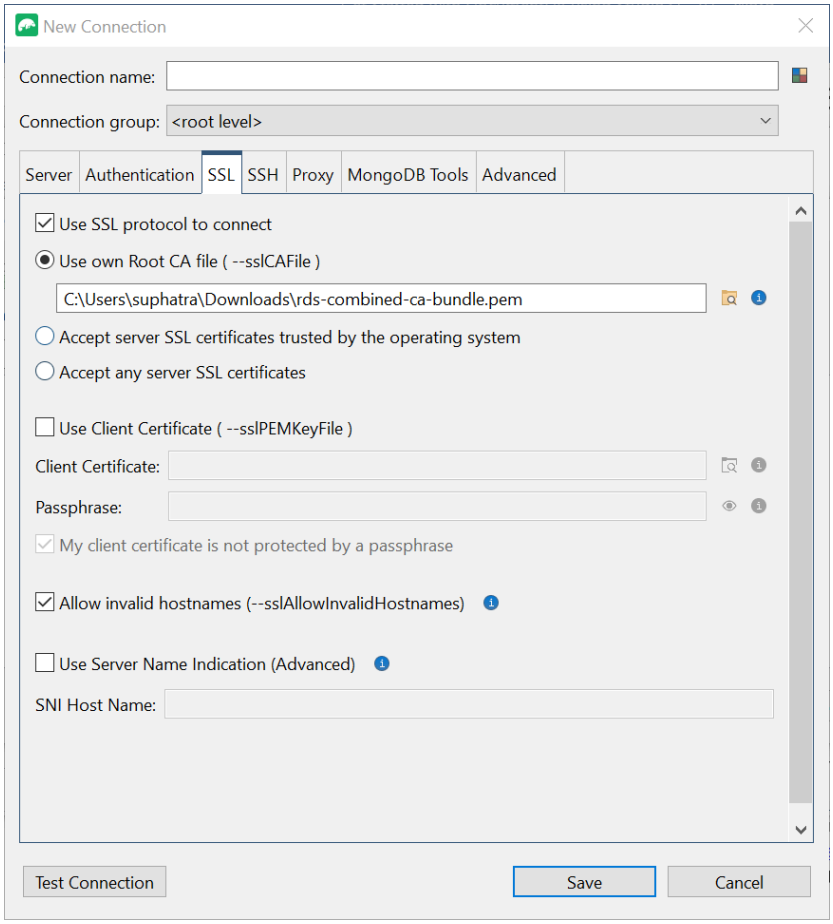
4. Wählen Sie die Registerkarte Authentifizierung und wählen Sie Legacy im Drop-down-Menü für Authentifizierungsmodus aus.



5. Geben Sie Ihren Benutzernamen und Ihre Anmeldeinformationen in die Felder Benutzername und Passwort ein.
6. Wählen Sie die Registerkarte SSL und aktivieren Sie das Kästchen SSL-Protokoll für die Verbindung verwenden.



7. Wählen Sie Eigene Root-CA-Datei verwenden. Fügen Sie dann das Amazon DocumentDB DocumentDB-Zertifikat hinzu (Sie können diesen Schritt überspringen, wenn SSL in Ihrem DocumentDB-Cluster deaktiviert ist). Markieren Sie das Kästchen, um ungültige Hostnamen zuzulassen.



> **Note**
>
> Sie haben das Zertifikat nicht? Sie können es mit dem folgenden Befehl herunterladen: `wget https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem`

8. Wenn Sie von einem Client-Computer außerhalb der Amazon VPC aus eine Verbindung herstellen, müssen Sie einen SSH-Tunnel erstellen. Sie werden dies auf der Registerkarte SSH tun.

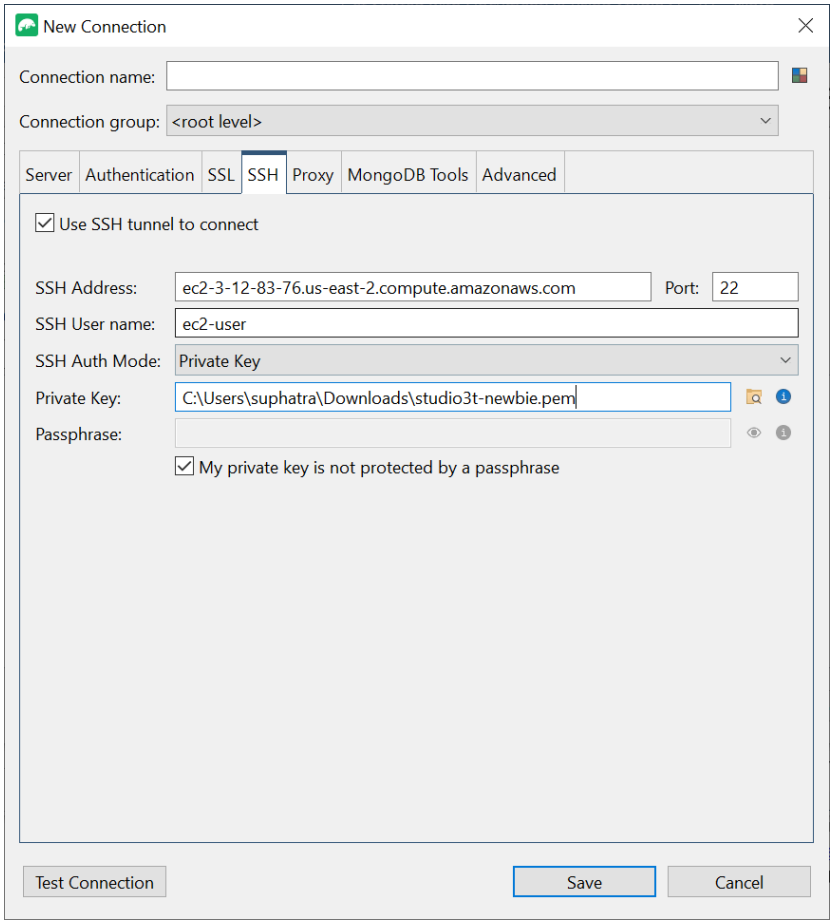
   a. Aktivieren Sie das Kontrollkästchen SSH-Tunnel verwenden und geben Sie die SSH-Adresse in das Feld SSH-Adresse ein. Dies ist Ihre Instanz Public DNS (IPV4). Sie können diese URL von Ihrer Amazon EC2-Managementkonsole abrufen.

   b. Geben Sie Ihren Nutzernamen ein. Dies ist der Benutzername Ihrer Amazon EC2 EC2-Instance

c. Wählen Sie für den SSH-Authentifizierungsmodus die Option Private Key aus. Wählen Sie im Feld Privater Schlüssel das Dateifinder-Symbol aus, um den privaten Schlüssel Ihrer Amazon EC2 EC2-Instance zu suchen und auszuwählen. Dies ist die PEM-Datei (key pair), die Sie beim Erstellen Ihrer Instance in der Amazon EC2 EC2-Konsole gespeichert haben.

d. Wenn Sie sich auf einem Linux/macOS Client-Computer befinden, müssen Sie möglicherweise die Berechtigungen Ihres privaten Schlüssels mit dem folgenden Befehl ändern:

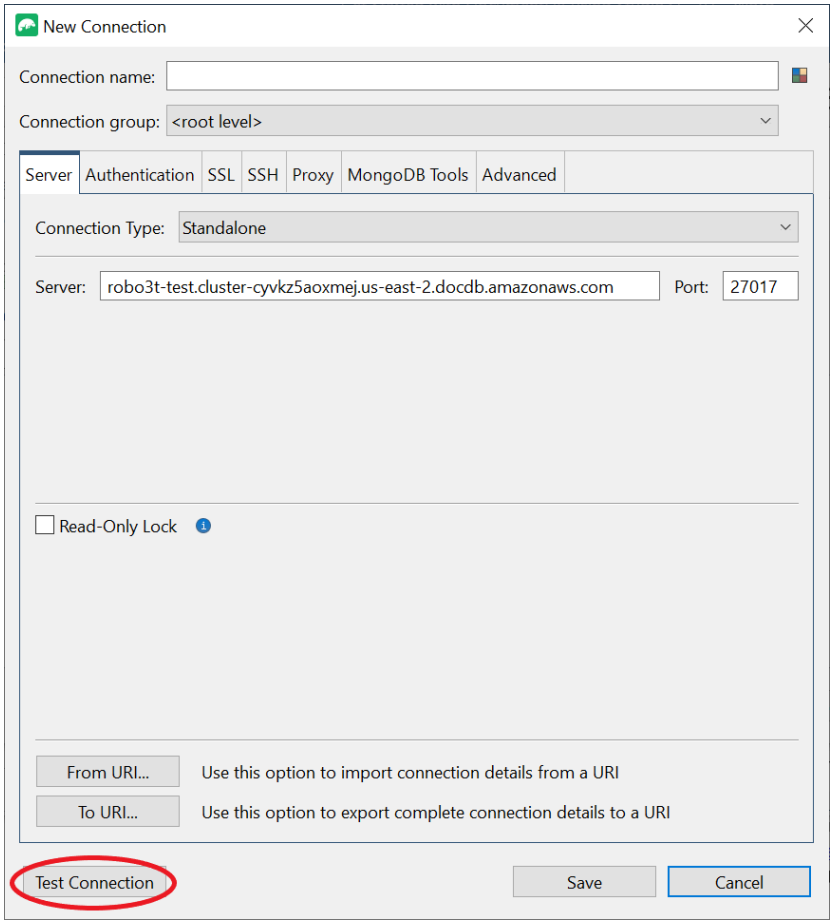
```
chmod 400 /fullPathToYourPemFile/<yourKey>.pem
```



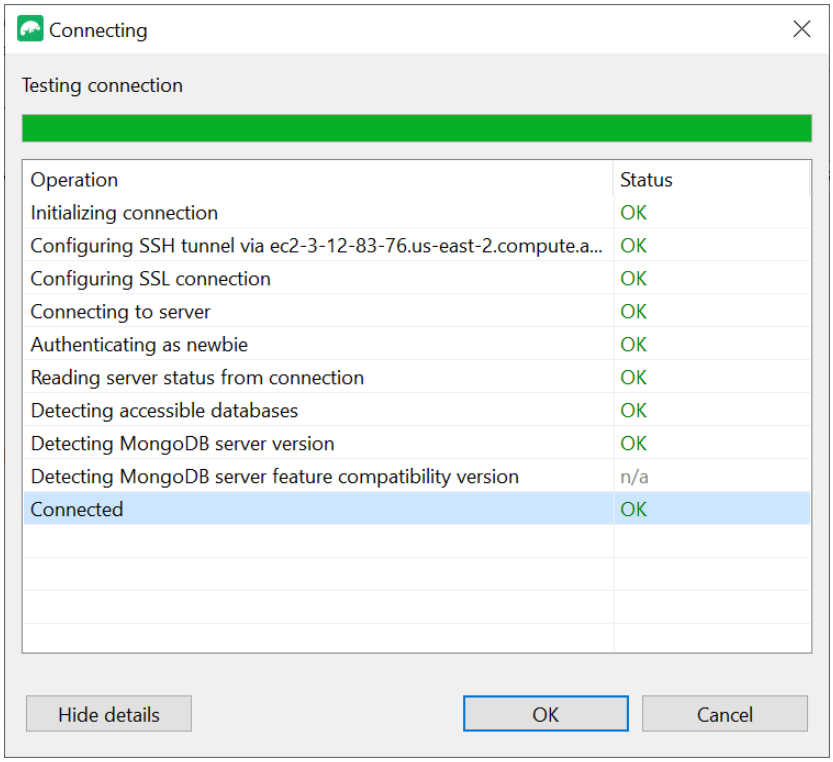
> **Note**
>
> Diese Amazon EC2 EC2-Instance sollte sich in derselben Amazon VPC und Sicherheitsgruppe wie Ihr DocumentDB-Cluster befinden. Sie können die SSH-

Adresse, den Benutzernamen und den privaten Schlüssel von Ihrer Amazon EC2-Managementkonsole abrufen.

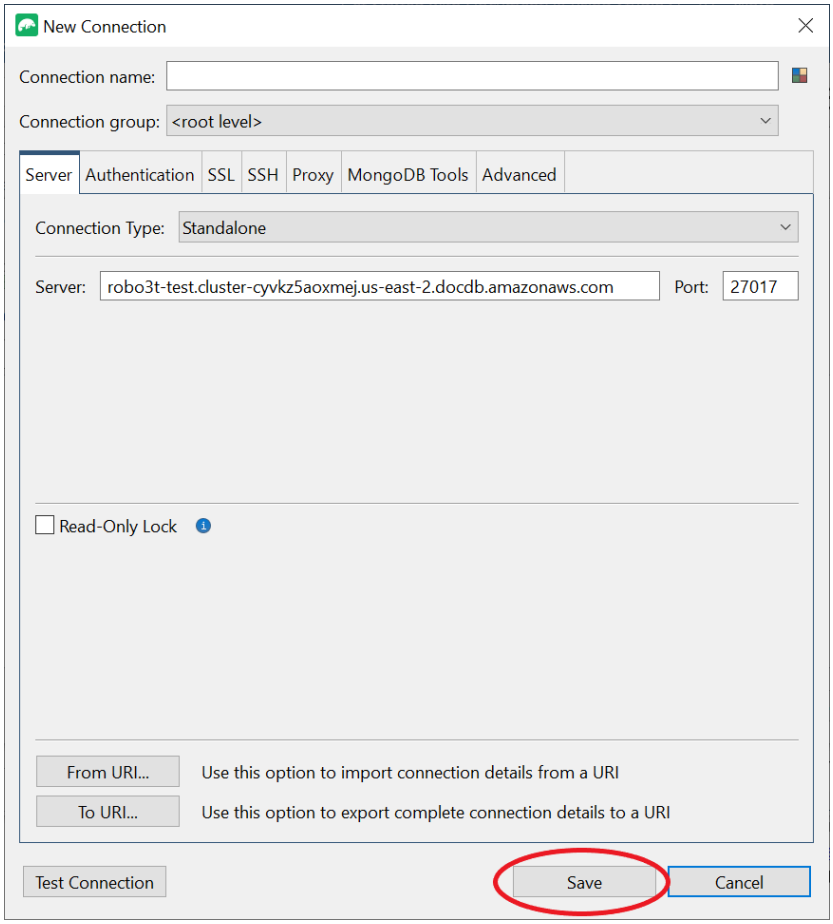
9. Testen Sie nun Ihre Konfiguration, indem Sie auf die Schaltfläche Verbindung testen klicken.



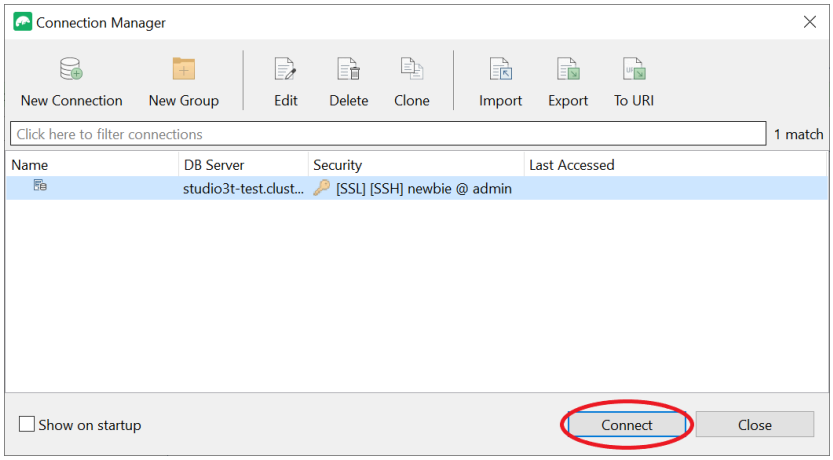
10. In einem Diagnosefenster sollte ein grüner Balken angezeigt werden, der anzeigt, dass der Test erfolgreich war. Wählen Sie nun OK, um das Diagnosefenster zu schließen.



11. Wählen Sie Speichern, um Ihre Verbindung für die future Verwendung zu speichern.



12. Wählen Sie nun Ihren Cluster aus und wählen Sie Connect.



Herzlichen Glückwunsch! Sie sind jetzt erfolgreich über Studio 3T mit Ihrem Amazon DocumentDB-Cluster verbunden.

Connect zu Amazon DocumentDB her mit DataGrip

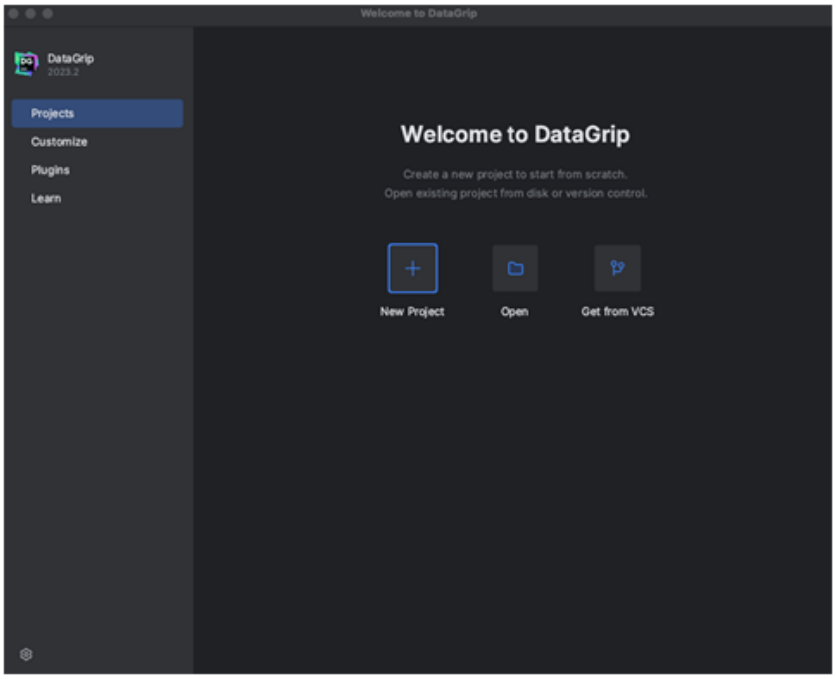
DataGripist eine leistungsstarke integrierte Entwicklungsumgebung (IDE), die verschiedene Datenbanksysteme unterstützt, darunter Amazon DocumentDB. Dieser Abschnitt führt Sie durch die Schritte, mit denen Sie eine Verbindung zu Ihrem Amazon DocumentDB-Cluster herstellen DataGrip, sodass Sie Ihre Daten einfach über eine grafische Oberfläche verwalten und abfragen können.

Voraussetzungen

- DataGrip IDE ist auf Ihrem Computer installiert. Sie können es von herunterladen JetBrains.
- Eine Amazon EC2 EC2-Instance, die in derselben VPC wie Ihr Amazon DocumentDB-Cluster läuft. Sie verwenden diese Instance, um einen sicheren Tunnel von Ihrem lokalen Computer zum Amazon DocumentDBCluster einzurichten. Folgen Sie den Anweisungen dazu. Stellen Sie mithilfe von Amazon EC2 eine Verbindung her
- Alternative zu einer Amazon EC2 EC2-Instance, einer VPN-Verbindung oder wenn Sie bereits über ein sicheres VPN auf Ihre AWS Infrastruktur zugreifen. Wenn Sie diese Option bevorzugen, folgen Sie den Anweisungen für den sicheren Zugriff auf Amazon DocumentDB mit AWS Client VPN.

Connect mit DataGrip

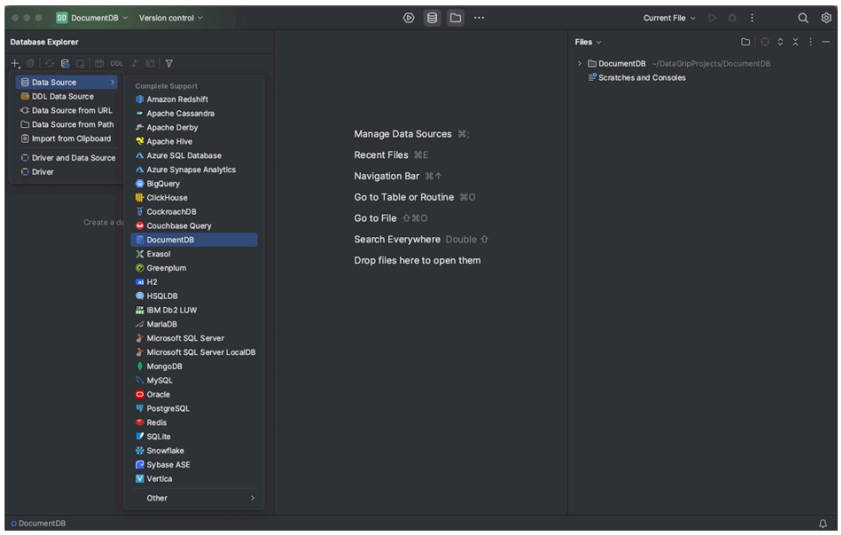
1. Starten Sie DataGrip auf Ihrem Computer und erstellen Sie ein neues Projekt.



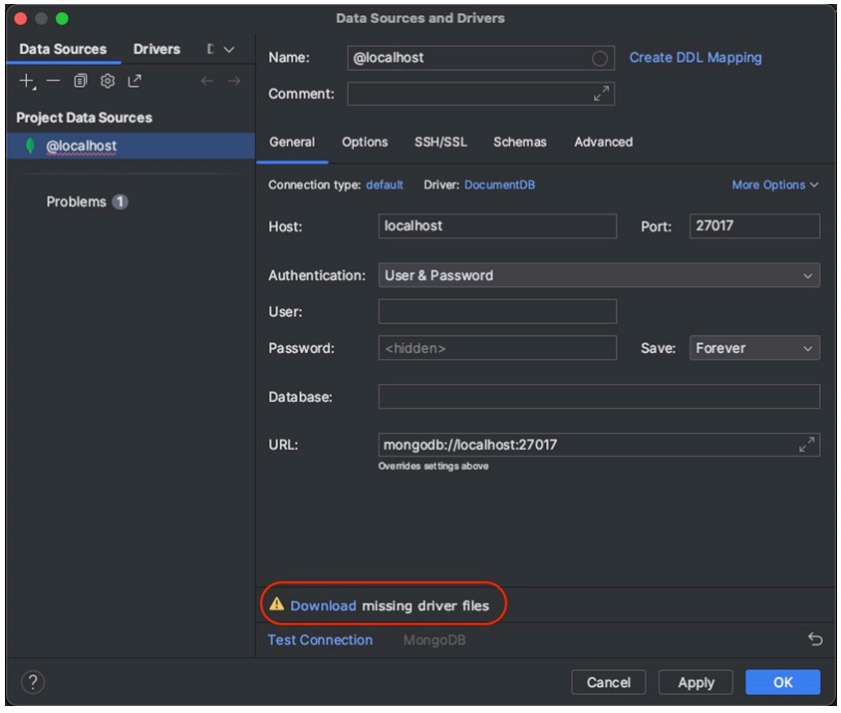
2. Fügen Sie mithilfe einer der folgenden Methoden eine neue Datenquelle hinzu:

a. Navigieren Sie im Hauptmenü zu Datei — Neu — Datenquelle und wählen Sie DocumentDB

b. Wählen Sie im Datenbank-Explorer das neue Symbol (+) in der Werkzeugleiste. Navigieren Sie zu Data Source und wählen Sie DocumentDB aus.



3. Überprüfen Sie auf der Seite Datenquellen auf der Registerkarte Allgemein, ob sich unten im Bereich mit den Verbindungseinstellungen der Link Fehlende Treiberdateien herunterladen befindet. Wählen Sie diesen Link, um Treiber herunterzuladen, die für die Interaktion mit einer Datenbank erforderlich sind. Einen direkten Download-Link finden Sie unter JetBrains JDBC-Treiber.



4. Geben Sie auf der Registerkarte Allgemein die Verbindungsdetails an:

a. Geben Sie im Feld Host den Amazon DocumentDB-Cluster-Endpunkt an.

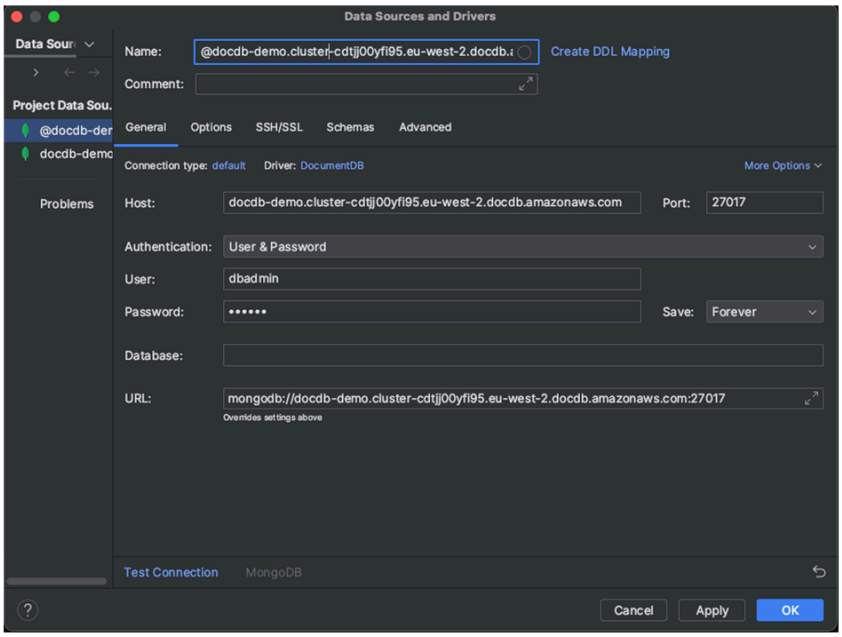
b. Der Port ist bereits auf 27017 eingestellt. Ändern Sie es, wenn Ihr Cluster auf einem anderen Port bereitgestellt wurde.

c. Wählen Sie für Authentifizierung die Option Benutzer und Passwort aus.

d. Geben Sie Ihren Benutzernamen und Ihr Passwort ein.

e. Das Datenbankfeld ist optional. Sie können die Datenbank angeben, zu der Sie eine Verbindung herstellen möchten.

f. Das URL-Feld wird automatisch vervollständigt, wenn Sie die vorherigen Details hinzufügen.



5. Aktivieren Sie auf der SSH/SSLRegisterkarte die Option SSH-Tunnel verwenden und wählen Sie dann das Symbol, um den SSH-Konfigurationsdialog zu öffnen. Geben Sie die folgenden Informationen ein:

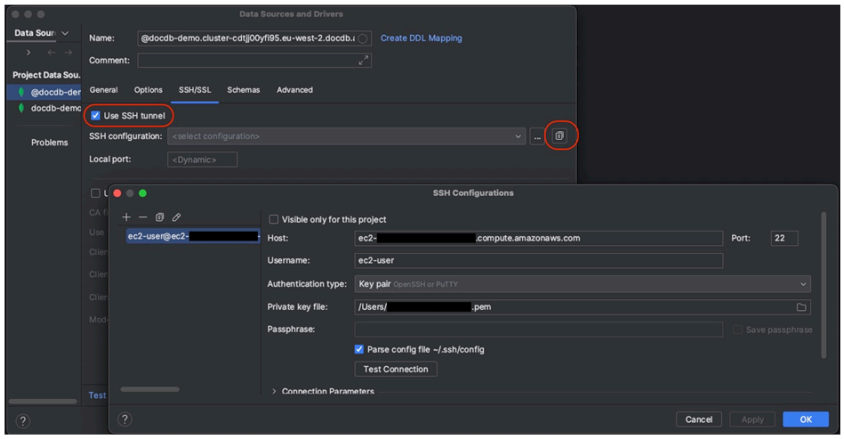
a. geben Sie im Feld Host den Hostnamen Ihrer Amazon EC2 EC2-Instance ein.

b. Geben Sie den Benutzernamen und das Passwort für Ihre Amazon EC2 EC2-Instance ein.

c. Wählen Sie als Authentifizierungstyp die Option Schlüsselpaar aus.

d. Geben Sie Ihre private Schlüsseldatei ein.

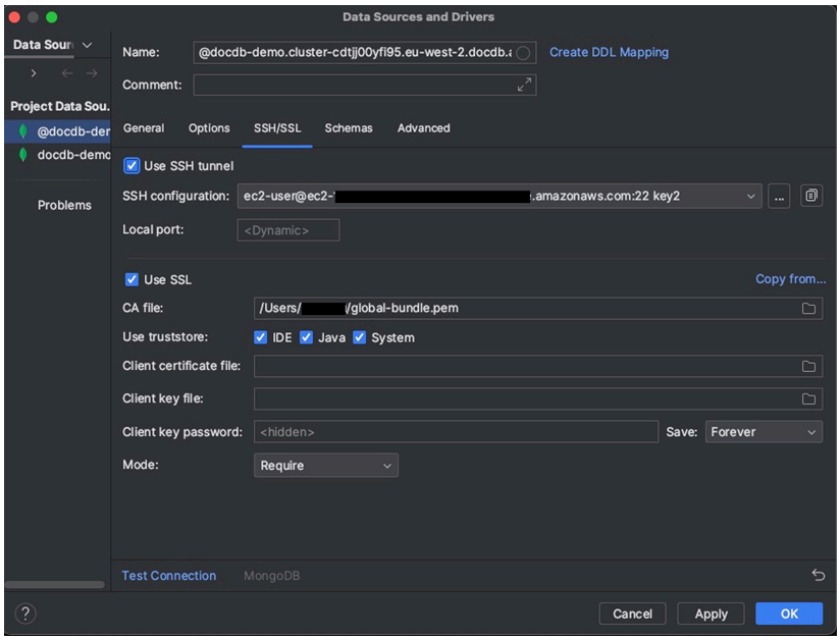
> **Note**
>
> Wenn Sie die VPN-Option verwenden, müssen Sie den SSH-Tunnel nicht konfigurieren.



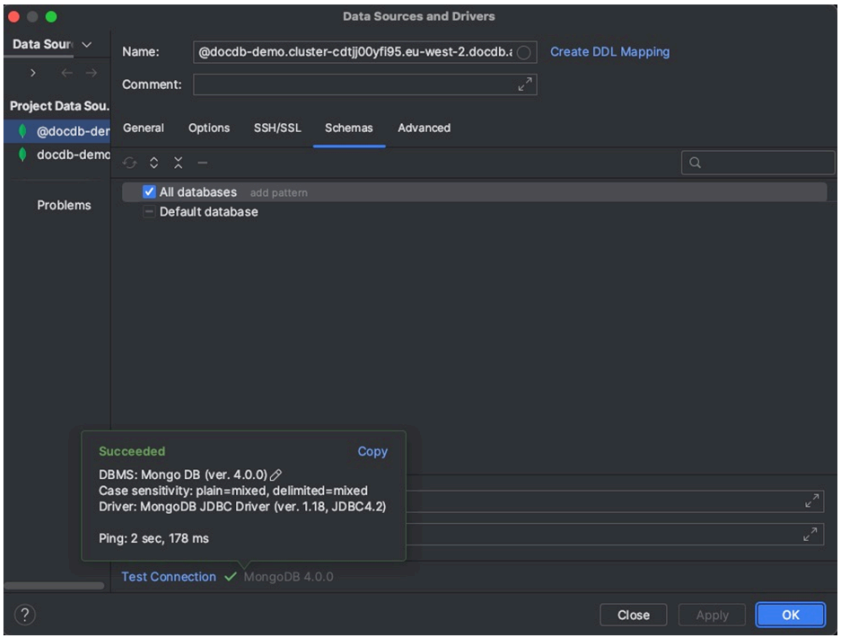
6. Aktivieren SSH/SSLSie auf der Registerkarte SSL verwenden. Geben Sie im Feld CA-Datei den Speicherort der `global-bundle.pem` Datei auf Ihrem Computer ein. Behalten Sie für Modus die Option Erforderlich bei.

> **Note**
>
> Sie können das Zertifikat von diesem Speicherort oder mit dem folgenden Befehl herunterladen: wget https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem

> **Note**
>
> Wenn Sie eine Verbindung zu Amazon DocumentDB Elastic Cluster herstellen, müssen Sie die CA-Datei nicht angeben. Lassen Sie die Option SSL verwenden aktiviert und lassen Sie alle anderen Optionen auf ihren Standardwerten stehen.



7. Wählen Sie auf der Registerkarte Schemas die Option Alle Datenbanken aus oder geben Sie den Filter „*: *“ in das Feld Schemamuster ein. Wählen Sie Verbindung testen, um die Verbindung zu testen.



8. Sobald die Verbindung erfolgreich getestet wurde, wählen Sie OK, um die Datenquellenkonfiguration zu speichern.

DataGrip features

DataGrip bietet verschiedene Funktionen, die Ihnen helfen, effizient mit Amazon DocumentDB zu arbeiten:

- SQL Editor — Schreiben Sie SQL-like Abfragen in Ihren DocumentDB-Sammlungen mit dem SQL-Editor in DataGrip und führen Sie sie aus.
- Visual Query Builder — Verwenden Sie den Visual Query Builder, um Abfragen grafisch zu erstellen, ohne SQL-Code schreiben zu müssen.
- Schemaverwaltung — Einfache Verwaltung Ihres Datenbankschemas, einschließlich des Erstellens, Änderns und Löschens von Sammlungen.
- Datenvisualisierung — Zeigen Sie Ihre Daten an und analysieren Sie sie mithilfe verschiedener Visualisierungstools, die unter verfügbar sind. DataGrip
- Daten exportieren und importieren — Übertragen Sie Daten zwischen Amazon DocumentDB und anderen Datenbanken mithilfe DataGrip der Export- und Importfunktionen.

Weiterführende Funktionen und Tipps zur Arbeit mit Amazon DocumentDB und anderen Datenbanksystemen finden Sie in der offiziellen DataGrip Dokumentation.

Stellen Sie mithilfe von Amazon EC2 eine Verbindung her

In diesem Abschnitt wird beschrieben, wie Sie die Konnektivität zwischen einem Amazon DocumentDB-Cluster und Amazon EC2 einrichten und von der Amazon EC2-Instance aus auf den Amazon DocumentDB-Cluster zugreifen.

Es gibt zwei Optionen für die Konfiguration der EC2-Verbindung:

- Automatisches Verbinden Ihrer EC2-Instance mit einer Amazon DocumentDB DocumentDB-Datenbank — Verwenden Sie die automatische Verbindungsfunktion in der EC2-Konsole, um die Verbindung zwischen Ihrer EC2-Instance und einer neuen oder vorhandenen Amazon DocumentDB DocumentDB-Datenbank automatisch zu konfigurieren. Diese Verbindung ermöglicht den Verkehr zwischen der EC2-Instance und der Amazon DocumentDB DocumentDB-Datenbank. Diese Option wird normalerweise zum Testen und Erstellen neuer Sicherheitsgruppen verwendet.
- Manuelles Verbinden Ihrer EC2-Instance mit Ihrer Amazon DocumentDB DocumentDB-Datenbank — Konfigurieren Sie die Verbindung zwischen Ihrer EC2-Instance und Ihrer Amazon DocumentDB DocumentDB-Datenbank, indem Sie die Sicherheitsgruppen manuell konfigurieren und zuweisen,

um die Konfiguration zu reproduzieren, die durch die automatische Verbindungsfunktion erstellt wird. Diese Option wird normalerweise verwendet, um erweiterte Einstellungen zu ändern und bestehende Sicherheitsgruppen zu verwenden.

Voraussetzungen

Unabhängig von der Option und bevor Sie Ihren ersten Amazon DocumentDB-Cluster erstellen, müssen Sie Folgendes tun:

Erstellen Sie ein Amazon Web Services (AWS) -Konto

Bevor Sie Amazon DocumentDB verwenden können, benötigen Sie ein Amazon Web Services (AWS) -Konto. Das AWS Konto ist kostenlos. Sie zahlen nur für die Services und Ressourcen, die Sie wirklich nutzen.

Wenn Sie noch keinen haben AWS-Konto, führen Sie die folgenden Schritte aus, um einen zu erstellen.

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie https://portal.aws.amazon.com/billing/signup.
2. Folgen Sie den Online-Anweisungen.

   Während der Anmeldung erhalten Sie einen Telefonanruf oder eine Textnachricht und müssen einen Verifizierungscode über die Telefontasten eingeben.

   Wenn Sie sich für eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontoswird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Als bewährte Sicherheitsmethode weisen Sie einem Benutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um Aufgaben auszuführen, die Root-Benutzerzugriff erfordern.

Richten Sie optional die erforderlichen AWS Identity and Access Management (IAM-) Berechtigungen ein.

Für den Zugriff auf die Verwaltung von Amazon DocumentDB DocumentDB-Ressourcen wie Clustern, Instances und Cluster-Parametergruppen sind Anmeldeinformationen erforderlich, mit denen Sie Ihre Anfragen authentifizieren AWS können. Weitere Informationen finden Sie unter Identity and Access Management für Amazon DocumentDB.

1. Geben Sie in der Suchleiste von IAM ein und wählen Sie im angezeigten Drop-down-Menü IAM aus. AWS-Managementkonsole
2. Sobald Sie sich in der IAM-Konsole befinden, wählen Sie im Navigationsbereich Benutzer aus.
3. Wählen Sie Ihren Nutzernamen aus.
4. Wählen Sie Add permissions (Berechtigungen hinzufügen) aus.
5. Wählen Sie die Option Attach existing policies directly (Vorhandene Richtlinien direkt anfügen) aus.
6. Geben Sie `AmazonDocDBFullAccess` in die Suchleiste ein und wählen Sie ihn aus, sobald er in den Suchergebnissen erscheint.
7. Wählen Sie Weiter: Prüfen aus.
8. Wählen Sie Add permissions.

Erstellen Sie eine Amazon Virtual Private Cloud (Amazon VPC)

Je nachdem, in welchem Bereich AWS-Region Sie sich befinden, haben Sie möglicherweise bereits eine Standard-VPC erstellt oder auch nicht. Wenn Sie keine Standard-VPC haben, führen Sie Schritt 1 der Anleitung Erste Schritte mit Amazon VPC im Amazon VPC-Benutzerhandbuch durch. Dies dauert weniger als fünf Minuten.

Amazon EC2 automatisch Connect

Topics

- Automatisches Verbinden einer EC2-Instance mit einer neuen Amazon DocumentDB DocumentDB-Datenbank
- Automatisches Verbinden einer EC2-Instance mit einer vorhandenen Amazon DocumentDB DocumentDB-Datenbank
- Übersicht über die automatische Verbindung mit einer EC2-Instance
- Anzeigen verbundener Rechenressourcen

Bevor Sie eine Verbindung zwischen einer EC2-Instance und einer neuen Amazon DocumentDB DocumentDB-Datenbank einrichten, stellen Sie sicher, dass Sie die unter beschriebenen Anforderungen erfüllen. Übersicht über die automatische Verbindung mit einer EC2-Instance Wenn Sie nach der Konfiguration der Konnektivität Änderungen an Sicherheitsgruppen vornehmen, können

sich die Änderungen auf die Verbindung zwischen der EC2-Instance und der Amazon DocumentDB DocumentDB-Datenbank auswirken.

> **Note**
>
> Sie können nur automatisch eine Verbindung zwischen einer EC2-Instance und einer Amazon DocumentDB DocumentDB-Datenbank einrichten, indem Sie die verwenden. AWS-Managementkonsole Sie können keine automatische Verbindung mit der AWS CLI oder der Amazon DocumentDB DocumentDB-API einrichten.

Automatisches Verbinden einer EC2-Instance mit einer neuen Amazon DocumentDB DocumentDB-Datenbank

Beim folgenden Prozess wird davon ausgegangen, dass Sie die Schritte im Thema abgeschlossen haben. Voraussetzungen

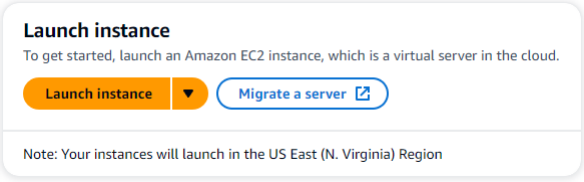
Schritte

- Schritt 1: Erstellen Sie eine Amazon EC2 EC2-Instance
- Schritt 2: Erstellen Sie einen Amazon DocumentDB-Cluster
- Schritt 3: Connect zu Ihrer Amazon EC2 EC2-Instance her
- Schritt 4: Installieren Sie die MongoDB-Shell
- Schritt 5: Amazon DocumentDB TLS verwalten
- Schritt 6: Connect zu Ihrem Amazon DocumentDB-Cluster her
- Schritt 7: Daten einfügen und abfragen
- Schritt 8: Erkunden

Schritt 1: Erstellen Sie eine Amazon EC2 EC2-Instance

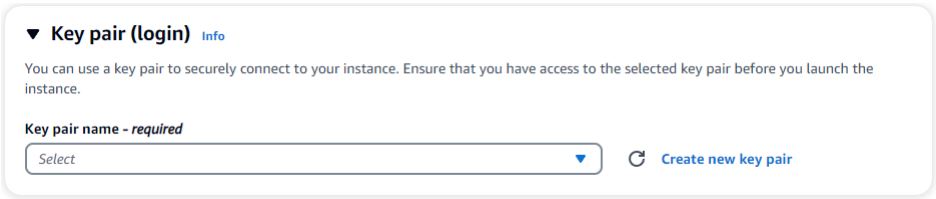
In diesem Schritt erstellen Sie eine Amazon EC2 EC2-Instance in derselben Region und Amazon VPC, die Sie später für die Bereitstellung Ihres Amazon DocumentDB-Clusters verwenden werden.

1. Wählen Sie auf der Amazon EC2 EC2-Konsole Launch instance aus.



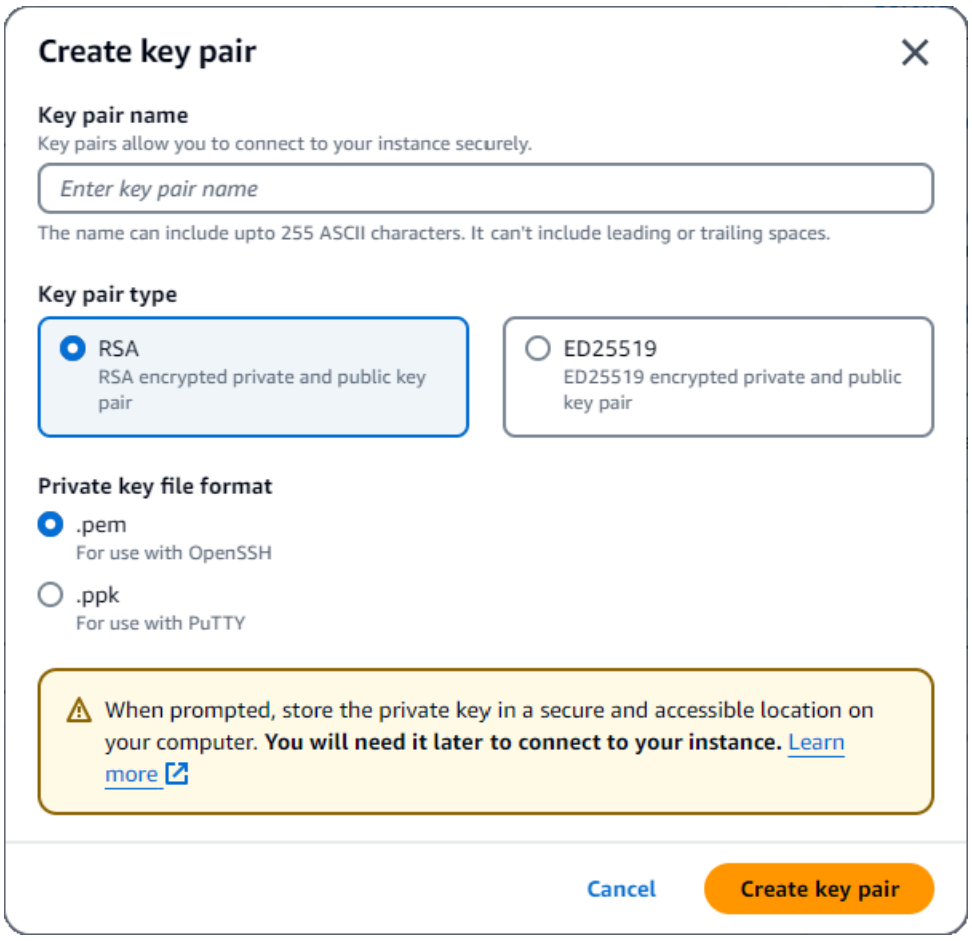
2. Geben Sie einen Namen oder eine Kennung in das Feld Name im Abschnitt Name und Tags ein.
3. Suchen Sie in der Dropdownliste Amazon Machine Image (AMI) nach Amazon Linux 2 AMI und wählen Sie es aus.

4. Suchen Sie in der Dropdownliste Instance-Typ nach t3.micro und wählen Sie es aus.
5. Geben Sie im Abschnitt key pair (Anmeldung) die Kennung eines vorhandenen Schlüsselpaars ein, oder wählen Sie Neues Schlüsselpaar erstellen.



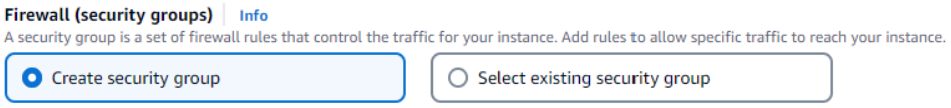
Sie müssen ein Amazon EC2 EC2-Schlüsselpaar angeben.

- Wenn Sie ein Amazon EC2 EC2-Schlüsselpaar haben:
  1. Wählen Sie ein key pair aus, wählen Sie Ihr key pair aus der Liste.
  2. Sie müssen die private Schlüsseldatei (.pem- oder .ppk-Datei) bereits verfügbar haben, um sich bei Ihrer Amazon EC2 EC2-Instance anmelden zu können.
- Wenn Sie kein Amazon EC2 EC2-Schlüsselpaar haben:
  1. Wählen Sie Neues key pair erstellen. Daraufhin wird das Dialogfeld key pair erstellen angezeigt.
  2. Geben Sie einen Namen in das Feld Name des Schlüsselpaars ein.
  3. Wählen Sie den Schlüsselpaartyp und das Dateiformat für den privaten Schlüssel.
  4. Wählen Sie Create Key Pair (Schlüsselpaar erstellen) aus.



> **Note**
>
> Aus Sicherheitsgründen empfehlen wir dringend, ein Schlüsselpaar sowohl für die SSH- als auch für die Internetverbindung zu Ihrer EC2-Instance zu verwenden.

6. Optional: Wählen Sie im Abschnitt Netzwerkeinstellungen unter Firewall (Sicherheitsgruppen) die Option Sicherheitsgruppe erstellen aus.



Wählen Sie Sicherheitsgruppe erstellen (überprüfen Sie alle Regeln für die Zulassung von Datenverkehr, die für Ihre EC2-Konnektivität gelten).

> **Note**
>
> Wenn Sie eine bestehende Sicherheitsgruppe verwenden möchten, folgen Sie den Anweisungen unterManuelles Connect von Amazon EC2.

7. Überprüfen Sie im Abschnitt Zusammenfassung Ihre EC2-Konfiguration und wählen Sie Launch instance, falls korrekt.

Schritt 2: Erstellen Sie einen Amazon DocumentDB-Cluster

Während die Amazon EC2 EC2-Instance bereitgestellt wird, erstellen Sie Ihren Amazon DocumentDB-Cluster.

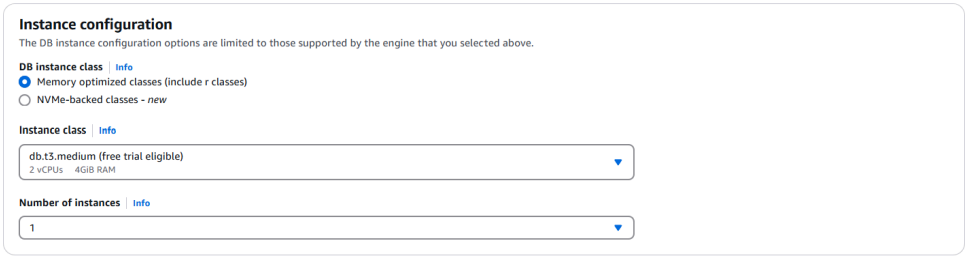
1. Navigieren Sie zur Amazon DocumentDB DocumentDB-Konsole und wählen Sie im Navigationsbereich Clusters aus.
2. Wählen Sie Erstellen aus.
3. Belassen Sie die Standardeinstellung für den Clustertyp auf Instance Based Cluster.
4. Geben Sie in Clusterkonfiguration für Cluster-ID einen eindeutigen Namen ein. Beachten Sie, dass die Konsole alle Clusternamen unabhängig von der Art der Eingabe in Kleinbuchstaben ändert.

   Behalten Sie für die Engine-Version den Standardwert 5.0.0 bei.
5. Behalten Sie für die Cluster-Speicherkonfiguration die Standardeinstellung von Amazon DocumentDB Standard bei.
6. In der Instanzkonfiguration:

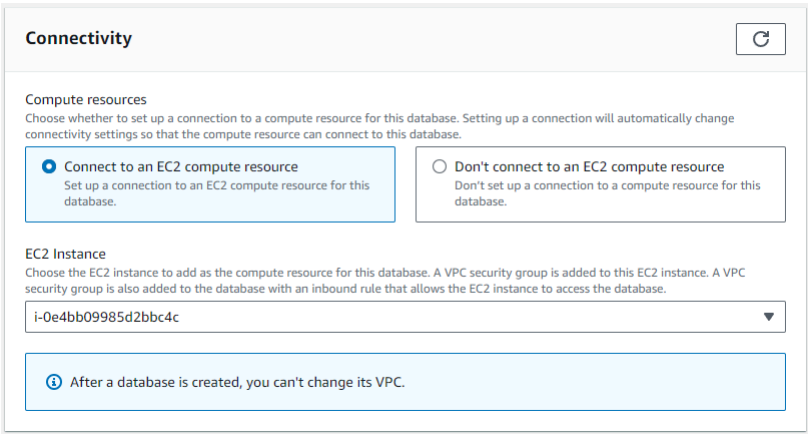
   - Wählen Sie für DB-Instance-Klasse die Option Speicheroptimierte Klassen (einschließlich R-Klassen) aus (dies ist die Standardeinstellung).

     Die andere Instance-Option ist NVMe-backed Klassen. Weitere Informationen hierzu finden Sie unter NVMe-backed Instanzen.
   - Wählen Sie für Instance-Klasse den Instance-Typ aus, der Ihren Anforderungen entspricht. Eine detailliertere Erläuterung der Instanzklassen finden Sie unterSpezifikationen der Instanzklasse.

- Wählen Sie für die Anzahl der Instances eine Zahl aus, die Ihren Anforderungen am besten entspricht. Denken Sie daran, je niedriger die Anzahl, desto niedriger die Kosten und desto geringer das read/write Volumen, das vom Cluster verwaltet werden kann.



7. Wählen Sie für Konnektivität die Option Mit einer EC2-Rechenressource Connect aus. Dies ist die EC2-Instance, die Sie in Schritt 1 erstellt haben.



> **Note**
>
> Wenn Sie eine Verbindung zu einer EC2-Rechenressource herstellen, wird automatisch eine Sicherheitsgruppe für Ihre EC2-Rechenressourcenverbindung zu Ihrem Amazon DocumentDB-Cluster erstellt. Wenn Sie mit der Erstellung Ihres Clusters fertig sind und die neu erstellte Sicherheitsgruppe sehen möchten, navigieren Sie zur Cluster-Liste und wählen Sie die Kennung Ihres Clusters aus. Gehen Sie auf der Registerkarte Konnektivität und Sicherheit zu Sicherheitsgruppen und suchen Sie unter Sicherheitsgruppenname (ID) nach Ihrer Gruppe. Sie wird den Namen Ihres Clusters enthalten und etwa so aussehen:`docdb-ec2-docdb-2023-12-11-21-33-41:i-0e4bb09985d2bbc4c (sg-0238e0b0bf0f73877)`.

8. Geben Sie im Abschnitt Authentifizierung einen Benutzernamen für den Hauptbenutzer ein und wählen Sie dann Selbstverwaltet aus. Geben Sie ein Passwort ein und bestätigen Sie es.

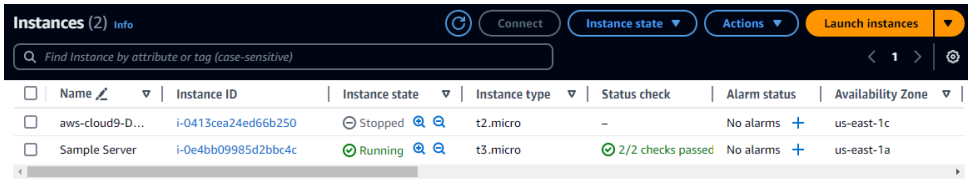
   Wenn Sie stattdessen Verwaltet in wählen AWS Secrets Manager, finden Sie Passwortverwaltung mit Amazon DocumentDB und AWS Secrets Manager weitere Informationen unter.

9. Wählen Sie Cluster erstellen.

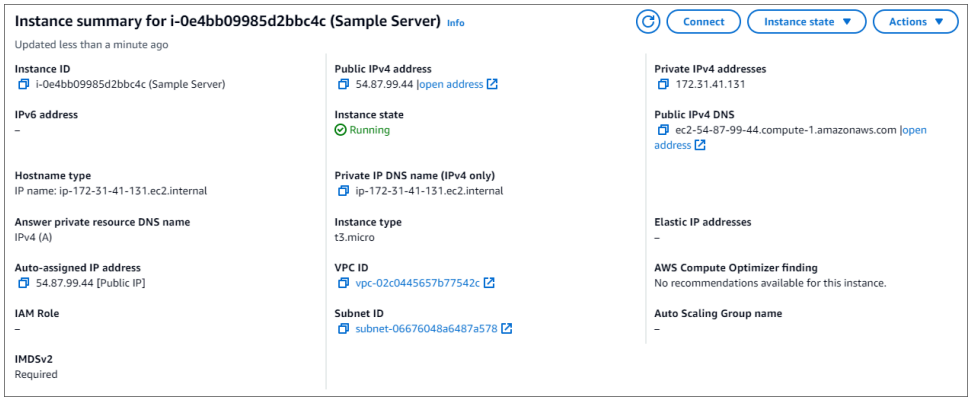
Schritt 3: Connect zu Ihrer Amazon EC2 EC2-Instance her

Um die Mongo-Shell zu installieren, müssen Sie zuerst eine Verbindung zu Ihrer Amazon EC2 EC2-Instance herstellen. Durch die Installation der Mongo-Shell können Sie eine Verbindung zu Ihrem Amazon DocumentDB-Cluster herstellen und ihn abfragen. Führen Sie folgende Schritte aus:

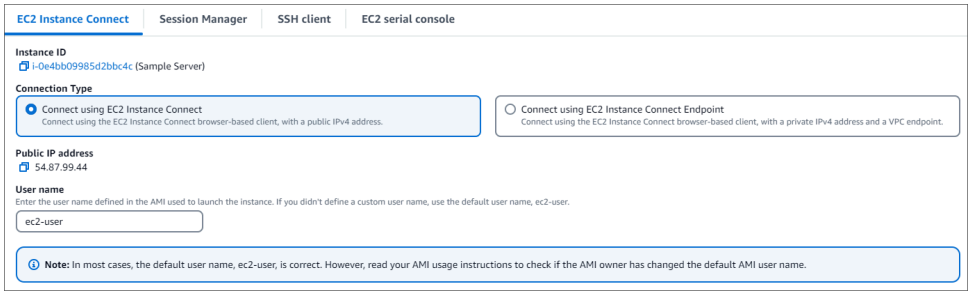
1. Navigieren Sie auf der Amazon EC2 EC2-Konsole zu Ihren Instances und überprüfen Sie, ob die gerade erstellte Instance läuft. Wenn ja, wählen Sie die Instance aus, indem Sie auf die Instance-ID klicken.



2. Wählen Sie Connect aus.



3. Es gibt vier Optionen mit Registerkarten für Ihre Verbindungsmethode: Amazon EC2 Instance Connect, Session Manager, SSH-Client oder serielle EC2-Konsole. Sie müssen eine auswählen und deren Anweisungen befolgen. Wenn Sie fertig sind, wählen Sie Connect.



Note

Wenn sich Ihre IP-Adresse geändert hat, nachdem Sie diesen Walkthrough gestartet haben, oder wenn Sie zu einem späteren Zeitpunkt zu Ihrer Umgebung zurückkehren, müssen Sie Ihre `demoEC2` Sicherheitsgruppenregel für eingehenden Datenverkehr aktualisieren, um eingehenden Datenverkehr von Ihrer neuen API-Adresse aus zu ermöglichen.

Schritt 4: Installieren Sie die MongoDB-Shell

Sie können jetzt die MongoDB-Shell installieren. Dabei handelt es sich um ein Befehlszeilenprogramm, mit dem Sie eine Verbindung herstellen und Ihren Amazon DocumentDB-Cluster abfragen können. Derzeit gibt es zwei Versionen der MongoDB-Shell: die neueste Version, Mongosh, und die vorherige Version, Mongo-Shell.

Important

Es gibt eine bekannte Einschränkung bei Node.js Treibern, die älter als Version 6.13.1 sind und derzeit nicht von der IAM-Identitätsauthentifizierung für Amazon DocumentDB unterstützt werden. Node.js Treiber und Tools, die Node.js Treiber verwenden (z. B. Mongosh), müssen aktualisiert werden, sodass sie die Node.js Treiberversion 6.13.1 oder höher verwenden.

Folgen Sie den nachstehenden Anweisungen, um die MongoDB-Shell für Ihr Betriebssystem zu installieren.

On Amazon Linux

So installieren Sie die MongoDB-Shell auf Amazon Linux

Wenn Sie keine IAM-Authentifizierung verwenden und die neueste MongoDB-Shell (mongosh) verwenden möchten, um eine Verbindung zu Ihrem Amazon DocumentDB-Cluster herzustellen, gehen Sie wie folgt vor:

1. Erstellen Sie die Repository-Datei. Führen Sie in der Befehlszeile Ihrer EC2-Instance, die Sie erstellt haben, den folgenden Befehl aus:

```
echo -e "[mongodb-org-5.0] \nname=MongoDB Repository\nbaseurl=https://
repo.mongodb.org/yum/amazon/2023/mongodb-org/5.0/x86_64/\ngpgcheck=1 \nenabled=1
 \ngpgkey=https://pgp.mongodb.com/server-5.0.asc" | sudo tee /etc/yum.repos.d/
mongodb-org-5.0.repo
```

2. Wenn der Vorgang abgeschlossen ist, installieren Sie mongosh mit einer der beiden folgenden Befehlsoptionen an der Befehlszeile:

   Option 1 — Wenn Sie während der Amazon EC2-Konfiguration den Standard Amazon Linux 2023 ausgewählt haben, geben Sie diesen Befehl ein:

```
sudo yum install -y mongodb-mongosh-shared-openssl3
```

   Option 2 — Wenn Sie bei der Amazon EC2-Konfiguration Amazon Linux 2 ausgewählt haben, geben Sie diesen Befehl ein:

```
sudo yum install -y mongodb-mongosh
```

Wenn Sie die IAM-Authentifizierung verwenden, müssen Sie die vorherige Version der MongoDB-Shell (5.0) verwenden, um eine Verbindung zu Ihrem Amazon DocumentDB-Cluster herzustellen. Gehen Sie wie folgt vor:

1. Erstellen Sie die Repository-Datei. Führen Sie in der Befehlszeile Ihrer EC2-Instance, die Sie erstellt haben, den folgenden Befehl aus:

```
echo -e "[mongodb-org-5.0] \nname=MongoDB Repository\nbaseurl=https://
repo.mongodb.org/yum/amazon/2023/mongodb-org/5.0/x86_64/\ngpgcheck=1 \nenabled=1
 \ngpgkey=https://pgp.mongodb.com/server-5.0.asc" | sudo tee /etc/yum.repos.d/
mongodb-org-5.0.repo
```

2. Wenn der Vorgang abgeschlossen ist, installieren Sie die Mongodb 5.0-Shell mit der folgenden Befehlsoption an der Befehlszeile:

```
sudo yum install -y mongodb-org-shell
```

On Ubuntu

Um mongosh auf Ubuntu zu installieren

1. Importieren Sie den öffentlichen Schlüssel, der von dem Paketverwaltungssystem verwendet wird.

   ```
   curl -fsSL https://pgp.mongodb.com/server-5.0.asc | sudo gpg --dearmor -o /usr/
   share/keyrings/mongodb-server-5.0.gpg
   ```

2. Erstellen Sie die Listendatei `mongodb-org-5.0.list` für MongoDB mit dem korrekten Befehl für Ihre Ubuntu-Version.

   ```
   echo "deb [ arch=amd64,arm64 signed-by=/usr/share/keyrings/mongodb-
   server-5.0.gpg ] https://repo.mongodb.org/apt/ubuntu focal/mongodb-org/5.0
    multiverse" | sudo tee /etc/apt/sources.list.d/mongodb-org-5.0.list
   ```

3. Importieren und aktualisieren Sie die lokale Paketdatenbank mit dem folgenden Befehl:

   ```
   sudo apt-get update
   ```

4. Installieren Sie Mongosh.

   ```
   sudo apt-get install -y mongodb-mongosh
   ```

Weitere Informationen zum Installieren von früheren Versionen von MongoDB auf Ihrem Ubuntu-System finden Sie unter Installieren von MongoDB Community Edition auf Ubuntu.

On other operating systems

Informationen zum Installieren der mongo-Shell auf anderen Betriebssystemen finden Sie unter Installieren von MongoDB Community Edition in der MongoDB-Dokumentation.

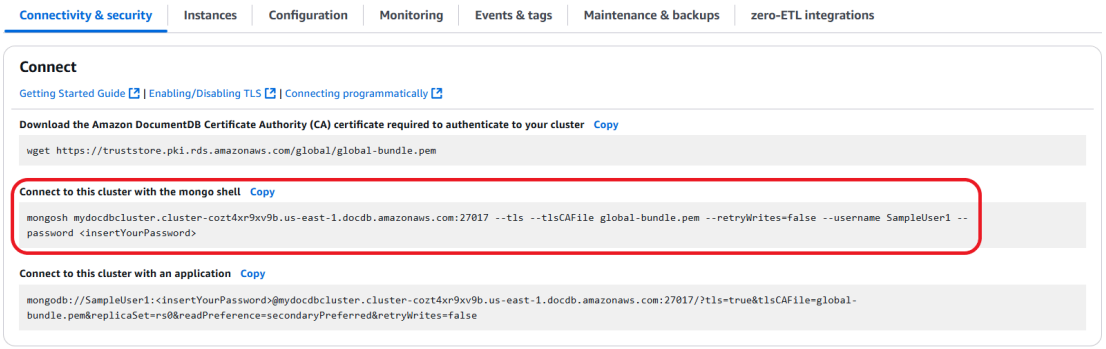
Schritt 5: Amazon DocumentDB TLS verwalten

Laden Sie das CA-Zertifikat für Amazon DocumentDB mit dem folgenden Code herunter: `wget https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem`

> **Note**
>
> Transport Layer Security (TLS) ist standardmäßig für alle neuen Amazon DocumentDB-Cluster aktiviert. Weitere Informationen finden Sie unter TLS-Einstellungen für Amazon DocumentDB-Cluster verwalten.

Schritt 6: Connect zu Ihrem Amazon DocumentDB-Cluster her

1. Suchen Sie auf der Amazon DocumentDB DocumentDB-Konsole unter Clusters Ihren Cluster. Wählen Sie den Cluster aus, den Sie erstellt haben, indem Sie auf die Cluster-ID für diesen Cluster klicken.
2. Suchen Sie auf der Registerkarte Konnektivität und Sicherheit im Feld Connect nach Connect to this cluster with the mongo shell:



   Kopieren Sie die angegebene Verbindungszeichenfolge und fügen Sie sie in Ihr Terminal ein.

   Nehmen Sie die folgenden Änderungen daran vor:

   a. Stellen Sie sicher, dass Sie den richtigen Benutzernamen in der Zeichenfolge haben.

   b. Auslassen, `<insertYourPassword>` sodass Sie beim Herstellen der Verbindung von der Mongo-Shell zur Eingabe des Passworts aufgefordert werden.

   c. Optional: Wenn Sie die IAM-Authentifizierung oder die vorherige Version der MongoDB-Shell verwenden, ändern Sie Ihre Verbindungszeichenfolge wie folgt:

```
mongo --ssl --host mydocdbcluster.cluster-cozt4xr9xv9b.us-
east-1.docdb.amazonaws.com:27017 --sslCAFile global-bundle.pem --
username SampleUser1 --password
```

`mydocdbcluster.cluster-cozt4xr9xv9b.us-east-1`Ersetzen Sie durch dieselben Informationen aus Ihrem Cluster.

3. Drücken Sie die Eingabetaste in Ihrem Terminal. Sie werden nun zur Eingabe Ihres Passworts aufgefordert. Geben Sie Ihr Passwort ein.
4. Wenn Sie Ihr Passwort eingeben und die `rs0 [direct: primary] <env-name>>` Aufforderung sehen, sind Sie erfolgreich mit Ihrem Amazon DocumentDB-Cluster verbunden.

Haben Sie Probleme mit der Verbindung? Weitere Informationen finden Sie unter Fehlerbehebung bei Amazon DocumentDB.

Schritt 7: Daten einfügen und abfragen

Nachdem Sie nun mit Ihrem Cluster verbunden sind, können Sie einige Abfragen ausführen, um sich mit der Verwendung einer Dokumentendatenbank vertraut zu machen.

1. Um ein einzelnes Dokument einzufügen, geben Sie Folgendes ein:

```
db.collection.insertOne({"hello":"DocumentDB"})
```

Sie erhalten die folgende Ausgabe:

```
{
  acknowledged: true,
  insertedId: ObjectId('673657216bdf6258466b128c')
}
```

2. Sie können das Dokument lesen, das Sie mit dem `findOne()` Befehl geschrieben haben (weil er nur ein einziges Dokument zurückgibt). Geben Sie Folgendes ein:

```
db.collection.findOne()
```

Sie erhalten die folgende Ausgabe:

```
{ "_id" : ObjectId("5e401fe56056fda7321fbd67"), "hello" : "DocumentDB" }
```

3. Um ein paar weitere Abfragen durchzuführen, sollten Sie einen Anwendungsfall für Spieleprofile in Betracht ziehen. Fügen Sie zunächst einige Einträge in eine Sammlung mit dem Titel ein`profiles`. Geben Sie Folgendes ein:

```
db.profiles.insertMany([{ _id: 1, name: 'Matt', status: 'active', level: 12, score:
 202 },
     { _id: 2, name: 'Frank', status: 'inactive', level: 2, score: 9 },
     { _id: 3, name: 'Karen', status: 'active', level: 7, score: 87 },
     { _id: 4, name: 'Katie', status: 'active', level: 3, score: 27 }
])
```

   Sie erhalten die folgende Ausgabe:

```
{ acknowledged: true, insertedIds: { '0': 1, '1': 2, '2': 3, '3': 4 } }
```

4. Verwenden Sie den `find()` Befehl, um alle Dokumente in der Profilsammlung zurückzugeben. Geben Sie Folgendes ein:

```
db.profiles.find()
```

   Sie erhalten eine Ausgabe, die den Daten entspricht, die Sie in Schritt 3 eingegeben haben.

5. Verwenden Sie mithilfe eines Filters eine Abfrage für ein einzelnes Dokument. Geben Sie Folgendes ein:

```
db.profiles.find({name: "Katie"})
```

   Sie erhalten die folgende Ausgabe:

```
{ "_id" : 4, "name" : "Katie", "status": "active", "level": 3, "score":27}
```

6. Versuchen wir nun, ein Profil zu finden und es mit dem `findAndModify` Befehl zu ändern. Wir geben dem Benutzer Matt zusätzliche 10 Punkte mit dem folgenden Code:

```
db.profiles.findAndModify({
        query: { name: "Matt", status: "active"},
        update: { $inc: { score: 10 } }
```

```
    })
```

Sie erhalten die folgende Ausgabe (beachten Sie, dass sein Punktestand noch nicht gestiegen ist):

```
{
    [{_id : 1, name : 'Matt', status: 'active', level: 12, score: 202}]
```

7. Sie können mit der folgenden Abfrage überprüfen, ob sich sein Punktestand geändert hat:

   ```
   db.profiles.find({name: "Matt"})
   ```

   Sie erhalten die folgende Ausgabe:

   ```
   { "_id" : 1, "name" : "Matt", "status" : "active", "level" : 12, "score" : 212 }
   ```

Schritt 8: Erkunden

Herzlichen Glückwunsch! Sie haben die Schnellstartanleitung für Amazon DocumentDB erfolgreich abgeschlossen.

Was kommt als Nächstes? Erfahren Sie, wie Sie diese leistungsstarke Datenbank mit einigen ihrer beliebten Funktionen voll ausschöpfen können:

- Amazon DocumentDB verwalten
- Skalierung
- Sichern und Wiederherstellen

> **Note**
>
> Um Kosten zu sparen, können Sie entweder Ihren Amazon DocumentDB-Cluster stoppen, um die Kosten zu senken, oder den Cluster löschen. Standardmäßig stoppt Ihre AWS Cloud9 Umgebung nach 30 Minuten Inaktivität die zugrunde liegende Amazon EC2 EC2-Instance.

Automatisches Verbinden einer EC2-Instance mit einer vorhandenen Amazon DocumentDB DocumentDB-Datenbank

Das folgende Verfahren setzt voraus, dass Sie über einen vorhandenen Amazon DocumentDB-Cluster und eine bestehende Amazon EC2 EC2-Instance verfügen.

Greifen Sie auf Ihren Amazon DocumentDB-Cluster zu und richten Sie die Amazon EC2 EC2-Verbindung ein

1. Greifen Sie auf Ihren Amazon DocumentDB-Cluster zu.

   a. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.

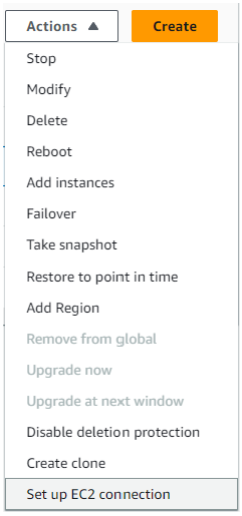
   b. Klicken Sie im Navigationsbereich auf Cluster.

   > **Tip**
   >
   > Wenn der Navigationsbereich auf der linken Seite des Bildschirms nicht angezeigt wird, wählen Sie links oben auf der Seite das Menüsymbol (≡) aus.

   c. Geben Sie den gewünschten Cluster an, indem Sie auf die Schaltfläche links neben dem Namen des Clusters klicken.

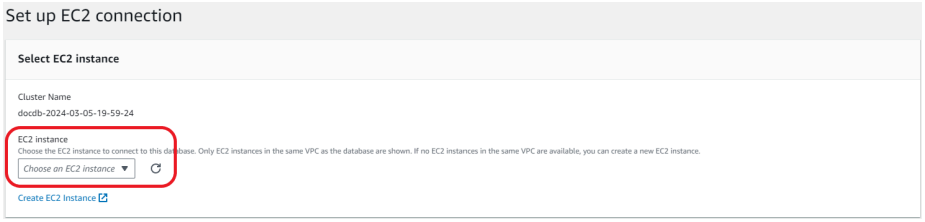
2. Richten Sie die Amazon EC2 EC2-Verbindung ein.

   a. Wählen Sie Aktionen und dann EC2-Verbindung einrichten.

   Das Dialogfeld EC2-Verbindung einrichten wird angezeigt.

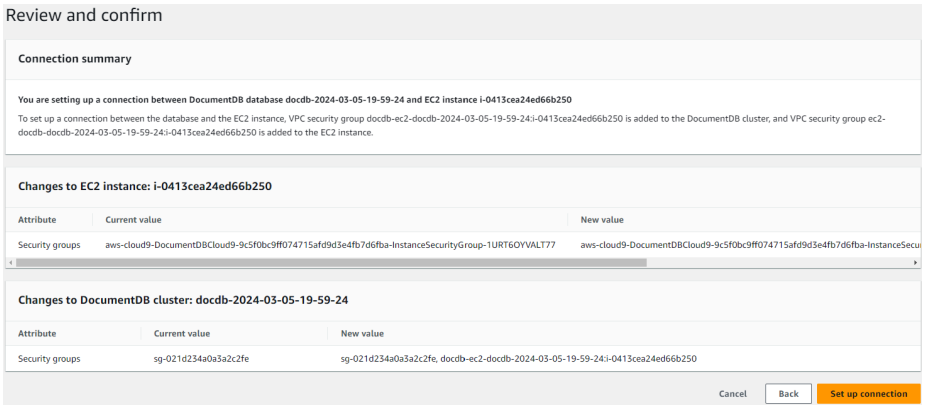
b. Wählen Sie im Feld EC2-Instance die EC2-Instance aus, die Sie mit Ihrem Cluster verbinden möchten.



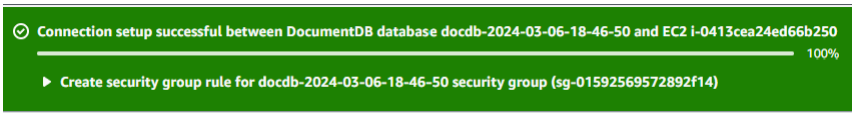
c. Klicken Sie auf Weiter.

Das Dialogfeld „Überprüfen und bestätigen“ wird angezeigt.

d. Vergewissern Sie sich, dass die Änderungen korrekt sind. Wählen Sie dann Verbindung einrichten.



Bei Erfolg wird die folgende Überprüfung angezeigt:



Übersicht über die automatische Verbindung mit einer EC2-Instance

Wenn Sie eine Verbindung zwischen einer EC2-Instance und einer Amazon DocumentDB-Datenbank einrichten, konfiguriert Amazon DocumentDB automatisch die VPC-Sicherheitsgruppe für Ihre EC2-Instance und für Ihre Amazon DocumentDB DocumentDB-Datenbank.

Die folgenden Anforderungen gelten für die Verbindung einer EC2-Instance mit einer Amazon DocumentDB DocumentDB-Datenbank:

- Die EC2-Instance muss in derselben VPC wie die Amazon DocumentDB DocumentDB-Datenbank existieren.

Wenn keine EC2-Instances in derselben VPC vorhanden sind, dann bietet die Konsole einen Link zum Erstellen einer solchen Instance.

- Der Benutzer, der die Verbindung einrichtet, muss über Berechtigungen zum Ausführen der folgenden Amazon-EC2-Vorgänge verfügen:
  - `ec2:AuthorizeSecurityGroupEgress`
  - `ec2:AuthorizeSecurityGroupIngress`
  - `ec2:CreateSecurityGroup`
  - `ec2:DescribeInstances`
  - `ec2:DescribeNetworkInterfaces`
  - `ec2:DescribeSecurityGroups`
  - `ec2:ModifyNetworkInterfaceAttribute`
  - `ec2:RevokeSecurityGroupEgress`

Auf Ihrem Konto fallen ggf. Kosten über Availability Zones hinweg an, wenn sich die DB-Instance und die EC2-Instance in unterschiedlichen Availability Zones befinden.

Wenn Sie eine Verbindung zu einer EC2-Instance einrichten, handelt Amazon DocumentDB gemäß der aktuellen Konfiguration der Sicherheitsgruppen, die der Amazon DocumentDB DocumentDB-Datenbank und EC2-Instance zugeordnet sind, wie in der folgenden Tabelle beschrieben:

Aktuelle Amazon DocumentDB-Sicherheitsgruppenkonfiguration	Aktuelle EC2-Sicherheitsgruppenkonfiguration	Amazon DocumentDB DocumentDB-Aktion
Der Amazon DocumentDB DocumentDB-Datenbank sind eine oder mehrere Sicherheitsgruppen zugeordnet, deren Name dem Muster `DocumentDB-ec2-n` entspricht. Eine Sicherheitsgruppe, die dem Muster entspricht, wurde nicht geändert. Diese Sicherhei	Der EC2-Instance sind eine oder mehrere Sicherheitsgruppen zugeordnet, deren Name dem Muster entspricht `DocumentDB-ec2-n` (wobei n eine Zahl ist). Eine Sicherheitsgruppe, die dem Muster entspricht, wurde nicht geändert. Diese Sicherheitsgruppe hat nur	Amazon DocumentDB ergreift keine Maßnahmen. Eine Verbindung zwischen der EC2-Instance und der Amazon DocumentDB DocumentDB-Datenbank wurde bereits automatisch konfiguriert. Da bereits eine Verbindung zwischen der EC2-Instance und der Amazon DocumentD

Aktuelle Amazon DocumentDB-Sicherheitsgruppenkonfiguration	Aktuelle EC2-Sicherheitsgruppenkonfiguration	Amazon DocumentDB DocumentDB-Aktion
tsgruppe enthält nur eine Regel für eingehenden Datenverkehr mit der VPC-Sicherheitsgruppe der EC2-Instance als Quelle.	eine ausgehende Regel mit der VPC-Sicherheitsgruppe der Amazon DocumentDB DocumentDB-Datenbank als Quelle.	B DocumentDB-Datenbank besteht, werden die Sicherheitsgruppen nicht geändert.

Aktuelle Amazon DocumentDB-Sicherheitsgruppenkonfiguration	Aktuelle EC2-Sicherheitsgruppenkonfiguration	Amazon DocumentDB DocumentDB-Aktion
Es gilt eine der folgenden Bedingungen: • Der Amazon DocumentDB DocumentDB-Datenbank ist keine Sicherheitsgruppe zugeordnet, deren Name dem Muster `DocumentDB-ec2-n` entspricht. • Der Amazon DocumentDB sind eine oder mehrere Sicherheitsgruppen zugeordnet, deren Name dem Muster `DocumentDB-ec2-n` entspricht. Amazon DocumentDB kann jedoch keine dieser Sicherheitsgruppen für die Verbindung mit der EC2-Instance verwenden. Amazon DocumentDB kann keine Sicherheitsgruppe verwenden, die keine Regel für eingehenden Datenverkehr mit der VPC-Sicherheitsgruppe der EC2-Instance als Quelle hat. Amazon DocumentDB kann auch keine Sicherheitsgruppe verwenden, die geändert wurde. Beispiele für Änderungen sind das Hinzufügen einer Regel	Es gilt eine der folgenden Bedingungen: • Der EC2-Instance ist keine Sicherheitsgruppe zugeordnet, deren Name dem Muster `ec2-DocumentDB-n` entspricht. • Der EC2-Instance sind eine oder mehrere Sicherheitsgruppen zugeordnet, deren Name dem Muster `ec2-DocumentDB-n` entspricht. Amazon DocumentDB kann jedoch keine dieser Sicherheitsgruppen für die Verbindung mit der Amazon DocumentDB DocumentDB-Datenbank verwenden. Amazon DocumentDB kann keine Sicherheitsgruppe verwenden, die keine einzige ausgehende Regel mit der VPC-Sicherheitsgruppe der Amazon DocumentDB DocumentDB-Datenbank als Quelle hat. Amazon DocumentDB kann auch keine Sicherheitsgruppe verwenden, die geändert wurde.	Amazon DocumentDB DocumentDB-Aktion: Neue Sicherheitsgruppen erstellen

Aktuelle Amazon DocumentDB-Sicherheitsgruppenkonfiguration	Aktuelle EC2-Sicherheitsgruppenkonfiguration	Amazon DocumentDB DocumentDB-Aktion
oder das Ändern des Ports einer vorhandenen Regel.		
Der Amazon DocumentDB DocumentDB-Datenbank sind eine oder mehrere Sicherheitsgruppen zugeordnet, deren Name dem Muster `DocumentDB-ec2-n` entspricht. Eine Sicherheitsgruppe, die dem Muster entspricht, wurde nicht geändert. Diese Sicherheitsgruppe enthält nur eine Regel für eingehenden Datenverkehr mit der VPC-Sicherheitsgruppe der EC2-Instance als Quelle.	Der EC2-Instance sind eine oder mehrere Sicherheitsgruppen zugeordnet, deren Name dem Muster `ec2-DocumentDB-n` entspricht. Amazon DocumentDB kann jedoch keine dieser Sicherheitsgruppen für die Verbindung mit der Amazon DocumentDB DocumentDB-Datenbank verwenden. Amazon DocumentDB kann keine Sicherheitsgruppe verwenden, die keine einzige ausgehende Regel mit der VPC-Sicherheitsgruppe der Amazon DocumentDB DocumentDB-Datenbank als Quelle hat. Amazon DocumentDB kann auch keine Sicherheitsgruppe verwenden, die geändert wurde.	Amazon DocumentDB DocumentDB-Aktion: Neue Sicherheitsgruppen erstellen

Aktuelle Amazon DocumentDB-Sicherheitsgruppenkonfiguration	Aktuelle EC2-Sicherheitsgruppenkonfiguration	Amazon DocumentDB DocumentDB-Aktion
Der Amazon DocumentDB DocumentDB-Datenbank sind eine oder mehrere Sicherheitsgruppen zugeordnet, deren Name dem Muster `DocumentDB-ec2-n` entspricht. Eine Sicherheitsgruppe, die dem Muster entspricht, wurde nicht geändert. Diese Sicherheitsgruppe enthält nur eine Regel für eingehenden Datenverkehr mit der VPC-Sicherheitsgruppe der EC2-Instance als Quelle.	Eine gültige EC2-Sicherheitsgruppe für die Verbindung ist vorhanden, jedoch nicht mit der EC2-Instance verknüpft. Die Sicherheitsgruppe trägt einen Namen, der dem Muster `DocumentDB-ec2-n` entspricht. Sie wurde nicht geändert. Es gibt nur eine ausgehende Regel mit der VPC-Sicherheitsgruppe der Amazon DocumentDB DocumentDB-Datenbank als Quelle.	Amazon DocumentDB DocumentDB-Aktion: EC2-Sicherheitsgruppe zuordnen

Aktuelle Amazon DocumentDB-Sicherheitsgruppenkonfiguration	Aktuelle EC2-Sicherheitsgruppenkonfiguration	Amazon DocumentDB DocumentDB-Aktion
Es gilt eine der folgenden Bedingungen: • Der Amazon DocumentDB DocumentDB-Datenbank ist keine Sicherheitsgruppe zugeordnet, deren Name dem Muster `DocumentDB-ec2-n` entspricht. • Der Amazon DocumentDB DocumentDB-Datenbank sind eine oder mehrere Sicherheitsgruppen zugeordnet, deren Name dem Muster `DocumentDB-ec2-n` entspricht. Amazon DocumentDB kann jedoch keine dieser Sicherheitsgruppen für die Verbindung mit der EC2-Instance verwenden. Amazon DocumentDB kann keine Sicherheitsgruppe verwenden, die keine Regel für eingehenden Datenverkehr mit der VPC-Sicherheitsgruppe der EC2-Instance als Quelle hat. Amazon DocumentDB kann auch keine Sicherheitsgruppe verwenden, die geändert wurde.	Der EC2-Instance sind eine oder mehrere Sicherheitsgruppen zugeordnet, deren Name dem Muster `DocumentDB-ec2-n` entspricht. Eine Sicherheitsgruppe, die dem Muster entspricht, wurde nicht geändert. Diese Sicherheitsgruppe hat nur eine ausgehende Regel mit der VPC-Sicherheitsgruppe der Amazon DocumentDB DocumentDB-Datenbank als Quelle.	Amazon DocumentDB DocumentDB-Aktion: Neue Sicherheitsgruppen erstellen

Amazon DocumentDB DocumentDB-Aktion: Neue Sicherheitsgruppen erstellen

Amazon DocumentDB ergreift die folgenden Aktionen:

- Erstellt eine neue Sicherheitsgruppe, die dem Muster `DocumentDB-ec2-n` entspricht. Diese Sicherheitsgruppe enthält eine Regel für eingehenden Datenverkehr mit der VPC-Sicherheitsgruppe der EC2-Instance als Quelle. Diese Sicherheitsgruppe ist mit der Amazon DocumentDB DocumentDB-Datenbank verknüpft und ermöglicht der EC2-Instance den Zugriff auf die Amazon DocumentDB DocumentDB-Datenbank.
- Erstellt eine neue Sicherheitsgruppe, die dem Muster `ec2-DocumentDB-n` entspricht. Diese Sicherheitsgruppe hat eine ausgehende Regel mit der VPC-Sicherheitsgruppe der Amazon DocumentDB DocumentDB-Datenbank als Quelle. Diese Sicherheitsgruppe ist der EC2-Instance zugeordnet und ermöglicht der EC2-Instance, Traffic an die Amazon DocumentDB DocumentDB-Datenbank zu senden.

Amazon DocumentDB DocumentDB-Aktion: EC2-Sicherheitsgruppe zuordnen

Amazon DocumentDB ordnet die gültige, bestehende EC2-Sicherheitsgruppe der EC2-Instance zu. Diese Sicherheitsgruppe ermöglicht es der EC2-Instance, Datenverkehr an die Amazon DocumentDB DocumentDB-Datenbank zu senden.

Anzeigen verbundener Rechenressourcen

Sie können den verwenden AWS-Managementkonsole , um die Rechenressourcen anzuzeigen, die mit einer Amazon DocumentDB DocumentDB-Datenbank verbunden sind. Zu den angezeigten Ressourcen gehören Rechenressourcenverbindungen, die automatisch eingerichtet wurden. Sie können die Konnektivität mit Rechenressourcen auf folgende Weise automatisch einrichten:

- Sie können die Rechenressource auswählen, wenn Sie die Datenbank erstellen. Weitere Informationen finden Sie unter Einen Amazon DocumentDB-Cluster erstellen und Einen Multi-AZ DB-Cluster erstellen.
- Sie können die Konnektivität zwischen einer vorhandenen Datenbank und einer Rechenressource einrichten. Weitere Informationen finden Sie unter Amazon EC2 automatisch Connect.

Die aufgelisteten Rechenressourcen enthalten keine Ressourcen, die manuell mit der Datenbank verbunden wurden. Sie können beispielsweise einer Rechenressource den manuellen Zugriff auf eine Datenbank erlauben, indem Sie der VPC-Sicherheitsgruppe, die der Datenbank zugeordnet ist, eine Regel hinzufügen.

Für die Auflistung einer Rechenressource müssen die folgenden Bedingungen erfüllt sei:

- Der Name der Sicherheitsgruppe, die der Rechenressource zugeordnet ist, entspricht dem Muster `ec2-DocumentDB-n` (wobei n eine Zahl ist).
- Die mit der Rechenressource verknüpfte Sicherheitsgruppe hat eine ausgehende Regel, bei der der Portbereich auf den Port festgelegt ist, den die Amazon DocumentDB DocumentDB-Datenbank verwendet.
- Die mit der Rechenressource verknüpfte Sicherheitsgruppe hat eine ausgehende Regel, bei der die Quelle auf eine Sicherheitsgruppe gesetzt ist, die der Amazon DocumentDB DocumentDB-Datenbank zugeordnet ist.
- Der Name der Sicherheitsgruppe, die mit der Amazon DocumentDB DocumentDB-Datenbank verknüpft ist, entspricht dem Muster `DocumentDB-ec2-n` (wobei n eine Zahl ist).
- Die mit der Amazon DocumentDB DocumentDB-Datenbank verknüpfte Sicherheitsgruppe hat eine Eingangsregel, bei der der Portbereich auf den Port festgelegt ist, den die Amazon DocumentDB DocumentDB-Datenbank verwendet.
- Die mit der Amazon DocumentDB DocumentDB-Datenbank verknüpfte Sicherheitsgruppe hat eine Eingangsregel, bei der die Quelle auf eine Sicherheitsgruppe gesetzt ist, die der Rechenressource zugeordnet ist.

Um Rechenressourcen anzuzeigen, die mit einer Amazon DocumentDB DocumentDB-Datenbank verbunden sind

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon DocumentDB DocumentDB-Konsole unter https://console.aws.amazon.com/docdb.
2. Wählen Sie im Navigationsbereich Datenbanken und dann den Namen der Amazon DocumentDB DocumentDB-Datenbank aus.
3. Sehen Sie sich auf der Registerkarte Konnektivität und Sicherheit die Rechenressourcen im Abschnitt Verbundene Rechenressourcen an.

Manuelles Connect von Amazon EC2

Topics

- Schritt 1: Erstellen Sie eine Amazon EC2 EC2-Instance
- Schritt 2: Erstellen einer Sicherheitsgruppe
- Schritt 3: Erstellen Sie einen Amazon DocumentDB-Cluster

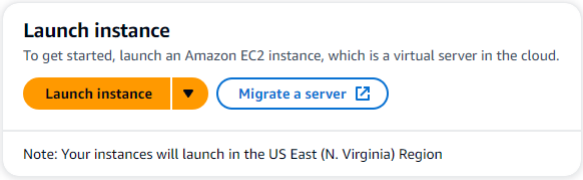
- Schritt 4: Connect zu Ihrer Amazon EC2 EC2-Instance her
- Schritt 5: Installieren Sie die MongoDB-Shell
- Schritt 6: Amazon DocumentDB TLS verwalten
- Schritt 7: Connect zu Ihrem Amazon DocumentDB-Cluster her
- Schritt 8: Daten einfügen und abfragen
- Schritt 9: Erkunden

Bei den folgenden Schritten wird davon ausgegangen, dass Sie die Schritte im Voraussetzungen Thema abgeschlossen haben.

Schritt 1: Erstellen Sie eine Amazon EC2 EC2-Instance

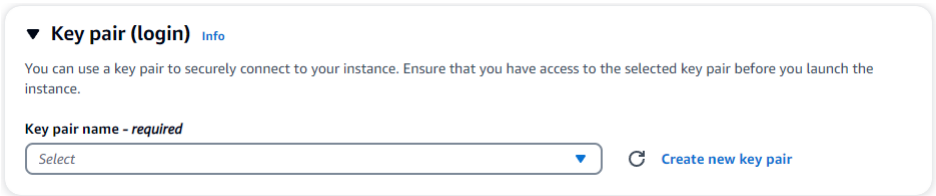
In diesem Schritt erstellen Sie eine Amazon EC2 EC2-Instance in derselben Region und Amazon VPC, die Sie später für die Bereitstellung Ihres Amazon DocumentDB-Clusters verwenden werden.

1. Wählen Sie auf der Amazon EC2 EC2-Konsole Launch instance aus.



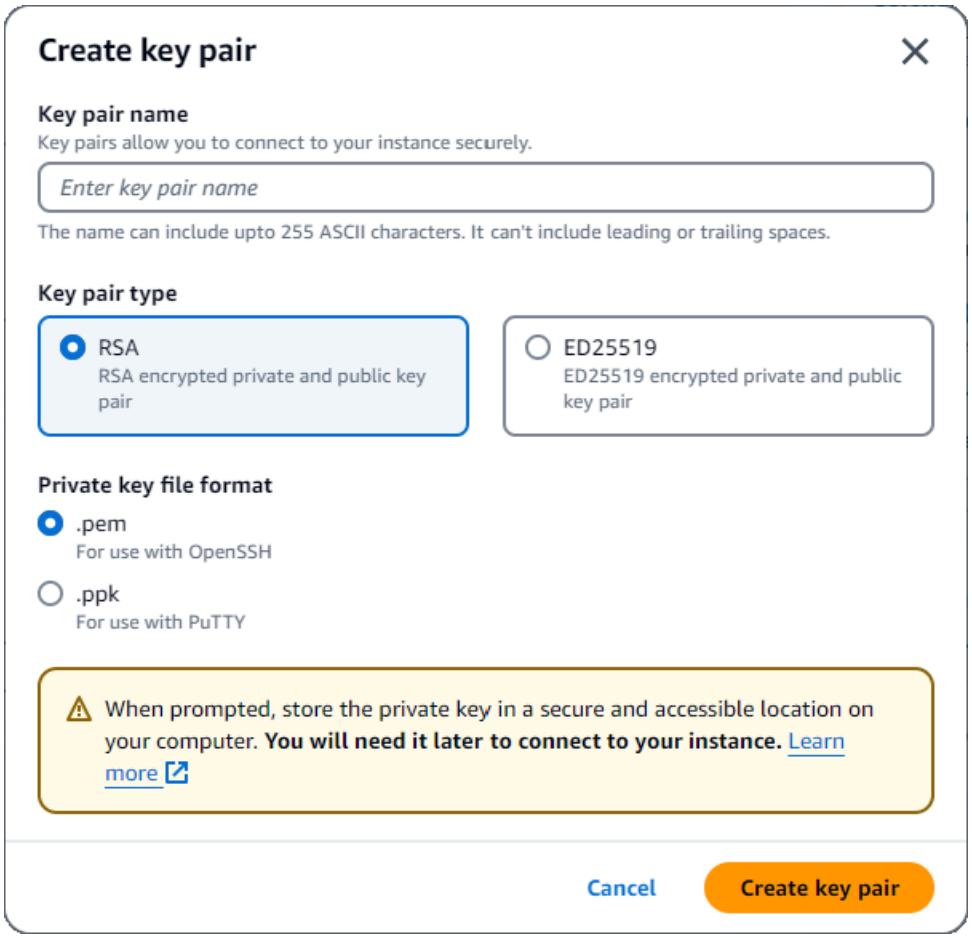
2. Geben Sie einen Namen oder eine Kennung in das Feld Name im Abschnitt Name und Tags ein.
3. Suchen Sie in der Dropdownliste Amazon Machine Image (AMI) nach Amazon Linux 2 AMI und wählen Sie es aus.

4. Suchen Sie in der Dropdownliste Instance-Typ nach t3.micro und wählen Sie es aus.
5. Geben Sie im Abschnitt key pair (Anmeldung) die Kennung eines vorhandenen Schlüsselpaars ein, oder wählen Sie Neues Schlüsselpaar erstellen.



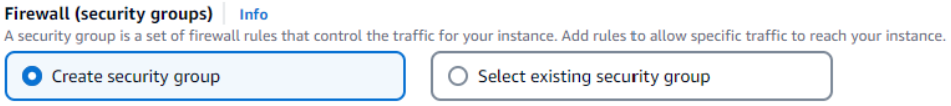
Sie müssen ein Amazon EC2 EC2-Schlüsselpaar angeben.

- Wenn Sie ein Amazon EC2 EC2-Schlüsselpaar haben:
  1. Wählen Sie ein key pair aus, wählen Sie Ihr key pair aus der Liste.
  2. Sie müssen die private Schlüsseldatei (.pem- oder .ppk-Datei) bereits verfügbar haben, um sich bei Ihrer Amazon EC2 EC2-Instance anmelden zu können.
- Wenn Sie kein Amazon EC2 EC2-Schlüsselpaar haben:
  1. Wählen Sie Neues key pair erstellen. Daraufhin wird das Dialogfeld key pair erstellen angezeigt.
  2. Geben Sie einen Namen in das Feld Name des Schlüsselpaars ein.
  3. Wählen Sie den Schlüsselpaartyp und das Dateiformat für den privaten Schlüssel.
  4. Wählen Sie Create Key Pair (Schlüsselpaar erstellen) aus.



> **Note**
>
> Aus Sicherheitsgründen empfehlen wir dringend, ein Schlüsselpaar sowohl für die SSH- als auch für die Internetverbindung zu Ihrer EC2-Instance zu verwenden.

6. Wählen Sie im Abschnitt Netzwerkeinstellungen unter Firewall (Sicherheitsgruppen) entweder Sicherheitsgruppe erstellen oder Bestehende Sicherheitsgruppe auswählen aus.



   Wenn Sie eine bestehende Sicherheitsgruppe auswählen möchten, wählen Sie eine aus der Dropdownliste Allgemeine Sicherheitsgruppen aus.

   Wenn Sie eine neue Sicherheitsgruppe erstellen möchten, gehen Sie wie folgt vor:

   a. Überprüfen Sie alle Regeln für die Zulassung von Datenverkehr, die für Ihre EC2-Konnektivität gelten.

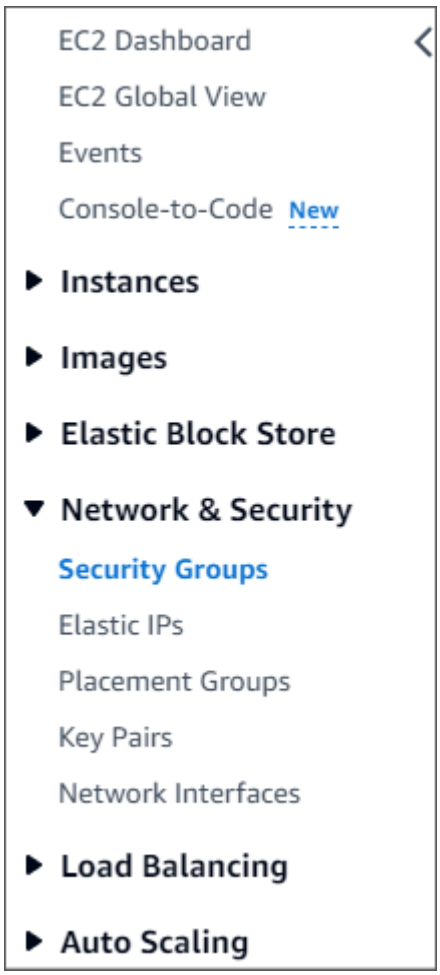
   b. Wählen Sie im Feld IP die Option Meine IP oder Benutzerdefiniert aus, um aus einer Liste von CIDR-Blöcken, Präfixlisten oder Sicherheitsgruppen auszuwählen. Wir empfehlen Anywhere nicht als Wahl, es sei denn, Ihre EC2-Instance befindet sich in einem isolierten Netzwerk, da sie beliebigen IP-Adressen den Zugriff auf Ihre EC2-Instance ermöglicht.

7. Überprüfen Sie im Abschnitt Zusammenfassung Ihre EC2-Konfiguration und wählen Sie, falls korrekt, die Option Launch instance aus.

Schritt 2: Erstellen einer Sicherheitsgruppe

Sie werden jetzt eine neue Sicherheitsgruppe in Ihrer Standard-Amazon-VPC erstellen. Die Sicherheitsgruppe `demoDocDB` ermöglicht es Ihnen, von Ihrer Amazon EC2-Instance aus eine Verbindung zu Ihrem Amazon DocumentDB-Cluster auf Port 27017 (dem Standardport für Amazon DocumentDB) herzustellen.

1. Wählen Sie in der Amazon EC2 Management Console unter Netzwerk und Sicherheit die Option Sicherheitsgruppen aus.



2. Wählen Sie Sicherheitsgruppe erstellen aus.

3. Gehen Sie im Abschnitt Grundlegende Details wie folgt vor:

   a. Geben Sie für Security group name (Name der Sicherheitsgruppe) `demoDocDB` ein.

   b. Geben Sie im Feld Description (Beschreibung) eine Beschreibung ein.

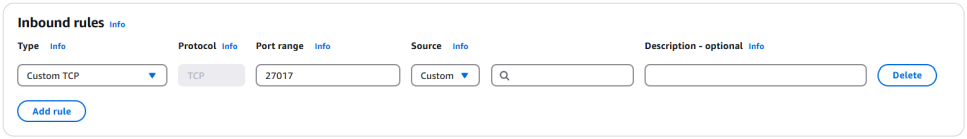
   c. Akzeptieren Sie für VPC die Verwendung Ihrer Standard-VPC.

4. Wählen Sie im Abschnitt Eingehende Regeln die Option Regel hinzufügen aus.

   a. Wählen Sie für Typ die Option Benutzerdefinierte TCP-Regel (Standard) aus.

   b. Geben Sie für Portbereich den Wert ein`27017`.

   c. Wählen Sie für Source (Quelle) die Option Custom (Benutzerdefiniert) aus. Suchen Sie im Feld daneben nach der Sicherheitsgruppe, die Sie gerade in Schritt 1 erstellt haben. Möglicherweise müssen Sie Ihren Browser aktualisieren, damit die Amazon EC2 EC2-Konsole den Quellnamen automatisch ausfüllt.



5. Akzeptieren Sie alle anderen Standardeinstellungen und wählen Sie Sicherheitsgruppe erstellen.

Schritt 3: Erstellen Sie einen Amazon DocumentDB-Cluster

Während die Amazon EC2 EC2-Instance bereitgestellt wird, erstellen Sie Ihren Amazon DocumentDB-Cluster.

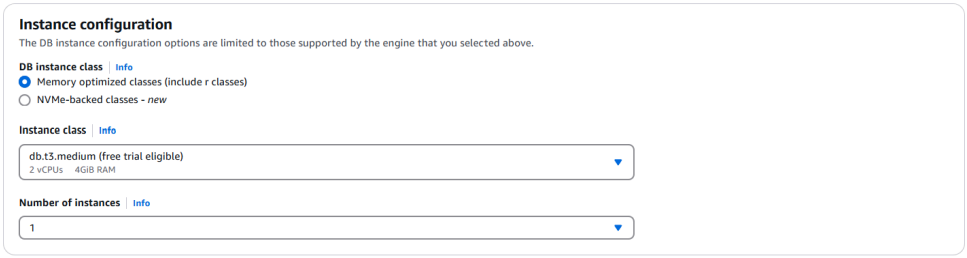
1. Navigieren Sie zur Amazon DocumentDB DocumentDB-Konsole und wählen Sie im Navigationsbereich Clusters aus.
2. Wählen Sie Erstellen aus.
3. Belassen Sie die Standardeinstellung für den Clustertyp auf Instance Based Cluster.
4. Geben Sie in Clusterkonfiguration für Cluster-ID einen eindeutigen Namen ein. Beachten Sie, dass die Konsole alle Clusternamen unabhängig von der Art der Eingabe in Kleinbuchstaben ändert.

   Behalten Sie für die Engine-Version den Standardwert 5.0.0 bei.
5. Behalten Sie für die Cluster-Speicherkonfiguration die Standardeinstellung von Amazon DocumentDB Standard bei.
6. In der Instanzkonfiguration:

   - Wählen Sie für DB-Instance-Klasse die Option Speicheroptimierte Klassen (einschließlich R-Klassen) aus (dies ist die Standardeinstellung).

     Die andere Instance-Option ist NVMe-backed Klassen. Weitere Informationen hierzu finden Sie unter NVMe-backed Instanzen.
   - Wählen Sie für Instance-Klasse den Instance-Typ aus, der Ihren Anforderungen entspricht. Eine detailliertere Erläuterung der Instanzklassen finden Sie unterSpezifikationen der Instanzklasse.

- Wählen Sie für die Anzahl der Instances eine Zahl aus, die Ihren Anforderungen am besten entspricht. Denken Sie daran, je niedriger die Anzahl, desto niedriger die Kosten und desto geringer das read/write Volumen, das vom Cluster verwaltet werden kann.



7. Behalten Sie für Konnektivität die Standardeinstellung „Keine Verbindung zu einer EC2-Rechenressource herstellen“ bei.

> **Note**
>
> Wenn Sie eine Verbindung zu einer EC2-Rechenressource herstellen, werden automatisch Sicherheitsgruppen für Ihre Verbindung zu Ihrem Cluster erstellt. Da Sie diese Sicherheitsgruppen im vorherigen Schritt manuell erstellt haben, sollten Sie „Keine Verbindung zu einer EC2-Rechenressource herstellen“ auswählen, um keinen zweiten Satz von Sicherheitsgruppen zu erstellen.

8. Geben Sie im Abschnitt Authentifizierung einen Benutzernamen für den Hauptbenutzer ein und wählen Sie dann Selbstverwaltet aus. Geben Sie ein Passwort ein und bestätigen Sie es.

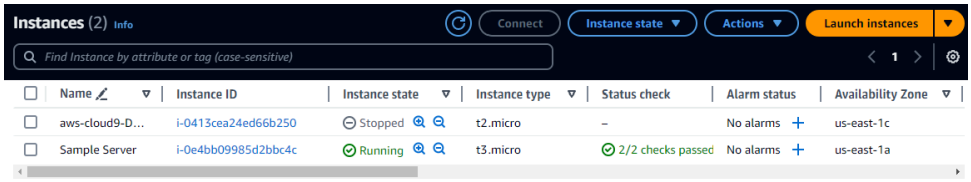
   Wenn Sie stattdessen Verwaltet in wählen AWS Secrets Manager, finden Sie Passwortverwaltung mit Amazon DocumentDB und AWS Secrets Manager weitere Informationen unter.

9. Wählen Sie Cluster erstellen.

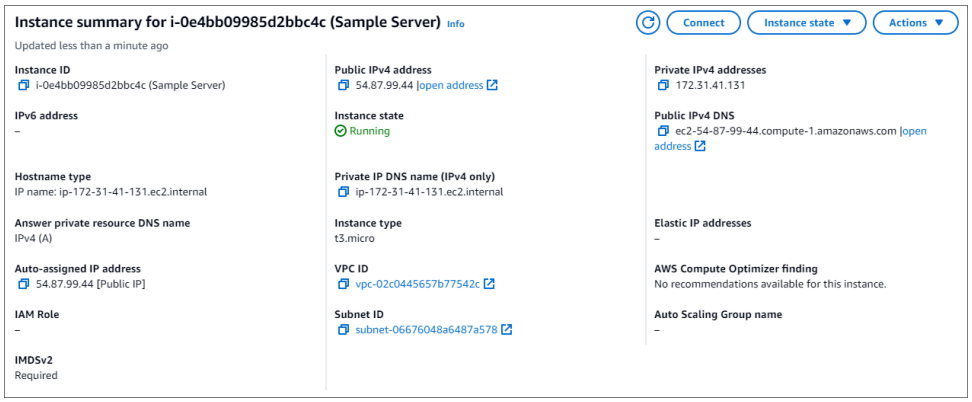
Schritt 4: Connect zu Ihrer Amazon EC2 EC2-Instance her

Wenn Sie eine Verbindung zu Ihrer Amazon EC2 EC2-Instance herstellen, können Sie die MongoDB-Shell installieren. Durch die Installation der Mongo-Shell können Sie eine Verbindung zu Ihrem Amazon DocumentDB-Cluster herstellen und ihn abfragen. Führen Sie folgende Schritte aus:

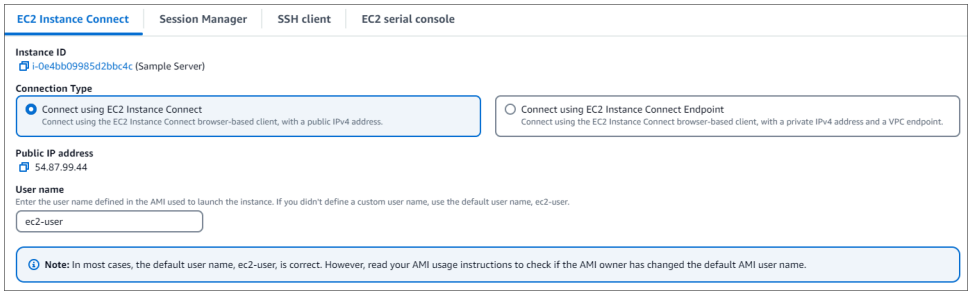
1. Navigieren Sie auf der Amazon EC2 EC2-Konsole zu Ihren Instances und überprüfen Sie, ob die gerade erstellte Instance läuft. Wenn ja, wählen Sie die Instance aus, indem Sie auf die Instance-ID klicken.



2. Wählen Sie Connect aus.



3. Es gibt vier Optionen mit Registerkarten für Ihre Verbindungsmethode: Amazon EC2 Instance Connect, Session Manager, SSH-Client oder serielle EC2-Konsole. Sie müssen eine auswählen und deren Anweisungen befolgen. Wenn Sie fertig sind, wählen Sie Connect.



> **Note**
>
> Wenn sich Ihre IP-Adresse geändert hat, nachdem Sie diesen Walkthrough gestartet haben, oder wenn Sie zu einem späteren Zeitpunkt zu Ihrer Umgebung zurückkehren, müssen Sie Ihre `demoEC2` Sicherheitsgruppenregel für eingehenden Datenverkehr aktualisieren, um eingehenden Datenverkehr von Ihrer neuen API-Adresse aus zu ermöglichen.

Schritt 5: Installieren Sie die MongoDB-Shell

Sie können jetzt die MongoDB-Shell installieren. Dabei handelt es sich um ein Befehlszeilenprogramm, mit dem Sie eine Verbindung herstellen und Ihren Amazon DocumentDB-Cluster abfragen können. Derzeit gibt es zwei Versionen der MongoDB-Shell: die neueste Version, Mongosh, und die vorherige Version, Mongo-Shell.

> **Important**
>
> Es gibt eine bekannte Einschränkung bei Node.js Treibern, die älter als Version 6.13.1 sind und derzeit nicht von der IAM-Identitätsauthentifizierung für Amazon DocumentDB unterstützt werden. Node.js Treiber und Tools, die Node.js Treiber verwenden (z. B. Mongosh), müssen aktualisiert werden, sodass sie die Node.js Treiberversion 6.13.1 oder höher verwenden.

Folgen Sie den nachstehenden Anweisungen, um die MongoDB-Shell für Ihr Betriebssystem zu installieren.

On Amazon Linux

So installieren Sie die MongoDB-Shell auf Amazon Linux

Wenn Sie IAM nicht verwenden und die neueste MongoDB-Shell (mongosh) verwenden möchten, um eine Verbindung zu Ihrem Amazon DocumentDB-Cluster herzustellen, gehen Sie wie folgt vor:

1. Erstellen Sie die Repository-Datei. Führen Sie in der Befehlszeile Ihrer EC2-Instance, die Sie erstellt haben, den folgenden Befehl aus:

   ```
   echo -e "[mongodb-org-5.0] \nname=MongoDB Repository\nbaseurl=https://
   repo.mongodb.org/yum/amazon/2023/mongodb-org/5.0/x86_64/\ngpgcheck=1 \nenabled=1
    \ngpgkey=https://pgp.mongodb.com/server-5.0.asc" | sudo tee /etc/yum.repos.d/
   mongodb-org-5.0.repo
   ```

2. Wenn der Vorgang abgeschlossen ist, installieren Sie mongosh mit einer der beiden folgenden Befehlsoptionen an der Befehlszeile:

   Option 1 — Wenn Sie während der Amazon EC2-Konfiguration den Standard Amazon Linux 2023 ausgewählt haben, geben Sie diesen Befehl ein:

   ```
   sudo yum install -y mongodb-mongosh-shared-openssl3
   ```

Option 2 — Wenn Sie bei der Amazon EC2-Konfiguration Amazon Linux 2 ausgewählt haben, geben Sie diesen Befehl ein:

```
sudo yum install -y mongodb-mongosh
```

Wenn Sie IAM verwenden, müssen Sie die vorherige Version der MongoDB-Shell (5.0) verwenden, um eine Verbindung zu Ihrem Amazon DocumentDB-Cluster herzustellen. Gehen Sie wie folgt vor:

1. Erstellen Sie die Repository-Datei. Führen Sie in der Befehlszeile Ihrer EC2-Instance, die Sie erstellt haben, den folgenden Befehl aus:

```
echo -e "[mongodb-org-5.0] \nname=MongoDB Repository\nbaseurl=https://
repo.mongodb.org/yum/amazon/2023/mongodb-org/5.0/x86_64/\ngpgcheck=1 \nenabled=1
 \ngpgkey=https://pgp.mongodb.com/server-5.0.asc" | sudo tee /etc/yum.repos.d/
mongodb-org-5.0.repo
```

2. Wenn der Vorgang abgeschlossen ist, installieren Sie die Mongodb 5.0-Shell mit der folgenden Befehlsoption an der Befehlszeile:

```
sudo yum install -y mongodb-org-shell
```

On Ubuntu

Um mongosh auf Ubuntu zu installieren

1. Importieren Sie den öffentlichen Schlüssel, der von dem Paketverwaltungssystem verwendet wird.

```
curl -fsSL https://pgp.mongodb.com/server-5.0.asc | sudo gpg --dearmor -o /usr/
share/keyrings/mongodb-server-5.0.gpg
```

2. Erstellen Sie die Listendatei `mongodb-org-5.0.list` für MongoDB mit dem korrekten Befehl für Ihre Ubuntu-Version.

```
echo "deb [ arch=amd64,arm64 signed-by=/usr/share/keyrings/mongodb-
server-5.0.gpg ] https://repo.mongodb.org/apt/ubuntu focal/mongodb-org/5.0
 multiverse" | sudo tee /etc/apt/sources.list.d/mongodb-org-5.0.list
```

3. Importieren und aktualisieren Sie die lokale Paketdatenbank mit dem folgenden Befehl:

```
sudo apt-get update
```

4. Installieren Sie Mongosh.

```
sudo apt-get install -y mongodb-mongosh
```

Weitere Informationen zum Installieren von früheren Versionen von MongoDB auf Ihrem Ubuntu-System finden Sie unter Installieren von MongoDB Community Edition auf Ubuntu.

On other operating systems

Informationen zum Installieren der mongo-Shell auf anderen Betriebssystemen finden Sie unter Installieren von MongoDB Community Edition in der MongoDB-Dokumentation.

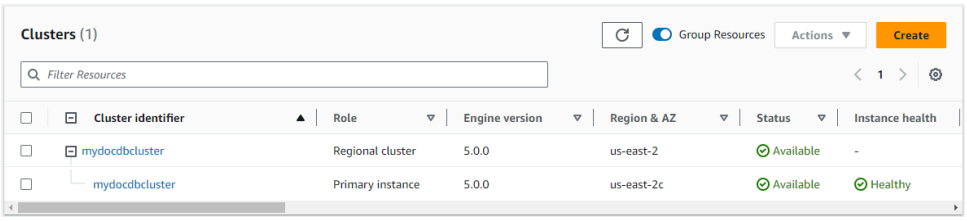
Schritt 6: Amazon DocumentDB TLS verwalten

Laden Sie das CA-Zertifikat für Amazon DocumentDB mit dem folgenden Code herunter: `wget https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem`

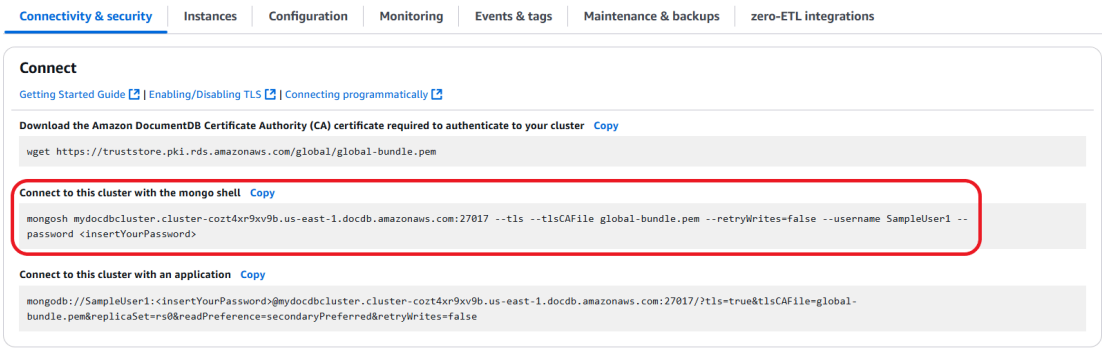
> **Note**
>
> Transport Layer Security (TLS) ist standardmäßig für alle neuen Amazon DocumentDB-Cluster aktiviert. Weitere Informationen finden Sie unter TLS-Einstellungen für Amazon DocumentDB-Cluster verwalten.

Schritt 7: Connect zu Ihrem Amazon DocumentDB-Cluster her

1. Suchen Sie auf der Amazon DocumentDB DocumentDB-Konsole unter Clusters Ihren Cluster. Wählen Sie den Cluster aus, den Sie erstellt haben, indem Sie auf die Cluster-ID für diesen Cluster klicken.



2. Suchen Sie auf der Registerkarte Konnektivität und Sicherheit im Feld Connect nach Connect to this cluster with the mongo shell:



   Kopieren Sie die angegebene Verbindungszeichenfolge und fügen Sie sie in Ihr Terminal ein.

   Nehmen Sie die folgenden Änderungen daran vor:

   a. Stellen Sie sicher, dass Sie den richtigen Benutzernamen in der Zeichenfolge haben.

   b. Auslassen, `<insertYourPassword>` sodass Sie beim Herstellen der Verbindung von der Mongo-Shell zur Eingabe des Passworts aufgefordert werden.

   c. Optional: Wenn Sie die IAM-Authentifizierung oder die vorherige Version der MongoDB-Shell verwenden, ändern Sie Ihre Verbindungszeichenfolge wie folgt:

      ```
      mongo --ssl --host mydocdbcluster.cluster-cozt4xr9xv9b.us-east-1.docdb.amazonaws.com:27017 --sslCAFile global-bundle.pem --username SampleUser1 --password
      ```

      `mydocdbcluster.cluster-cozt4xr9xv9b.us-east-1`Ersetzen Sie durch dieselben Informationen aus Ihrem Cluster.

3. Drücken Sie die Eingabetaste in Ihrem Terminal. Sie werden nun zur Eingabe Ihres Passworts aufgefordert. Geben Sie Ihr Passwort ein.

4. Wenn Sie Ihr Passwort eingeben und die `rs0 [direct: primary] <env-name>>` Aufforderung sehen, sind Sie erfolgreich mit Ihrem Amazon DocumentDB-Cluster verbunden.

Haben Sie Probleme mit der Verbindung? Weitere Informationen finden Sie unter Fehlerbehebung bei Amazon DocumentDB.

Schritt 8: Daten einfügen und abfragen

Nachdem Sie nun mit Ihrem Cluster verbunden sind, können Sie einige Abfragen ausführen, um sich mit der Verwendung einer Dokumentendatenbank vertraut zu machen.

1. Um ein einzelnes Dokument einzufügen, geben Sie Folgendes ein:

```
db.collection.insertOne({"hello":"DocumentDB"})
```

   Sie erhalten die folgende Ausgabe:

```
{
  acknowledged: true,
  insertedId: ObjectId('673657216bdf6258466b128c')
}
```

2. Sie können das Dokument lesen, das Sie mit dem `findOne()` Befehl geschrieben haben (weil er nur ein einziges Dokument zurückgibt). Geben Sie Folgendes ein:

```
db.collection.findOne()
```

   Sie erhalten die folgende Ausgabe:

```
{ "_id" : ObjectId("5e401fe56056fda7321fbd67"), "hello" : "DocumentDB" }
```

3. Um ein paar weitere Abfragen durchzuführen, sollten Sie einen Anwendungsfall für Spieleprofile in Betracht ziehen. Fügen Sie zunächst einige Einträge in eine Sammlung mit dem Titel ein`profiles`. Geben Sie Folgendes ein:

```
db.profiles.insertMany([{ _id: 1, name: 'Matt', status: 'active', level: 12, score:
 202 },
      { _id: 2, name: 'Frank', status: 'inactive', level: 2, score: 9 },
      { _id: 3, name: 'Karen', status: 'active', level: 7, score: 87 },
      { _id: 4, name: 'Katie', status: 'active', level: 3, score: 27 }
])
```

   Sie erhalten die folgende Ausgabe:

```
{ acknowledged: true, insertedIds: { '0': 1, '1': 2, '2': 3, '3': 4 } }
```

4. Verwenden Sie den `find()` Befehl, um alle Dokumente in der Profilsammlung zurückzugeben. Geben Sie Folgendes ein:

```
db.profiles.find()
```

   Sie erhalten eine Ausgabe, die den Daten entspricht, die Sie in Schritt 3 eingegeben haben.

5. Verwenden Sie mithilfe eines Filters eine Abfrage für ein einzelnes Dokument. Geben Sie Folgendes ein:

```
db.profiles.find({name: "Katie"})
```

   Sie erhalten die folgende Ausgabe:

```
{ "_id" : 4, "name" : "Katie", "status": "active", "level": 3, "score":27}
```

6. Versuchen wir nun, ein Profil zu finden und es mit dem `findAndModify` Befehl zu ändern. Wir geben dem Benutzer Matt zusätzliche 10 Punkte mit dem folgenden Code:

```
db.profiles.findAndModify({
        query: { name: "Matt", status: "active"},
        update: { $inc: { score: 10 } }
    })
```

   Sie erhalten die folgende Ausgabe (beachten Sie, dass sein Punktestand noch nicht gestiegen ist):

```
{
    [{_id : 1, name : 'Matt', status: 'active', level: 12, score: 202}]
```

7. Sie können mit der folgenden Abfrage überprüfen, ob sich sein Punktestand geändert hat:

   `db.profiles.find({name: "Matt"})`

   Sie erhalten die folgende Ausgabe:

```
{ "_id" : 1, "name" : "Matt", "status" : "active", "level" : 12, "score" : 212 }
```

Schritt 9: Erkunden

Herzlichen Glückwunsch! Sie haben die Schnellstartanleitung für Amazon DocumentDB erfolgreich abgeschlossen.

Was kommt als Nächstes? Erfahren Sie, wie Sie diese leistungsstarke Datenbank mit einigen ihrer beliebten Funktionen voll ausschöpfen können:

- Amazon DocumentDB verwalten
- Skalierung
- Sichern und Wiederherstellen

> **Note**
>
> Um Kosten zu sparen, können Sie entweder Ihren Amazon DocumentDB-Cluster stoppen, um die Kosten zu senken, oder den Cluster löschen. Standardmäßig stoppt Ihre AWS Cloud9 Umgebung nach 30 Minuten Inaktivität die zugrunde liegende Amazon EC2 EC2-Instance.

Stellen Sie mithilfe des Amazon DocumentDB DocumentDB-JDBC-Treibers eine Verbindung her

Der JDBC-Treiber für Amazon DocumentDB bietet eine SQL-relational Schnittstelle für Entwickler und ermöglicht die Konnektivität von BI-Tools wie Tableau und. DbVisualizer

Weitere Informationen finden Sie in der Amazon DocumentDB DocumentDB-JDBC-Treiber-Dokumentation unter. GitHub

Themen

- Erste Schritte
- Stellen Sie von Tableau Desktop aus eine Connect zu Amazon DocumentDB her
- Connect zu Amazon DocumentDB her von DbVisualizer
- Automatische JDBC-Schemagenerierung
- SQL-Unterstützung und Einschränkungen
- Fehlerbehebung

Erste Schritte

Schritt 1. Amazon DocumentDB-Cluster erstellen

Wenn Sie keinen Amazon DocumentDB-Cluster erstellt haben, erstellen Sie einen anhand der Anweisungen im Abschnitt Erste Schritte im Amazon DocumentDB DocumentDB-Entwicklerhandbuch.

> **Note**
>
> Amazon DocumentDB ist ein reiner Virtual Private Cloud (VPC) -Service. Wenn Sie eine Verbindung von einem lokalen Computer außerhalb der VPC des Clusters herstellen, müssen Sie eine SSH-Verbindung zu einer Amazon EC2 EC2-Instance herstellen. Starten Sie in diesem Fall Ihren Cluster anhand der Anweisungen unter Connect with EC2. Weitere Informationen zum SSH-Tunneling und wann Sie es möglicherweise benötigen, finden Sie unter Verwenden eines SSH-Tunnels zum Herstellen einer Connect zu Amazon DocumentDB.

Schritt 2. JRE- oder JDK-Installation

Abhängig von Ihrer BI-Anwendung müssen Sie möglicherweise sicherstellen, dass eine 64-Bit-JRE- oder JDK-Installationsversion 8 oder höher auf Ihrem Computer installiert ist. Sie können das Java SE Runtime Environment 8 hier herunterladen.

Schritt 3. Laden Sie den DocumentDB-JDBC-Treiber herunter

Laden Sie den DocumentDB-JDBC-Treiber von hier herunter. Der Treiber ist als einzelne JAR-Datei verpackt (z. B. documentdb-jdbc-1.0.0-all.jar).

Schritt 4. Verwenden eines SSH-Tunnels zum Connect zu Amazon DocumentDB

Amazon DocumentDB-Cluster (mit MongoDB-Kompatibilität) werden in einer Amazon Virtual Private Cloud (Amazon VPC) bereitgestellt. Auf sie kann direkt von Amazon EC2 EC2-Instances oder anderen AWS Services zugegriffen werden, die in derselben Amazon VPC bereitgestellt werden. Darüber hinaus können EC2a-Instances oder andere AWS Services in verschiedenen VPCs in derselben AWS Region oder anderen Regionen über VPC-Peering auf Amazon DocumentDB zugreifen.

Sie können SSH-Tunneling (auch bekannt als Portweiterleitung) verwenden, um von außerhalb der VPC des Clusters auf Ihre Amazon DocumentDB DocumentDB-Ressourcen zuzugreifen. Dies

wird bei den meisten Benutzern der Fall sein, die ihre Anwendung nicht auf einer VM in derselben VPC wie der DocumentDB-Cluster ausführen.

Um einen SSH-Tunnel zu erstellen, benötigen Sie eine Amazon EC2 EC2-Instance, die in derselben Amazon VPC wie Ihr Amazon DocumentDB-Cluster läuft. Sie können entweder eine vorhandene EC2-Instance in derselben VPC wie Ihr Cluster verwenden oder eine erstellen. Sie können einen SSH-Tunnel zum Amazon DocumentDB-Cluster einrichten, `sample-cluster.node.us-east-1.docdb.amazonaws.com` indem Sie den folgenden Befehl auf Ihrem lokalen Computer ausführen.

```
ssh -i "ec2Access.pem" -L 27017:sample-cluster.node.us-
east-1.docdb.amazonaws.com:27017 ubuntu@ec2-34-229-221-164.compute-1.amazonaws.com -
N
```

Das Flag -L wird für die Weiterleitung eines lokalen Ports verwendet. Dies ist eine Voraussetzung für die Verbindung zu einem BI-Tool, das auf einem Client außerhalb Ihrer VPC ausgeführt wird. Sobald Sie den obigen Schritt ausgeführt haben, können Sie mit den nächsten Schritten für das BI-Tool Ihrer Wahl fortfahren.

Weitere Informationen zum SSH-Tunneling finden Sie in der Dokumentation Verwenden eines SSH-Tunnels zur Verbindung mit Amazon DocumentDB.

Stellen Sie von Tableau Desktop aus eine Connect zu Amazon DocumentDB her

Themen

- Hinzufügen des Amazon DocumentDB DocumentDB-JDBC-Treibers
- Mit Tableau eine Verbindung zu Amazon DocumentDB herstellen — SSH-Tunnel

Hinzufügen des Amazon DocumentDB DocumentDB-JDBC-Treibers

Um von Tableau Desktop aus eine Verbindung zu Amazon DocumentDB herzustellen, müssen Sie den Amazon DocumentDB DocumentDB-JDBC-Treiber und den DocumentDB-Tableau-Connector herunterladen und installieren.

1. Laden Sie die JAR-Datei des Amazon DocumentDB DocumentDB-JDBC-Treibers aus dem Amazon DocumentDB DocumentDB-JDBC-Treiber-Repository herunter und kopieren Sie sie je nach Betriebssystem in eines der folgenden Verzeichnisse:

- Windows - `C:\Program Files\Tableau\Drivers`
- macOS - `~/Library/Tableau/Drivers`

2. Laden Sie den DocumentDB Tableau-Connector (eine TACO-Datei) von der Tableau Exchange-Website herunter und kopieren Sie ihn in Ihr My Repository/Connectors Tableau-Verzeichnis.

   - Windows - `C:\Users\[user]\Documents\My Tableau Repository\Connectors`
   - macOS - `/Users/[user]/Documents/My Tableau Repository/Connectors`

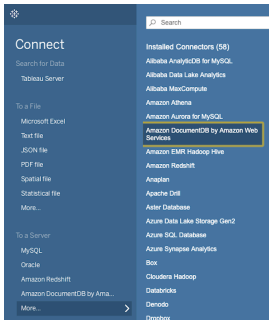
Weitere Informationen finden Sie in der Tableau-Dokumentation.

> **Note**
>
> Wenn Sie neuere CA-Zertifikate verwenden, stellen Sie sicher, dass Sie Ihren JDBC-Treiber auf Version 1.4.5 aktualisieren (in diesem AWS GitHub Repository verfügbar).

Mit Tableau eine Verbindung zu Amazon DocumentDB herstellen — SSH-Tunnel

Um von einem Client-Computer außerhalb der VPC Ihres DocumentDB-Clusters aus eine Verbindung zu Tableau herzustellen, müssen Sie einen SSH-Tunnel einrichten, bevor Sie die folgenden Schritte ausführen:

1. Starten Sie die Tableau Desktop-Anwendung.
2. Navigieren Sie zu Connect > Zu einem Server > Mehr.
3. Wählen Sie unter Installierte Konnektoren die Option Amazon DocumentDB by Amazon Web Services aus.

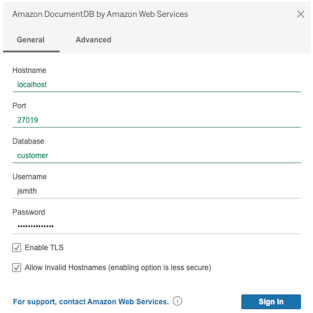


Herstellen einer Verbindung zu Amazon DocumentDB mithilfe von Tableau — Externer SSH-Tunnel

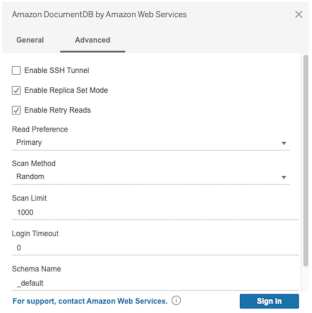
1. Geben Sie die erforderlichen Verbindungsparameter Hostname, Port, Datenbank, Benutzername und Passwort ein. Die Verbindungsparameter im folgenden Beispiel entsprechen der JDBC-Verbindungszeichenfolge:

   ```
   jdbc:documentdb://localhost:27019/test?
   tls=true&tlsAllowInvalidHostnames=true&scanMethod=random&scanLimit=1000&logir
   ```

   die Parameter Benutzername und Passwort separat in einer Eigenschaftensammlung übergeben werden. Weitere Informationen zu Verbindungszeichenfolgenparametern finden Sie in der Github-Dokumentation des Amazon DocumentDB DocumentDB-JDBC-Treibers.



2. (Optional) Weitere erweiterte Optionen finden Sie auf der Registerkarte Erweitert.

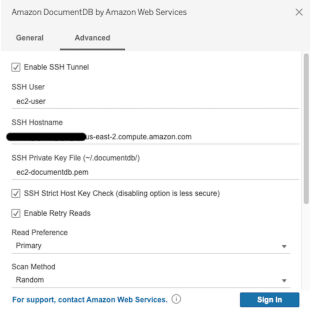


3. Klicken Sie auf Sign in.

Mit Tableau eine Verbindung zu Amazon DocumentDB herstellen — Interner SSH-Tunnel

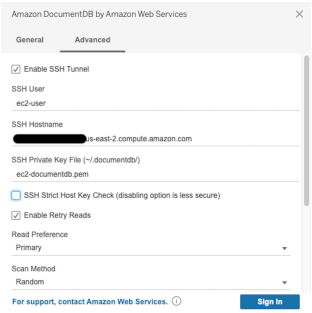
> **Note**
>
> Wenn Sie es vorziehen, den SSH-Tunnel nicht über ein Terminal einzurichten, können Sie die Tableau-GUI verwenden, um Ihre EC2-Instanzdetails anzugeben, die der JDBC-Treiber standardmäßig zur Erstellung eines SSH-Tunnels verwenden wird.

1. Wählen Sie auf der Registerkarte Erweitert die Option SSH-Tunnel aktivieren aus, um weitere Eigenschaften zu überprüfen.



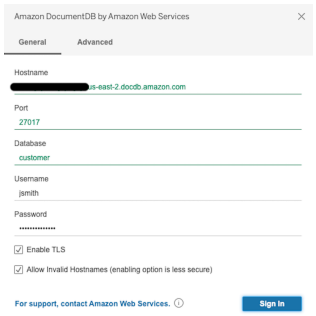
2. Geben Sie den SSH-Benutzer, den SSH-Hostnamen und die private SSH-Schlüsseldatei ein.
3. (Optional) Sie können die Option SSH Strict Host Key Check deaktivieren, wodurch die Überprüfung des Hostschlüssels anhand einer Datei mit bekannten Hosts umgangen wird.

> **Note**
>
> Die Deaktivierung dieser Option ist weniger sicher, da sie zu einem Man-in-the-Middle-Angriff führen kann.



4. Geben Sie die erforderlichen Parameter ein: Hostname, Port, Datenbank, Benutzername und Passwort.

> **Note**
>
> Stellen Sie sicher, dass Sie den DocumentDB-Clusterendpunkt und nicht localhost verwenden, wenn Sie die interne SSH-Tunneloption verwenden.



5. Klicken Sie auf Sign In.

Connect zu Amazon DocumentDB her von DbVisualizer

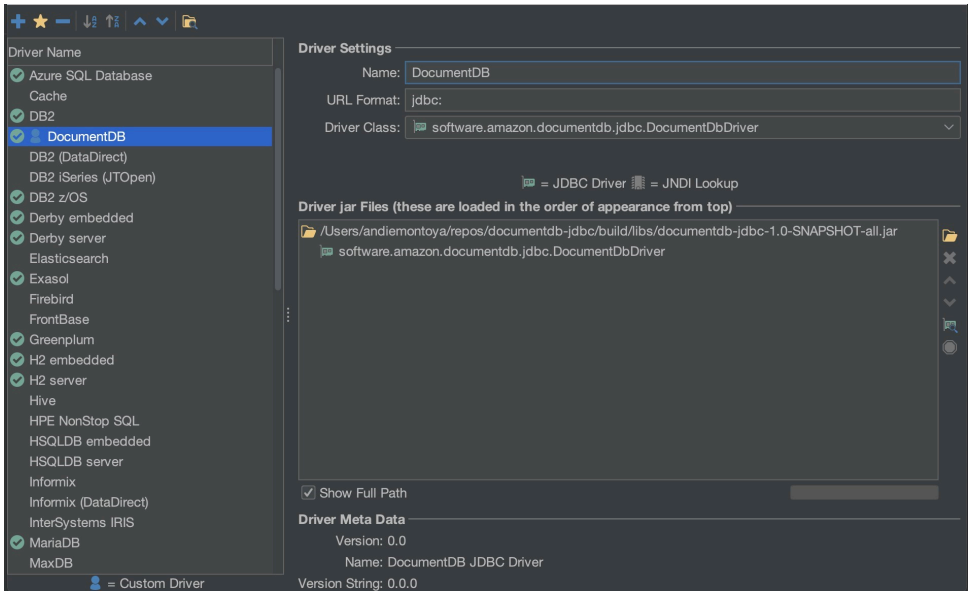
Themen

- Hinzufügen des Amazon DocumentDB DocumentDB-JDBC-Treibers
- Verbindung zu Amazon DocumentDB herstellen mit DbVisualizer

Hinzufügen des Amazon DocumentDB DocumentDB-JDBC-Treibers

Um eine Verbindung zu Amazon DocumentDB herzustellen, müssen DbVisualizer Sie zuerst den Amazon DocumentDB DocumentDB-JDBC-Treiber importieren.

1. Starten Sie die DbVisualizer Anwendung und navigieren Sie zum Menüpfad: Tools > Driver Manager...
2. Wählen Sie + (oder wählen Sie im Menü Treiber > Treiber erstellen).
3. Legen Sie Name auf `DocumentDB` fest.
4. Stellen Sie das URL-Format ein auf `jdbc:documentdb://<host>[:port]/<database>[?option=value[&option=value[...]]]`
5. Wählen Sie die Ordnerschaltfläche und dann die JAR-Datei des Amazon DocumentDB DocumentDB-JDBC-Treibers aus und klicken Sie auf die Schaltfläche Öffnen.
6. Stellen Sie sicher, dass das Feld Treiberklasse auf eingestellt ist. `software.amazon.documentdb.jdbc.DocumentDbDriver` Ihre Driver Manager-Einstellungen für DocumentDB sollten wie im folgenden Beispiel aussehen.



7. Schließen Sie das Dialogfeld. Der Amazon DocumentDB DocumentDB-JDBC-Treiber wird eingerichtet und ist einsatzbereit.

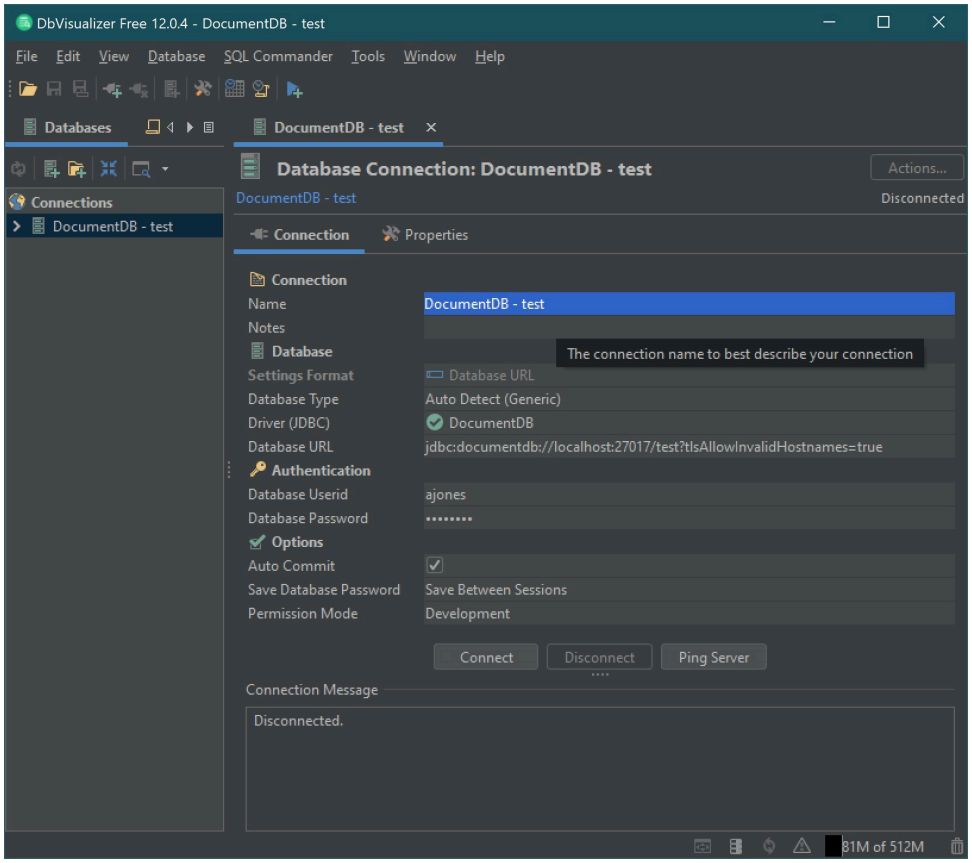
Verbindung zu Amazon DocumentDB herstellen mit DbVisualizer

Stellen Sie mithilfe von Amazon DocumentDB eine Connect DbVisualizer

1. Wenn Sie von außerhalb der VPC des Amazon DocumentDB-Clusters eine Verbindung herstellen, stellen Sie sicher, dass Sie einen SSH-Tunnel eingerichtet haben.
2. Wählen Sie im Menü der obersten Ebene Datenbank > Datenbankverbindung erstellen.
3. Geben Sie einen aussagekräftigen Namen für das Feld „Name“ ein.
4. Stellen Sie Driver (JDBC) auf den DocumentDB-Treiber ein, den Sie im vorherigen Abschnitt erstellt haben.
5. Stellen Sie die Datenbank-URL auf Ihre JDBC-Verbindungszeichenfolge ein.

   Beispiel: `jdbc:documentdb://localhost:27017/database?tlsAllowInvalidHostnames=true`
6. Setzen Sie Database Userid auf Ihre Amazon DocumentDB DocumentDB-Benutzer-ID.
7. Stellen Sie das Datenbankpasswort auf das entsprechende Passwort für die Benutzer-ID ein.

   Ihr Datenbankverbindungsdialog sollte wie der folgende Dialog aussehen:



8. Wählen Sie Connect aus.

Automatische JDBC-Schemagenerierung

Amazon DocumentDB ist eine Dokumentendatenbank und hat daher nicht das Konzept von Tabellen und Schemas. BI-Tools wie Tableau erwarten jedoch, dass die Datenbank, mit der sie eine Verbindung herstellen, ein Schema darstellt. Insbesondere wenn die JDBC-Treiberverbindung das Schema für die Sammlung in der Datenbank abrufen muss, fragt sie nach allen Sammlungen in der Datenbank ab. Der Treiber ermittelt, ob bereits eine zwischengespeicherte Version des Schemas für diese Sammlung vorhanden ist. Wenn keine zwischengespeicherte Version vorhanden ist, wird anhand der Sammlung nach Dokumenten gesucht und ein Schema erstellt, das auf dem folgenden Verhalten basiert.

Themen

- Einschränkungen bei der Schemagenerierung
- Optionen für die Scanmethode
- Amazon-DocumentDB-Datentypen

- Zuordnung skalarer Dokumentfelder
- Behandlung von Objekt- und Array-Datentypen

Einschränkungen bei der Schemagenerierung

Der DocumentDB-JDBC-Treiber begrenzt die Länge von Bezeichnern auf 128 Zeichen. Der Schema-Generator kann die Länge der generierten Bezeichner (Tabellennamen und Spaltennamen) kürzen, um sicherzustellen, dass sie dieser Grenze entsprechen.

Optionen für die Scanmethode

Das Sampling-Verhalten kann mithilfe von Verbindungszeichenfolgen- oder Datenquellenoptionen geändert werden.

- ScanMethod= <option>
  - random — (Standard) — Die Beispieldokumente werden in zufälliger Reihenfolge zurückgegeben.
  - idForward — Die Beispieldokumente werden in der Reihenfolge ihrer ID zurückgegeben.
  - idReverse — Die Beispieldokumente werden in umgekehrter Reihenfolge der ID zurückgegeben.
  - all — Alle Dokumente in der Sammlung werden als Stichprobe ausgewählt.
- scanLimit= <n>— Die Anzahl der Dokumente, die gesampelt werden sollen. Der Wert muss eine positive ganze Zahl sein. Der Standardwert ist 1000. Wenn ScanMethod auf all gesetzt ist, wird diese Option ignoriert.

Amazon-DocumentDB-Datentypen

Der Amazon DocumentDB-Server unterstützt eine Reihe von MongoDB-Datentypen. Im Folgenden sind die unterstützten Datentypen und die zugehörigen JDBC-Datentypen aufgeführt.

MongoDB-Datentyp	In DocumentDB unterstützt	JDBC-Datentyp
Binäre Daten	Ja	VARBINARY
Boolesch	Ja	BOOLEAN
Double	Ja	DOUBLE
32-Bit-Ganzzahl	Ja	INTEGER

MongoDB-Datentyp	In DocumentDB unterstützt	JDBC-Datentyp
64-Bit-Ganzzahl	Ja	BIGINT
Zeichenfolge	Ja	VARCHAR
ObjectId	Ja	VARCHAR
Date	Ja	TIMESTAMP (ZEITSTEMPEL)
Null	Ja	VARCHAR
Regulärer Ausdruck	Ja	VARCHAR
Zeitstempel	Ja	VARCHAR
MinKey	Ja	VARCHAR
MaxKey	Ja	VARCHAR
Objekt	Ja	virtuelle Tabelle
Array	Ja	virtueller Tisch
Decimal128	Nein	DECIMAL
JavaScript	Nein	VARCHAR
JavaScript (mit Umfang)	Nein	VARCHAR
Undefined	Nein	VARCHAR
Symbol	Nein	VARCHAR
dbPointer (4.0+)	Nein	VARCHAR

Zuordnung skalarer Dokumentfelder

Beim Scannen einer Stichprobe von Dokumenten aus einer Sammlung erstellt der JDBC-Treiber ein oder mehrere Schemas, um die Beispiele in der Sammlung darzustellen. Im Allgemeinen wird ein Skalarfeld im Dokument einer Spalte im Tabellenschema zugeordnet. In einer Sammlung mit dem

Namen Team und einem einzelnen Dokument würde dies `{ "_id" : "112233", "name" : "Alastair", "age": 25 }` beispielsweise dem Schema entsprechen:

Tabellenname	Spaltenname	Datentyp	Key (Schlüssel)
Team	Team-ID	VARCHAR	PK
Team	Name	VARCHAR	
Team	age	INTEGER	

Förderung von Datentypkonflikten

Beim Scannen der Musterdokumente ist es möglich, dass die Datentypen für ein Feld von Dokument zu Dokument nicht einheitlich sind. In diesem Fall stuft der JDBC-Treiber den JDBC-Datentyp auf einen gemeinsamen Datentyp herauf, der für alle Datentypen aus den Stichprobendokumenten geeignet ist.

Zum Beispiel:

```
{
"_id" : "112233",
"name" : "Alastair", "age" : 25
}

{
"_id" : "112244",
"name" : "Benjamin",
"age" : "32"
}
```

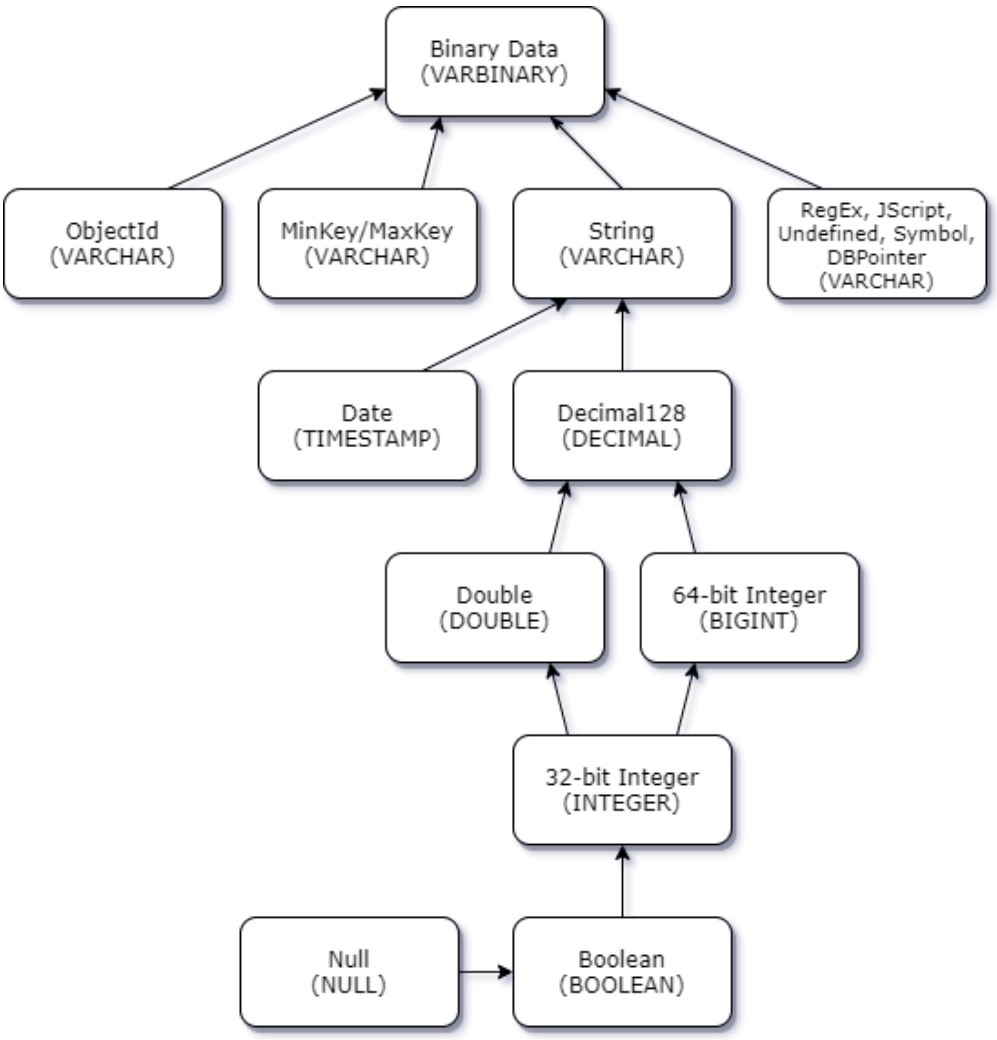
Das Altersfeld ist im ersten Dokument vom Typ 32-Bit-Ganzzahl, im zweiten Dokument vom Typ Zeichenfolge. In diesem Fall wird der JDBC-Treiber den JDBC-Datentyp auf VARCHAR heraufstufen, um einen der beiden Datentypen zu verarbeiten, wenn er angetroffen wird.

Tabellenname	Spaltenname	Datentyp	Key (Schlüssel)
Team	Team-ID	VARCHAR	PK

Tabellenname	Spaltenname	Datentyp	Key (Schlüssel)
Team	Name	VARCHAR	
Team	age	VARCHAR	

Scalar-scalar Förderung von Konflikten

Das folgende Diagramm zeigt, wie Konflikte zwischen skalaren und skalaren Datentypen gelöst werden.



Scalar-complex Geben Sie Konfliktförderung ein

Wie bei Skalar-Skalar-Typkonflikten kann dasselbe Feld in verschiedenen Dokumenten widersprüchliche Datentypen zwischen komplexen (Array und Objekt) und skalaren Datentypen

(Integer, Boolean usw.) aufweisen. All diese Konflikte werden für diese Felder in VARCHAR aufgelöst (heraufgestuft). In diesem Fall werden Array- und Objektdaten als JSON-Darstellung zurückgegeben.

Beispiel für einen Konflikt zwischen eingebettetem Array und Zeichenkettenfeld:

```
{
   "_id":"112233",
   "name":"George Jackson",
   "subscriptions":[
      "Vogue",
      "People",
      "USA Today"
   ]
}
{
   "_id":"112244",
   "name":"Joan Starr",
   "subscriptions":1
}
```

Das vorherige Beispiel ist dem Schema für die Tabelle customer2 zugeordnet:

Tabellenname	Spaltenname	Datentyp	Key (Schlüssel)
Kunde2	Kunde2-ID	VARCHAR	PK
Kunde2	Name	VARCHAR	
Kunde2	Abonnement	VARCHAR	

und die virtuelle Tabelle customer1_subscriptions:

Tabellenname	Spaltenname	Datentyp	Key (Schlüssel)
customer1_subscriptions	Kunden1-ID	VARCHAR	PK/FK
customer1_subscriptions	subscriptions_index_lvl0	BIGINT	PK

Tabellenname	Spaltenname	Datentyp	Key (Schlüssel)
customer1_abonnements	value	VARCHAR	
customer_address	city	VARCHAR	
customer_address	Region	VARCHAR	
customer_address	country	VARCHAR	
customer_address	Code	VARCHAR	

Behandlung von Objekt- und Array-Datentypen

Bisher haben wir nur beschrieben, wie skalare Datentypen zugeordnet werden. Objekt- und Array-Datentypen werden (derzeit) virtuellen Tabellen zugeordnet. Der JDBC-Treiber erstellt eine virtuelle Tabelle, die entweder Objekt- oder Array-Felder in einem Dokument darstellt. Der Name der zugewiesenen virtuellen Tabelle verkettet den Namen der ursprünglichen Sammlung, gefolgt vom Feldnamen, getrennt durch einen Unterstrich („_“).

Der Primärschlüssel der Basistabelle („_id“) nimmt in der neuen virtuellen Tabelle einen neuen Namen an und wird als Fremdschlüssel für die zugehörige Basistabelle bereitgestellt.

Für Felder vom Typ eingebettetes Array werden Indexspalten generiert, um den Index im Array auf jeder Ebene des Arrays darzustellen.

Beispiel für ein eingebettetes Objektfeld

Für Objektfelder in einem Dokument wird vom JDBC-Treiber eine Zuordnung zu einer virtuellen Tabelle erstellt.

```
{
   "Collection: customer",
   "_id":"112233",
   "name":"George Jackson",
   "address":{
      "address1":"123 Avenue Way",
      "address2":"Apt. 5",
      "city":"Hollywood",
```

```
      "region":"California",
      "country":"USA",
      "code":"90210"
   }
}
```

Das vorherige Beispiel ist dem Schema für die Kundentabelle zugeordnet:

Tabellenname	Spaltenname	Datentyp	Key (Schlüssel)
customer	Kunden-ID	VARCHAR	PK
customer	Name	VARCHAR	

und die virtuelle Tabelle customer_address:

Tabellenname	Spaltenname	Datentyp	Key (Schlüssel)
customer_address	Kunden-ID	VARCHAR	PK/FK
customer_address	Adresse 1	VARCHAR	
customer_address	Adresse2	VARCHAR	
customer_address	city	VARCHAR	
customer_address	Region	VARCHAR	
customer_address	country	VARCHAR	
customer_address	Code	VARCHAR	

Beispiel für ein eingebettetes Array-Feld

Für Array-Felder in einem Dokument wird vom JDBC-Treiber auch eine Zuordnung zu einer virtuellen Tabelle erstellt.

```
{
   "Collection: customer1",
```

```
   "_id":"112233",
   "name":"George Jackson",
   "subscriptions":[
      "Vogue",
      "People",
      "USA Today"
   ]
}
```

Das vorherige Beispiel ist dem Schema für die Tabelle customer1 zugeordnet:

Tabellenname	Spaltenname	Datentyp	Key (Schlüssel)
Kunde1	Kunde1-ID	VARCHAR	PK
Kunde1	Name	VARCHAR	

und die virtuelle Tabelle customer1_subscriptions:

Tabellenname	Spaltenname	Datentyp	Key (Schlüssel)
customer1_subscriptions	Kunden1-ID	VARCHAR	PK/FK
customer1_subscriptions	subscriptions_index_lvl0	BIGINT	PK
customer1_abonnements	value	VARCHAR	
customer_address	city	VARCHAR	
customer_address	Region	VARCHAR	
customer_address	country	VARCHAR	
customer_address	Code	VARCHAR	

SQL-Unterstützung und Einschränkungen

Der Amazon DocumentDB JDBC-Treiber ist ein schreibgeschützter Treiber, der eine Teilmenge und einige gängige Erweiterungen unterstützt. SQL-92 Weitere Informationen finden Sie in der Dokumentation zu den SQL-Einschränkungen und in der Dokumentation zu den JDBC-Einschränkungen.

Fehlerbehebung

Wenn Sie Probleme mit der Verwendung des Amazon DocumentDB DocumentDB-JDBC-Treibers haben, finden Sie weitere Informationen im Leitfaden zur Fehlerbehebung.

Stellen Sie mithilfe des Amazon DocumentDB DocumentDB-ODBC-Treibers eine Verbindung her

Der ODBC-Treiber für Amazon DocumentDB bietet eine SQL-relational Schnittstelle für Entwickler und ermöglicht die Konnektivität von BI-Tools wie Power BI Desktop und Microsoft Excel.

Weitere Informationen finden Sie in der Amazon DocumentDB ODBC-Treiber-Dokumentation unter. GitHub

Topics

- Erste Schritte
- Den Amazon DocumentDB ODBC-Treiber in Windows einrichten
- Stellen Sie von Microsoft Excel aus eine Connect zu Amazon DocumentDB her
- Stellen Sie von Microsoft Power BI Desktop aus eine Connect zu Amazon DocumentDB her
- Automatische Schemagenerierung
- SQL-Unterstützung und Einschränkungen
- Fehlerbehebung

Erste Schritte

Schritt 1. Amazon DocumentDB-Cluster erstellen

> Wenn Sie noch keinen Amazon DocumentDB-Cluster haben, gibt es eine Reihe von Möglichkeiten, um loszulegen.

> **Note**
>
> Amazon DocumentDB ist ein Dienst, der nur für Virtual Private Cloud (VPC) verfügbar ist. Wenn Sie eine Verbindung von einem lokalen Computer außerhalb der VPC des Clusters herstellen, müssen Sie eine SSH-Verbindung zu einer Amazon EC2 EC2-Instance herstellen. Starten Sie in diesem Fall Ihren Cluster anhand der Anweisungen unter Connect with EC2. Weitere Informationen zum SSH-Tunneling und wann Sie es möglicherweise benötigen, finden Sie unter Verwenden eines SSH-Tunnels zum Herstellen einer Connect zu Amazon DocumentDB.

Schritt 2. JRE- oder JDK-Installation

Abhängig von Ihrer BI-Anwendung müssen Sie möglicherweise sicherstellen, dass eine 64-Bit-JRE- oder JDK-Installationsversion 8 oder höher auf Ihrem Computer installiert ist. Sie können das Java SE Runtime Environment 8 hier herunterladen.

Schritt 3. Laden Sie den Amazon DocumentDB ODBC-Treiber herunter

Laden Sie den Amazon DocumentDB ODBC-Treiber hier herunter. Wählen Sie das richtige Installationsprogramm (z. B. documentdb-odbc-1.0.0.msi). Folgen Sie der Installationsanleitung.

Schritt 4. Verwenden eines SSH-Tunnels für die Connect Amazon DocumentDB

Amazon DocumentDB-Cluster werden in einer Amazon Virtual Private Cloud (Amazon VPC) bereitgestellt. Auf sie kann direkt von Amazon EC2 EC2-Instances oder anderen AWS Services zugegriffen werden, die in derselben Amazon VPC bereitgestellt werden. Darüber hinaus können Amazon EC2 EC2-Instances oder andere AWS Services in verschiedenen VPCs in derselben AWS Region oder anderen Regionen über VPC-Peering auf Amazon DocumentDB zugreifen.

Nehmen wir jedoch an, dass Ihr Anwendungsfall erfordert, dass Sie (oder Ihre Anwendung) von außerhalb der VPC des Clusters auf Ihre Amazon DocumentDB DocumentDB-Ressourcen zugreifen. Dies wird bei den meisten Benutzern der Fall sein, die ihre Anwendung nicht auf einer VM in derselben VPC wie der Amazon DocumentDB-Cluster ausführen. Wenn Sie eine Verbindung von außerhalb der VPC herstellen, können Sie SSH-Tunneling (auch als Portweiterleitung bezeichnet) verwenden, um auf Ihre Amazon DocumentDB DocumentDB-Ressourcen zuzugreifen.

Um einen SSH-Tunnel zu erstellen, benötigen Sie eine Amazon EC2 EC2-Instance, die in derselben Amazon VPC wie Ihr Amazon DocumentDB-Cluster läuft. Sie können entweder eine

vorhandene EC2-Instance in derselben VPC wie Ihr Cluster verwenden oder eine erstellen. Sie können einen SSH-Tunnel zum Amazon DocumentDB-Cluster einrichten, `sample-cluster.node.us-east-1.docdb.amazonaws.com` indem Sie den folgenden Befehl auf Ihrem lokalen Computer ausführen:

```
ssh -i "ec2Access.pem" -L 27017:sample-cluster.node.us-
east-1.docdb.amazonaws.com:27017 ubuntu@ec2-34-229-221-164.compute-1.amazonaws.com -
N
```

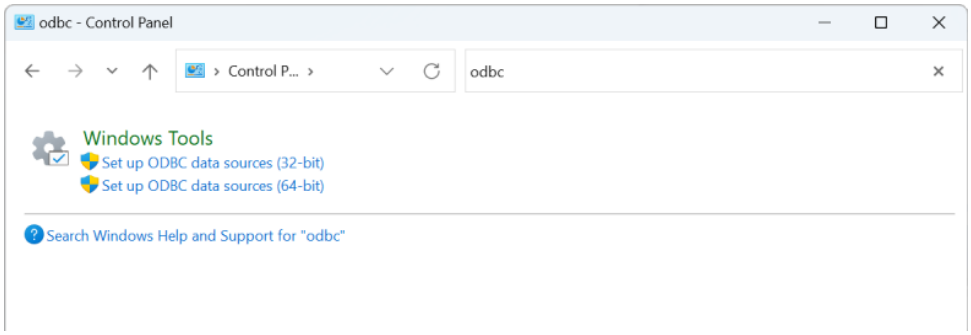
Das `-L`-Flag dient zur Weiterleitung eines lokalen Ports. Dies ist eine Voraussetzung für die Verbindung zu einem BI-Tool, das auf einem Client außerhalb Ihrer VPC ausgeführt wird. Sobald Sie den obigen Schritt ausgeführt haben, können Sie mit den nächsten Schritten für das BI-Tool Ihrer Wahl fortfahren.

Weitere Informationen zum SSH-Tunneling finden Sie in der Dokumentation Using an SSH Tunnel to Connect to Amazon DocumentDB.

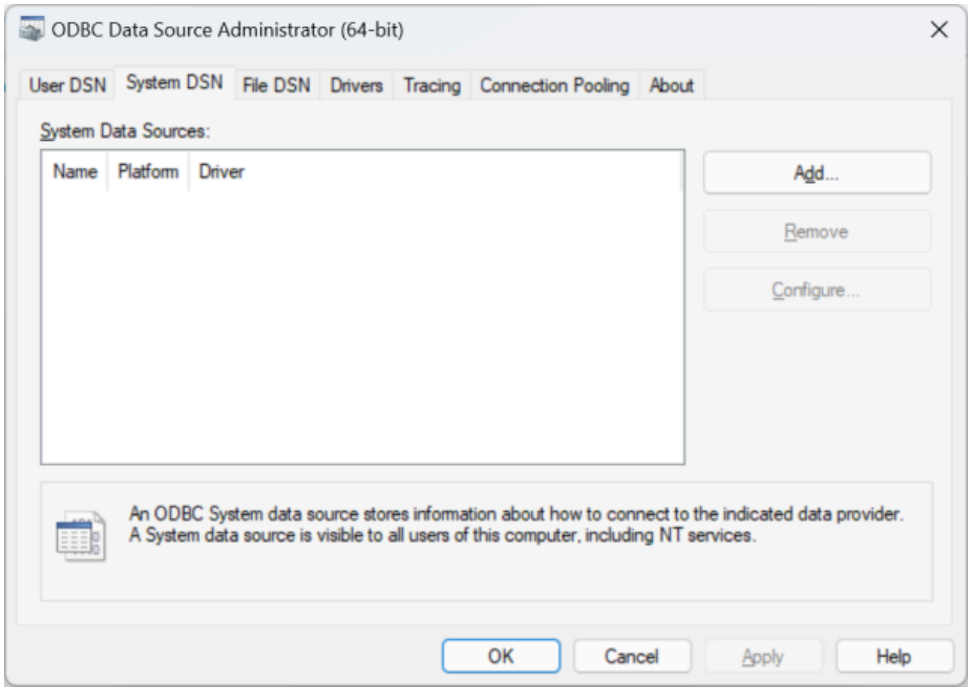
Den Amazon DocumentDB ODBC-Treiber in Windows einrichten

Gehen Sie wie folgt vor, um den Amazon DocumentDB DocumentDB-ODBC-Treiber in Windows einzurichten:

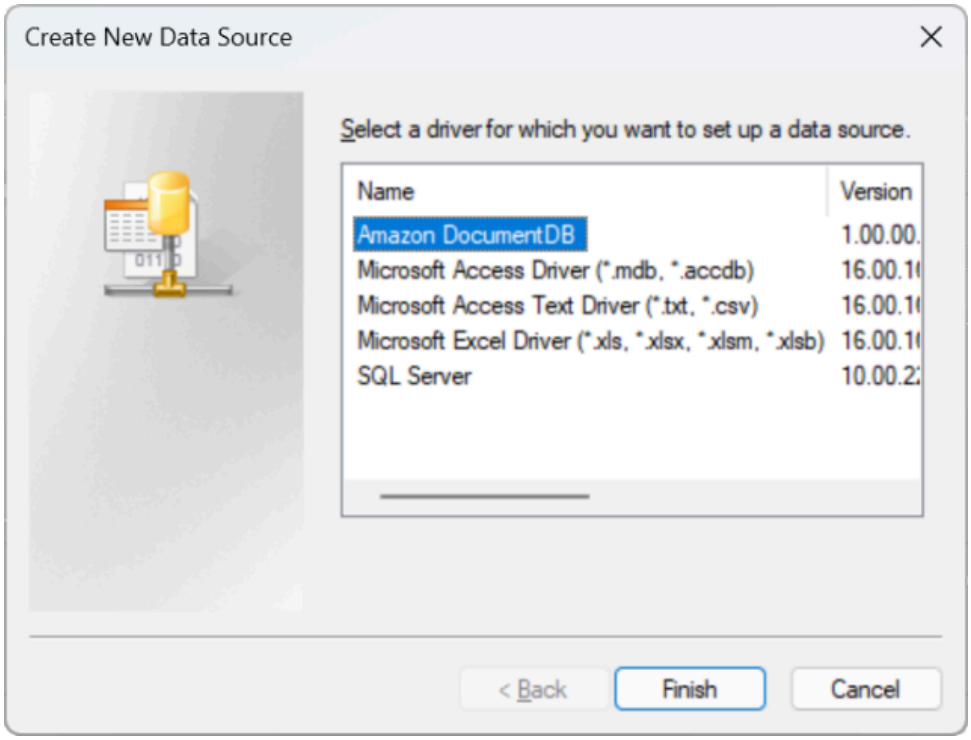
1. Öffnen Sie die Systemsteuerung in Windows und suchen Sie nach ODBC (oder wählen Sie im Menü Windows-Tools > ODBC-Datenquellen (32-Bit) oder ODBC-Datenquellen (64-Bit)):



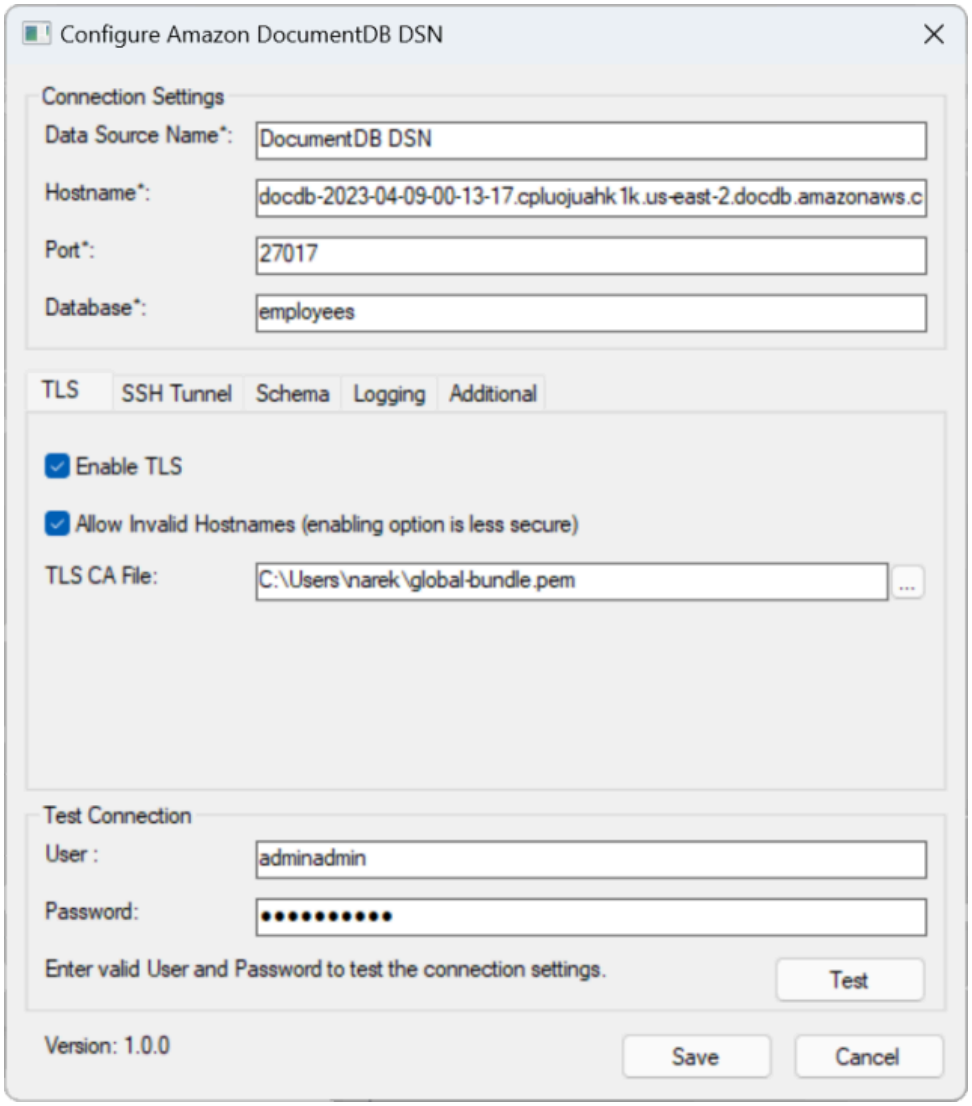
2. Wählen Sie den entsprechenden ODBC-Treiber-Datenquellenadministrator aus: Wählen Sie die 32-Bit-Version, falls diese installiert ist, andernfalls wählen Sie die 64-Bit-Version.
3. Wählen Sie die Registerkarte System-DSN und dann Hinzufügen... um einen neuen DSN hinzuzufügen:



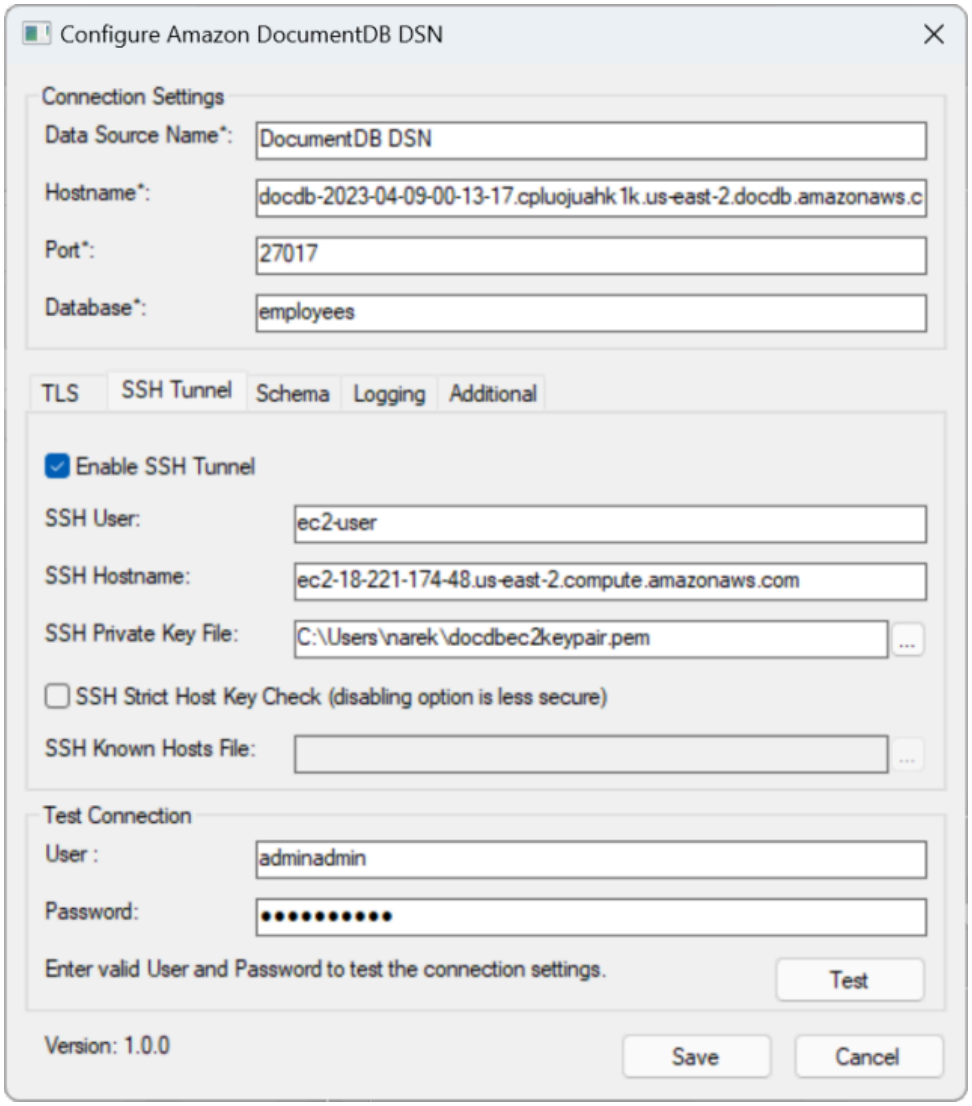
4. Wählen Sie Amazon DocumentDB aus der Liste der Datenquellentreiber aus:



5. Füllen Sie im Dialogfeld Amazon DocumentDB DSN konfigurieren die Felder Verbindungseinstellungen, Registerkarte TLS und Verbindung testen aus und wählen Sie dann Speichern:



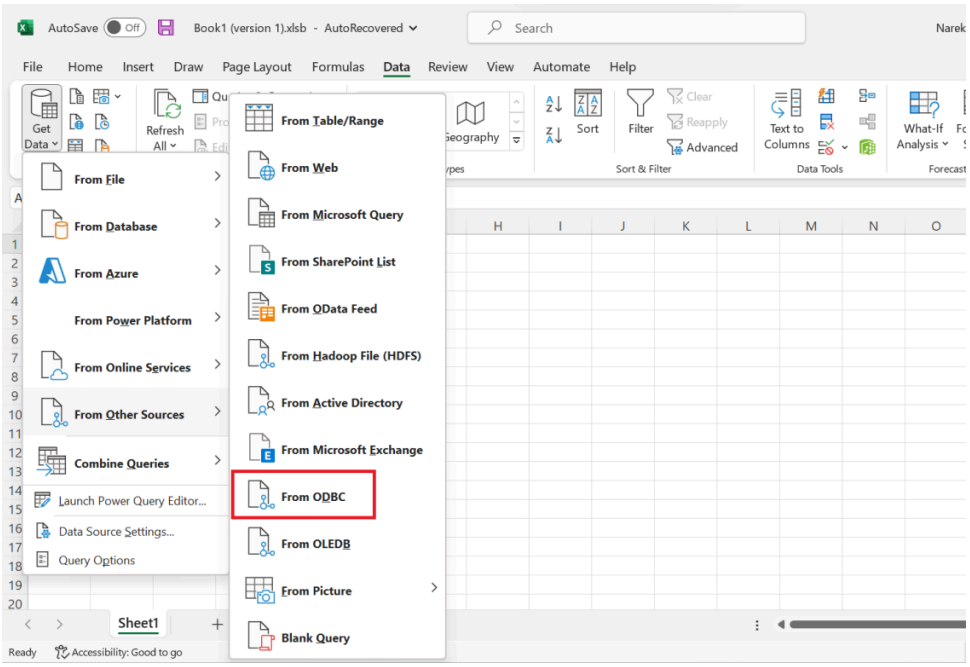
6. Stellen Sie sicher, dass Sie das Windows-Formular korrekt ausfüllen, da die Verbindungsdetails je nach der von Ihnen gewählten SSH-Tunneling-Methode zur EC2-Instance unterschiedlich sein können. Informationen zu SSH-Tunneling-Methoden finden Sie hier. Weitere Informationen zu den einzelnen Eigenschaften finden Sie unter Syntax und Optionen für Verbindungszeichenfolgen.



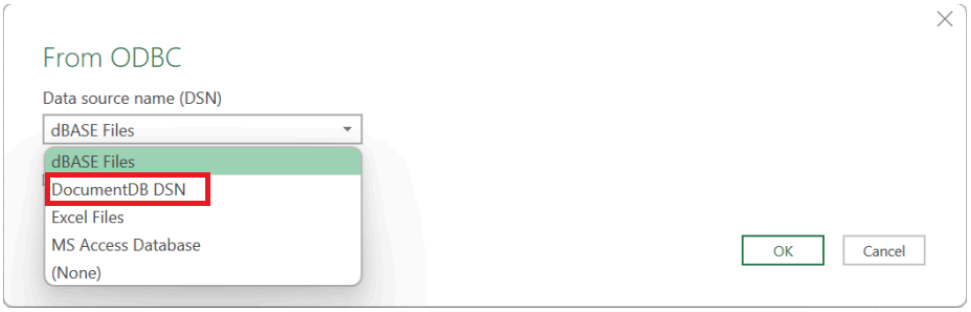
Weitere Informationen zur Konfiguration des Amazon DocumentDB DocumentDB-ODBC-Treibers unter Windows finden Sie hier.

Stellen Sie von Microsoft Excel aus eine Connect zu Amazon DocumentDB her

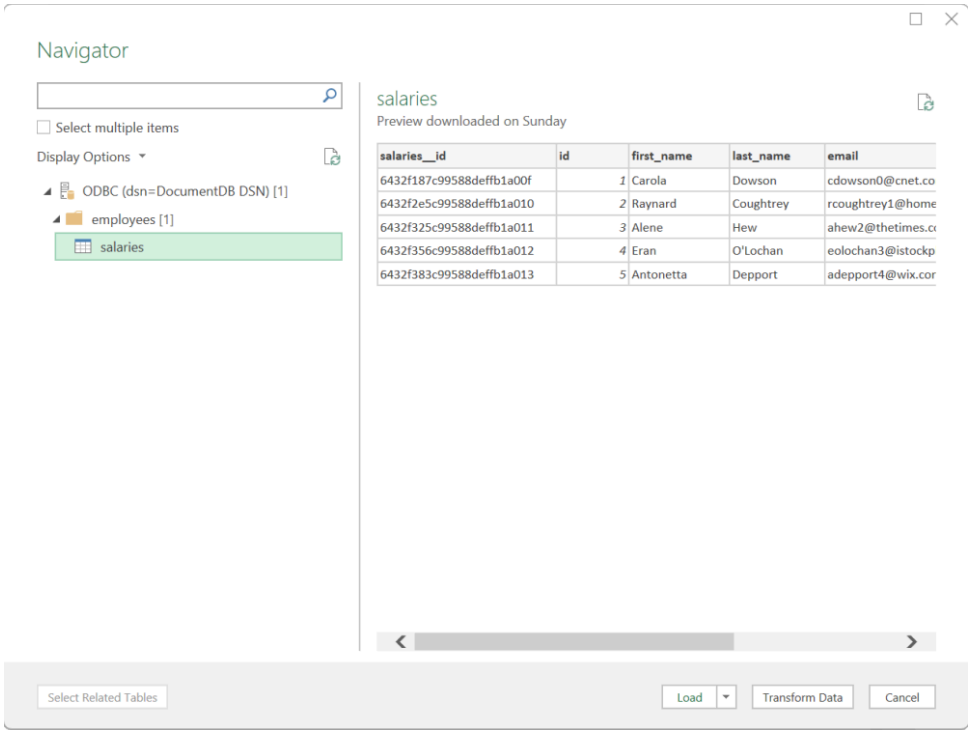
1. Stellen Sie sicher, dass der Amazon DocumentDB-Treiber korrekt installiert und konfiguriert wurde. Weitere Informationen finden Sie unter Einrichten des ODBC-Treibers in Windows.
2. Starten Sie Microsoft Excel.
3. Navigieren Sie zu Daten > Daten abrufen > Aus anderen Quellen.
4. Wählen Sie „Aus ODBC“:



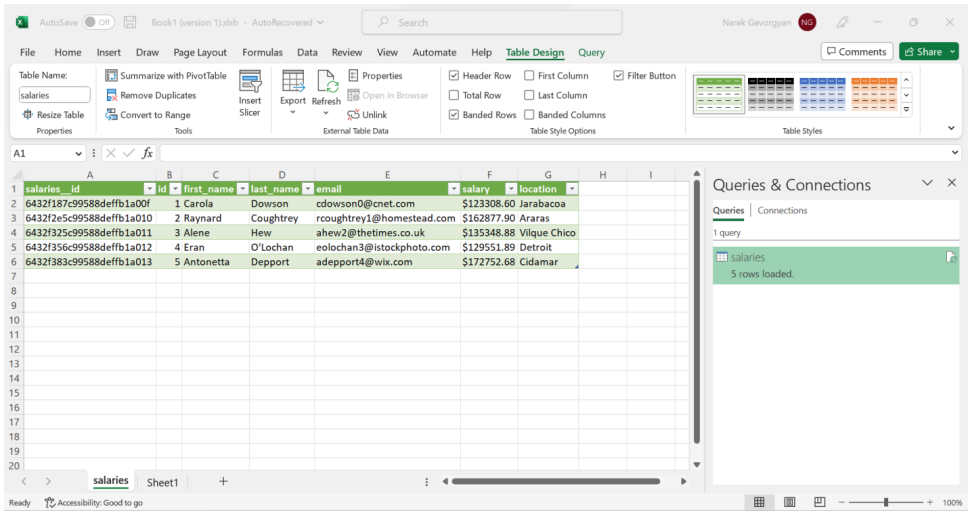
5. Wählen Sie im Dropdownmenü Datenquellenname (DSN) die Datenquelle aus, die Amazon DocumentDB zugeordnet ist:



6. Wählen Sie die Sammlung aus, aus der Sie Daten in Excel laden möchten:



7. Daten in Excel laden:



Stellen Sie von Microsoft Power BI Desktop aus eine Connect zu Amazon DocumentDB her

Topics

- Voraussetzungen
- Benutzerdefinierter Microsoft Power BI Desktop-Connector hinzufügen
- Verbindung mit dem benutzerdefinierten Amazon DocumentDB DocumentDB-Konnektor herstellen

- Konfiguration von Microsoft Power BI Gateway

Voraussetzungen

Bevor Sie beginnen, stellen Sie sicher, dass der Amazon DocumentDB ODBC-Treiber korrekt installiert ist.

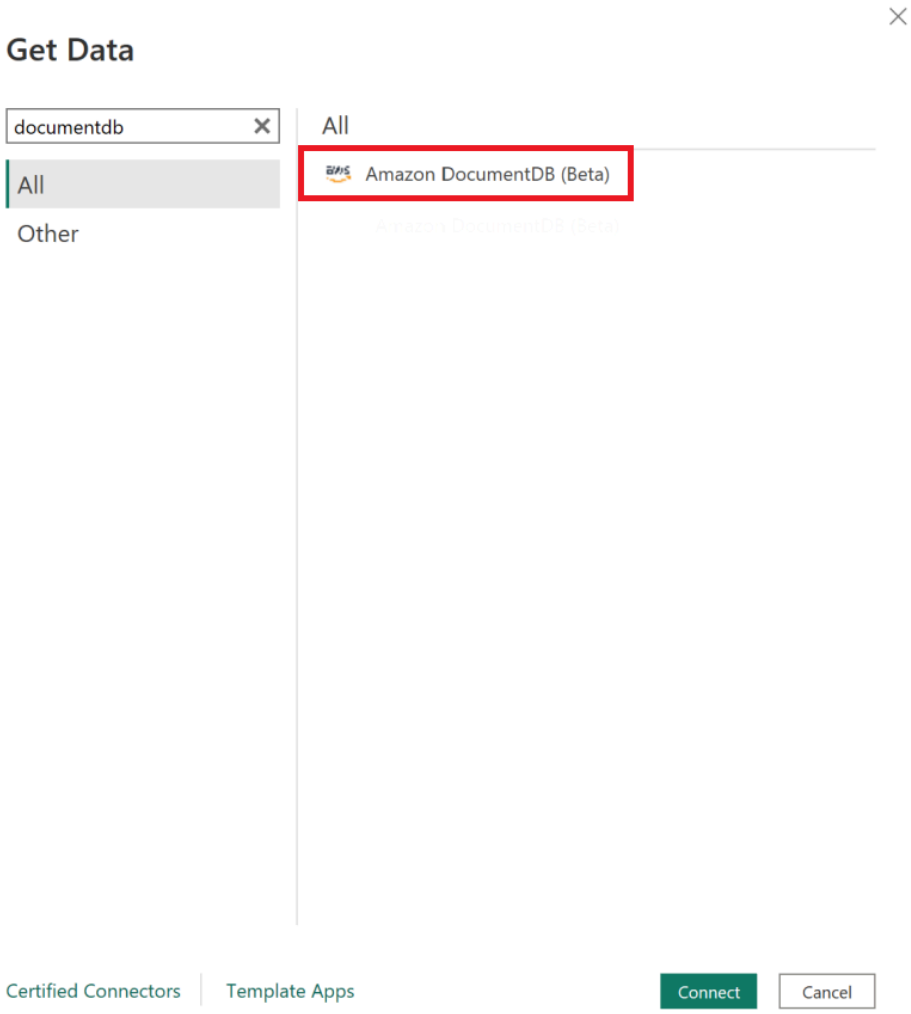
Benutzerdefinierter Microsoft Power BI Desktop-Connector hinzufügen

Kopieren Sie die `AmazonDocumentDBConnector.mez` Datei in den `<User>\Documents\Power BI Desktop\Custom Connectors\` Ordner (oder in den Ordner, `<User>\OneDrive\Documents\Power BI Desktop\Custom Connectors` falls Sie ihn verwenden OneDrive). Dadurch kann Power BI auf den benutzerdefinierten Connector zugreifen. Den Connector für Power BI Desktop erhalten Sie hier. Starten Sie Power BI Desktop neu, um sicherzustellen, dass der Connector geladen ist.

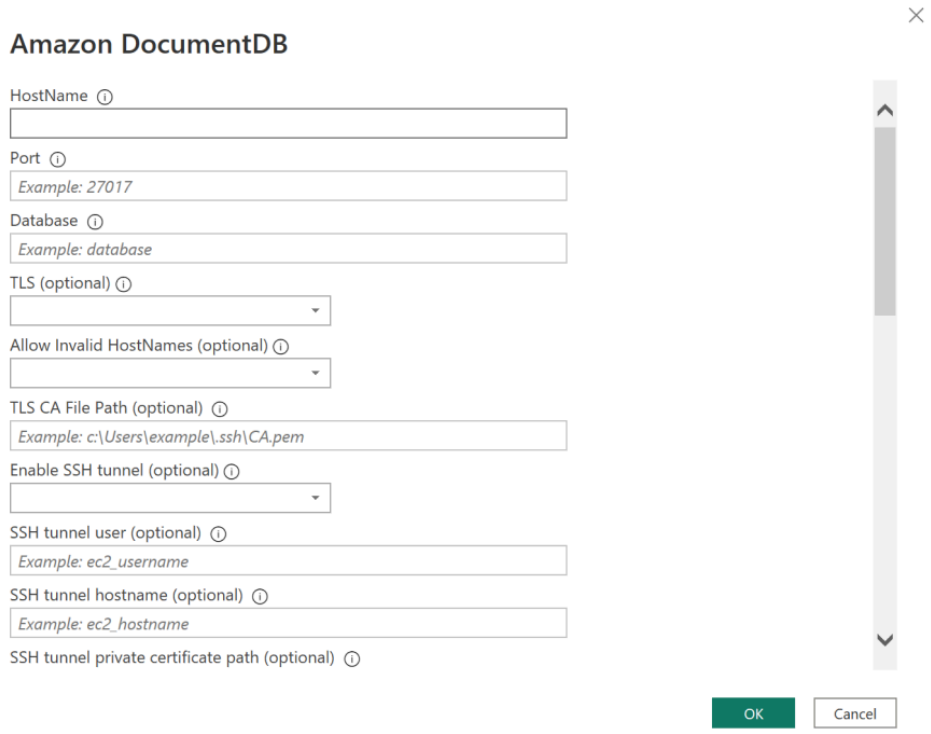
> **Note**
>
> Der benutzerdefinierte Connector unterstützt nur Amazon DocumentDB DocumentDB-Benutzernamen und -Passwort für die Authentifizierung.

Verbindung mit dem benutzerdefinierten Amazon DocumentDB DocumentDB-Konnektor herstellen

1. Wählen Sie Amazon DocumentDB (Beta) aus Get Data und dann Connect aus. Wenn Sie wegen der Nutzung eines Drittanbieterdienstes eine Warnung erhalten, wählen Sie Weiter.



2. Geben Sie alle erforderlichen Informationen ein, um eine Verbindung zu Ihrem Amazon DocumentDB-Cluster herzustellen, und wählen Sie dann OK:



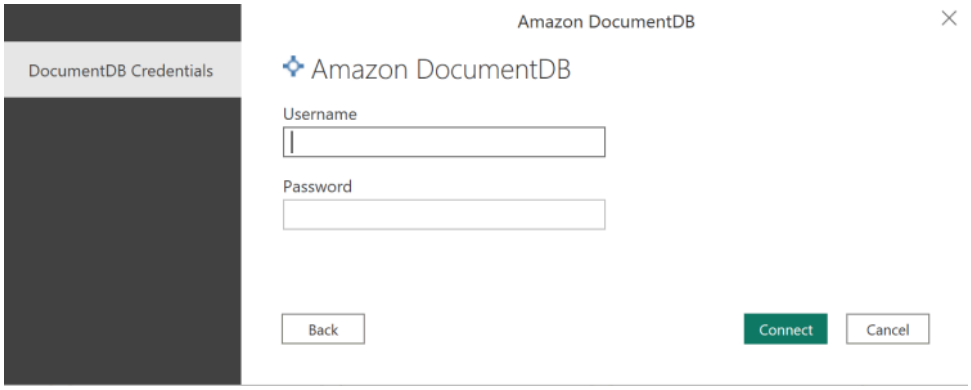
> **Note**
>
> Abhängig von der Konfiguration des Datenquellennamens (DSN) Ihres ODBC-Treibers wird der Bildschirm mit den SSH-Verbindungsdetails möglicherweise nicht angezeigt, wenn Sie die erforderlichen Informationen bereits in den DSN-Einstellungen angegeben haben.

3. Wählen Sie den Datenverbindungsmodus:

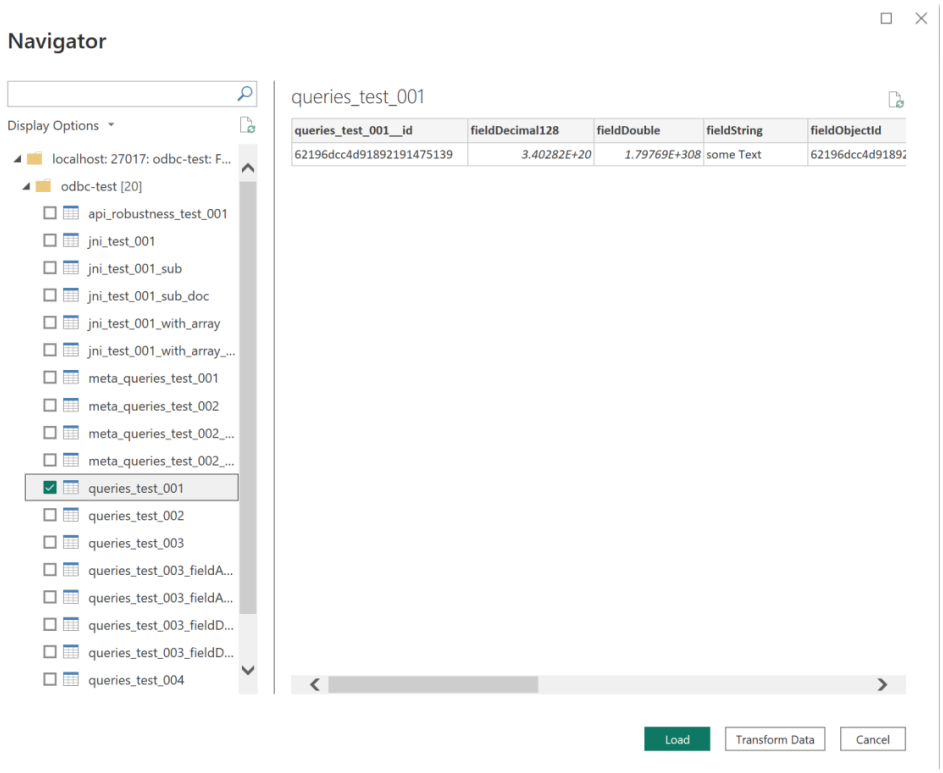
   - Import - lädt alle Daten und speichert die Informationen auf der Festplatte. Die Daten müssen aktualisiert und neu geladen werden, damit Datenaktualisierungen angezeigt werden.
   - Direkte Abfrage — lädt keine Daten, sondern führt Live-Abfragen der Daten durch. Das bedeutet, dass Daten nicht aktualisiert und neu geladen werden müssen, um Datenaktualisierungen anzuzeigen.

> **Note**
>
> Wenn Sie einen sehr großen Datensatz verwenden, kann der Import aller Daten einen längeren Zeitraum in Anspruch nehmen.

4. Wenn Sie zum ersten Mal eine Verbindung zu dieser Datenquelle herstellen, wählen Sie den Authentifizierungstyp aus und geben Sie Ihre Anmeldeinformationen ein, wenn Sie dazu aufgefordert werden. Wählen Sie dann Connect:



5. Wählen Sie im Navigator-Dialogfeld die gewünschten Datenbanktabellen aus und wählen Sie dann entweder Laden, um die Daten zu laden, oder Daten transformieren, um mit der Transformation der Daten fortzufahren.



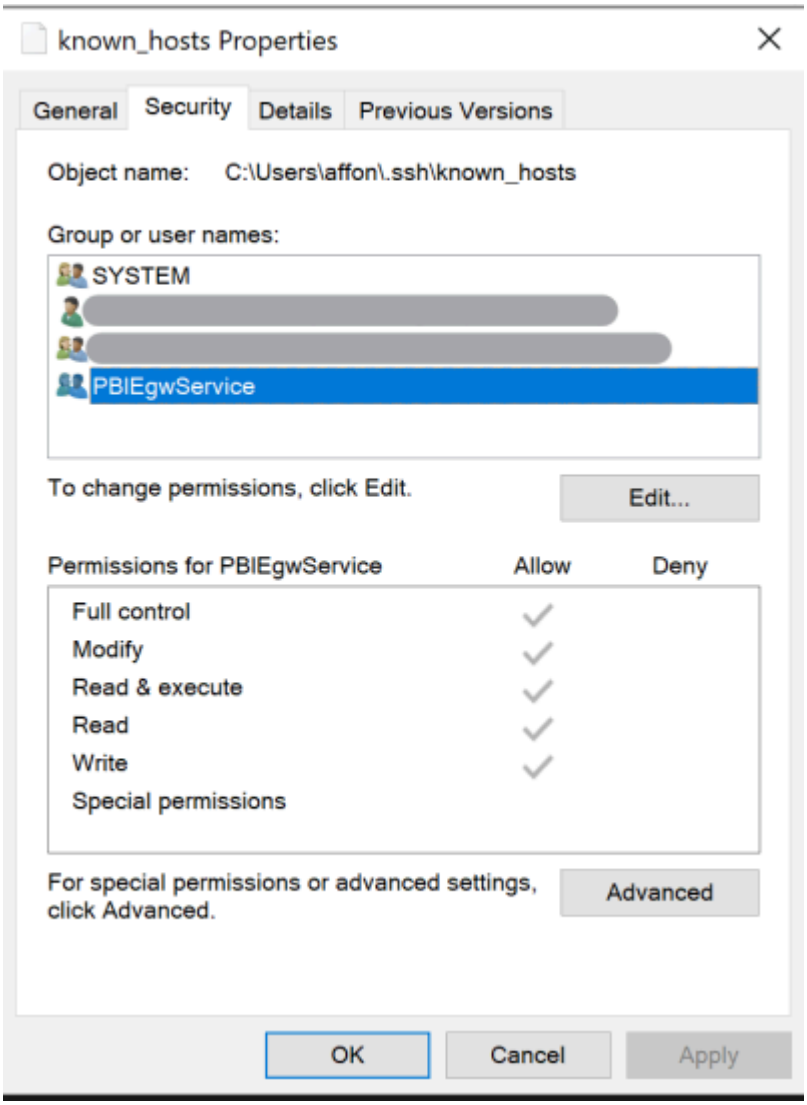
> **Note**
>
> Ihre Datenquelleneinstellungen werden gespeichert, sobald Sie eine Verbindung hergestellt haben. Um sie zu ändern, wählen Sie Daten transformieren > Datenquelleneinstellungen.

Konfiguration von Microsoft Power BI Gateway

Voraussetzungen:

- Stellen Sie sicher, dass der benutzerdefinierte Connector mit Power BI Gateway funktioniert.
- Stellen Sie sicher, dass der ODBC-DSN in den ODBC-Datenquellen auf der Registerkarte System auf dem Computer erstellt wurde, auf dem Power BI Gateway installiert ist.

Wenn Sie die interne SSH-Tunnelfunktion verwenden, `known_hosts` muss sich die Datei dort befinden, wo das Power BI-Dienstkonto Zugriff darauf hat.



> **Note**
>
> Dies gilt auch für alle Dateien, die Sie möglicherweise benötigen, um eine Verbindung zu Ihrem Amazon DocumentDB-Cluster herstellen zu können, z. B. eine Zertifizierungsstelle (CA) -Zertifikatsdatei (PEM-Datei).

Automatische Schemagenerierung

Der ODBC-Treiber verwendet den Amazon DocumentDB DocumentDB-JDBC-Treiber über JNI (Java Native Interface), sodass die automatische Schemagenerierung im JDBC-Treiber ähnlich funktioniert. Weitere Informationen zur automatischen Schemagenerierung finden Sie unter Automatische JDBC-Schemagenerierung. Weitere Informationen zur ODBC-Treiberarchitektur finden Sie hier.

SQL-Unterstützung und Einschränkungen

Der Amazon DocumentDB ODBC-Treiber ist ein schreibgeschützter Treiber, der eine Teilmenge SQL-92 und einige gängige Erweiterungen unterstützt. Weitere Informationen finden Sie in der Dokumentation zu ODBC-Support und Einschränkungen.

Fehlerbehebung

Wenn Sie Probleme mit der Verwendung des Amazon DocumentDB DocumentDB-ODBC-Treibers haben, finden Sie weitere Informationen im Leitfaden zur Fehlerbehebung.

Programm mit Amazon DocumentDB

Der Dienst unterstützt die JSON-Schemavalidierung.

Themen

- Amazon DocumentDB Java-Programmierhandbuch
- Verwenden der JSON-Schemavalidierung

Amazon DocumentDB Java-Programmierhandbuch

Dieses umfassende Handbuch bietet eine detaillierte Anleitung zur Arbeit mit Amazon DocumentDB unter Verwendung der Java-Treiber von MongoDB und behandelt wichtige Aspekte des Datenbankbetriebs und der Datenbankverwaltung.

Themen

- Einführung
- Voraussetzungen
- Datenmodelle für diesen Leitfaden
- Mit einem MongoDB-Java-Treiber eine Verbindung zu Amazon DocumentDB herstellen
- Durchführen von CRUD-Vorgängen in Amazon DocumentDB mit Java
- Indexverwaltung in Amazon DocumentDB mit Java
- Event-driven Programmieren mit Amazon DocumentDB und Java

Einführung

Das Handbuch beginnt mit der Konnektivität und erklärt, wie sichere Verbindungen zu DocumentDB-Clustern mithilfe des MongoDB-Java-Treibers hergestellt werden. Es beschreibt die Komponenten der Verbindungszeichenfolge, die SSL/TLS Implementierung und die verschiedenen Verbindungsoptionen, einschließlich IAM-Authentifizierung und Verbindungspooling, sowie robuste Strategien zur Fehlerbehandlung.

Im Abschnitt CRUD-Operationen (Create, Read, Update, Delete) behandelt das Handbuch ausführlich die Bearbeitung von Dokumenten und zeigt, wie Dokumente sowohl mit Einzel- als auch mit Massenoperationen erstellt, gelesen, aktualisiert und gelöscht werden. Es erklärt die Verwendung von Filtern, Abfragen und verschiedenen Operationsoptionen und betont gleichzeitig bewährte Methoden für die Fehlerbehandlung und die Implementierung von Wiederholungslogik zur Erhöhung der Zuverlässigkeit. Der Leitfaden befasst sich auch ausführlich mit der Indexverwaltung und beschreibt detailliert die Erstellung und Verwaltung verschiedener Indextypen, darunter Einzelfeld-, zusammengesetzte Indizes, Sparse-Indizes und Textindizes. Es wird erklärt, wie die Abfrageleistung durch die richtige Indexauswahl und die Verwendung der `explain()` Funktion zur Analyse von Abfrageausführungsplänen optimiert werden kann.

Der letzte Abschnitt konzentriert sich auf ereignisgesteuertes Programmieren mithilfe der Change-Streams von Amazon DocumentDB und zeigt, wie die Überwachung von Datenänderungen in Echtzeit in Java-Anwendungen implementiert werden kann. Er behandelt die Implementierung von Change-Stream-Cursors, den Umgang mit Resume-Token für den kontinuierlichen Betrieb und zeitbasierte Operationen für die Verarbeitung historischer Daten. Der gesamte Leitfaden enthält praktische Codebeispiele und bewährte Methoden, was ihn zu einer unschätzbaren Ressource für Sie macht, wenn Sie robuste Java-Anwendungen mit Amazon DocumentDB erstellen möchten.

Voraussetzungen

Stellen Sie vor dem Beginn sicher, dass Sie über das Folgende verfügen:

- Ein AWS Konto mit einem konfigurierten DocumentDB-Cluster. Informationen zur Einrichtung eines DocumentDB-Clusters finden Sie in diesem Blogbeitrag „Erste Schritte“.
- Java Development Kit (JDK) installiert (wir werden Amazon Corretto 21 für dieses Handbuch verwenden).
- Maven für das Abhängigkeitsmanagement.

Datenmodelle für diesen Leitfaden

Der gesamte Beispielcode in diesem Handbuch geht von einer Verbindung zu einer Testdatenbank „ProgGuideData“ aus, die eine Sammlung „Restaurants“ enthält. Alle Beispielcodes in diesem Handbuch funktionieren auf einem Restauranteintragssystem. Im Folgenden finden Sie ein Beispiel dafür, wie ein Dokument in diesem System aussieht:

```
{
    "_id": "ab6ad8f119b5bca3efa2c7ae",
    "restaurantId": "REST-CRT9BL",
    "name": "Thai Curry Palace",
    "description": "Amazing Restaurant, must visit",
    "cuisine": "Thai",
    "address": {
        "street": "914 Park Street",
        "city": "Bryan",
        "state": "AL",
        "zipCode": "96865",
        "location": {
            "type": "Point",
            "coordinates": [-25.4619, 8.389]
        }
    },
    "contact": {
        "phone": "(669) 915-9056 x6657"
    },
    "rating": {
        "average": 3.4,
        "totalReviews": 275
    },
    "priceRange": "$",
    "menu": [{
        "category": "Appetizers",
        "items": [{
            "name": "Buffalo Chicken Wings",
            "price": 13.42
        }]
    }],
    "features": [
        "Private Dining"
    ],
    "isActive": false“ michelin”: {“
        star”: 3,
```

```
        “ranking_years”: 4
    }
}
```

Alle Codebeispiele, die CRUD, Indexverwaltung und ereignisgesteuerte Programmierung zeigen, gehen davon aus, dass Sie über ein `MongoClient`Objekt`dbClient`, ein Objekt und ein `MongoDatabase`Objekt `connection`DB verfügen. `MongoCollection``collection`

> **Note**
>
> Alle Codebeispiele in diesem Handbuch wurden mit der MongoDB-Java-Treiberversion 5.3.0 getestet.

Mit einem MongoDB-Java-Treiber eine Verbindung zu Amazon DocumentDB herstellen

Dieser Abschnitt enthält eine schrittweise Anleitung für die Verbindung mit Amazon DocumentDB mithilfe von Java-Treibern. Auf diese Weise können Sie mit der Integration von DocumentDB in Ihre Java-Anwendungen beginnen.

Themen

- Schritt 1: Einrichten des Projekts
- Schritt 2: Erstellen Sie die Verbindungszeichenfolge
- Schritt 3: Schreiben Sie den Verbindungscode
- Schritt 4: Verbindungsausnahmen behandeln
- Schritt 5: Den Code ausführen
- Bewährte Methoden für Verbindungen

Schritt 1: Einrichten des Projekts

1. Erstellen Sie mit Maven ein Java-Projekt:

```
mvn archetype:generate -DgroupId=com.docdb.guide -DartifactId=my-docdb-project -
DarchetypeArtifactId=maven-archetype-quickstart -DinteractiveMode=false
```

2. Fügen Sie den MongoDB-Java-Treiber als Abhängigkeit für das Projekt in Ihrer Datei 'pom.xml' hinzu:

```
<dependency>
    <groupId>org.mongodb</groupId>
    <artifactId>mongodb-driver-sync</artifactId>
    <version>5.3.0</version>
</dependency>
```

Schritt 2: Erstellen Sie die Verbindungszeichenfolge

Die Amazon DocumentDB DocumentDB-Verbindungszeichenfolge ist wichtig, um eine Verbindung zwischen Ihrer Anwendung und Ihrem DocumentDB-Cluster herzustellen. Diese Zeichenfolge enthält wichtige Informationen wie den Cluster-Endpunkt, den Port, Authentifizierungsdetails und verschiedene Verbindungsoptionen. Um eine DocumentDB-Verbindungszeichenfolge zu erstellen, beginnen Sie normalerweise mit dem Basisformat:

```
"mongodb://username:password@cluster-endpoint:port/?[connection options]"
```

Sie müssen „Benutzername“ und „Passwort“ durch Ihre tatsächlichen Anmeldeinformationen ersetzen. Den Endpunkt und die Portnummer Ihres Clusters finden Sie sowohl im AWS-Managementkonsole als auch über AWS CLI. Informationen Die Endpunkte eines Clusters finden zum Finden des Cluster-Endpunkts für Ihren Cluster finden Sie unter. Der Standardport für DocumentDB ist 27017.

Beispiele für Verbindungszeichenfolgen

- Herstellen einer Verbindung zu DocumentDB mithilfe von Verschlüsselung bei der Übertragung und Sicherstellung, dass Leseanforderungen an Read Replicas und Schreiben an Primary weitergeleitet werden:

```
"mongodb://username:password@cluster-endpoint:27017/?tls=true&
   tlsCAFile=global-bundle.pem&
   readPreference=secondaryPreferred&
   retryWrites=false"
```

- Herstellen einer Verbindung zu DocumentDB mithilfe der IAM-Authentifizierung:

```
"mongodb://cluster-endpoint:27017/?tls=true&
```

```
    tlsCAFile=global-bundle.pem&
    readPreference=secondaryPreferred&
    retryWrites=false&
    authSource=%24external&
    authMechanism=MONGODB-AWS"
```

Die verschiedenen Optionen, die für die Verbindungszeichenfolge verfügbar sind, lauten wie folgt:

- TLS-Zertifikat
- Aus gelesenen Replikaten lesen
- Schreiben Sie ein Anliegen und führen Sie ein Tagebuch
- RetryWrites
- IAM-Authentifizierung
- Verbindungspool
- Parameter für das Verbindungs-Timeout

TLS-Zertifikat

`tls=true|false`— Diese Option aktiviert oder deaktiviert Transport Layer Security (TLS). Standardmäßig ist die Verschlüsselung bei der Übertragung auf dem Amazon DocumentDB-Cluster aktiviert. Daher sollte der Wert für diese Option lauten, sofern TLS nicht auf Cluster-Ebene deaktiviert ist. `true`

Bei Verwendung von TLS muss der Code ein SSL-Zertifikat bereitstellen, wenn eine Verbindung zu einem DocumentDB-Cluster hergestellt wird. Laden Sie das Zertifikat herunter, das für die sichere Verbindung zum Cluster erforderlich ist: `global-bundle.pem`. Es gibt zwei Möglichkeiten, die `global-bundle.pem` Datei zu verwenden.

- Option 1 — Extrahieren Sie alle Zertifikate aus der `global-bundle.pem` Datei und speichern Sie sie mit dem Keytool von Java in einer `.jks` Datei, die später im Code verwendet werden kann. Das Skript, das zeigt, wie Verbindung bei aktiviertem TLS herstellen das geht, finden Sie auf der Registerkarte Java.
- Option 2 — Fügen Sie die `global-bundle.pem` Datei dynamisch zum Code hinzu, erstellen Sie einen Keystore im Arbeitsspeicher und verwenden Sie ihn`SSLContext`, um das Zertifikat beim Herstellen der Verbindung bereitzustellen.

Aus gelesenen Replikaten lesen

`replicaSet=rs0&readPreference=secondaryPreferred`— Wenn Sie diese beiden Optionen angeben, werden alle Leseanforderungen an die Read Replicas und Schreibanforderungen an die primäre Instanz weitergeleitet. Durch die Verwendung `replicaSet=rs0` in der Verbindungszeichenfolge kann der MongoDB-Treiber eine automatisch aktualisierte Ansicht der Cluster-Topologie beibehalten, sodass Anwendungen die Sichtbarkeit der aktuellen Knotenkonfigurationen beibehalten können, wenn Instanzen hinzugefügt oder entfernt werden. Wenn Sie diese Optionen nicht angeben oder angeben, werden alle Lese- und Schreibvorgänge an die primäre Instanz `readPreference=primary` gesendet. Weitere Optionen für finden `readPreference` Sie unterLesen Sie die Einstellungsoptionen.

Schreiben Sie ein Anliegen und führen Sie ein Tagebuch

Das Problem mit Schreibvorgängen bestimmt den Grad der Bestätigung, die von der Datenbank für Schreibvorgänge angefordert wird. MongoDB-Treiber bieten eine Option zur Optimierung von Schreib-, Bedenken- und Journaldateien. Amazon DocumentDB erwartet nicht, dass Sie Write Concern und Journal festlegen, und ignoriert die Werte, die für `w` und `j` (`writeConcernundjournal`) gesendet werden. DocumentDB schreibt Daten immer mit`writeConcern`: `majority` und`journal`:, `true` sodass die Schreibvorgänge auf den meisten Knoten dauerhaft aufgezeichnet werden, bevor eine Bestätigung an den Client gesendet wird.

RetryWrites

`retryWrites=false`— DocumentDB unterstützt keine wiederholbaren Schreibvorgänge und daher sollte dieses Attribut immer auf gesetzt werden. `false`

IAM-Authentifizierung

`authSource=%24external`und **`authMechanism=MONGODB-AWS`** — Diese beiden Parameter werden zur Authentifizierung mit verwendet. AWS Identity and Access Management Die IAM-Authentifizierung ist derzeit nur in der instanzbasierten Cluster-Version 5.0 verfügbar. Weitere Informationen finden Sie unter Authentifizierung mit IAM-Identität.

Verbindungspool

Diese Optionen sind für das Verbindungspooling verfügbar:

- **`maxPoolSize`**— Legt die maximale Anzahl von Verbindungen fest, die im Pool erstellt werden können. Wenn alle Verbindungen verwendet werden und eine neue Anfrage eingeht, wartet es

darauf, dass eine Verbindung verfügbar wird. Die Standardeinstellung für MongoDB-Java-Treiber ist 100.

- **`minPoolSize`**— Gibt die Mindestanzahl von Verbindungen an, die jederzeit im Pool aufrechterhalten werden sollten. Die Standardeinstellung für MongoDB-Java-Treiber ist 0.
- **`maxIdleTimeMS`**— Legt fest, wie lange eine Verbindung im Pool inaktiv bleiben kann, bevor sie geschlossen und entfernt wird. Die Standardeinstellung für MongoDB-Java-Treiber ist 100 Millisekunden.
- **`waitQueueTimeoutMS`**— Konfiguriert, wie lange ein Thread warten soll, bis eine Verbindung verfügbar wird, wenn der Pool seine maximale Größe erreicht hat. Wenn innerhalb dieser Zeit keine Verbindung verfügbar ist, wird eine Ausnahme ausgelöst. Der Standardwert für MongoDB-Java-Treiber ist 120.000 Millisekunden (2 Minuten).

Parameter für das Verbindungs-Timeout

Timeout ist ein Mechanismus zur Begrenzung der Zeit, die ein Vorgang oder ein Verbindungsversuch dauern kann, bis er als fehlgeschlagen betrachtet wird. Die folgenden Timeout-Parameter sind verfügbar, um unbefristete Wartezeiten zu verhindern und die Ressourcenzuweisung zu verwalten:

- **`connectTimeoutMS`**— Konfiguriert, wie lange der Treiber warten soll, um eine Verbindung zum Cluster herzustellen. Die Standardeinstellung ist 10.000 Millisekunden (10 Sekunden).
- **`socketTimeoutMS`**— Gibt an, wie lange der Treiber auf eine Antwort des Servers wartet, wenn es sich nicht um einen Schreibvorgang handelt. Die Standardeinstellung ist 0 (kein Timeout oder unendlich).
- **`serverSelectionTimeoutMS`**— Gibt an, wie lange der Treiber warten wird, um einen verfügbaren Server im Cluster zu finden. Der Standardwert für diese Einstellung ist 30 Sekunden und reicht aus, damit beim Failover eine neue primäre Instanz ausgewählt werden kann.

Schritt 3: Schreiben Sie den Verbindungscode

Das folgende Codebeispiel zeigt, wie eine TLS-Verbindung zu Amazon DocumentDB hergestellt wird:

- Es erstellt die Objekte Java `KeyStore`und `SSLContext>`.
- Es erstellt das `MongoClientSettings`Objekt auch, indem es es an das `ConnectionString`Objekt übergibt. Um eine TLS-Verbindung herzustellen, müssen Sie das `MongoClientSettings` Objekt verwenden, um das `connectionstring` und zu bindens`slcontext`.

- Using MongoClientsruft ein MongoClientObjekt ab.

```
public static MongoClient makeDbConnection(String dbName, String DbUserName, String
 DbPassword,
    String DbClusterEndPoint, String keyStorePass) throws Exception {
    MongoClient connectedClient;
    String connectionOptions = "?
replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false";
    String connectionUrl = "mongodb://" + DbUserName + ":" + DbPassword + "@" +
 DbClusterEndPoint + ":27017/" +
        dbName + connectionOptions;

    try {
        KeyStore trustStore = KeyStore.getInstance(KeyStore.getDefaultType());
        try (FileInputStream fis = new FileInputStream("src/main/resources/certs/
truststore.jks")) {
            trustStore.load(fis, keyStorePass.toCharArray());
            TrustManagerFactory tmf =
 TrustManagerFactory.getInstance(TrustManagerFactory.getDefaultAlgorithm());
            tmf.init(trustStore);

            SSLContext sslContext = SSLContext.getInstance("TLSv1.2");
            sslContext.init(null, tmf.getTrustManagers(), new SecureRandom());
            ConnectionString connectionString = new ConnectionString(connectionUrl);
            MongoClientSettings settings = MongoClientSettings.builder()
                .applyConnectionString(connectionString)
                .applyToSslSettings(builder - > {
                    builder.enabled(true);
                    builder.context(sslContext);
                })
                .build();
            connectedClient = MongoClients.create(settings);
        }
        return connectedClient;
    } catch (MongoException e5) {
        throw new RuntimeException(e5);
    } catch (Exception e) {
        throw new RuntimeException(e);
    }
}
```

Schritt 4: Verbindungsausnahmen behandeln

Bei der Arbeit mit DocumentDB in Java-Anwendungen ist die Behandlung von Verbindungsausnahmen entscheidend für die Aufrechterhaltung robuster und zuverlässiger Datenbankoperationen. Durch die richtige Verwaltung helfen diese Ausnahmen nicht nur bei der schnellen Diagnose von Problemen, sondern stellen auch sicher, dass Ihre Anwendung mit vorübergehenden Netzwerkunterbrechungen oder Serverausfällen problemlos umgehen kann, was zu einer verbesserten Stabilität und Benutzererfahrung führt. Zu den wichtigsten Ausnahmen im Zusammenhang mit dem Verbindungsaufbau gehören:

- **`MongoException`**— Eine allgemeine Ausnahme, die für verschiedene Szenarien gelten könnte, die nicht durch speziellere Ausnahmen abgedeckt sind. Stellen Sie sicher, dass diese Ausnahme nach allen anderen spezifischen Ausnahmen behandelt wird, da es sich um eine catch MongoDB-Ausnahme handelt.
- **`MongoTimeoutException`**— Wird ausgegeben, wenn bei einem Vorgang das Zeitlimit überschritten wird. Zum Beispiel die Abfrage eines nicht vorhandenen Cluster-Endpunkts.
- **`MongoSocketException`**— Ausgestellt für Netzwerkprobleme. Zum Beispiel eine plötzliche Netzwerkunterbrechung während eines Vorgangs.
- **`MongoSecurityException`**— Wird ausgegeben, wenn die Authentifizierung fehlschlägt. Zum Beispiel, wenn eine Verbindung mit falschen Anmeldeinformationen hergestellt wird.
- **`MongoConfigurationException`**— Wird ausgegeben, wenn in der Client-Konfiguration ein Fehler auftritt. Zum Beispiel, wenn eine ungültige Verbindungszeichenfolge verwendet wird.

Schritt 5: Den Code ausführen

Das folgende Codebeispiel erstellt eine Amazon DocumentDB DocumentDB-Verbindung und druckt alle Datenbanken:

```
public static void TestConnection() {
    try (MongoClient mongoClient = makeDbConnection(DATABASE_NAME, DB_USER_NAME,
 DB_PASSWORD, DB_CLUSTER_ENDPOINT, KEYSTORE_PASSWORD)) {
        List < String > databases = mongoClient.listDatabaseNames().into(new ArrayList
 < > ());
        System.out.println("Databases: " + databases);
    } catch (MongoException e) {
        System.err.println("MongoDB error: " + e.getMessage());
        throw new RuntimeException(e);
    }
```

```
}
```

Bewährte Methoden für Verbindungen

Im Folgenden finden Sie bewährte Methoden, die Sie berücksichtigen sollten, wenn Sie mit einem MongoDB-Java-Treiber eine Verbindung zu Amazon DocumentDB herstellen:

- Schließen Sie Ihren immer `MongoClient`dann, wenn Sie den Client nicht mehr benötigen, um Ressourcen freizugeben.
- Behandeln Sie Ausnahmen angemessen und implementieren Sie eine korrekte Fehlerprotokollierung.
- Verwenden Sie Umgebungsvariablen oder speichern AWS Secrets Manager Sie vertrauliche Informationen wie Benutzernamen und Passwörter.

Durchführen von CRUD-Vorgängen in Amazon DocumentDB mit Java

In diesem Abschnitt wird die Durchführung von CRUD-Vorgängen (Create, Read, Update, Delete) in Amazon DocumentDB mithilfe von MongoDB-Java-Treibern beschrieben.

Themen

- Dokumente in einer DocumentDB-Sammlung erstellen und einfügen
- Lesen und Abrufen von Daten aus einer DocumentDB-Sammlung
- Aktualisieren vorhandener Dokumente in einer DocumentDB-Sammlung
- Dokumente aus einer DocumentDB-Sammlung entfernen
- Fehlerbehandlung mit Wiederholungslogik

Dokumente in einer DocumentDB-Sammlung erstellen und einfügen

Durch das Einfügen von Dokumenten in Amazon DocumentDB können Sie Ihren Sammlungen neue Daten hinzufügen. Je nach Ihren Bedürfnissen und dem Datenvolumen, mit dem Sie arbeiten, gibt es mehrere Möglichkeiten, Einfügungen durchzuführen. Die einfachste Methode zum Einfügen eines einzelnen Dokuments in die Sammlung ist. `insertOne()` Um mehrere Dokumente gleichzeitig einzufügen, können Sie die `insertMany()` Methode verwenden, mit der Sie eine Reihe von Dokumenten in einem einzigen Vorgang hinzufügen können. Eine andere Methode zum Einfügen vieler Dokumente in eine DocumentDB-Sammlung ist. `bulkWrite()` In diesem Handbuch werden all diese Methoden zum Erstellen von Dokumenten in einer DocumentDB-Sammlung beschrieben.

`insertOne()`

Lassen Sie uns zunächst untersuchen, wie ein einzelnes Dokument in eine Amazon DocumentDBB-Sammlung eingefügt wird. Das Einfügen eines einzelnen Dokuments erfolgt mithilfe der Methode. `insertOne()` Diese Methode verwendet BsonDocumentfür das Einfügen einen Wert und gibt ein `InsertOneResult`Objekt zurück, mit dem die Objekt-ID des neu eingefügten Dokuments abgerufen werden kann. Der folgende Beispielcode zeigt das Einfügen eines Restaurantdokuments in die Sammlung:

```
Document article = new Document()
    .append("restaurantId", "REST-21G145")
    .append("name", "Future-proofed Intelligent Bronze Hat")
    .append("cuisine", "International")
    .append("rating", new Document()
        .append("average", 1.8)
        .append("totalReviews", 267))
    .append("features", Arrays.asList("Outdoor Seating", "Live Music"));

try {
    InsertOneResult result = collection.insertOne(article);
    System.out.println("Inserted document with the following id: " +
 result.getInsertedId());
} catch (MongoWriteException e) {
    // Handle duplicate key or other write errors
    System.err.println("Failed to insert document: " + e.getMessage());
    throw e;
} catch (MongoException e) {
    // Handle other MongoDB errors
    System.err.println("MongoDB error: " + e.getMessage());
    throw e;
}
```

Achten Sie bei der Verwendung darauf`insertOne()`, eine angemessene Fehlerbehandlung einzubeziehen. Im obigen Code hat „`restaurantId`“ beispielsweise einen eindeutigen Index. Wenn Sie diesen Code erneut ausführen, wird Folgendes ausgelöst`MongoWriteException`:

```
Failed to insert document: Write operation error on server
 docdbCluster.docdb.amazonaws.com:27017.
Write error: WriteError{code=11000, message='E11000 duplicate key error collection:
 Restaurants index: restaurantId_1', details={}}.
```

insertMany ()

Die wichtigsten Methoden, die zum Einfügen vieler Dokumente in eine Sammlung verwendet werden, sind insertMany () und. `bulkWrite()`

Die `insertMany()` Methode ist die einfachste Methode, mehrere Dokumente in einem einzigen Vorgang einzufügen. Sie akzeptiert eine Liste von Dokumenten und fügt sie in die Sammlung ein. Diese Methode ist ideal, wenn Sie einen Stapel neuer Dokumente einfügen, die unabhängig voneinander sind und keine speziellen Verarbeitungs- oder Mischoperationen erfordern. Der folgende Code zeigt, wie JSON-Dokumente aus einer Datei gelesen und in die Sammlung eingefügt werden. Die `insertMany()` Funktion gibt ein `InsertManyResult`InsertManyResultObjekt zurück, mit dem die IDs aller eingefügten Dokumente abgerufen werden können.

```
// Read JSON file content
String content = new String(Files.readAllBytes(Paths.get(jsonFileName)));
JSONArray jsonArray = new JSONArray(content);

// Convert JSON articles to Documents
List < Document > restaurants = new ArrayList < > ();
for (int i = 0; i < jsonArray.length(); i++) {
    JSONObject jsonObject = jsonArray.getJSONObject(i);
    Document doc = Document.parse(jsonObject.toString());
    restaurants.add(doc);
}
//insert documents in collection
InsertManyResult result = collection.insertMany(restaurants);

System.out.println("Count of inserted documents: " + result.getInsertedIds().size());
```

`bulkWrite()`

Die `bulkWrite()` Methode ermöglicht es, mehrere Schreiboperationen (Einfügen, Aktualisieren, Löschen) in einem einzigen Stapel durchzuführen. Sie können `bulkWrite()` sie verwenden, wenn Sie verschiedene Arten von Vorgängen in einem einzigen Stapel ausführen müssen, z. B. wenn Sie einige Dokumente einfügen und andere aktualisieren müssen. `bulkWrite()`unterstützt zwei Arten von Batch-Schreibvorgängen, geordnet und ungeordnet:

- Geordnete Operationen — (Standard) Amazon DocumentDB verarbeitet die Schreibvorgänge sequentiell und stoppt beim ersten Fehler, auf den es stößt. Dies ist nützlich, wenn die Reihenfolge der Operationen wichtig ist, z. B. wenn spätere Operationen von früheren Vorgängen abhängen. Geordnete Operationen sind jedoch im Allgemeinen langsamer als ungeordnete Operationen. Bei

geordneten Vorgängen müssen Sie den Fall berücksichtigen, dass der Stapel beim ersten Fehler stoppt und einige Operationen möglicherweise unbearbeitet bleiben.

- Ungeordnete Operationen — Ermöglicht Amazon DocumentDB, Einfügungen als einzelne Ausführung in der Datenbank zu verarbeiten. Wenn bei einem Dokument ein Fehler auftritt, wird der Vorgang mit den übrigen Dokumenten fortgesetzt. Dies ist besonders nützlich, wenn Sie große Datenmengen einfügen und einige Fehler tolerieren können, z. B. bei der Datenmigration oder bei Massenimporten, bei denen einige Dokumente aufgrund doppelter Schlüssel fehlschlagen können. Bei ungeordneten Vorgängen müssen Sie teilweise Erfolgsszenarien berücksichtigen, in denen einige Operationen erfolgreich sind, während andere fehlschlagen.

Bei der Arbeit mit der `bulkWrite()` Methode sind einige wichtige Klassen erforderlich. Erstens dient die `WriteModel`Klasse als Basisklasse für alle Schreiboperationen und für spezifische Implementierungen wie `InsertOneModel`,, `UpdateOneModelUpdateManyModelDeleteOneModel`, und `DeleteManyModel`behandelt verschiedene Arten von Operationen.

Die `BulkWriteOptions`Klasse ist notwendig, um das Verhalten von Massenoperationen zu konfigurieren, z. B. die ordered/unordered Ausführung festzulegen oder die Dokumentenvalidierung zu umgehen. Die `BulkWriteResult`Klasse bietet detaillierte Informationen zu den Ausführungsergebnissen, einschließlich der Anzahl der eingefügten, aktualisierten und gelöschten Dokumente.

Für die Fehlerbehandlung ist die `MongoBulkWriteException`Klasse von entscheidender Bedeutung, da sie Informationen über alle Fehler während des Massenvorgangs enthält, während die `BulkWriteError`Klasse spezifische Details zu einzelnen Vorgangsfehlern enthält. Der folgende Code zeigt ein Beispiel für das Einfügen einer Liste von Dokumenten sowie das Aktualisieren und Löschen eines einzelnen Dokuments, alles innerhalb der Ausführung eines einzigen `bulkWrite()` Methodenaufrufs. Der Code zeigt auch `BulkWriteResult`, wie mit `BulkWriteOptions`und gearbeitet wird und wie die `bulkWrite()` Operation korrekt mit Fehlern umgeht.

```
List < WriteModel < Document >> bulkOperations = new ArrayList < > ();
// get list of 10 documents representing 10 restaurants
List < Document > restaurantsToInsert = getSampleData();

for (Document doc: restaurantsToInsert) {
    bulkOperations.add(new InsertOneModel < > (doc));
}
// Update operation
```

```
bulkOperations.add(new UpdateOneModel < > (
    new Document("restaurantId", "REST-Y2E9H5"),
    new Document("", new Document("stats.likes", 20))
    .append("", new Document("rating.average", 4.5))));
// Delete operation
bulkOperations.add(new DeleteOneModel < > (new Document("restaurantId", "REST-
D2L431")));

// Perform bulkWrite operation
try {
    BulkWriteOptions options = new BulkWriteOptions()
        .ordered(false); // Allow unordered inserts

    BulkWriteResult result = collection.bulkWrite(bulkOperations, options);

    System.out.println("Inserted: " + result.getInsertedCount());
    System.out.println("Updated: " + result.getModifiedCount());
    System.out.println("Deleted: " + result.getDeletedCount());
} catch (MongoBulkWriteException e) {
    System.err.println("Bulk write error occurred: " + e.getMessage());
    // Log individual write errors
    for (BulkWriteError error: e.getWriteErrors()) {
        System.err.printf("Error at index %d: %s (Code: %d)%n", error.getIndex(),
 error.getMessage(),
            error.getCode());

        // Log the problematic document
        Document errorDoc = new Document(error.getDetails());
        if (errorDoc != null) {
            System.err.println("Problematic document: " + errorDoc);
        }
    }
} catch (Exception e) {
    System.err.println("Error during bulkWrite: " + e.getMessage());
}
```

Wiederholbare Schreibvorgänge

Im Gegensatz zu MongoDB unterstützt Amazon DocumentDB keine wiederholbaren Schreibvorgänge. Daher müssen Sie in ihren Anwendungen eine benutzerdefinierte Wiederholungslogik implementieren, insbesondere zur Behandlung von Netzwerkproblemen oder vorübergehender Nichtverfügbarkeit von Diensten. Eine gut implementierte Wiederholungsstrategie besteht in der Regel darin, die Verzögerung zwischen Wiederholungsversuchen zu erhöhen und die

Gesamtzahl der Wiederholungsversuche zu begrenzen. Fehlerbehandlung mit WiederholungslogikIm Folgenden finden Sie ein Codebeispiel für die Erstellung einer Wiederholungslogik mit Fehlerbehandlung.

Lesen und Abrufen von Daten aus einer DocumentDB-Sammlung

Das Abfragen von Dokumenten in Amazon DocumentDB basiert auf mehreren Schlüsselkomponenten, mit denen Sie Daten präzise abrufen und bearbeiten können. Die `find()`Methode ist die grundlegende Abfrage-API in MongoDB-Java-Treibern. Sie ermöglicht den komplexen Datenabruf mit zahlreichen Optionen zum Filtern, Sortieren und Projizieren von Ergebnissen. Neben der `find()` Methode `FindIterable`sind dies zwei weitere grundlegende Komponenten, `Filters`die die Bausteine für Abfrageoperationen in MongoDB-Java-Treibern bereitstellen.

Die `Filters` Klasse ist eine Hilfsklasse im MongoDB-Java-Treiber, die eine flüssige API zum Erstellen von Abfragefiltern bereitstellt. Diese Klasse bietet statische Factory-Methoden, die Instanzen von `Bson` Objekten erstellen, die verschiedene Abfragebedingungen repräsentieren. Zu den am häufigsten verwendeten Methoden gehören `eq()` für Gleichheitsvergleiche`gt()`,`lt()`,`gte()`, und `lte()` für numerische Vergleiche `and()` und `or()` für die Kombination mehrerer Bedingungen `in()` sowie `nin()` für Array-Zugehörigkeitstests und `regex()` für den Mustervergleich. Die Klasse ist typsicher konzipiert und bietet im Vergleich zu Abfragen, die auf Rohdokumenten basieren, eine bessere Überprüfung bei der Kompilierung, was sie zum bevorzugten Ansatz für die Erstellung von DocumentDB-Abfragen in Java-Anwendungen macht. Die Fehlerbehandlung ist robust und bei ungültigen Filterkonstruktionen werden eindeutige Ausnahmen ausgelöst.

`FindIterable`ist eine spezielle Schnittstelle, die für die Verarbeitung des Ergebnisses der `find()` Methode entwickelt wurde. Es bietet eine Vielzahl von Methoden zur Verfeinerung und Steuerung der Abfrageausführung und bietet eine flüssige API für die Methodenverkettung. Die Schnittstelle umfasst grundlegende Methoden zur Änderung von Abfragen, z. B. `limit()` zur Beschränkung der Anzahl der zurückgegebenen Dokumente, `skip()` zur Seitennummerierung, zur Reihenfolge der Ergebnisse, `sort()` zur Auswahl bestimmter Felder und `projection()` zur Indexauswahl. `hint()` Die Batch-, Skip- und Limit-Operationen in `FindIterable` sind wichtige Tools zur Seitennummerierung und Datenverwaltung, mit deren Hilfe gesteuert werden kann, wie Dokumente aus der Datenbank abgerufen und verarbeitet werden.

Batching (`batchSize`) steuert, wie viele Dokumente DocumentDB in einem einzigen Netzwerk-Roundtrip an den Client zurückgibt. Wenn Sie eine Stapelgröße festlegen, gibt DocumentDB nicht

alle passenden Dokumente auf einmal zurück, sondern gibt sie in Gruppen mit der angegebenen Stapelgröße zurück.

Mit Skip können Sie den Startpunkt Ihrer Ergebnisse verschieben und DocumentDB im Wesentlichen anweisen, eine bestimmte Anzahl von Dokumenten zu überspringen, bevor Treffer zurückgegeben werden. Beispielsweise `skip(20)` werden die ersten 20 übereinstimmenden Dokumente umgangen. Dies wird häufig in Paginierungsszenarien verwendet, in denen Sie nachfolgende Ergebnisseiten abrufen möchten.

Limit schränkt die Gesamtzahl der Dokumente ein, die von einer Abfrage zurückgegeben werden können. Wenn Sie angeben`limit(n)`, beendet DocumentDB die Rückgabe von Dokumenten, nachdem 'n' Dokumente zurückgegeben wurden, auch wenn es mehr Treffer in der Datenbank gibt.

`FindIterable`unterstützt sowohl Iterator- als auch Cursormuster beim Abrufen von Dokumenten aus Amazon DocumentDB. Der Vorteil der Verwendung `FindIterable` als Iterator besteht darin, dass Dokumente verzögert geladen werden können und Dokumente nur abgerufen werden, wenn sie von der Anwendung angefordert werden. Ein weiterer Vorteil der Verwendung von Iterator besteht darin, dass Sie nicht für die Aufrechterhaltung der Verbindung zum Cluster verantwortlich sind und daher kein explizites Schließen der Verbindung erforderlich ist.

`FindIterable`bietet auch Unterstützung für `MongoCursor`die Verwendung von Cursormustern bei der Arbeit mit Amazon DocumentDB DocumentDB-Abfragen. `MongoCursor`ist eine mongoDB-Java-Treiberspezifische Implementierung, die die Kontrolle über Datenbankoperationen und Ressourcenmanagement bietet. Sie implementiert die `AutoCloseable` Schnittstelle und ermöglicht so eine explizite Ressourcenverwaltung mithilfe von Try-with-Resources-Blöcken, was für das korrekte Schließen von Datenbankverbindungen und die Freigabe von Serverressourcen von entscheidender Bedeutung ist. Standardmäßig läuft der Cursor innerhalb von 10 Minuten ab, und DocumentDB bietet Ihnen nicht die Möglichkeit, dieses Timeout-Verhalten zu ändern. Achten Sie bei der Arbeit mit Batchdaten darauf, den nächsten Datenstapel abzurufen, bevor der Cursor das Timeout erreicht. Ein wichtiger Aspekt bei der Verwendung `MongoCursor` ist, dass ein explizites Schließen erforderlich ist, um Ressourcenlecks zu verhindern.

In diesem Abschnitt werden mehrere Beispiele für`find()`, `Filters` und vorgestelltFindIterable.

Das folgende Codebeispiel zeigt, wie Sie `find()` mithilfe des Felds „RestaurantID“ ein einzelnes Dokument abrufen können:

```
Document filter = new Document("restaurantId", "REST-21G145");
Document result = collection.find(filter).first();
```

Die Verwendung `Filters` ermöglicht zwar eine bessere Fehlerprüfung bei der Kompilierung, mit dem Java-Treiber können Sie jedoch auch einen `Bson` Filter direkt in der `find()` Methode angeben. Der folgende Beispielcode übergibt `Bson` das Dokument an`find()`:

```
result = collection.find(new Document("$and", Arrays.asList(
    new Document("rating.totalReviews", new Document("$gt", 1000)),
    new Document("priceRange", "$$"))))
```

Der nächste Beispielcode zeigt mehrere Beispiele für die Verwendung der `Filters` Klasse mit`find()`:

```
FindIterable < Document > results;

// Exact match
results = collection.find(Filters.eq("name", "Thai Curry Palace"));

// Not equal
results = collection.find(Filters.ne("cuisine", "Thai"));

// find an element in an array
results = collection.find(Filters.in("features", Arrays.asList("Private Dining")));

// Greater than
results = collection.find(Filters.gt("rating.average", 3.5));

// Between (inclusive)
results = collection.find(Filters.and(
    Filters.gte("rating.totalReviews", 100),
    Filters.lte("rating.totalReviews", 200)));
// AND
results = collection.find(Filters.and(
    Filters.eq("cuisine", "Thai"),
    Filters.gt("rating.average", 4.5)));

// OR
results = collection.find(Filters.or(
    Filters.eq("cuisine", "Thai"),
    Filters.eq("cuisine", "American")));


// All document where the Field exists
results = collection.find(Filters.exists("michelin"));
```

```
// Regex
results = collection.find(Filters.regex("name", Pattern.compile("Curry",
 Pattern.CASE_INSENSITIVE)));

// Find all document where the array contain the list of value regardless of its order
results = collection.find(Filters.all("features", Arrays.asList("Private Dining",
 "Parking")));

// Array size
results = collection.find(Filters.size("features", 4));
```

Das folgende Beispiel zeigt, wie die Operationen von`sort()`, `skip()``limit()`, und `batchSize()` an einem `FindIterable` Objekt verkettet werden. Die Reihenfolge, in der diese Operationen ausgeführt werden, beeinflusst die Leistung Ihrer Abfrage. Als bewährte Methode sollte die Reihenfolge dieser Operationen`sort()`, `projection()``skip()`, `limit()` und lauten`batchSize()`.

```
FindIterable < Document > results = collection.find(Filters.gt("rating.totalReviews",
 1000))
    // Sorting
    .sort(Sorts.orderBy(
        Sorts.descending("address.city"),
        Sorts.ascending("cuisine")))
    // Field selection
    .projection(Projections.fields(
        Projections.include("name", "cuisine", "priceRange"),
        Projections.excludeId()))

    // Pagination
    .skip(20)
    .limit(10)
    .batchSize(2);
```

Der folgende Beispielcode zeigt die Erstellung eines Iterators am`FindIterable`. Es verwendet das `forEach` Java-Konstrukt, um die Ergebnismenge zu durchlaufen.

```
collection.find(Filters.eq("cuisine", "American")).forEach(doc ->
 System.out.println(doc.toJson()));
```

Im letzten `find()` Codebeispiel wird gezeigt, wie es zum Abrufen von Dokumenten verwendet `cursor()` wird. Es erstellt den Cursor im Try-Block, wodurch sichergestellt wird, dass der Cursor geschlossen wird, wenn der Code den Try-Block verlässt.

```
try (MongoCursor < Document > cursor = collection.find(Filters.eq("cuisine",
 "American"))
    .batchSize(25)
    .cursor()) {
    while (cursor.hasNext()) {
        Document doc = cursor.next();
        System.out.println(doc.toJson());
    }
} // Cursor automatically closed
```

Aktualisieren vorhandener Dokumente in einer DocumentDB-Sammlung

Amazon DocumentDB bietet flexible und leistungsstarke Mechanismen zum Ändern vorhandener Dokumente und zum Einfügen neuer Dokumente, wenn sie nicht existieren. Der MongoDB-Java-Treiber bietet mehrere Methoden für Updates: `updateOne()` für die Aktualisierung einzelner Dokumente, `updateMany()` für die Aktualisierung mehrerer Dokumente und `replaceOne()` für den vollständigen Austausch von Dokumenten. Neben diesen drei Methoden `UpdateResult`sind, `UpdatesUpdateOptions`, und weitere grundlegende Komponenten, die die Bausteine für Aktualisierungsvorgänge in MongoDB-Java-Treibern bereitstellen.

Die `Updates` Klasse im MongoDB-Java-Treiber ist eine Hilfsklasse, die statische Factory-Methoden zum Erstellen von Aktualisierungsoperatoren bereitstellt. Sie dient als primärer Builder für die typsichere und lesbare Konstruktion von Aktualisierungsoperationen. Grundlegende Methoden wie `set()``unset()`, und `inc()` ermöglichen die direkte Änderung der Dokumente. Die Leistungsfähigkeit dieser Klasse wird deutlich, wenn mehrere Operationen mit der `Updates.combine()` Methode kombiniert werden, mit der mehrere Aktualisierungsvorgänge atomar ausgeführt werden können, wodurch die Datenkonsistenz gewährleistet wird.

`UpdateOptions`ist eine leistungsstarke Konfigurationsklasse im Java-Treiber von MongoDB, die grundlegende Anpassungsmöglichkeiten für Dokumentaktualisierungsvorgänge bietet. Zwei wichtige Aspekte dieser Klasse sind die Unterstützung von Upsert- und Array-Filtern für Aktualisierungsvorgänge. Die Upsert-Funktion, aktiviert durch`upsert(true)`, ermöglicht die Erstellung neuer Dokumente, wenn während eines Aktualisierungsvorgangs keine passenden Dokumente gefunden werden. Durch `arrayFilters()` den Aktualisierungsvorgang können Array-Elemente, die bestimmte Kriterien erfüllen, präzise aktualisiert werden.

`UpdateResult`Der Java-Treiber von MongoDB bietet den Feedback-Mechanismus, der das Ergebnis eines Aktualisierungsvorgangs detailliert beschreibt. Diese Klasse fasst drei wichtige Kennzahlen zusammen: die Anzahl der Dokumente, die den Aktualisierungskriterien entsprechen (`matchedCount`), die Anzahl der tatsächlich geänderten Dokumente (`modifiedCount`) und Informationen über alle geänderten Dokumente (). `upsertedId` Das Verständnis dieser Metriken ist für die korrekte Fehlerbehandlung, die Überprüfung von Aktualisierungsvorgängen und die Aufrechterhaltung der Datenkonsistenz in Anwendungen unerlässlich.

Aktualisieren und ersetzen Sie ein einzelnes Dokument

In DocumentDB kann die Aktualisierung eines einzelnen Dokuments mit der Methode updateOne () durchgeführt werden. Diese Methode verwendet einen Filterparameter, der normalerweise von der `Filters` Klasse bereitgestellt wird, um das zu aktualisierende Dokument zu identifizieren, einen `Updat` e-Parameter, der bestimmt, welche Felder aktualisiert werden sollen, und einen optionalen `UpdateOptions` Parameter, um verschiedene Optionen für die Aktualisierung festzulegen. Bei Verwendung `updateOne()` dieser Methode wird nur das erste Dokument aktualisiert, das den Auswahlkriterien entspricht. Der folgende Beispielcode aktualisiert ein einzelnes Feld eines Dokuments:

```
collection.updateOne(Filters.eq("restaurantId", "REST-Y2E9H5"),
    Updates.set("name", "Amazing Japanese sushi"));
```

Um mehrere Felder in einem Dokument zu aktualisieren, verwenden Sie `updateOne()` with `Update.combine()` wie im folgenden Beispiel gezeigt. Dieses Beispiel zeigt auch, wie ein Element zu einem Array im Dokument hinzugefügt wird.

```
List<Bson> updates = new ArrayList<>();
// Basic field updates
updates.add(Updates.set("name", "Shanghai Best"));
// Array operations
updates.add(Updates.addEachToSet("features", Arrays.asList("Live Music")));
// Counter updates
updates.add(Updates.inc("rating.totalReviews", 10));
// Combine all updates
Bson combinedUpdates = Updates.combine(updates);
// Execute automic update with one call
collection.updateOne(Filters.eq("restaurantId","REST-1J83NH"), combinedUpdates);
```

Das folgende Codebeispiel zeigt, wie ein Dokument in der Datenbank aktualisiert wird. Wenn das angegebene Dokument nicht existiert, wird es stattdessen automatisch als neues Dokument

eingefügt. Dieser Code zeigt auch, wie die über das `UpdateResult` Objekt verfügbaren Metriken verwendet werden.

```
Bson filter = Filters.eq("restaurantId", "REST-0Y9GL0");
Bson update = Updates.set("cuisine", "Indian");
// Upsert operation
UpdateOptions options = new UpdateOptions().upsert(true);
UpdateResult result = collection.updateOne(filter, update, options);

if (result.getUpsertedId() != null) {
    System.out.println("Inserted document with _id: " + result.getUpsertedId());
} else {
     System.out.println("Updated " + result.getModifiedCount() + " document(s)");
}
```

Das folgende Codebeispiel zeigt, wie Sie mithilfe der `replaceOne()` Methode ein vorhandenes Dokument vollständig durch ein neues Dokument ersetzen können, anstatt einzelne Felder zu aktualisieren. Die `replaceOne()` Methode überschreibt das gesamte Dokument und behält nur das `_id` Feld des Originals bei. Wenn mehrere Dokumente den Filterkriterien entsprechen, wird nur das zuerst gefundene Dokument ersetzt.

```
Document newDocument = new Document()
                .append("restaurantId", "REST-0Y9GL0")
                .append("name", "Bhiryani Adda")
                .append("cuisine", "Indian")
                .append("rating", new Document()
                        .append("average", 4.8)
                        .append("totalReviews", 267))
                .append("features", Arrays.asList("Outdoor Seating", "Live Music"));

UpdateResult result = collection.replaceOne(
                    Filters.eq("restaurantId", "REST-0Y9GL0"),
                    newDocument);
System.out.printf("Modified %d document%n", result.getModifiedCount());
```

Aktualisieren Sie mehrere Dokumente

Es gibt zwei Möglichkeiten, mehrere Dokumente in einer Sammlung gleichzeitig zu aktualisieren. Sie können die `updateMany()` Methode oder die `UpdateManyModel`zusammen mit der `bulkWrite()` Methode verwenden. Die `updateMany()` Methode verwendet einen Filterparameter, um Dokumente für die Aktualisierung auszuwählen, den `Update` Parameter zur Identifizierung

der zu aktualisierenden Felder und einen optionalen `UpdateOptions` Parameter zur Angabe von Aktualisierungsoptionen.

Der folgende Beispielcode veranschaulicht die Verwendung der `updateMany()` Methode:

```
Bson filter = Filters.and(
    Filters.in("features", Arrays.asList("Private Dining")),
    Filters.eq("cuisine", "Thai"));
UpdateResult result1 = collection.updateMany(filter, Updates.set("priceRange", "$$$"));
```

Der folgende Beispielcode demonstriert die `bulkWrite()` Methode mit demselben Update:

```
BulkWriteOptions options = new BulkWriteOptions().ordered(false);
List < WriteModel < Document >> updates = new ArrayList < > ();
Bson filter = Filters.and(
    Filters.in("features", Arrays.asList("Private Dining")),
    Filters.eq("cuisine", "Indian"));
Bson updateField = Updates.set("priceRange", "$$$");
updates.add(new UpdateManyModel < > (filter, updateField));
BulkWriteResult result = collection.bulkWrite(updates, options);
System.out.printf("Modified %d document%n", result.getModifiedCount());
```

Dokumente aus einer DocumentDB-Sammlung entfernen

Der MongoDB-Java-Treiber bietet `deleteOne()` die Möglichkeit, ein einzelnes Dokument und mehrere Dokumente `deleteMany()` zu entfernen, die bestimmten Kriterien entsprechen. Genau wie beim Aktualisieren kann auch der Löschvorgang mit der `bulkWrite()` Methode verwendet werden. Beides `deleteOne()` und gibt ein `DeleteResult`Objekt `deleteMany()` zurück, das Informationen über das Ergebnis des Vorgangs enthält, einschließlich der Anzahl der gelöschten Dokumente. Im Folgenden finden Sie ein Beispiel für die Verwendung `deleteMany()` zum Entfernen mehrerer Dokumente:

```
Bson filter = Filters.and(
    Filters.eq("cuisine", "Thai"),
    Filters.lt("rating.totalReviews", 50));
DeleteResult result = collection.deleteMany(filter);
System.out.printf("Deleted %d document%n", result.getDeletedCount());
```

Fehlerbehandlung mit Wiederholungslogik

Eine robuste Strategie zur Fehlerbehandlung für Amazon DocumentDB sollte die Kategorisierung von Fehlern in wiederholbare Fehler (wie Netzwerk-Timeouts, Verbindungsprobleme) und nicht wiederholbare Fehler (wie Authentifizierungsfehler, ungültige Abfragen) implementieren. Bei Betriebsfehlern aufgrund von Fehlern, die wiederholt werden sollten, sollte eine Zeitverzögerung zwischen den einzelnen Wiederholungsversuchen sowie die maximale Anzahl von Wiederholungsversuchen vorgesehen werden. Die CRUD-Operationen sollten sich in einem Try-Catch-Block befinden, der Catches `MongoException`und seine Unterklassen enthält. Darüber hinaus sollte es die Überwachung und Protokollierung von Fehlern beinhalten, um die betriebliche Transparenz zu gewährleisten. Im Folgenden finden Sie einen Beispielcode, der zeigt, wie die Behandlung von Wiederholungsfehlern implementiert wird:

```
int MAX_RETRIES = 3;
int INITIAL_DELAY_MS = 1000;
int retryCount = 0;

while (true) {
    try {
        crud_operation(); //perform crud that will throw MongoException or one of its
 subclass
        break;
    } catch (MongoException e) {
        if (retryCount < MAX_RETRIES) {
            retryCount++;
            long delayMs = INITIAL_DELAY_MS * (long) Math.pow(2, retryCount - 1);
            try {
                TimeUnit.MILLISECONDS.sleep(delayMs);
            } catch (InterruptedException t) {
                Thread.currentThread().interrupt();
                throw new RuntimeException("Retry interrupted", t);
            }
            continue;
        } else
            throw new RuntimeException("Crud operation failed", e);
    }
}
```

Indexverwaltung in Amazon DocumentDB mit Java

Indizes ermöglichen das effiziente Abrufen von Daten aus einer Amazon DocumentDB-Sammlung. Ohne Indizes muss DocumentDB jedes Dokument in der Sammlung scannen, um Ergebnisse zurückzugeben, die einer bestimmten Abfrage entsprechen. Dieses Thema enthält Informationen zum Erstellen, Löschen und Auflisten von Indizes mithilfe der MongoDB-Java-Treiber. Außerdem wird erläutert, wie ermittelt werden kann, ob ein bestimmter Index in der Abfrage verwendet wird, und wie Amazon DocumentDB Hinweise zur Verwendung eines bestimmten Indexes gegeben werden kann.

Themen

- Indizes mit Java erstellen
- Indizes löschen
- Festlegung der Indexauswahl und Bereitstellung eines Indexhinweises

Amazon DocumentDB unterstützt viele Arten von Indizes. Einen umfassenden Überblick über alle unterstützten Indizes finden Sie in diesem Blogbeitrag.

Indizes mit Java erstellen

Es gibt zwei Mechanismen zum Erstellen von Indizes in Amazon DocumentDB mithilfe von MongoDB-Java-Treibern: durch `runCommand()` und entweder durch die `createIndex()` Methode für einen einzelnen Index oder durch die `createIndexes()` Methode für mehrere Indizes. Ein Grund für die Verwendung der `createIndexes()` Methoden `createIndex()` und besteht darin, dass Sie eine bessere Fehlerbehandlung aufbauen können, indem Sie bestimmte Fehler im Zusammenhang mit der Indexerstellung abfangen. Ein weiterer Grund für die Verwendung dieser Methode `runCommand()` ist, dass der MongDB-Java-Treiber eine Vielzahl von unterstützenden Klassen für die Indexerstellung und -manipulation bereitstellt. Beachten Sie, dass diese unterstützenden Klassen nur verwendet werden können, wenn Sie die Methoden `createIndex()` oder `createIndexes()` verwenden. Es gibt drei unterstützende Klassen:

- **`Indexes`**— Diese Klasse dient als Hilfsklasse und bietet statische Factory-Methoden zur Erstellung verschiedener Arten von Indizes. Sie vereinfacht den Prozess der Erstellung komplexer Indexdefinitionen und wird häufig in Verbindung mit anderen indexbezogenen Klassen verwendet.
- **`IndexModel`**— Dies ist eine grundlegende Klasse, die sowohl die Definition der Indexschlüssel als auch ihre Optionen kapselt. Sie stellt eine vollständige Indexspezifikation dar, die kombiniert, was indexiert werden soll (die Schlüssel) und wie indexiert werden soll (die Optionen). Diese Klasse ist besonders nützlich, wenn Sie mehrere Indizes gleichzeitig erstellen, da Sie damit eine Sammlung

von Indexspezifikationen definieren können, die an die `createIndexes()` Methode übergeben werden können.

- **`IndexOptions`**— Dies ist eine umfassende Konfigurationsklasse, die eine Vielzahl von Methoden zur Anpassung des Indexverhaltens bietet. Sie umfasst Einstellungen für eindeutige Indizes, Sparse-Indizes, Ablaufzeit (TTL) und partielle Filterausdrücke. Durch Methodenverkettung können Sie mehrere Optionen wie die Indexerstellung im Hintergrund und eindeutige Einschränkungen konfigurieren.

Erstellen Sie einen einzelnen Index

Dieses Beispiel zeigt, wie ein einzelner Index mit der Methode `createIndex( ()` im Hintergrund erstellt wird. Informationen zur Indexerstellung im Hintergrund und Vordergrund finden Sie unterTypen der Indexerstellung. Im folgenden Codebeispiel wird `IndexOptions`ein eindeutiger Index mit dem Namen „unique_restaurantId_idx“ im Hintergrund erstellt. Dieses `IndexOptions` Objekt wird dann an die Methode übergeben. `createIndex()`

```
collection.createIndex(
    Indexes.ascending("restaurantId"),
    new IndexOptions()
        .unique(true)
        .name("unique_restaurantId_idx")
        .background(true));
```

Erstellen Sie mehrere Indizes

In diesem Beispiel werden mithilfe der Methode mehrere Indizes erstellt. `createIndexes()` Es erstellt zuerst die Option für jeden Index mithilfe des `IndexModel`Objekts und übergibt dann eine Liste von `IndexModel` Objekten an die `createIndexes()` Methode. Das folgende Codebeispiel zeigt, wie ein zusammengesetzter Index mithilfe der `Indexes`Utility-Klasse erstellt wird. Diese Klasse wird auch verwendet, um anzugeben, ob Sie einen Index mit aufsteigender oder absteigender Sortierreihenfolge erstellen möchten. Nach dem Erstellen mehrerer Indizes überprüft sie die Indexerstellung, indem sie die Methode aufruft. `listIndexes()`

```
// Single Field Index on cuisine
IndexModel singleIndex = new IndexModel(
    Indexes.ascending("cuisine"),
    new IndexOptions().name("cuisine_idx"));
```

```
// Compound Index
IndexModel compoundIndex = new IndexModel(
    Indexes.compoundIndex(
        Indexes.ascending("address.state"),
        Indexes.ascending("priceRange")),
    new IndexOptions().name("location_price_idx"));

// Build a list of IndexModel for the indexes
List < IndexModel > indexes = Arrays.asList(
    singleIndex,
    compoundIndex
);

collection.createIndexes(indexes);

// Verify created indexes
collection.listIndexes().forEach(index - > System.out.println("Created index: " +
 index.toJson()));
```

Erstellen Sie dünnbesetzte Indizes und partielle Indizes

Dieses Beispiel zeigt, dass ein dünnbesetzter Index und ein partieller Index erstellt werden, indem `IndexModel`für jeden Indextyp ein Index erstellt wird.

```
// Sparse Index Model, this will identify only those documents that have a
// michelin star rating
IndexModel sparseIndex = new IndexModel(
    Indexes.ascending("michelin.star"),
    new IndexOptions()
    .name("michelin_sparse_idx")
    .sparse(true));

// Partial Index Model where the restaurant is active and has a rating of 4 and above
IndexModel partialIndex = new IndexModel(
    Indexes.ascending("rating.average"),
    new IndexOptions()
    .name("high_rated_active_idx")
    .partialFilterExpression(
        Filters.and(
            Filters.eq("isActive", true),
            Filters.gte("rating.average", 4.0))));
```

Erstellen Sie einen Textindex

Dieses Beispiel zeigt, wie ein Textindex erstellt wird. In einer Sammlung ist nur ein Textindex zulässig, aber dieser eine Textindex kann ein zusammengesetzter Index sein, der mehrere Felder abdeckt. Wenn Sie mehrere Felder im Textindex verwenden, können Sie auch jedem Feld im Index Gewichtungen zuweisen. Textindizes für Array-Felder werden von Amazon DocumentDB nicht unterstützt, und obwohl Sie bis zu 30 Felder im zusammengesetzten Textindex verwenden können, kann nur drei Feldern eine Gewichtung zugewiesen werden.

```
IndexModel textIndex = new IndexModel(
    new Document()
    .append("name", "text")
    .append("description", "text")
    .append("cuisine", "text"),
    new IndexOptions()
    .name("restaurant_text_idx")
    .weights(new Document()
        .append("name", 10) // Restaurant name gets highest weight
        .append("description", 5) // Description get medium weight
        .append("cuisine", 2) // Cuisine type gets low weight
    ));

collection.createIndex(textIndex.getKeys(), textIndex.getOptions());
```

Erstellen Sie einen Index mit **`runCommand()`**

Amazon DocumentDB unterstützt die parallel Indexerstellung, um den Zeitaufwand für die Erstellung von Indizes zu verringern. Bei der parallelen Indizierung werden mehrere Worker gleichzeitig verwendet. Für die Indexerstellung werden standardmäßig zwei Worker verwendet. Dieser Blogbeitrag bietet eine eingehende Diskussion zur parallel Indizierung. Derzeit unterstützen MongDB-Java-Treiber die Angabe der Worker-Option nicht, wenn Sie `createIndex()` oder `createIndexes()` verwenden. Daher können Sie Worker nur über die angeben. `runCommand` Das folgende Codebeispiel zeigt, wie Sie `runCommand` einen Index erstellen, der den Worker auf vier erhöht:

```
Document command = new Document("createIndexes", "Restaurants")
    .append("indexes", Arrays.asList(
        new Document("key", new Document("name", 1))
        .append("name", "restaurant_name_idx")
        .append("workers", 4) // Specify number of workers
    ));
```

```
Document commendResult = connectedDB.runCommand(command);
```

Indizes löschen

Der MongoDB-Java-Treiber bietet mehrere Methoden zum Löschen von Indizes, die auf unterschiedliche Szenarien und Ihre Präferenzen zugeschnitten sind. Sie können Indizes nach Namen, nach Schlüsselspezifikation oder alle Indizes auf einmal löschen. Die Methoden `dropIndex()` und `dropIndexes()` können für ein Auflistungsobjekt aufgerufen werden, um einen Index zu löschen. Wenn Sie einen Index nach Namen löschen, sollten Sie sicherstellen, dass der richtige Indexname verwendet wird, was möglicherweise nicht immer intuitiv ist, insbesondere bei zusammengesetzten oder automatisch generierten Indizes. Der Versuch, einen nicht existierenden Index zu löschen, führt zu einem. `MongoCommandException` Der `default _id` Index kann nicht gelöscht werden, da er die Einzigartigkeit des Dokuments innerhalb der Sammlung sicherstellt.

Das folgende Codebeispiel zeigt, wie ein Index gelöscht wird, indem der Feldname angegeben wird, in dem der Index erstellt wurde, oder indem alle Indizes gelöscht werden:

```
String indexName = "unique_restaurantId_idx";
Document keys = new Document("cuisine", 1);
// Drop index by name
collection.dropIndex(indexName);

// Drop index by keys
collection.dropIndex(keys);

// Drop all indexes
collection.dropIndexes();
```

Stellen Sie beim Löschen von Indizes mit mehreren Schlüsseln sicher, dass ein zusammengesetzter Index vorhanden ist, der alle angegebenen Schlüssel enthält und dass die Reihenfolge der Schlüssel korrekt ist. Der obige Beispielcode zur Indexerstellung zeigt einen zusammengesetzten Schlüssel für „Küche“ und Funktionen. Wenn Sie versuchen, diesen zusammengesetzten Schlüssel zu löschen, aber die Reihenfolge nicht der Reihenfolge entspricht, in der er erstellt wurde, tritt ein MongoCommnadException Fehler wie folgt auf:

```
Document keys = new Document("features", 1)
    .append("cuisine", 1);
try {
    // Drop index by keys
    collection.dropIndex(keys);
```

```
    System.out.println("Successfully dropped index with keys: " + keys.toJson());

} catch (MongoCommandException commErr) {
    System.out.println("Error dropping index: " + commErr.getErrorMessage());
    throw new RuntimeException("MongoCommandException was thrown while dropping index",
 commErr);
}
```

Der folgende Fehler wird angezeigt:

```
Error dropping index: Cannot drop index: index not found.
Tests run: 3, Failures: 1, Errors: 0, Skipped: 0, Time elapsed: 0.819 sec <<< FAILURE!
com.amazon.docdb.guide.DocDBGuideTest.testindexGuide()  Time elapsed: 0.817 sec  <<<
 FAILURE!
org.opentest4j.AssertionFailedError: Unexpected exception thrown:
 java.lang.RuntimeException: MongoCommandException was thrown while dropping index
```

Festlegung der Indexauswahl und Bereitstellung eines Indexhinweises

Die Arbeit mit der Erklärungsfunktion in Amazon DocumentDB ist entscheidend, um die Abfrageleistung und die Indexnutzung zu verstehen. Wenn Sie eine Abfrage ausführen, können Sie die `explain()` Methode anhängen, um detaillierte Informationen über den Abfrageplan zu erhalten, einschließlich der verwendeten Indizes. Die `explain()` Ausgabe bietet Einblicke in die Phasen der Abfrageausführung, die Anzahl der untersuchten Dokumente und die für jede Phase benötigte Zeit. Diese Informationen sind von unschätzbarem Wert, um festzustellen, ob ein bestimmter Index effektiv verwendet wird oder ob die Abfrage von einer anderen Indexstruktur profitieren könnte.

Die `explain()` Methode kann mit der Methode verkettet werden. `find()` Die `explain()` Methode kann eine optionale `ExplainVerbosity`Aufzählung verwenden, die den Grad der Ausführlichkeit bestimmt, der von zurückgegeben wird. `explain()` Derzeit werden nur die `QUERY_PLANNER` Enumeratoren `EXECUTION_STATS` und von DocumentDB unterstützt. Das folgende Codebeispiel zeigt, wie der Abfrageplaner für eine bestimmte Abfrage abgerufen wird:

```
// Query we want to analyze
Document query = new Document()
    .append("cuisine", "Thai")
    .append("rating.average", new Document("$gte", 4.0));


Document allPlansExplain =
 collection.find(query).explain(ExplainVerbosity.QUERY_PLANNER);
```

```
System.out.println("All Plans Explain:\n" + allPlansExplain.toJson());
```

Das folgende JSON-Dokument wird für die Ausführlichkeitsstufe des Abfrageplaners zurückgegeben:

```
{
  "queryPlanner": {
    "plannerVersion": 1,
    "namespace": "ProgGuideData.Restaurants",
    "winningPlan": {
      "stage": "IXSCAN",
      "indexName": "cuisine_idx",
      "direction": "forward"
    }
  },
  "serverInfo": {
    "host": "guidecluster3",
    "port": 27017,
    "version": "5.0.0"
  },
  "ok": 1,
  "operationTime": {
    "$timestamp": {
      "t": 1739221668,
      "i": 1
    }
  }
}
```

Sie haben mehrere Möglichkeiten, Amazon DocumentDB zu beeinflussen oder zu zwingen, einen bestimmten Index zu verwenden. Mit den `hintString()` Methoden `hint()` und können Sie das Standardverhalten des Abfrageoptimierers bei der Indexauswahl außer Kraft setzen, indem Sie explizit angeben, welcher Index für eine Abfrage verwendet werden soll. Der Abfrageoptimierer von DocumentDB ist zwar generell eine gute Wahl für die Indexauswahl, es gibt jedoch auch Szenarien, in denen das `hint()` Durchsetzen eines bestimmten Indexes von Vorteil sein `hintString()` kann, z. B. beim Umgang mit verzerrten Daten oder beim Testen der Indexleistung.

Das folgende Codebeispiel erzwingt die Verwendung des zusammengesetzten Index „cuisine_features_idx“ für dieselbe Abfrage, die im obigen Code ausgeführt wurde:

```
// Query we want to analyze
Document query = new Document()
    .append("cuisine", "Thai")
```

```
    .append("rating.average", new Document("$gte", 4.0));

List < Document > queryDocs = new ArrayList < > ();
collection.find(query).hintString("cuisine_features_idx").forEach(doc - >
 queryDocs.add(doc));
```

Event-driven Programmieren mit Amazon DocumentDB und Java

Event-driven Die Programmierung im Kontext von Amazon DocumentDB stellt ein leistungsstarkes Architekturmuster dar, bei dem Datenbankänderungen als primäre Ereignisgeneratoren dienen, die nachfolgende Geschäftslogik und -prozesse auslösen. Wenn Datensätze in eine DocumentDB-Auflistung eingefügt, aktualisiert oder gelöscht werden, wirken sich diese Änderungen als Ereignisse aus, die automatisch verschiedene nachgelagerte Prozesse, Benachrichtigungen oder Datensynchronisierungsaufgaben auslösen. Dieses Muster ist besonders nützlich in modernen verteilten Systemen, in denen mehrere Anwendungen oder Dienste in Echtzeit auf Datenänderungen reagieren müssen. Der Hauptmechanismus für die Implementierung ereignisgesteuerter Programmierung in DocumentDB sind Change-Streams.

> **Note**
>
> In diesem Handbuch wird davon ausgegangen, dass Sie Change-Streams für eine Sammlung aktiviert haben, mit der Sie arbeiten. Weitere Informationen Change-Streams mit Amazon DocumentDB verwenden zum Aktivieren von Change-Streams in der Sammlung finden Sie unter.

Arbeiten mit Change-Streams aus der Java-Anwendung

Die `watch()` Methode im Java-Treiber von MongoDB ist der wichtigste Mechanismus zur Überwachung von Datenänderungen in Echtzeit in Amazon DocumentDB. Die `watch()` Methode kann von Objekten `MongoClient` `MongoDatabase`, und `MongoCollection`aufgerufen werden.

Die `watch()` Methode gibt eine Instanz zurück `ChangeStreamIterable`, die verschiedene Konfigurationsoptionen unterstützt, darunter die vollständige Suche nach Aktualisierungen in Dokumenten, die Bereitstellung von Wiederaufnahmetokens und Zeitstempeln für die Zuverlässigkeit sowie Pipeline-Aggregationsphasen zum Filtern von Änderungen.

`ChangeStreamIterable`implementiert die Java-Kernschnittstelle `Iterable` und kann mit verwendet werden. `forEach()` Um Ereignisse mithilfe von zu erfassen`forEach()`, übergeben Sie eine Callback-Funktion an`forEach()`, die das geänderte Ereignis verarbeitet. Der folgende

Codeausschnitt zeigt, wie Sie einen Change-Stream für eine Sammlung öffnen, um die Überwachung von Änderungsereignissen zu starten:

```
ChangeStreamIterable < Document > iterator = collection.watch();
iterator.forEach(event - > {
    System.out.println("Received a change: " + event);
});
```

Eine andere Möglichkeit, alle Änderungsereignisse zu durchlaufen, besteht darin, einen Cursor zu öffnen, der eine Verbindung zum Cluster aufrechterhält und kontinuierlich neue Änderungsereignisse empfängt, sobald sie auftreten. Um einen Change-Streams-Cursor zu erhalten, verwenden Sie die `cursor()` Methode object. `ChangeStreamIterable` Das folgende Codebeispiel zeigt, wie Änderungsereignisse mithilfe des Cursors überwacht werden:

```
try (MongoChangeStreamCursor < ChangeStreamDocument < Document >> cursor =
 collection.watch().cursor()) {
    System.out.println(cursor.tryNext());
}
```

Es hat sich bewährt, entweder die Anweisung `MongoChangeStreamCursor`in einer Try-with-Resource-Anweisung zu erstellen oder den Cursor manuell zu schließen. Beim Aufrufen der `cursor()` Methode on wird eine `ChangeStreamIterable`zurückgegeben`MongoChangeStreamCursor`, die über einem Objekt erstellt wurde. `ChangeStreamDocument`

Die `ChangeStreamDocument`Klasse ist eine wichtige Komponente, die einzelne Änderungsereignisse im Stream darstellt. Sie enthält detaillierte Informationen zu jeder Änderung, einschließlich des Vorgangstyps (Einfügen, Aktualisieren, Löschen, Ersetzen), des Dokumentschlüssels, der Namespace-Informationen und des vollständigen Dokumentinhalts, sofern verfügbar. Die Klasse bietet Methoden für den Zugriff auf verschiedene Aspekte des Änderungsereignisses, z. B. `getOperationType()` für die Bestimmung der Art der Änderung, für den `getFullDocument()` Zugriff auf den vollständigen Status des Dokuments und `getDocumentKey()` für die Identifizierung des geänderten Dokuments.

Das `ChangeStreamDocument`Objekt stellt zwei wichtige Informationen bereit: ein Wiederaufnahme-Token und die Uhrzeit des Änderungsereignisses.

Resume-Tokens und zeitbasierte Operationen in DocumentDB-Change-Streams bieten wichtige Mechanismen für die Aufrechterhaltung der Kontinuität und die Verwaltung des Zugriffs auf

historische Daten. Ein Resume-Token ist eine eindeutige Kennung, die für jedes Änderungsereignis generiert wird. Sie dient als Lesezeichen, mit dem Anwendungen die Verarbeitung von Change-Streams nach Verbindungsabbrüchen oder Ausfällen an einem bestimmten Punkt wieder aufnehmen können. Wenn ein Change-Stream-Cursor erstellt wird, kann er über `resumeAfter()` diese Option ein zuvor gespeichertes Resume-Token verwenden, sodass der Stream dort weitergeführt werden kann, wo er aufgehört hat, anstatt am Anfang zu beginnen oder Ereignisse zu verlieren.

Time-based Operationen in Change-Streams bieten unterschiedliche Ansätze, um den Ausgangspunkt der Überwachung von Änderungsereignissen zu verwalten. Mit dieser `startAtOperationTime()` Option können Sie beginnen, Änderungen zu beobachten, die zu oder nach einem bestimmten Zeitstempel eingetreten sind. Diese zeitbasierten Funktionen sind besonders nützlich in Szenarien, in denen historische Daten verarbeitet, zeitpunktbezogene Wiederherstellung oder Synchronisation zwischen Systemen erforderlich sind.

Im folgenden Codebeispiel wird das Ereignis abgerufen, das mit dem Einfügedokument verknüpft ist, dessen Resume-Token erfasst und dann dieses Token bereitgestellt, um die Überwachung auf Ereignisse nach dem Einfügeereignis zu starten. Das Ereignis wird dem Aktualisierungsereignis zugeordnet, ruft dann die Clusterzeit ab, zu der die Aktualisierung stattgefunden hat, und verwendet diesen Zeitstempel als Ausgangspunkt für die weitere Verarbeitung.

```
BsonDocument resumeToken;
BsonTimestamp resumeTime;

try (MongoChangeStreamCursor < ChangeStreamDocument < Document >> cursor =
 collection.watch().cursor()) {
    System.out.println("****************** Insert Document ******************");
    ChangeStreamDocument < Document > insertChange = cursor.tryNext();
    resumeToken = insertChange.getResumeToken();
    printJson(cursor.tryNext());
}
try (MongoChangeStreamCursor < ChangeStreamDocument < Document >> cursor =
 collection.watch()
    .resumeAfter(resumeToken)
    .cursor()) {
    System.out.println("****************** Update Document ******************");
    ChangeStreamDocument < Document > insertChange = cursor.tryNext();
    resumeTime = insertChange.getClusterTime();
    printJson(cursor.tryNext());
}
try (MongoChangeStreamCursor < ChangeStreamDocument < Document >> cursor =
 collection.watch()
```

```
    .startAtOperationTime(resumeTime)
    .cursor()) {
    System.out.println("****************** Delete Document ******************");
    printJson(cursor.tryNext());
  }
```

Standardmäßig umfasst das Aktualisierungsänderungsereignis nicht das gesamte Dokument und nur die vorgenommenen Änderungen. Wenn Sie auf das gesamte aktualisierte Dokument zugreifen müssen, können Sie die `fullDocument()` Methode für das `ChangeStreamIterable`Objekt aufrufen. Denken Sie daran, dass, wenn Sie bei einem Aktualisierungsereignis die Rückgabe eines vollständigen Dokuments anfordern, das Dokument zurückgegeben wird, das zum Zeitpunkt des Aufrufs der Change-Streams vorhanden war.

Diese Methode verwendet eine `FullDocument`Aufzählung als Parameter. Derzeit unterstützt Amazon DocumentDB nur DEFAULT und `UPDATE_LOOKUP` Werte. Der folgende Codeausschnitt zeigt, wie Sie das vollständige Dokument für Aktualisierungsereignisse anfordern, wenn Sie beginnen, nach Änderungen zu suchen:

```
try (MongoChangeStreamCursor < ChangeStreamDocument < Document >> cursor =
 collection.watch().fullDocument(FullDocument.UPDATE_LOOKUP).cursor())
```

Verwenden der JSON-Schemavalidierung

Mithilfe des `$jsonSchema` Testabfrageoperators können Sie überprüfen, ob Dokumente in Ihre Sammlungen eingefügt werden.

Topics

- JSON-Schemavalidierung erstellen und verwenden
- Unterstützte Schlüsselwörter
- umgehen DocumentValidation
- Einschränkungen

JSON-Schemavalidierung erstellen und verwenden

Eine Sammlung mit Schemavalidierung erstellen

Sie können eine Sammlung mit `createCollection` Betriebs- und Validierungsregeln erstellen. Diese Validierungsregeln werden beim Einfügen oder Aktualisieren von Amazon DocumentDB

DocumentDB-Dokumenten angewendet. Das folgende Codebeispiel zeigt Validierungsregeln für eine Sammlung von Mitarbeitern:

```
db.createCollection("employees", {
   "validator": {
      "$jsonSchema": {
         "bsonType": "object",
         "title": "employee validation",
         "required": [ "name", "employeeId"],
         "properties": {
            "name": {
                  "bsonType": "object",
                  "properties": {
                     "firstName": {
                        "bsonType": ["string"]
                     },
                     "lastName": {
                        "bsonType": ["string"]
                     }
                  },
                  "additionalProperties" : false
            },
            "employeeId": {
               "bsonType": "string",
               "description": "Unique Identifier for employee"
            },
             "salary": {
               "bsonType": "double"
            },
            "age": {
               "bsonType": "number"
            }
         },
         "additionalProperties" : true
      }
   },
   "validationLevel": "strict", "validationAction": "error"
} )
```

Ein gültiges Dokument einfügen

Im folgenden Beispiel werden Dokumente eingefügt, die den oben genannten Schemavalidierungsregeln entsprechen:

```
db.employees.insert({"name" : { "firstName" : "Carol" , "lastName" : "Smith"},
 "employeeId": "c720a" , "salary": 1000.0 })
db.employees.insert({ "name" : { "firstName" : "William", "lastName" : "Taylor" },
 "employeeId" : "c721a", "age" : 24})
```

Ein ungültiges Dokument wird eingefügt

Im folgenden Beispiel werden Dokumente eingefügt, die den obigen Schemavalidierungsregeln nicht entsprechen. In diesem Beispiel ist der EmployeeID-Wert keine Zeichenfolge:

```
db.employees.insert({
    "name" : { "firstName" : "Carol" , "lastName" : "Smith"},
    "employeeId": 720 ,
    "salary": 1000.0
})
```

Dieses Beispiel zeigt eine falsche Syntax innerhalb des Dokuments.

Eine Sammlung ändern

Der `collMod` Befehl wird verwendet, um Validierungsregeln einer vorhandenen Sammlung hinzuzufügen oder zu ändern. Im folgenden Beispiel wird der Liste der erforderlichen Felder ein Gehaltsfeld hinzugefügt:

```
db.runCommand({"collMod" : "employees",
   "validator": {
      "$jsonSchema": {
         "bsonType": "object",
         "title": "employee validation",
         "required": [ "name", "employeeId", "salary"],
         "properties": {
            "name": {
                  "bsonType": "object",
                  "properties": {
                     "firstName": {
                        "bsonType": ["string"]
                     },
                     "lastName": {
                        "bsonType": ["string"]
                     }
                  },
                  "additionalProperties" : false
```

```
            },
            "employeeId": {
               "bsonType": "string",
               "description": "Unique Identifier for employee"
            },
             "salary": {
               "bsonType": "double"
            },
            "age": {
               "bsonType": "number"
            }
         },
         "additionalProperties" : true
      }
   }
} )
```

Adressierung von Dokumenten, die vor der Änderung der Validierungsregeln hinzugefügt wurden

Verwenden Sie die folgenden `validationLevel` Modifikatoren, um Dokumente zu adressieren, die Ihrer Sammlung hinzugefügt wurden, bevor die Validierungsregeln geändert wurden:

- Strikt: Wendet Validierungsregeln auf alle Einfügungen und Aktualisierungen an.
- moderat: Wendet Validierungsregeln auf bestehende gültige Dokumente an. Bei Aktualisierungen werden vorhandene ungültige Dokumente nicht überprüft.

Im folgenden Beispiel ist nach der Aktualisierung der Validierungsregeln für die Sammlung mit dem Namen „Mitarbeiter“ das Feld Gehalt erforderlich. Die Aktualisierung des folgenden Dokuments schlägt fehl:

```
db.runCommand({
    update: "employees",
    updates: [{
        q: { "employeeId": "c721a" },
        u: { age: 25 , salary : 1000},
        upsert: true }]
})
```

Amazon DocumentDB gibt die folgende Ausgabe zurück:

```
{
```

```
"n" : 0,
    "nModified" : 0,
    "writeErrors" : [
        {
"index" : 0,
            "code" : 121,
            "errmsg" : "Document failed validation"
        }
    ],
    "ok" : 1,
    "operationTime" : Timestamp(1234567890, 1)
}
```

Wenn Sie die Validierungsstufe `moderate` auf aktualisieren, kann das obige Dokument erfolgreich aktualisiert werden:

```
db.runCommand({
    "collMod" : "employees",
    validationLevel : "moderate"
})

db.runCommand({
    update: "employees",
    updates: [{
        q: { "employeeId": "c721a" },
        u: { age: 25 , salary : 1000},
        upsert: true }]
})
```

Amazon DocumentDB gibt die folgende Ausgabe zurück:

```
{
"n" : 1,
    "nModified" : 1,
    "ok" : 1,
    "operationTime" : Timestamp(1234567890, 1)
}
```

Dokumente werden mit dem $JsonSchema abgerufen

Der `$jsonSchema` Operator kann als Filter verwendet werden, um Dokumente abzufragen, die dem JSON-Schema entsprechen. Dies ist ein Operator der obersten Ebene, der in Filterdokumenten

als Feld der obersten Ebene vorhanden sein oder mit Abfrageoperatoren wie andor, und $nor verwendet werden kann. Die folgenden Beispiele zeigen die Verwendung von $jsonSchema als Einzelfilter und mit anderen Filteroperatoren:

Dokument, das in eine Sammlung „Mitarbeiter“ eingefügt wurde:

```
{ "name" : { "firstName" : "Carol", "lastName" : "Smith" }, "employeeId" : "c720a",
 "salary" : 1000 }
{ "name" : { "firstName" : "Emily", "lastName" : "Brown" }, "employeeId" : "c720b",
 "age" : 25, "salary" : 1050.2 }
{ "name" : { "firstName" : "William", "lastName" : "Taylor" }, "employeeId" : "c721a",
 "age" : 24, "salary" : 1400.5 }
{ "name" : { "firstName" : "Jane", "lastName" : "Doe" }, "employeeId" : "c721a",
 "salary" : 1300 }
```

Sammlung wurde nur mit dem $jsonSchema Operator gefiltert:

```
db.employees.find({
       $jsonSchema: { required: ["age"] } })
```

Amazon DocumentDB gibt die folgende Ausgabe zurück:

```
{ "_id" : ObjectId("64e5f91c6218c620cf0e8f8b"), "name" : { "firstName" : "Emily",
 "lastName" : "Brown" }, "employeeId" : "c720b", "age" : 25, "salary" : 1050.2 }
{ "_id" : ObjectId("64e5f94e6218c620cf0e8f8c"), "name" : { "firstName" : "William",
 "lastName" : "Taylor" }, "employeeId" : "c721a", "age" : 24, "salary" : 1400.5 }
```

Sammlung, die mit dem $jsonSchema Operator und einem anderen Operator gefiltert wurde:

```
db.employees.find({
       $or: [{ $jsonSchema: { required: ["age", "name"]}},
            { salary: { $lte:1000}}]});
```

Amazon DocumentDB gibt die folgende Ausgabe zurück:

```
{ "_id" : ObjectId("64e5f8886218c620cf0e8f8a"), "name" : { "firstName" : "Carol",
 "lastName" : "Smith" }, "employeeId" : "c720a", "salary" : 1000 }
{ "_id" : ObjectId("64e5f91c6218c620cf0e8f8b"), "name" : { "firstName" : "Emily",
 "lastName" : "Brown" }, "employeeId" : "c720b", "age" : 25, "salary" : 1050.2 }
```

```
{ "_id" : ObjectId("64e5f94e6218c620cf0e8f8c"), "name" : { "firstName" : "William",
 "lastName" : "Taylor" }, "employeeId" : "c721a", "age" : 24, "salary" : 1400.5 }
```

Sammlung, die mit dem `$jsonSchema` Operator und mit dem `$match` im Aggregatfilter enthaltenen Filter gefiltert wurde:

```
db.employees.aggregate(
    [{ $match: {
        $jsonSchema: {
            required: ["name", "employeeId"],
            properties: {"salary" :{"bsonType": "double"}}
        }
       }
    }]
)
```

Amazon DocumentDB gibt die folgende Ausgabe zurück:

```
{
"_id" : ObjectId("64e5f8886218c620cf0e8f8a"),
 "name" : { "firstName" : "Carol", "lastName" : "Smith" },
"employeeId" : "c720a",
"salary" : 1000
}
{
"_id" : ObjectId("64e5f91c6218c620cf0e8f8b"),
"name" : { "firstName" : "Emily", "lastName" : "Brown" },
"employeeId" : "c720b",
"age" : 25,
"salary" : 1050.2
}
{
"_id" : ObjectId("64e5f94e6218c620cf0e8f8c"),
"name" : { "firstName" : "William", "lastName" : "Taylor" },
"employeeId" : "c721a",
"age" : 24,
"salary" : 1400.5
}
{
"_id" : ObjectId("64e5f9786218c620cf0e8f8d"),
"name" : { "firstName" : "Jane", "lastName" : "Doe" },
"employeeId" : "c721a",
"salary" : 1300
```

```
}
```

Bestehende Validierungsregeln anzeigen

Um die vorhandenen Validierungsregeln für eine Sammlung zu sehen, verwenden Sie:

```
db.runCommand({
    listCollections: 1,
    filter: { name: 'employees' }
})
```

Amazon DocumentDB gibt die folgende Ausgabe zurück:

```
{
    "waitedMS" : NumberLong(0),
    "cursor" : {
        "firstBatch" : [
            {
                "name" : "employees",
                "type" : "collection",
                "options" : {
                    "autoIndexId" : true,
                    "capped" : false,
                    "validator" : {
                        "$jsonSchema" : {
                            "bsonType" : "object",
                            "title" : "employee validation",
                            "required" : [
                                "name",
                                "employeeId",
                                "salary"
                            ],
                            "properties" : {
                                "name" : {
                                    "bsonType" : "object",
                                    "properties" : {
                                        "firstName" : {
                                            "bsonType" : [
                                                "string"
                                            ]
                                        },
                                        "lastName" : {
                                            "bsonType" : [
```

```
                                        "string"
                                    ]
                                }
                            },
                            "additionalProperties" : false
                        },
                        "employeeId" : {
                            "bsonType" : "string",
                            "description" : "Unique Identifier for employee"
                        },
                        "salary" : {
                            "bsonType" : "double"
                        },
                        "age" : {
                            "bsonType" : "number"
                        }
                    },
                    "additionalProperties" : true
                }
            },
            "validationLevel" : "moderate",
            "validationAction" : "error"
        },
        "info" : {
            "readOnly" : false
        },
        "idIndex" : {
            "v" : 2,
            "key" : {
                "_id" : 1
            },
            "name" : "_id_",
            "ns" : "test.employees"
        }
    }
],
"id" : NumberLong(0),
"ns" : "test.$cmd.listCollections"
},
"ok" : 1,
"operationTime" : Timestamp(1692788937, 1)
}
```

Amazon DocumentDB behält auch die Validierungsregeln in der `$out` Aggregationsphase bei.

Unterstützte Schlüsselwörter

Die folgenden Felder werden in den `collMod` Befehlen `create` und unterstützt:

- **`Validator`**— Unterstützt den `$jsonSchem` Operator a.
- **`ValidationLevel`**— Unterstützt `moderate` Werte `offstrict`, und.
- **`ValidationAction`**— Unterstützt den `error` Wert.

Der $jsonSchema-Operator unterstützt die folgenden Schlüsselwörter:

- `additionalItems`
- `additionalProperties`
- `allOf`
- `anyOf`
- `bsonType`
- `dependencies`
- `description`
- `enum`
- `exclusiveMaximum`
- `exclusiveMinimum`
- `items`
- `maximum`
- `minimum`
- `maxItems`
- `minItems`
- `maxLength`
- `minLength`
- `maxProperties`
- `minProperties`
- `multipleOf`
- `not`

- `oneOf`
- `pattern`
- `patternProperties`
- `properties`
- `required`
- `title`
- `type`
- `uniqueItems`

umgehen DocumentValidation

Amazon DocumentDB unterstützt by`passDocumentValidation` die folgenden Befehle und Methoden:

- `insert`
- `update`
- `findAndModify`
- `$out`Stufe im `aggregate` Befehl und in der Methode `db.collection.aggregate()`

Amazon DocumentDB unterstützt die folgenden Befehle nicht für`bypassDocumentValidation`:

- `$merge`im `aggregate` Befehl und in der Methode `db.collection.aggregate()`
- `mapReduce`Befehl und `db.collection.mapReduce()` Methode
- `applyOps` command

Einschränkungen

Für die `$jsonSchema` Validierung gelten die folgenden Einschränkungen:

- Amazon DocumentDB gibt den Fehler „Dokument konnte nicht validiert werden“ zurück, wenn ein Vorgang die Validierungsregel nicht erfüllt.
- Elastische Amazon DocumentDB-Cluster werden nicht unterstützt`$jsonSchema`.

Amazon DocumentDB Kontingente und Beschränkungen

In diesem Thema werden die Ressourcenkontingente, Grenzwerte und Namensbeschränkungen für Amazon DocumentDB (mit MongoDB-Kompatibilität) beschrieben.

Für bestimmte Verwaltungsfunktionen verwendet Amazon DocumentDB Betriebstechnologie, die mit Amazon Relational Database Service (Amazon RDS) und Amazon Neptune gemeinsam genutzt wird.

Themen

- Unterstützte Instance-Typen
- Unterstützte -Regionen
- Regionale Kontingente
- Aggregationsgrenzen
- Cluster-Grenzwerte
- Instance-Limits
- Benennungseinschränkungen:
- TTL-Einschränkungen
- Elastische Cluster-Grenzwerte
- Limits für elastische Cluster-Shards
- CPU-, Speicher-, Verbindungs- und Cursorlimits für Elastic Cluster pro Shard

Unterstützte Instance-Typen

Amazon DocumentDB unterstützt On-Demand-Instances und die folgenden Instance-Typen:

- NVMe-backed:
  - R6GD-Instance-Typen:`db.r6gd.xlarge`,,`db.r6gd.2xlarge`,`db.r6gd.4xlarge`,`db.r6gd.8xlarge`. `db.r6gd.12xlarge` `db.r6gd.16xlarge`
- RAM-optimiert:
  - R8G-Instanztypen:`db.r8g.large`,,,,`db.r8g.xlarge`,`db.r8g.2xlarge`,`db.r8g.4xlarge`,`db.r8g.8xla` `db.r8g.12xlarge` `db.r8g.16xlarge` `db.r8g.24xlarge`

  - R6G-Instanztypen:`db.r6g.large`,,,,`db.r6g.xlarge`,`db.r6g.2xlarge`,`db.r6g.4xlarge`. `db.r6g.8xlarge` `db.r6g.12xlarge` `db.r6g.16xlarge`
  - R5-Instance-Typen:`db.r5.large`,,`db.r5.xlarge`,`db.r5.2xlarge`,`db.r5.4xlarge`,`db.r5.8xlarge`. `db.r5.12xlarge` `db.r5.16xlarge`
  - R4-Instance-Typen: `db.r4.large`, `db.r4.2xlarge`, `db.r4.4xlarge`, `db.r4.8xlarge`, `db.r4.16xlarge`.
- Überragende Leistung:
  - T4G-Instanztypen:. `db.t4g.medium`
  - T3-Instanztypen:. `db.t3.medium`

Weitere Informationen zu den unterstützten Instance-Typen und deren Spezifikationen finden Sie unter Spezifikationen der Instanzklasse.

Unterstützte -Regionen

Amazon DocumentDB ist in den folgenden AWS Regionen verfügbar:

Name der Region	Region	Verfügbarkeitszonen (Compute)
USA Ost (Ohio)	`us-east-2`	3
USA Ost (Nord-Virginia)	`us-east-1`	6
USA West (Oregon)	`us-west-2`	4
Afrika (Kapstadt)	`af-south-1`	3
Südamerika (São Paulo)	`sa-east-1`	3
Asien-Pazifik (Hongkong)	`ap-east-1`	3
Asien-Pazifik (Hyderabad)	`ap-south-2`	3
Asien-Pazifik (Malaysia)	`ap-southeast-5`	3
Asien-Pazifik (Mumbai)	`ap-south-1`	3
Asien-Pazifik (Osaka)	`ap-northeast-3`	3
Asien-Pazifik (Seoul)	`ap-northeast-2`	4
Asien-Pazifik (Singapur)	`ap-southeast-1`	3
Asien-Pazifik (Sydney)	`ap-southeast-2`	3

Name der Region	Region	Verfügbarkeitszonen (Compute)
Asien-Pazifik (Jakarta)	ap-southeast-3	3
Asien-Pazifik (Melbourne)	ap-southeast-4	3
Asien-Pazifik (Thailand)	ap-southeast-7	3
Asien-Pazifik (Tokio)	ap-northeast-1	3
Kanada (Zentral)	ca-central-1	3
Kanada West (Calgary)	ca-west-1	3
Region China (Peking)	cn-north-1	3
China (Ningxia)	cn-northwest-1	3
Europa (Frankfurt)	eu-central-1	3
Europa (Zürich)	eu-central-2	3
Europa (Irland)	eu-west-1	3
Europa (London)	eu-west-2	3
Europa (Milan)	eu-south-1	3
Europa (Paris)	eu-west-3	3
Europa (Spain)	eu-south-2	3
Europa (Stockholm)	eu-north-1	3
Mexiko (Zentral)	mx-central-1	3

Name der Region	Region	Verfügbarkeitszonen (Compute)
Naher Osten (VAE)	`me-central-1`	3
Israel (Tel Aviv)	`il-central-1`	3
AWS GovCloud (US-West)	`us-gov-west-1`	3
AWS GovCloud (US-East)	`us-gov-east-1`	3

Regionale Kontingente

Für bestimmte Verwaltungsfunktionen verwendet Amazon DocumentDB eine Betriebstechnologie, die mit Amazon Relational Database Service (Amazon RDS) gemeinsam genutzt wird. Die folgende Tabelle enthält regionale Beschränkungen, die von Amazon DocumentDB und Amazon RDS gemeinsam genutzt werden.

> **Note**
>
> Die oben beschriebene gemeinsame Amazon RDS-Technologie gilt nur für Amazon DocumentDB DocumentDB-Instance-basierte Cluster. Elastische Amazon DocumentDB-Cluster teilen sich keine Technologie mit Amazon RDS.

Die folgenden Beschränkungen gelten für Amazon DocumentDB DocumentDB-Instance-basierte Cluster und gelten pro AWS Konto und Region.

Ressource	AWS Standardlimit
Cluster	40
Cluster-Parametergruppen	50
Cluster pro Parametergruppe	100
Instanzen pro Parametergruppe	300

Ressource	AWS Standardlimit
Ereignisabonnements	20
Instances	40
Manuelle Cluster-Snapshots	100
Read Replicas pro Cluster	15
Subnetzgruppen	50
Subnetze pro Subnetzgruppe	20
Tags pro Ressource	50
VPC-Sicherheitsgruppen pro Instance	5

Die folgenden Beschränkungen gelten für elastische Amazon DocumentDB-Cluster und gelten pro AWS Konto und Region.

Ressource	AWS Standardlimit
Elastische Cluster	20
Elastische Cluster vCPU	1024
Manueller elastischer Cluster-Snapshot	20

Sie können mit Service Quotas eine Erhöhung für ein Kontingent beantragen, sofern das Kontingent anpassbar ist. Einige Anfragen werden automatisch gelöst, während andere an gesendet werden Support. Sie können den Status eines Antrags auf Erhöhung des Kontingents verfolgen, der an eingereicht wurde Support. Anfragen zur Erhöhung der Servicekontingente erhalten keinen bevorzugten Support. Wenn Sie eine dringende Anfrage haben, wenden Sie sich an Support. Weitere Informationen zu Service Quotas finden Sie unter What Is Service Quotas?.

Um eine Erhöhung des Kontingents für Amazon DocumentDB zu beantragen:

1. Öffnen Sie die Service Quotas-Konsole unter https://console.aws.amazon.com/servicequotas und melden Sie sich bei Bedarf an.
2. Wählen Sie im Navigationsbereich AWS -Services.
3. Wählen Sie Amazon DocumentDB (mit MongoDB-Kompatibilität) oder Amazon DocumentDB Elastic Cluster aus der Liste aus, oder geben Sie eines davon in das Suchfeld ein.
4. Wenn das Kontingent einstellbar ist, können Sie sein Optionsfeld oder seinen Namen auswählen und dann rechts oben auf der Seite die Option Request quota increase (Kontingenterhöhung beantragen) auswählen.
5. Geben Sie unter Change quota value (Kontingentwert ändern) den neuen Wert ein. Der neue Wert muss größer als der aktuelle Wert sein.
6. Wählen Sie Anfrage aus. Nachdem die Anfrage genehmigt wurde, wird Applied quota value (Angewandter Kontingentwert) für das Kontingent auf den neuen Wert eingestellt.
7. Um ausstehende oder kürzlich genehmigte Anfragen anzuzeigen, wählen Sie im Navigationsbereich die Option Dashboard . Wählen Sie für ausstehende Anfragen den Status der Anfrage, um die Anfrage zu öffnen. Der Anfangsstatus einer Anfrage ist `Pending`. Nachdem sich der Status auf geändert hat`Quota requested`, sehen Sie die Fallnummer mit. Support Wählen Sie die Fallnummer, um das Ticket für Ihre Anfrage zu öffnen.

Aggregationsgrenzen

In der folgenden Tabelle werden die Aggregationsbeschränkungen in Amazon DocumentDB beschrieben.

Ressource	Limit
Maximale Anzahl der unterstützten Stages	500

Cluster-Grenzwerte

In der folgenden Tabelle werden die auf Amazon DocumentDB DocumentDB-Instanzen basierenden Clustergrenzwerte beschrieben.

Ressource	Limit
Cluster-Größe (Summe aller Sammlungen und Indizes)	128 TiB
Sammlungsgröße (die Summe aller Sammlungen darf das Cluster-Limit nicht überschreiten) — beinhaltet nicht die Indexgröße	32 TiB
Sammlungen pro Cluster	100 000
Datenbanken pro Cluster	100 000
Datenbankgröße (Summe aller Datenbanken darf die Cluster-B eschränkung nicht überschreiten)	128 TiB
Verschachtelungstiefe für Dokumente	200 Stufen
Dokumentengröße	16 MiB
Indexschlüsselgröße	2048 Bytes
Indizes pro Sammlung	64
Schlüssel in einem zusammengesetzten Index	32

Ressource	Limit
Maximale Anzahl der Schreibvorgänge in einem einzelnen Stapelbefehl	100 000
Anzahl Benutzer pro Cluster	1000

Instance-Limits

In der folgenden Tabelle werden die Amazon DocumentDB DocumentDB-Grenzwerte pro Instance beschrieben.

Amazon DocumentDB 8.0

Instance-Typ	Instanzspeicher (GiB)	Verbindungen (alle)	Cursorlimit	Transaktionen öffnen	Verbindungen (aktiv)
T3.medium	4	1000	30	50	102
T4G.medium	4	1000	30	50	102
R5.large	16	3400	450	200	1100
R5.xlarge	32	7000	450	400	2700
R5.2xlarge	64	14200	450	800	4500
R5.4xlarge	128	28400	760	1600	4500
R5.8xlarge	256	60000	1520	3200	4500
R5.12xlarge	384	60000	2280	4800	4500
R5.16xlarge	512	60000	3040	6400	4500
R6G.large*	16	3400	450	200	1100
R6G.xlarge*	32	7000	450	400	2700
R6G.2xlarge*	64	14200	450	800	4500
R6G.4xlarge*	128	28400	760	1600	4500
R6G.8xlarge*	256	60000	1520	3200	4500

Instance-Typ	Instanzspeicher (GiB)	Verbindungen (alle)	Cursorlimit	Transaktionen öffnen	Verbindungen (aktiv)
R6G.12xlarge*	384	60000	2280	4800	4500
R6G.16xlarge*	512	60000	3040	6400	4500
R8G.large	16	3400	450	200	1100
R8G.xlarge	32	7000	450	400	2700
R8G.2xlarge	64	14200	450	800	4500
R8G.4xlarge	128	28400	760	1600	4500
R8G.8xlarge	256	60000	1520	3200	4500
R8G.12xlarge	384	60000	2280	4800	4500
R8G.16xlarge	512	60000	3040	6400	4500
R8G.24xlarge	768	60000	4560	9600	4500

* einschließlich R6GD

Amazon DocumentDB 5.0

Instance-Typ	Instanzspeicher (GiB)	Verbindungen (alle)	Cursorlimit	Transaktionen öffnen	Verbindungen (aktiv)
T3.medium	4	1000	30	50	102
T4G.medium	4	1000	30	50	102
R5.large	16	3400	450	200	1100

Instance-Typ	Instanzspeicher (GiB)	Verbindungen (alle)	Cursorlimit	Transaktionen öffnen	Verbindungen (aktiv)
R5.xlarge	32	7000	450	400	2700
R5.2xlarge	64	14200	450	800	4500
R5.4xlarge	128	28400	760	1600	4500
R5.8xlarge	256	60000	1520	3200	4500
R5.12xlarge	384	60000	2280	4800	4500
R5.16xlarge	512	60000	3040	6400	4500
R6G.large*	16	3400	450	200	1100
R6G.xlarge*	32	7000	450	400	2700
R6G.2xlarge*	64	14200	450	800	4500
R6G.4xlarge*	128	28400	760	1600	4500
R6G.8xlarge*	256	60000	1520	3200	4500
R6G.12xlarge*	384	60000	2280	4800	4500
R6G.16xlarge*	512	60000	3040	6400	4500
R8G.large	16	3400	450	200	1100
R8G.xlarge	32	7000	450	400	2700
R8G.2xlarge	64	14200	450	800	4500
R8G.4xlarge	128	28400	760	1600	4500

Instance-Typ	Instanzspeicher (GiB)	Verbindungen (alle)	Cursorlimit	Transaktionen öffnen	Verbindungen (aktiv)
R8G.8xlarge	256	60000	1520	3200	4500
R8G.12xlarge	384	60000	2280	4800	4500
R8G.16xlarge	512	60000	3040	6400	4500
R8G.24xlarge	768	60000	4560	9600	4500

* einschließlich R6GD

Amazon DocumentDB 4.0

Instance-Typ	Instanzspeicher (GiB)	Verbindungen (alle)	Cursorlimit	Transaktionen öffnen	Verbindungen (aktiv)
T3.medium	4	1000	30	50	102
T4G.medium	4	1000	30	50	102
R5.large	16	3400	450	200	1100
R5.xlarge	32	7000	450	400	2700
R5.2xlarge	64	14200	450	800	4500
R5.4xlarge	128	28400	760	1600	4500
R5.8xlarge	256	60000	1520	3200	4500
R5.12xlarge	384	60000	2280	4800	4500
R5.16xlarge	512	60000	3040	6400	4500
R6G.large*	16	3400	450	200	1100

Instance-Typ	Instanzspeicher (GiB)	Verbindungen (alle)	Cursorlimit	Transaktionen öffnen	Verbindungen (aktiv)
R6G.xlarge*	32	7000	450	400	2700
R6G.2xlarge*	64	14200	450	800	4500
R6G.4xlarge*	128	28400	760	1600	4500
R6G.8xlarge*	256	60000	1520	3200	4500
R6G.12xlarge*	384	60000	2280	4800	4500
R6G.16xlarge*	512	60000	3040	6400	4500

* einschließlich R6GD

Amazon DocumentDB 3.6

Instance-Typ	Instanzspeicher (GiB)	Verbindungen (alle)	Cursorlimit	Transaktionen öffnen	Verbindungen (aktiv)
T3.medium	4	500	30	N/A	102
R4.large	15,25	1700	450	N/A	1100
R4.xlarge	30,5	3400	450	N/A	2700
R4.2xlarge	61	6800	450	N/A	4500
R4.4xlarge	122	13600	725	N/A	4500
R4.8xlarge	288	27200	1450	N/A	4500
R4.16xlarge	488	30000	2900	N/A	4500

Instance-Typ	Instanzspeicher (GiB)	Verbindungen (alle)	Cursorlimit	Transaktionen öffnen	Verbindungen (aktiv)
R5.large	16	1700	450	N/A	1100
R5.xlarge	32	3500	450	N/A	2700
R5.2xlarge	64	7100	450	N/A	4500
R5.4xlarge	128	14200	760	N/A	4500
R5.8xlarge	256	28400	1520	N/A	4500
R5.12xlarge	384	30000	2280	N/A	4500
R5.16xlarge	512	30000	3040	N/A	4500

Mithilfe der folgenden CloudWatch Messwerte können Sie die Limits pro Instanz überwachen und Alarme ausgeben. Weitere Informationen zu Amazon CloudWatch DocumentDB-Metriken finden Sie unterÜberwachen von Amazon DocumentDB mit CloudWatch.

Ressource	CloudWatch Metrik einschränken	CloudWatch Nutzungsmetrik (max. 1 Minute)	CloudWatch Nutzungsmetrik
Instanzspeicher	-	-	FreeableMemory
Verbindungen (alle)	DatabaseConnectionsLimit	DatabaseConnectionsMax	DatabaseConnections
Cursor	DatabaseCursorsLimit	DatabaseCursorsMax	DatabaseCursors
Transaktionen	TransactionsOpenLimit	TransactionsOpenMax	TransactionsOpen

Benennungseinschränkungen:

In der folgenden Tabelle werden Benennungseinschränkungen in Amazon DocumentDB beschrieben.

Ressource	Standardlimit
Cluster-Kennung	• Die Länge beträgt [1—63] Buchstaben, Zahlen oder Bindestriche. • Muss mit einem Buchstaben beginnen. • Darf nicht mit einem Bindestri ch enden oder zwei aufeinand erfolgende Bindestriche enthalten. • Muss für alle Cluster (in Amazon RDS, Amazon Neptune und Amazon DocumentDB) pro AWS Konto und Region eindeutig sein.
Name der Sammlung: `<col>`	Die Länge beträgt [1—57] Zeichen.
Datenbankname: `<db>`	Die Länge beträgt [1—63] Zeichen.
Vollqualifizierter Sammlungsname: `<db>.<col>`	Die Länge beträgt [3—120] Zeichen.
Vollqualifizierter Indexname: `<db>.<col>$<index>`	Die Länge beträgt [6—377] Zeichen.
Indexname: `<col>$<index>`	Die Länge beträgt [3—255] Zeichen.
Instance-ID	• Die Länge beträgt [1—63] Buchstaben, Zahlen oder Bindestriche

Ressource	Standardlimit
	• Muss mit einem Buchstaben beginnen • Darf nicht mit einem Bindestrich enden oder zwei aufeinanderfolgende Bindestriche enthalten • Muss für alle Instances (in Amazon RDS, Amazon Neptune und Amazon DocumentDB) pro AWS Konto und Region eindeutig sein.

Primäres Passwort	• Länge beträgt [8–100] druckbare ASCII-Zeichen.
	• Es können alle druckbaren ASCII-Zeichen mit Ausnahme der folgenden verwendet werden:
	  • **/** (Schrägstrich)
	  • **"** (doppeltes Anführungszeichen)
	  • **@** ('At'-Symbol)

Primärer Nutzername	• Die Länge beträgt [1 bis 63] alphanumerische Zeichen. • Muss mit einem Buchstaben beginnen. • Darf kein Wort sein, das von der Datenbank-Engine reserviert ist.

Ressource	Standardlimit
Parametergruppenname	• Die Länge muss [1 bis 255] alphanumerische Zeichen betragen. • Muss mit einem Buchstaben beginnen. • Darf nicht mit einem Bindestrich enden oder zwei aufeinanderfolgende Bindestriche enthalten.

TTL-Einschränkungen

Es kann nicht garantiert werden, dass Löschoperationen über einem TTL-Index innerhalb eines bestimmten Zeitraums abgeschlossen und mit höchster Priorität behandelt werden. Faktoren wie Ressourcenauslastung der Instance, Dokumentgröße und Gesamtdurchsatz können Einfluss auf die Dauer von TTL-Löschoperationen haben.

Elastische Cluster-Grenzwerte

In der folgenden Tabelle werden die Höchstgrenzen in elastischen Amazon DocumentDB-Clustern beschrieben.

Ressource	Limit
Elastische Cluster pro Region	20
vCPU summiert über alle elastischen Cluster pro Region	1024
Manuelle Cluster-Snapshots pro Region	20
Shards pro Cluster	32
Speicher pro Cluster (wenn die Daten gleichmäßig per Shard-Key verteilt werden)	4 PiB

Ressource	Limit
Verbindungen zum Cluster	Der niedrigere Wert von entweder 300.000 oder die Anzahl der Shards x das Verbindungslimit, das mit vCPU pro Shard verknüpft ist
UnSharded Größe der Sammlung	32 TiB
Größe der Datenerfassung (wenn die Daten gleichmäßig per Shard-Key verteilt werden)	1 PB
Datenbanken pro Cluster	10.000
UnSharded Sammlungen pro Cluster	100 000
Geteilte Sammlungen pro Cluster	1000
Benutzer pro Cluster	100
Schreibt in einem einzigen Batch-Befehl	100 000
Indizes pro Sammlung	64
Verschachtelungstiefe für Dokumente	100 Ebenen
Dokumentengröße	16 MB
Indexschlüsselgröße	2048 Bytes
Schlüssel in einem zusammengesetzten Index	32

Limits für elastische Cluster-Shards

In der folgenden Tabelle werden die maximalen Shard-Limits in elastischen Amazon DocumentDB-Clustern beschrieben.

Ressource	Limit
vCPU pro Shard-Instanz	64

Ressource	Limit
Instanzen pro Shard	16
Speicher pro Shard	128 TiB
Speicherplatz pro Sammlung pro Shard	32 TiB

CPU-, Speicher-, Verbindungs- und Cursorlimits für Elastic Cluster pro Shard

In der folgenden Tabelle werden die maximalen CPU-, Arbeitsspeicher-, Verbindungs- und Cursorlimits in Amazon DocumentDB Elastic Cluster Shards beschrieben.

vCPUs pro Shard	Instanzspeicher (GiB)	Verbindungslimit	Cursorlimit
2	16	1700	450
4	32	3500	450
8	64	7100	450
16	128	14200	760
32	256	28400	1520
48	384	30000	2280
64	512	30000	3040

Abfragen in Amazon DocumentDB

In diesem Abschnitt werden alle Aspekte der Abfrage mit Amazon DocumentDB erklärt.

Themen

- Dokumente abfragen
- Plan abfragen
- Erläutern Sie die Ergebnisse
- Abfrageplaner v2
- Abfrageplaner v3
- Geodaten mit Amazon DocumentDB abfragen
- Teilweiser Index
- Textsuche mit Amazon DocumentDB durchführen

Dokumente abfragen

Manchmal müssen Sie möglicherweise den Bestand Ihres Online-Shops nachschlagen, damit Kunden das Angebot sehen und kaufen können. Die Abfrage einer Sammlung ist relativ einfach, unabhängig davon, ob Sie alle Dokumente in der Sammlung haben möchten oder nur die Dokumente, die ein bestimmtes Kriterium erfüllen.

Verwenden Sie die Operation `find()`, um Dokumente abzufragen. Der Befehl `find()` hat einen einzigen Dokumentenparameter, der die Kriterien für die Auswahl der zurückzugebenden Dokumente definiert. Die Ausgabe von `find()` ist ein Dokument, das als einzelne Textzeile ohne Zeilenumbrüche formatiert ist. Um das Ausgabedokument für eine bessere Lesbarkeit zu formatieren, verwenden Sie `find().pretty()`. Alle Beispiele in diesem Thema verwenden `.pretty()` zum Formatieren der Ausgabe.

In den folgenden Codebeispielen werden die vier Dokumente verwendet, die Sie in den beiden vorangegangenen Übungen in `insertMany()` die `example` Sammlung eingefügt haben. Sie befinden sich im Abschnitt Dokumente hinzufügen von Arbeiten mit Dokumenten. `insertOne()`

Themen

- Alle Dokumente in einer Sammlung werden abgerufen
- Dokumente werden abgerufen, die einem Feldwert entsprechen

- Dokumente werden abgerufen, die einem eingebetteten Dokument entsprechen
- Dokumente werden abgerufen, die einem Feldwert in einem eingebetteten Dokument entsprechen
- Dokumente werden abgerufen, die einem Array entsprechen
- Dokumente werden abgerufen, die einem Wert in einem Array entsprechen
- Dokumente mithilfe von Operatoren abrufen

Alle Dokumente in einer Sammlung werden abgerufen

Um alle Dokumente in Ihrer Sammlung abzurufen, verwenden Sie die Operation `find()` mit einem leeren Abfragedokument.

Die folgende Abfrage gibt alle Dokumente der Sammlung `example` zurück.

```
db.example.find( {} ).pretty()
```

Dokumente werden abgerufen, die einem Feldwert entsprechen

Um alle Dokumente abzurufen, die mit einem Feld und einem Wert übereinstimmen, verwenden Sie die Operation `find()` mit einem Abfragedokument, das die entsprechenden Felder und Werte identifiziert.

Bei Verwendung der vorangegangenen Dokumente gibt diese Abfrage alle Dokumente zurück, bei denen das Feld "Item" (Element) "Pen" (Stift) entspricht.

```
db.example.find( { "Item": "Pen" } ).pretty()
```

Dokumente werden abgerufen, die einem eingebetteten Dokument entsprechen

Um alle Dokumente zu suchen, die mit einem eingebetteten Dokument übereinstimmen, verwenden Sie die Operation `find()` mit einem Abfragedokument, in dem der Name des eingebetteten Dokuments sowie alle Felder und Werte für dieses eingebettete Dokument angegeben werden.

Beim Vergleichen mit einem eingebetteten Dokument muss das eingebettete Dokument denselben Namen haben wie in der Abfrage. Zudem müssen die Felder und Werte im eingebetteten Dokument mit der Abfrage übereinstimmen.

Die folgende Abfrage gibt nur das Dokument "Poster Paint" zurück. Dies liegt daran, dass "Pen" über verschiedene Werte für "`OnHand`" und "`MinOnHand`" verfügt und "Spray Paint" ein weiteres Feld (`OrderQnty`) als das Abfragedokument besitzt.

```
db.example.find({"Inventory": {
    "OnHand": 47,
    "MinOnHand": 50 } } ).pretty()
```

Dokumente werden abgerufen, die einem Feldwert in einem eingebetteten Dokument entsprechen

Um alle Dokumente zu suchen, die mit einem eingebetteten Dokument übereinstimmen, verwenden Sie die Operation `find()` mit einem Abfragedokument, in dem der Name des eingebetteten Dokuments sowie alle Felder und Werte für dieses eingebettete Dokument angegeben werden.

Aufgrund der vorangegangenen Dokumente verwendet die folgende Abfrage "Punktnotation", um das eingebettete Dokument und die Felder von Interesse anzugeben. Jedes Dokument, das damit übereinstimmt, wird zurückgegeben, unabhängig davon, welche anderen Felder im eingebetteten Dokument vorhanden sind. Die Abfrage gibt "Poster Paint" und "Spray Paint" zurück, weil sie beide den angegebenen Feldern und Werten entsprechen.

```
db.example.find({"Inventory.OnHand": 47, "Inventory.MinOnHand": 50 }).pretty()
```

Dokumente werden abgerufen, die einem Array entsprechen

Um alle Dokumente zu finden, die einem Array entsprechen, verwenden Sie die Operation `find()` mit dem Namen des Arrays, an dem Sie interessiert sind, und allen Werten in diesem Array. Die Abfrage gibt alle Dokumente zurück, in denen sich ein Array mit diesem Namen befindet und in denen die Array-Werte identisch sind und die gleiche Reihenfolge wie in der Abfrage aufweisen.

Die folgende Abfrage gibt nur "Pen" zurück, da "Poster Paint" über eine zusätzlichen Farbe (White) verfügt und die Farben in "Spray Paint" in einer anderen Reihenfolge vorliegen.

```
db.example.find( { "Colors": ["Red","Green","Blue","Black"] } ).pretty()
```

Dokumente werden abgerufen, die einem Wert in einem Array entsprechen

Um alle Dokumente mit einem bestimmten Array-Wert zu finden, verwenden Sie die Operation `find()` mit dem Namen und Wert des Arrays, an dem Sie interessiert sind.

```
db.example.find( { "Colors": "Red" } ).pretty()
```

Bei der vorherigen Operation werden alle drei Dokumente zurückgegeben, da jedes davon ein Array mit dem Namen `Colors` und den Wert "`Red`" irgendwo im Array besitzt. Wenn Sie den Wert "`White`" angeben, gibt die Abfrage nur "Poster Paint" zurück.

Dokumente mithilfe von Operatoren abrufen

Die folgende Abfrage gibt alle Dokumente zurück, in denen der Wert "`Inventory.OnHand`" kleiner als 50 ist.

```
db.example.find(
        { "Inventory.OnHand": { $lt: 50 } } )
```

Eine Liste der unterstützten Abfrageoperatoren finden Sie unter Abfrage- und Projektionsoperatoren.

Plan abfragen

Wie kann ich die **`executionStats`** für einen Abfrageplan sehen?

Wenn Sie ermitteln, warum eine Abfrage langsamer als erwartet ausgeführt wird, kann es hilfreich sein zu verstehen, was die `executionStats` für den Abfrageplan sind. Die `executionStats` geben die Anzahl der Dokumente an, die von einer bestimmten Stufe zurückgegeben wurden (`nReturned`), die in jeder Stufe verbrachte Ausführungszeit (`executionTimeMillisEstimate`) und die Zeit, die zum Generieren eines Abfrageplans benötigt wird (`planningTimeMillis`). Wie in den folgenden Abfragebeispielen gezeigt, können Sie die zeitintensivsten Phasen Ihrer Abfrage ermitteln`executionStats`, sodass Sie Ihre Optimierungsbemühungen auf der Grundlage der Ergebnisse von konzentrieren können. Der `executionStats`-Parameter unterstützt derzeit keine `update`- und `delete`-Befehle.

> **Note**
>
> Amazon DocumentDB emuliert die MongoDB 3.6-API auf einer speziell entwickelten Datenbank-Engine, die ein verteiltes, fehlertolerantes, selbstheilendes Speichersystem verwendet. Daher `explain()` können sich die Abfragepläne und die Ausgabe von zwischen Amazon DocumentDB und MongoDB unterscheiden. Kunden, die die Kontrolle über ihren

Abfrageplan wünschen, können den `$hint`-Operator verwenden, um die Auswahl eines bevorzugten Indexes zu erzwingen.

Führen Sie die Abfrage, die Sie verbessern möchten, unter dem Befehl `explain()` wie folgt aus.

```
db.runCommand({explain: {query document}}).
explain("executionStats").executionStats;
```

Im Folgenden finden Sie eine Beispieloperation.

```
db.fish.find({}).limit(2).explain("executionStats");
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus.

```
{
    "queryPlanner" : {
        "plannerVersion" : 1,
        "namespace" : "test.fish",
        "winningPlan" : {
            "stage" : "SUBSCAN",
            "inputStage" : {
                "stage" : "LIMIT_SKIP",
                "inputStage" : {
                    "stage" : "COLLSCAN"
                }
            }
        }
    },
    "executionStats" : {
        "executionSuccess" : true,
        "executionTimeMillis" : "0.063",
        "planningTimeMillis" : "0.040",
        "executionStages" : {
            "stage" : "SUBSCAN",
            "nReturned" : "2",
            "executionTimeMillisEstimate" : "0.012",
            "inputStage" : {
                "stage" : "LIMIT_SKIP",
                "nReturned" : "2",
                "executionTimeMillisEstimate" : "0.005",
```

```
                "inputStage" : {
                    "stage" : "COLLSCAN",
                    "nReturned" : "2",
                    "executionTimeMillisEstimate" : "0.005"
                }
            }
        }
    },
    "serverInfo" : {
        "host" : "enginedemo",
        "port" : 27017,
        "version" : "3.6.0"
    },
    "ok" : 1
}
```

Wenn Sie nur die `executionStats` aus der obigen Abfrage sehen möchten, können Sie den folgenden Befehl verwenden. Bei kleinen Sammlungen kann der Amazon DocumentDB DocumentDB-Abfrageprozessor entscheiden, keinen Index zu verwenden, wenn die Leistungssteigerung vernachlässigbar ist.

```
db.fish.find({}).limit(2).explain("executionStats").executionStats;
```

Cache für den Abfrageplan

Um die Leistung zu optimieren und die Planungsdauer zu verkürzen, speichert Amazon DocumentDB interne Abfragepläne im Cache. Auf diese Weise können Abfragen mit derselben Form direkt mithilfe eines zwischengespeicherten Plans ausgeführt werden.

Dieses Zwischenspeichern kann jedoch manchmal zu einer zufälligen Verzögerung für dieselbe Abfrage führen. Beispielsweise kann eine Abfrage, deren Ausführung normalerweise eine Sekunde dauert, gelegentlich zehn Sekunden dauern. Das liegt daran, dass die Leserinstanz im Laufe der Zeit verschiedene Formen der Abfrage zwischengespeichert hat, wodurch Speicherplatz verbraucht wurde. Wenn Sie diese zufällige Verlangsamung feststellen, müssen Sie nichts unternehmen, um den Speicher freizugeben. Das System verwaltet die Speicherauslastung für Sie, und sobald der Speicher einen bestimmten Schwellenwert erreicht hat, wird er automatisch freigegeben.

Erläutern Sie die Ergebnisse

Wenn Sie Informationen zu Abfrageplänen zurückgeben möchten, unterstützt Amazon DocumentDB den Ausführlichkeitsmodus. `queryPlanner` Die `explain` Ergebnisse geben den ausgewählten Abfrageplan zurück, der vom Optimierer ausgewählt wurde, in einem Format, das dem folgenden ähnelt:

```
{
   "queryPlanner" : {
      "plannerVersion" : <int>,
      "namespace" : <string>,
      "winningPlan" : {
         "stage" : <STAGE1>,
         ...
         "inputStage" : {
            "stage" : <STAGE2>,
            ...
            "inputStage" : {
               ...
            }
         }
      }
   }
}
```

In den folgenden Abschnitten werden allgemeine `explain` Ergebnisse definiert.

Themen

- Phase des Scannens und Filterns
- Schnittmenge im Index
- Vereinigung des Indexes
- Mehrfacher Index intersection/union
- Zusammengesetzter Index
- Phase „Sortieren“
- Gruppenphase

Phase des Scannens und Filterns

Der Optimierer kann einen der folgenden Scans wählen:

COLLSCAN

Bei dieser Phase handelt es sich um einen sequentiellen Sammlungsscan.

```
{
    "stage" : "COLLSCAN"
}
```

ISCAN

In dieser Phase werden die Indexschlüssel gescannt. Der Optimierer kann das Dokument in dieser Phase abrufen, was dazu führen kann, dass später eine FETCH-Phase angehängt wird.

```
db.foo.find({"a": 1})
{
    "stage" : "IXSCAN",
    "direction" : "forward",
    "indexName" : <idx_name>
}
```

FETCH

Wenn der Optimierer Dokumente in einer anderen Phase als IXSCAN abgerufen hat, enthält das Ergebnis eine FETCH-Phase. Die obige IXSCAN-Abfrage kann beispielsweise zu einer Kombination der Stufen FETCH und IXSCAN führen:

```
db.foo.find({"a": 1})
{
    "stage" : "FETCH",
    "inputStage" : {
        "stage" : "IXSCAN",
        "indexName" : <idx_name>
    }
}
```

IXONLYSCAN scannt nur den Indexschlüssel. Beim Erstellen zusammengesetzter Indizes wird FETCH nicht vermieden.

Schnittmenge im Index

IX UND

Amazon DocumentDB kann einen IXAND-Schritt mit einem InputStages-Array von IXSCAN enthalten, wenn es Indexüberschneidungen nutzen kann. Beispielsweise könnten wir eine Ausgabe wie die folgende sehen:

```
{
    "stage" : "FETCH",
    "inputStage" : {
        "stage" : "IXAND",
        "inputStages" : [
            {
                "stage" : "IXSCAN",
                "indexName" : "a_1"
            },
            {
                "stage" : "IXSCAN",
                "indexName" : "b_1"
            }
        ]
    }
}
```

Vereinigung des Indexes

IXOR

Ähnlich wie bei der Indexüberschneidung kann Amazon DocumentDB eine `IXOR` Stufe mit einem `inputStages` Array für den `$or` Operator enthalten.

```
db.foo.find({"$or": [{"a": {"$gt": 2}}, {"b": {"$lt": 2}}]})
```

Für die obige Abfrage könnte die Ausgabe von Explain wie folgt aussehen:

```
{
    "stage" : "FETCH",
    "inputStage" : {
        "stage" : "IXOR",
        "inputStages" : [
            {
                "stage" : "IXSCAN",
                "indexName" : "a_1"
            },
            {
                "stage" : "IXSCAN",
                "indexName" : "b_1"
            }
        ]
    }
}
```

Mehrfacher Index intersection/union

Amazon DocumentDB kann mehrere Indexüberschneidungs- oder Union-Phasen miteinander kombinieren und dann das Ergebnis abrufen. Beispiel:

```
{
    "stage" : "FETCH",
    "inputStage" : {
        "stage" : "IXOR",
        "inputStages" : [
            {
                "stage" : "IXSCAN",
                ...
            },
            {
                "stage" : "IXAND",
                "inputStages" : [
                    {
                        "stage" : "IXSCAN",
                        ...
                    },
                    {
                        "stage" : "IXSCAN",
                        ...
```

```
                    }
                ]
            }
        ]
    }
}
```

Der Indextyp (Sparse, Compound usw.) hat keinen Einfluss auf die Verwendung der Stufen „Indexüberschneidung“ oder „Union“.

Zusammengesetzter Index

Die Verwendung des zusammengesetzten Indexes von Amazon DocumentDB ist nicht auf die ersten Teilmengen indizierter Felder beschränkt. Es kann den Index mit dem Suffixteil verwenden, ist aber möglicherweise nicht sehr effizient.

Beispielsweise `{ a: 1, b: -1 }` kann der zusammengesetzte Index von alle drei folgenden Abfragen unterstützen:

```
db.orders.find( { a: 1 } )
```

```
db.orders.find( { b: 1 } )
```

```
db.orders.find( { a: 1, b: 1 } )
```

Phase „Sortieren“

Wenn es einen Index für die angeforderten Sortierschlüssel gibt, kann Amazon DocumentDB den Index verwenden, um die Reihenfolge abzurufen. In diesem Fall enthält das Ergebnis keine `SORT` Phase, sondern eine `IXSCAN` Phase. Wenn der Optimierer eine einfache Sortierung bevorzugt, wird er eine Phase wie die folgende enthalten:

```
{
    "stage" : "SORT",
    "sortPattern" : {
        "a" : 1,
        "b" : -1
    }
}
```

Gruppenphase

Amazon DocumentDB unterstützt zwei verschiedene Gruppenstrategien:

- `SORT_AGGREGATE`: Aggregat zum Sortieren auf der Festplatte.
- `HASH_AGGREGATE`: Hash-Aggregat im Speicher.

Abfrageplaner v2

Der neue Abfrageplaner für Amazon DocumentDB (Planner Version 2.0) bietet erweiterte Funktionen zur Abfrageoptimierung und verbesserte Leistung. Planner Version 2.0 für Amazon DocumentDB 5.0 bietet eine bis zu 10-fache Leistungsverbesserung gegenüber der Vorgängerversion bei der Verwendung von `find update` Operatoren mit Indizes. Leistungsverbesserungen ergeben sich hauptsächlich aus der Verwendung optimalerer Indexpläne und der Aktivierung der Indexscanunterstützung für Operatoren wie Negationsoperatoren (`$neq`,`$nin`) und verschachtelte Operatoren. `$elementMatch` Abfragen in Planner Version 2.0 werden dank besserer Techniken zur Kostenschätzung, optimierter Algorithmen und verbesserter Stabilität schneller ausgeführt. Planner Version 2.0 unterstützt auch Plan-Cache-Filter-APIs, was die Stabilität von Planner verbessert. Mit dieser Funktion bietet Amazon DocumentDB 5.0 jetzt die Möglichkeit, aus den verschiedenen Versionen von Query Planner auszuwählen.

Topics

- Voraussetzungen
- Planner Version 2.0 als Standard-Abfrageplaner auswählen
- Best Practices
- Einschränkungen
- Verbesserungen bei den Operatoren „Suchen und Aktualisieren“
- Planen Sie die Cache-Filter-API
- Mögliche Verhaltensunterschiede zwischen Planner Version 1.0, 2.0 und MongoDB
- Planner Version 2.0 schließt Verhaltenslücke mit MongoDB

Voraussetzungen

Für Planner Version 2.0 gelten die folgenden Voraussetzungen:

- Planner Version 2.0 ist in allen Regionen verfügbar, in denen Engine-Version 5.0 verfügbar ist.
- Um sich für die Verwendung von Version 2.0 als Standard-Abfrageplaner zu entscheiden, muss Ihr Cluster auf der Engine-Patch-Version 3.0.15902 oder höher von Amazon DocumentDB Version 5.0 installiert sein. Anweisungen zur Aktualisierung auf den neuesten Engine-Versionspatch finden Sie unter. Durchführen eines Patch-Updates für die Engine-Version eines Clusters
- Um Planner Version 2.0 als Standard-Abfrageplaner festzulegen, benötigen Sie IAM-Berechtigungen, um Cluster-Parametergruppen zu aktualisieren.
- Für Amazon DocumentDB 8.0 ist Planner Version 3.0 der Standard-Abfrageplaner. Details dazu finden Sie unter Abfrageplaner v3.

Planner Version 2.0 als Standard-Abfrageplaner auswählen

Gehen Sie wie folgt vor, um 2.0 über die Konsole oder CLI als Standard-Abfrageplaner auszuwählen:

- Folgen Sie den Schritten unterAmazon DocumentDB-Cluster-Parameter ändern, um die Parametergruppe Ihres Clusters zu ändern.
- Ändern Sie für den Parameter mit dem Titel 'PlannerVersion' den Wert auf 2.0, was auf Planner-Version 2.0 hinweist.
- Wählen Sie Sofort anwenden (wenn Sie Beim Neustart anwenden auswählen, wird die Auswahl bis zum nächsten Neustart des Clusters unwirksam).

Best Practices

Verwenden Sie die folgenden bewährten Methoden, um die erwarteten Ergebnisse zu erzielen, wenn Sie Planner Version 2.0 anwenden:

- Wählen Sie in einem globalen Cluster denselben `plannerVersion` Wert (1,0 oder 2,0) in den Cluster-Parametergruppen für beide Regionen aus. Beachten Sie, dass die Auswahl verschiedener Planner-Versionen in primären und sekundären Regionen zu einem inkonsistenten Abfrageverhalten und einer inkonsistenten Leistung führen kann.
- Die Aktualisierung auf Planner Version 2.0 während eines geplanten Wartungsfensters oder in Zeiten mit reduziertem Datenverkehr ist am wenigsten störend, da es zu erhöhten Fehlerraten kommen kann, wenn die Planner-Version geändert wird, während Workloads aktiv ausgeführt werden.
- Planner Version 2.0 funktioniert am besten mit der MongoDB-Shell-Version 5.0.

Einschränkungen

Die folgenden Einschränkungen gelten für Planner Version 2.0:

- Planner Version 2.0 wird in Elastic Clustern nicht unterstützt, da hier auf Planner Version 1.0 zurückgegriffen wird.
- Planner-Version 2.0 wird für Aggregation und unterschiedliche Befehle nicht unterstützt. Stattdessen wird auf Planner Version 1.0 zurückgegriffen.
- Abfragen, die Regex, Textsuche, Geodaten, Jsonschema oder Filter enthalten, werden mit dem Plan-Cache-Filter `$expr` in Planner Version 2.0 nicht unterstützt.

Verbesserungen bei den Operatoren „Suchen und Aktualisieren“

Planner Version 2.0 optimiert grundlegende Operationen wie`find`, `updatedelete`, und `find-and-modify` Befehle. In den folgenden Abschnitten mit Registern werden die erweiterten Funktionen für Indizes sowie die Verbesserungen der Abfrageleistung mit Planner Version 2.0 beschrieben:

Enhanced index support

- Planner Version 2.0 bietet Indexunterstützung für Negationsoperatoren wie `$nin`$ne, `$not {eq}`$not {in}, und sowie und. `$type` `$elemMatch`

```
Sample Document: { "x": 10, "y": [1, 2, 3] }

db.foo.createIndex({ "x": 1, "y": 1 })
db.foo.find({ "x": {$nin: [20, 30] }})
db.foo.find({"x":{ $type: "string" }})

db.foo.createIndex({"x.y": 1})
db.foo.find({"x":{$elemMatch:{"y":{$elemMatch:{"$gt": 3 }}}}})
```

- Planner Version 2.0 verwendet dünnbesetzte Indizes oder partielle Indizes, auch wenn sie nicht im `$exists` Abfrageausdruck enthalten sind.

```
Sample Document: {"name": "Bob", "email": "example@fake.com" }

Using Planner Version 1.0, you can specify the command as shown below:
db.foo.find({email: "example@fake.com", email: {$exists: true}})
```

```
Using Planner Version 2.0, you can specify command without $exists:
db.foo.find({ email: "example@fake.com" })
```

- Planner Version 2.0 verwendet Teilindizes auch dann, wenn die Abfragebedingung nicht genau mit dem Filterausdruck für den Teilindex übereinstimmt.

```
Sample Document: {"name": "Bob", "age": 34}
db.foo.createIndex({"age":1},{partialFilterExpression:{"age":{$lt:50}}})

With Planner Version 1.0, index is used only when the query condition meets the
 partial
 index filter criterion:
     db.foo.find({"age":{$lt:50}})

With Planner Version 2.0, index is used even when the query condition doesn't meet
 the index
criterion:
db.foo.find({"age":{$lt:30}})
```

- Planner Version 2.0 verwendet einen partiellen Indexscan mit $elemMatch-Abfragen.

```
Sample Document: {"name": "Bob", "age": [34,35,36]}
db.foo.createIndex({"age":1},{partialFilterExpression:{"age":{$lt:50,$gt:20}}})
db.foo.find({age:{$elemMatch:{$lt:50,$gt:20}}})
```

- Planner Version 2.0 bietet Unterstützung für Indexscans`$regex`, ohne dass Sie `$hint` in Ihrem Anwendungscode angeben müssen. `$regex`unterstützt nur Indexsuchen nach Präfixen.

```
Sample Document: { "x": [1, 2, 3], "y": "apple" }
db.foo.createIndex({ "x": 1, "y": 1 })
db.foo.find({"y":{ $regex: "^a" }})
```

- Planner Version 2.0 verbessert die Leistung von Abfragen mit Indizes mit mehreren Schlüsseln, wobei Gleichheitsbedingungen für Felder mit mehreren Schlüsseln gelten.

```
Sample Document: {"x": [1, 2, 3],
"y": 5}
db.foo.createIndex({"x": 1, "y":1})
db.foo.find({"x": 2,
"y": {$gt: 1}}).limit(1)
```

- Planner Version 2.0 verbessert die Leistung von Abfragen, die mehrere Filter verwenden, insbesondere bei Sammlungen mit Dokumenten, die größer als 8 KB sind.

```
Sample Document: {"x": 2,
"y": 4,
"z": 9,
"t": 99}
db.foo.find({$and: [{"x": {$gt : 1}, "y": {$gt : 3}, "z": {$lt : 10},
"t":{$lt : 100}}]})
```

- Planner Version 2.0 verbessert die Leistung von Abfragen, wenn der `$in` Operator mit einem zusammengesetzten Index verwendet wird, da die Sortierphase entfällt.

```
Sample Document: {"x": 2,
"y": 4,
"z": 9,
"t": 99}
db.foo.createIndex({"x":1, "y":1})
db.foo.find({"x":2,
"y":$in:[1,2,3,4]}).sort({x:1,y:1})
```

  Es verbessert auch die Leistung von Abfragen, die Mehrschlüsselindizes mit `$in` Elementen verwenden.

```
Sample Document: {"x": [1, 2, 3]}
db.foo.createIndex({"x": 1})
db.foo.find("x":{$in:[>100 elements]})
```

Query performance improvements

- Planner Version 2.0 verbessert die Leistung von Abfragen, die mehrere Filter verwenden, insbesondere bei Sammlungen mit Dokumenten, die größer als 8 KB sind.

```
Sample Document: {"x": 2,
"y": 4,
"z": 9,
"t": 99}
db.foo.find({$and: [{"x": {$gt : 1}, "y": {$gt : 3}, "z": {$lt : 10},
"t":{$lt : 100}}]})
```

- Planner Version 2.0 verbessert die Leistung von Abfragen, wenn der `$in` Operator mit einem zusammengesetzten Index verwendet wird, da die Sortierphase entfällt.

```
Sample Document: {"x": 2,
"y": 4,
"z": 9,
"t": 99}
db.foo.createIndex({"x":1, "y":1})
db.foo.find({"x":2,
"y":$in:[1,2,3,4]}).sort({x:1,y:1})
```

  Es verbessert auch die Leistung von Abfragen, die Mehrschlüsselindizes mit `$in` Elementen verwenden.

```
Sample Document: {"x": [1, 2, 3]}
db.foo.createIndex({"x": 1})
db.foo.find("x":{$in:[>100 elements]})
```

Planen Sie die Cache-Filter-API

> **Note**
>
> Der Textindex wird vom Plan-Cache-Filter nicht unterstützt.

- Planner Version 2.0 bietet Unterstützung für die Indexfilterfunktion, mit der Sie eine Liste von Indizes angeben können, die ein bestimmtes Abfrage-Shape verwenden kann. Auf diese Funktion kann über die API zugegriffen werden und sie kann von der Serverseite aus gesteuert werden. Wenn Sie eine Abfrageregression feststellen, bietet Ihnen diese Funktion eine schnellere und flexiblere Möglichkeit, das Problem zu beheben, ohne Ihren Anwendungscode ändern zu müssen.

```
db.runCommand({ planCacheSetFilter: <collection>, query: <query>,
sort: <sort>, // optional,
indexes: [ <index1>, <index2>, ...],
comment: <any> // optional})
```

  Verwenden Sie den folgenden Befehl, um alle Filter in der Sammlung aufzulisten:

```
db.runCommand(
{
planCacheListFilters: <collection>
}
)
```

Dieser Befehl zeigt alle Indexfilter für die Sammlung an. Beispielausgabe:

```
{
"filters" : [
{
"query" : {a: "@", b: "@"},
"sort" : {a: 1},
"indexes" : [
<index1>,
...
]
},
...
],
"ok": 1
}
```

- Sie können zwei neue Felder aus der `explain` Befehlsausgabe verwenden, um die Indexfilterung von Planner Version 2.0 zu analysieren: `indexFilterSet` und`indexFilterApplied`. `indexFilterSet`ist auf „true“ gesetzt, wenn für die Sammlung ein Indexfilter festgelegt ist, der der Abfrageform entspricht. `indexFilterApplied`dist genau dann auf „true“ gesetzt, wenn die Abfrage einen Indexfilter angewendet und einen Plan ausgewählt hat, der einen Index in der Filterliste verwendet.

  Sie können den Indexfilter mit dem folgenden Befehl löschen:

```
db.runCommand(
{
planCacheClearFilters: <collection>>
query: <query pattern>, // optional
sort: <sort specification>, // optional
comment: <any>. //optional
}
)
```

Verwenden Sie den folgenden Befehl, um alle Filter in der Sammlung „foo“ zu löschen:

```
db.runCommand({planCacheClearFilters: "foo"})
```

Um ein bestimmtes Abfrage-Shape mit beliebiger Sortierung zu löschen, können Sie das Abfrage-Shape aus der Ausgabe von `planCacheListFilters` kopieren und einfügen:

```
db.runCommand({planCacheClearFilters: "foo", query: {a: @}})
```

Um ein bestimmtes Abfrage-Shape mit einem bestimmten Feld zu löschen, nach dem sortiert werden soll, können Sie das Abfrage-Shape aus der Ausgabe von kopieren und einfügen`planCacheListFilters`:

```
db.runCommand({planCacheClearFilters: "foo", query: {a: @},sort: {a: 1}})
```

Mögliche Verhaltensunterschiede zwischen Planner Version 1.0, 2.0 und MongoDB

In einigen Randfällen ist es möglich, dass Planner Version 2.0 Ergebnisse liefert, die geringfügig von den Ergebnissen in MongoDB abweichen. In diesem Abschnitt werden einige Beispiele für diese Möglichkeiten beschrieben.

$(update) and $(projection)

- In einigen Fällen verhalten sich `$(update)` `$(projection)` Operatoren in MongoDB möglicherweise anders als die Planer-Version 1.0 von Amazon DocumentDB. Im Folgenden finden Sie einige Beispiele:

```
db.students_list.insertMany( [ { _id: 5, student_ids: [ 100, 200 ], grades: [ 95,
 100 ], grad_year: [ 2024, 2023 ] } ] )
```

```
db.students_list.updateOne({ student_ids: 100, grades: 100, grad_year: 2024 },
{ $set: { “grad_year.$”: 2025 } }
```

  - Planner Version 1.0 — Feld Updates 2022

  - MongoDB — Feld Updates 2022
  - Planner Version 2.0 — Feld Aktualisierungen 2021
- ```
  db.col.insert({x:[1,2,3]})
  db.col.update({$and:[{x:1},{x:3}]},{$set:{"x.$":500}})
  ```
  - Planner Version 1.0 — Aktualisiert das erste übereinstimmende Element nach dem Zufallsprinzip
  - MongoDB — Aktualisiert nach dem Zufallsprinzip das erste übereinstimmende Element
  - Planner Version 2.0 — Führt keine Aktualisierungen durch
- ```
  db.col.insert({x:[1,2,3]})
  db.col.find()
  ```
  - Planner Version 1.0 — Wählt das passende Element nach dem Zufallsprinzip aus
  - MongoDB — Wählt nach dem Zufallsprinzip das passende Element aus
  - Planner Version 2.0 — Trifft keine Auswahl
- ```
  db.col.insert({x:100})
  db.col.update({x:100},{x:100})
  ```
  - Planner Version 1.0 — Änderungen an der Anzahl modifizierter Änderungen
  - MongoDB — Geänderte Zähländerungen
  - Planner Version 2.0 — Die Anzahl von nModified ändert sich nicht, wenn sie mit demselben Wert aktualisiert wird.
- Wenn der `$(update)` Operator mit verwendet wird`$setOnInsert`, geben Planner Version 1.0 und MongoDB einen Fehler aus, Planner Version 2.0 jedoch nicht.
- Das Umbenennen eines nicht existierenden Felds in `$field` löst in Planner Version 2.0 einen Fehler aus, wohingegen in Planner Version 1.0 und MongoDB keine Updates erzeugt werden.

Index behavior

- Planner Version 2.0 gibt einen Fehler aus, wenn sie mit einem ungeeigneten Index angewendet `$hint` wird, während Planner Version 1.0 und MongoDB dies nicht tun.

  ```
  // Insert
  db.col.insert({x:1})
  ```
  ```

```
db.col.insert({x:2})
db.col.insert({x:3})

// Create index on x with partialFilter Expression {x:{$gt:2}}
db.col.createIndex({x:1},{partialFilterExpression:{x:{$gt:2}}})

// Mongodb allows hint on the following queries
db.col.find({x:1}).hint("x_1")
// result is no documents returned because {x:1} is not indexed by the partial
 index
// Without $hint mongo should return {x:1}, thus the difference in result between
 COLSCAN and IXSCAN

DocumentDB will error out when $hint is applied on such cases.
db.col.find({x:1}).hint("x_1")
Error: error: {
    "ok" : 0,
    "operationTime" : Timestamp(1746473021, 1),
    "code" : 2,
    "errmsg" : "Cannot use Hint for this Query. Index is multi key index , partial
 index or sparse index and query is not optimized to use this index."
}

rs0:PRIMARY> db.runCommand({"planCacheSetFilter": "col", "query": { location:
 {$nearSphere: {$geometry: {type: "Point", coordinates: [1, 1]}}}}, "indexes":
 ["name_1"]})
{
    "ok" : 0,
    "operationTime" : Timestamp(1750815778, 1),
    "code" : 303,
    "errmsg" : "Unsupported query shape for index filter $nearSphere"
}
```

- `$near`kann `$hint({“$natural”:1})` in Planner Version 2.0 nicht verwendet werden.

```
// indexes present are index on x and geo index

rs0:PRIMARY> db.usarestaurants.getIndexes()
[
    {
        "v" : 4,
        "key" : {
            "_id" : 1
        },
```

```
        "name" : "_id_",
        "ns" : "test.usarestaurants"
    },
    {
        "v" : 4,
        "key" : {
            "location" : "2dsphere"
        },
        "name" : "location_2dsphere",
        "ns" : "test.usarestaurants",
        "2dsphereIndexVersion" : 1
    }
]

// Planner Version 2.0 will throw an error when $hint is applied with index "x_1"
rs0:PRIMARY> db.usarestaurants.find({    "location":{       "$nearSphere":{
         "$geometry":{             "type":"Point",             "coordinates":
[                -122.3516,                47.6156             ]          },
          "$minDistance":1,          "$maxDistance":2000       }    } }, {
  "name":1 }).hint({"$natural": 1})
Error: error: {
    "ok" : 0,
    "operationTime" : Timestamp(1746475524, 1),
    "code" : 291,
    "errmsg" : "unable to find index for $geoNear query"
}

// Planner Version 1.0 and MongoDB will not throw an error
 db.usarestaurants.find({    "location":{       "$nearSphere":{
  "$geometry":{             "type":"Point",             "coordinates":[
            -122.3516,                47.6156             ]          },
        "$minDistance":1,          "$maxDistance":2000       }    } }, {
  "name":1 }).hint({"$natural": 1})
{ "_id" : ObjectId("681918e087dadfd99b7f0172"), "name" : "Noodle House" }
```

- Während MongoDB vollständige Regex-Indexscans unterstützt, unterstützt Planner Version 2.0 den Regex-Indexscan nur für Präfixfelder.

```
// index on x
db.col.createIndex({x:1})

// index scan is used only for prefix regexes
rs0:PRIMARY> db.col.find({x: /^x/}).explain()
```

```
{
    "queryPlanner" : {
        "plannerVersion" : 2,
        "namespace" : "test.col",
        "winningPlan" : {
            "stage" : "IXSCAN",
            "indexName" : "x_1",
            "direction" : "forward",
            "indexCond" : {
                "$and" : [
                    {
                        "x" : {
                            "$regex" : /^x/
                        }
                    }
                ]
            },
            "filter" : {
                "x" : {
                    "$regex" : /^x/
                }
            }
        }
    },
    "indexFilterSet" : false,
    "indexFilterApplied" : false,
    "ok" : 1,
    "operationTime" : Timestamp(1746474527, 1)
}

// COLSCAN is used for non-prefix regexes
rs0:PRIMARY> db.col.find({x: /x$/}).explain()
{
    "queryPlanner" : {
        "plannerVersion" : 2,
        "namespace" : "test.col",
        "winningPlan" : {
            "stage" : "COLLSCAN",
            "filter" : {
                "x" : {
                    "$regex" : /x$/
                }
            }
        }
```

```
    },
    "indexFilterSet" : false,
    "indexFilterApplied" : false,
    "ok" : 1,
    "operationTime" : Timestamp(1746474575, 1)
```

- Es gibt einige inhärente Unterschiede bei der Verwendung von Plan-Cache-Filtern mit Planner Version 2.0 im Vergleich zu MongoDB. Während die Planner-Version 2.0 die Angabe von „Projektion“ und „Kollation“ mit Plan-Cache-Filtern nicht unterstützt, tut MongoDB dies. Der MongoDB-Indexfilter befindet sich jedoch nur im Arbeitsspeicher und geht nach dem Neustart verloren. Planner Version 2.0 behält Indexfilter auch bei Neustarts und Patches bei.

Others

- Das Format der DML-Prüfprotokolle bei Verwendung von Planner Version 2.0 unterscheidet sich geringfügig von dem Format der Planner-Version 1.0.

```
command -  db.col.find({x:1})

************** Audit logs generated ******************

// v1 format for dml audit logs
{"atype":"authCheck","ts":1746473479983,"timestamp_utc":"2025-05-05
 19:31:19.983","remote_ip":"127.0.0.1:47022","users":
[{"user":"serviceadmin","db":"test"}],"param":
{"command":"find","ns":"test.col","args":{"batchSize":101,"filter":
{"x":1},"find":"col","limit":18446744073709551615,"lsid":
{"id":{"$binary":"P6RCGz9ZS4iWBSSHWXW15A==","$type":"4"},"uid":
{"$binary":"6Jo8PisnEi3dte03+pJFjdCyn/5cGQL8V2KqaoWsnk8=","$type":"0"}},"maxScan":18446744

// v2 formal for dml audit logs
{"atype":"authCheck","ts":1746473583711,"timestamp_utc":"2025-05-05
 19:33:03.711","remote_ip":"127.0.0.1:37754","users":
[{"user":"serviceadmin","db":"test"}],"param":
{"command":"find","ns":"test.col","args":{"find":"col","filter":{"x":1},"lsid":
{"id":{"$binary":"nJ88TGCSSd
+BeD2+ZtrhQg==","$type":"4"}},"$db":"test"},"result":0}}
```

- Die Indexbedingung als Teil des Explain-Plans:

```
rs0:PRIMARY> db.col.createIndex({index1:1})
{
```

```
 "createdCollectionAutomatically" : false,
 "numIndexesBefore" : 1,
 "numIndexesAfter" : 2,
 "ok" : 1,
 "operationTime" : Timestamp(1761149251, 1)
}
```

Planner Version 2.0 erklärt die Planausgabe mit Anzeige der Indexbedingung und des Filters:

```
rs0:PRIMARY> db.col.find({$and:[{price:{$eq:300}},{item:
{$eq:"apples"}}]}).explain()
{
 "queryPlanner" : {
  "plannerVersion" : 2,
  "namespace" : "test.col",
  "winningPlan" : {
   "stage" : "IXSCAN",
   "indexName" : "price_1",
   "direction" : "forward",
   "indexCond" : {
    "$and" : [
     {
      "price" : {
       "$eq" : 300
      }
     }
    ]
   },
   "filter" : {
    "$and" : [
     {
      "item" : {
       "$eq" : "apples"
      }
     }
    ]
   }
  }
 },
 "indexFilterSet" : false,
 "indexFilterApplied" : false,
 "ok" : 1,
 "operationTime" : Timestamp(1761149497, 1)
```

```
}
```

Planner Version 1.0 erklärt die Planausgabe:

```
rs0:PRIMARY> db.col.find({$and:[{price:{$eq:300}},{item:
{$eq:"apples"}}]}).explain()
{
 "queryPlanner" : {
  "plannerVersion" : 1,
  "namespace" : "test.col",
  "winningPlan" : {
   "stage" : "IXSCAN",
   "indexName" : "price_1",
   "direction" : "forward"
  }
 },
 "ok" : 1,
 "operationTime" : Timestamp(1761149533, 1)
}
```

Planner Version 2.0 schließt Verhaltenslücke mit MongoDB

Es gibt einige Bereiche, in denen Planner Version 2.0 die Verhaltenslücken von MongoDB schließt:

- Planner Version 2.0 ermöglicht die numerische Indexsuche in abgeflachten Arrays für: `$elemMatch`

```
doc: {"x" : [ [ { "y" : 1 } ] ] }

// Planner Version 2 and mongo
> db.bar.find({"x.0": {$elemMatch: {y: 1}}})
{ "_id" : ObjectId("68192947945e5846634c455a"), "x" : [ [ { "y" : 1 } ] ] }
> db.bar.find({"x": {$elemMatch: {"0.y": 1}}})
{ "_id" : ObjectId("68192947945e5846634c455a"), "x" : [ [ { "y" : 1 } ] ] }

//Whereas Planner Version 1 wouldn't return any results.
> db.bar.find({"x.0": {$elemMatch: {y: 1}}})
> db.bar.find({"x": {$elemMatch: {"0.y": 1}}})
```

- Während Planner Version 1.0 Zeichenketten in der Projektion ausschloss, stimmt das Verhalten von Planner Version 2.0 mit MongoDB überein und behandelt sie als Literalwerte.“

```
// Planner V2/ MongoDB
> db.col.find()
{ "_id" : ObjectId("681537738aa101903ed2fe05"), "x" : 1, "y" : 1 }
> db.col.find({},{x:"string"})
{ "_id" : ObjectId("681537738aa101903ed2fe05"), "x" : "string" }

// Planner V1 treats strings as exclude in projection
rs0:PRIMARY> db.col.find()
{ "_id" : ObjectId("68153744d42969f11d5cca72"), "x" : 1, "y" : 1 }
rs0:PRIMARY> db.col.find({},{x:"string"})
{ "_id" : ObjectId("68153744d42969f11d5cca72"), "y" : 1 }
```

- Planner Version 2.0 erlaubt wie MongoDB keine Projektion auf dieselben Felder „x“ und „x.a“:

```
// Planner version 2/MongoDB will error out
> db.col.find()
{ "_id" : ObjectId("68153da2012265816bc9ba23"), "x" : [ { "a" : 1 }, 3 ] }
 db.col.find({},{"x.a":1,"x":1}) // error

// Planner Version 1 does not error out
db.col.find()
{ "_id" : ObjectId("68153da2012265816bc9ba23"), "x" : [ { "a" : 1 }, 3 ] }

db.col.find({},{"x.a":1,"x":1})
{ "_id" : ObjectId("68153d60143af947c720d099"), "x" : [ { "a" : 1 }, 3 ] }
```

- Planner Version 2.0 ermöglicht wie MongoDB die Projektion auf Unterdokumente:

```
// Planner Version2/MongoDB supports projections on subdocuments
 db.col.find()
{ "_id" : ObjectId("681542d8f35ace71f0a50004"), "x" : [ { "y" : 100 } ] }
> db.col.find({},{"x":{"y":1}})
{ "_id" : ObjectId("681542b7a22d548e4ac9ddea"), "x" : [ { "y" : 100 } ] }

// Planner V1 throws error if projection is subdocument
 db.col.find()
{ "_id" : ObjectId("681542d8f35ace71f0a50004"), "x" : [ { "y" : 100 } ] }
rs0:PRIMARY> db.col.find({},{"x":{"y":1}})
Error: error: {
    "ok" : 0,
    "operationTime" : Timestamp(1746223914, 1),
    "code" : 2,
```

```
    "errmsg" : "Unknown projection operator y"
}
```

- Mit Planner Version 2.0 unterstützt die Projektion wie MongoDB keine Felder nach dem $ Operator:

```
// Mongo and Planner Version 2 will error out
  db.col.find()
{ "_id" : ObjectId("68155fa812f843439b593f3f"), "x" : [ { "a" : 100 } ] }
 db.col.find({"x.a":100},{"x.$.a":1}) - // error

// v1 will not error out
 db.col.find()
{ "_id" : ObjectId("68155fa812f843439b593f3f"), "x" : [ { "a" : 100 } ] }
db.col.find({"x.a":100},{"x.$.a":1})
{ "_id" : ObjectId("68155dee13b051d58239cd0a"), "x" : [ { "a" : 100 } ] }
```

- Planner Version 2.0 ermöglicht wie MongoDB die `$hint` Verwendung von:

```
// v1 will error out on $hint if there are no filters
db.col.find({}).hint("x_1")
Error: error: {
    "ok" : 0,
    "operationTime" : Timestamp(1746466616, 1),
    "code" : 2,
    "errmsg" : "Cannot use Hint for this Query. Index is multi key index , partial
 index or sparse index and query is not optimized to use this index."
}


// Mongo and Planner Version 2 will allow $hint usage
 db.col.find({}).hint("x_1")
{ "_id" : ObjectId("6818f790d5ba9359d68169cf"), "x" : 1 }
```

Abfrageplaner v3

Planner Version 3 in Amazon DocumentDB 8.0 unterstützt 21 Aggregationsphasen, darunter 6 neue Phasen. Planner V3 bietet integrierte Unterstützung für unterschiedliche Befehle. Es bietet eine bis zu 2-fache Gesamtleistungsverbesserung gegenüber Planner v2 in Amazon DocumentDB 5.0. Alle neuen Funktionen und Operatoren in Amazon DocumentDB 8.0 sind mit Planner v3 kompatibel. Zu den neuen Aggregationsstufen in Amazon DocumentDB 8.0, die von Planner v3 unterstützt werden, gehören $replaceWith, $vectorSearch, $merge, $set, $unset, $bucket. Planner v3 unterstützt auch

neue Funktionen und Operatoren in Amazon DocumentDB 8.0, darunter Collation, Views, $merge, $pow, $rand, $dateTrunc, $date, $date. ToParts FromParts

Topics

- Voraussetzungen
- Auswahl der Planner-Version 3.0 als Standard-Abfrageplaner
- Best Practices
- Einschränkungen
- Verbesserungen bei aggregierten und unterschiedlichen Operatoren
- Mögliche Verhaltensunterschiede zwischen Planner Version 1.0, 3.0 und MongoDB

Voraussetzungen

Die folgenden Voraussetzungen gelten für Planner Version 3.0:

- Planner Version 3.0 ist in allen Regionen verfügbar, in denen Engine-Version 8.0 verfügbar ist.
- Planner Version 3.0 ist der Standard-Abfrageplaner, wenn Engine-Version 8.0 ausgewählt ist.

Auswahl der Planner-Version 3.0 als Standard-Abfrageplaner

Wenn Sie Ihren Standard-Abfrageplaner in Amazon DocumentDB 8.0 geändert haben und zu Planner v3 zurückkehren müssen, können Sie dies über die Konsole oder CLI tun:

- Folgen Sie den Schritten unterAmazon DocumentDB-Cluster-Parameter ändern, um die Parametergruppe Ihres Clusters zu ändern.
- Ändern Sie für den Parameter mit dem Titel 'PlannerVersion' den Wert auf 3.0, was Planner-Version 3.0 bedeutet.
- Wählen Sie Sofort anwenden (wenn Sie Beim Neustart anwenden auswählen, wird die Auswahl bis zum nächsten Neustart des Clusters unwirksam).

Best Practices

Verwenden Sie die folgenden bewährten Methoden, um die erwarteten Ergebnisse zu erzielen, wenn Sie Planner Version 3.0 anwenden:

- Wählen Sie in einem globalen Cluster denselben `plannerVersion` Wert (1,0 oder 2,0 oder 3,0) in den Cluster-Parametergruppen für beide Regionen aus. Beachten Sie, dass die Auswahl verschiedener Planner-Versionen in primären und sekundären Regionen zu inkonsistentem Abfrageverhalten und inkonsistenter Leistung führen kann.
- Die Aktualisierung auf Planner Version 3.0 während eines geplanten Wartungsfensters oder in Zeiten mit reduziertem Datenverkehr ist am wenigsten störend, da es zu erhöhten Fehlerraten kommen kann, wenn die Planner-Version geändert wird, während Workloads aktiv ausgeführt werden.

Einschränkungen

Für Planner Version 3.0 gelten die folgenden Einschränkungen:

- Planner Version 3.0 wird in Elastic Clustern nicht unterstützt, da hier auf Planner Version 1.0 zurückgegriffen wird.

- Planner v1 ermöglicht zwar die Verwendung von 'PlanHint', um sicherzustellen, dass ein bestimmter Abfrageplan vom Abfrageoptimierer ausgewählt wird, Planner v3 erlaubt jedoch nicht die Verwendung von 'PlanHint' und stützt sich auf interne Optimierungen, um den besten Plan für die jeweilige Abfrage auszuwählen.

Verbesserungen bei aggregierten und unterschiedlichen Operatoren

Planner Version 3.0 bietet Verbesserungen in den Stufen $aggregate und $distinct. Im Folgenden sind einige der bemerkenswertesten Verbesserungen aufgeführt..

- Der Planer verschiebt die $match-Phasen nach Möglichkeit früher in der Pipeline und reduziert so die Anzahl der Dokumente, die in nachfolgenden Phasen verarbeitet werden.

```
//Planner v1
db.orders.aggregate([
  { $project: { customerId: 1, orderDate: 1, totalAmount: 1 } },
  { $match: { customerId: { $gt: 1000 } } }
])

// Planner v3 pulls up the match since customerId exists in original documents
```

```
// Optimized internally as:
db.orders.aggregate([
  { $match: { customerId: { $gt: 1000 } } },  // Pulled up before project
  { $project: { customerId: 1, orderDate: 1, totalAmount: 1 } }
])
```

- Der Planer kombiniert automatisch die Phasen $lookup und $unwind, wenn sie sich auf dasselbe Feld beziehen. Dadurch wird die zwischenzeitliche Datenverarbeitung reduziert und die Leistung verbessert.

```
                Example query:
//Planner v1
db.orders.aggregate([
  { $lookup: { from: "products", localField: "productId", foreignField: "_id", as:
 "productInfo" } },
  { $unwind: "$productInfo" },
  { $project: { orderDate: 1, "productInfo.name": 1, "productInfo.price": 1 } }
])

// Planner version 3.0 optimizes this internally by coalescing the $lookup and
 $unwind stages
```

- Planner Version 3.0 führt eine neue Ausführungsstrategie für Distinct Scan ein, die die Leistung bestimmter Operationen mit Indizes mit niedriger Kardinalität erheblich verbessert.

```
                Example query:
//// If there is a low cardinality index on "category", you may see a query plan like
 below
db.explain().products.distinct("category")

"queryPlanner" : {
        "plannerVersion" : 3,
        "namespace" : "db.products",
        "winningPlan" : {
                "stage" : "AGGREGATE",
                "inputStage" : {
                        "stage" : "DISTINCT_SCAN",
                        "inputStage" : {
                                "stage" : "IXONLYSCAN",
                                "indexName" : "category_1",
```

```
                                "direction" : "forward"
                        }
                }
        }
}
```

Mögliche Verhaltensunterschiede zwischen Planner Version 1.0, 3.0 und MongoDB

In einigen Ausnahmefällen ist es möglich, dass Planner Version 3.0 zu Ergebnissen führt, die leicht von Planner Version 1.0 abweichen. In diesem Abschnitt werden einige Beispiele für diese Möglichkeiten beschrieben.

Feature Differences

- Bei einer leeren Sammlung oder wenn vorherige Schritte wie Match alle Dokumente gefiltert haben, gibt Planner v1 die Ausgabe „field“ :0 zurück. Planner v3 und MongoDB geben keine Ausgaben aus.
- Bei Plannerv1 überspringt {"$skip“ :n} nicht, wenn in der vorherigen Phase weniger als n Dokumente zurückgegeben wurden. Plannerv3 und MongoDB werden unabhängig von der Anzahl der zurückgegebenen Dokumente korrekt übersprungen.
- Wenn eine fremde Sammlung, auf die in $lookup verwiesen wird, nicht existiert, gibt Plannerv1 einen Fehler aus. Planner v3 und MongoDB behandeln die fremde Sammlung als leere Sammlung und führen $lookup durch.

  ```
  db.coll.aggregate([
      {$lookup: {from: "does_not_exist", localField: "a", foreignField: "a", as:
   "c"}}
  ])
  ```

- Nur Planner v1 erlaubt die Verwendung mehrerer $search in einer Pipeline. Planner v2/v3 gibt einen Fehler aus und MongoDB unterstützt ihn nicht.

  ```
  VectorSearch = { "$search": { "vectorSearch": {
     "vector": [0.2, 0.5, 0.8],
     "path": "vectorEmbedding",
     "similarity": "cosine",
  ```

```
   "k": 2,
   "efSearch": 1
   }}}
db.coll.aggregate([VectorSearch, VectorSearch])
```

- Nur Planner v3 funktioniert, wenn die VectorSearch-Phase nicht die erste Phase ist. In diesem Fall gibt MongoDB einen Fehler aus und Planner v1 unterstützt die $vectorSearch-Stufe nicht.

```
VectorSearch = { {"$vectorSearch": {
    "queryVector": [0.2, 0.5, 0.8],
    "path": "vectorEmbedding",
    "similarity": "euclidean",
    "limit": 4,
    "numCandidates": 100} }

db.coll.aggregate([$match:{}, VectorSearch])
```

Geodaten mit Amazon DocumentDB abfragen

In diesem Abschnitt wird beschrieben, wie Sie Geodaten mit Amazon DocumentDB abfragen können. Nachdem Sie diesen Abschnitt gelesen haben, können Sie beantworten, wie Geodaten in Amazon DocumentDB gespeichert, abgefragt und indexiert werden.

Themen

- -Übersicht
- Indizierung und Speicherung von Geodaten
- Abfragen von koordinatenbasierten Daten
- Einschränkungen

-Übersicht

Zu den häufigsten Anwendungsfällen für Geospatial gehört die Näherungsanalyse Ihrer Daten. Zum Beispiel „Suche nach allen Flughäfen im Umkreis von 50 Meilen von Seattle“ oder „Suche nach den nächstgelegenen Restaurants an einem bestimmten Ort“. Amazon DocumentDB verwendet die GeoJSON-Spezifikation zur Darstellung von Geodaten. GeoJSON ist eine Open-Source-Spezifikation für Formen in einem Koordinatenraum. JSON-formatting GeoJSON-Koordinaten erfassen sowohl Längen- als auch Breitengrad und repräsentieren Positionen auf einer erdähnlichen Kugel.

Indizierung und Speicherung von Geodaten

Amazon DocumentDB verwendet den GeoJSON-Typ „Point“ zum Speichern von Geodaten. Jedes GeoJSON-Dokument (oder Unterdokument) besteht im Allgemeinen aus zwei Feldern:

- type — die dargestellte Form, die Amazon DocumentDB darüber informiert, wie das Feld „Koordinaten“ zu interpretieren ist. Derzeit unterstützt Amazon DocumentDB nur Punkte
- Koordinaten — ein Paar aus Breitengrad und Längengrad, dargestellt als Objekt in einem Array — [Längengrad, Breitengrad]

Amazon DocumentDB verwendet auch 2dSphere-Indizes, um Geodaten zu indizieren. Amazon DocumentDB unterstützt Indexierungspunkte. Amazon DocumentDB unterstützt Proximity-Abfragen mit 2dSphere-Indexierung.

Stellen wir uns ein Szenario vor, in dem Sie eine Anwendung für den Lieferservice von Lebensmitteln erstellen. Sie möchten die Längen- und Breitengrade verschiedener Restaurants in Amazon DocumentDB speichern. Zu diesem Zweck empfehlen wir Ihnen, zunächst einen Index für das Geospatial-Feld zu erstellen, das das Breitengrad- und Längengradpaar enthält.

```
use restaurantsdb
db.usarestaurants.createIndex({location:"2dsphere"})
```

Die Ausgabe dieses Befehls würde etwa so aussehen:

```
{
 "createdCollectionAutomatically" : true,
 "numIndexesBefore" : 1,
 "numIndexesAfter" : 2,
 "ok" : 1
}
```

Sobald Sie einen Index erstellt haben, können Sie damit beginnen, Daten in Ihre Amazon DocumentDB-Sammlung einzufügen.

```
db.usarestaurants.insert({
   "state":"Washington",
   "city":"Seattle",
   "name":"Thai Palace",
   "rating": 4.8,
```

```
   "location":{
      "type":"Point",
      "coordinates":[
         -122.3264,
         47.6009
      ]
   }
});

db.usarestaurants.insert({
   "state":"Washington",
   "city":"Seattle",
   "name":"Noodle House",
   "rating": 4.8,
   "location":{
      "type":"Point",
      "coordinates":[
        -122.3517,
         47.6159
      ]
   }
});

db.usarestaurants.insert({
   "state":"Washington",
   "city":"Seattle",
   "name":"Curry House",
   "rating": 4.8,
   "location":{
      "type":"Point",
      "coordinates":[
         -121.4517,
         47.6229
      ]
   }
});
```

Abfragen von koordinatenbasierten Daten

Amazon DocumentDB unterstützt die Abfrage von räumlichen Daten nach Nähe, Inklusion und Schnittmenge. Ein gutes Beispiel für eine Näherungsabfrage ist die Suche nach allen Punkten (allen Flughäfen), die weniger als eine bestimmte Entfernung und mehr als eine Entfernung von einem anderen Punkt (Stadt) liegen. Ein gutes Beispiel für Inklusionsabfragen ist die Suche nach allen

Punkten (allen Flughäfen), die sich in einem bestimmten Bereich area/polygon (Bundesstaat New York) befinden. Ein gutes Beispiel für eine Kreuzungsabfrage ist die Suche nach einem Polygon (Bundesstaat), das sich mit einem Punkt (Stadt) überschneidet. Sie können die folgenden Geospatial-Operatoren verwenden, um Erkenntnisse aus Ihren Daten zu gewinnen.

- **`$nearSphere`**- `$nearSphere` ist ein Suchoperator, der das Suchen von Punkten unterstützt, die einem GeoJSON-Punkt am nächsten und am weitesten entfernt sind.
- **`$geoNear`**- `$geoNear` ist ein Aggregationsoperator, der die Berechnung der Entfernung von einem GeoJSON-Punkt in Metern unterstützt.
- **`$minDistance`**- `$minDistance` ist ein Suchoperator, der in Verbindung mit `$nearSphere` oder `$geoNear` zum Filtern von Dokumenten verwendet wird, die sich mindestens in der angegebenen Mindestentfernung vom Mittelpunkt befinden.
- **`$maxDistance`**- `$maxDistance` ist ein Suchoperator, der in Verbindung mit `$nearSphere` oder verwendet wird, `$geoNear` um Dokumente zu filtern, die sich höchstens in der angegebenen maximalen Entfernung vom Mittelpunkt befinden.
- **`$geoWithin`**- `$geoWithin` ist ein Suchoperator, der das Auffinden von Dokumenten mit Geodaten unterstützt, die vollständig innerhalb einer bestimmten Form, z. B. eines Polygons, vorliegen.
- **`$geoIntersects`**- `$geoIntersects` ist ein Suchoperator, der die Suche nach Dokumenten unterstützt, deren Geodaten sich mit einem angegebenen GeoJSON-Objekt überschneiden.

> **Note**
>
> `$geoNear`und `$nearSphere` benötigen einen 2dSphere-Index für das GeoJSON-Feld, das Sie in Ihrer Näherungsabfrage verwenden.

Beispiel 1

In diesem Beispiel erfahren Sie, wie Sie alle Restaurants (Punkte) nach der nächstgelegenen Entfernung zu einer Adresse (Punkt) sortiert finden.

Um eine solche Abfrage durchzuführen, können Sie die Entfernung einer Reihe von Punkten `$geoNear` zu einem anderen Punkt berechnen. Sie können auch das hinzufügen`distanceMultiplier`, um die Entfernung in Kilometern zu messen.

```
db.usarestaurants.aggregate([
```

```
   {
      "$geoNear":{
         "near":{
            "type":"Point",
            "coordinates":[
               -122.3516,
               47.6156
            ]
         },
         "spherical":true,
         "distanceField":"DistanceKilometers",
         "distanceMultiplier":0.001
      }
   }
])
```

Mit dem obigen Befehl würden Restaurants sortiert nach Entfernung (am nächsten zum weitesten) vom angegebenen Punkt zurückgegeben. Die Ausgabe dieses Befehls würde ungefähr so aussehen

```
{ "_id" : ObjectId("611f3da985009a81ad38e74b"), "state" : "Washington", "city" :
 "Seattle", "name" : "Noodle House", "rating" : 4.8, "location" : { "type" : "Point",
 "coordinates" : [ -122.3517, 47.6159 ] }, "DistanceKilometers" : 0.03422834547294996 }
{ "_id" : ObjectId("611f3da185009a81ad38e74a"), "state" : "Washington", "city" :
 "Seattle", "name" : "Thai Palace", "rating" : 4.8, "location" : { "type" : "Point",
 "coordinates" : [ -122.3264, 47.6009 ] }, "DistanceKilometers" : 2.5009390081704277 }
{ "_id" : ObjectId("611f3dae85009a81ad38e74c"), "state" : "Washington", "city" :
 "Seattle", "name" : "Curry House", "rating" : 4.8, "location" : { "type" : "Point",
 "coordinates" : [ -121.4517, 47.6229 ] }, "DistanceKilometers" : 67.52845344856914 }
```

> **Note**
>
> Die num Optionen `limit` und für die `$geoNear` Phase sowie das Standardlimit von 100 Dokumenten sind in Amazon DocumentDB 8.0 (Engine-Patch Version 4.0.5748) und höher veraltet. Die folgenden Beispiele verwenden Amazon DocumentDB 8.0 (Engine-Patch-Version 4.0.4448) und frühere Versionen `limit` und num gelten nur für diese.

Um die Anzahl der Ergebnisse in einer Abfrage zu begrenzen, verwenden Sie die Option oder. `limit` num

`limit`:

```
db.usarestaurants.aggregate([
   {
      "$geoNear":{
         "near":{
            "type":"Point",
            "coordinates":[
               -122.3516,
               47.6156
            ]
         },
         "spherical":true,
         "distanceField":"DistanceKilometers",
         "distanceMultiplier":0.001,
         "limit": 10
      }
   }
])
```

num:

```
db.usarestaurants.aggregate([
   {
      "$geoNear":{
         "near":{
            "type":"Point",
            "coordinates":[
               -122.3516,
               47.6156
            ]
         },
         "spherical":true,
         "distanceField":"DistanceKilometers",
         "distanceMultiplier":0.001,
         "num": 10
      }
   }
])
```

Beispiel 2

In diesem Beispiel erfahren Sie, wie Sie alle Restaurants (Punkte) im Umkreis von 2 Kilometern von einer bestimmten Adresse (Punkt) finden. Um eine solche Abfrage durchzuführen, können Sie

`$nearSphere` innerhalb eines Minimums `$minDistance` und Maximums `$maxDistance` von einem GeoJSON-Punkt aus verwenden

```
db.usarestaurants.find({
   "location":{
      "$nearSphere":{
         "$geometry":{
            "type":"Point",
            "coordinates":[
               -122.3516,
               47.6156
            ]
         },
         "$minDistance":1,
         "$maxDistance":2000
      }
   }
},
{
   "name":1
})
```

Der obige Befehl würde Restaurants in einer maximalen Entfernung von 2 Kilometern vom angegebenen Punkt zurückgeben. Die Ausgabe dieses Befehls würde ungefähr so aussehen

```
{ "_id" : ObjectId("611f3da985009a81ad38e74b"), "name" : "Noodle House" }
```

Einschränkungen

Amazon DocumentDB unterstützt nicht die Abfrage oder Indizierung von Polygonen,, LineString, MultiPoint und. MultiPolygon MultiLineString GeometryCollection

Teilweiser Index

Ein partieller Index indiziert Dokumente in einer Sammlung, die ein bestimmtes Filterkriterium erfüllen. Die Funktion für den teilweisen Index wird in instanzbasierten Amazon DocumentDB 5.0-Clustern unterstützt.

Topics

- Erstellen Sie einen Teilindex

- Unterstützte Operatoren
- Abfrage mit einem Teilindex
- Funktionen des partiellen Indexes
- Einschränkungen des partiellen Indexes

Erstellen Sie einen Teilindex

Um einen Teilindex zu erstellen, verwenden Sie die `createIndex()` Methode mit der `partialFilterExpression` Option. Mit der folgenden Operation wird beispielsweise ein eindeutiger zusammengesetzter Index in der Orders-Auflistung erstellt, der Dokumente indexiert, die ein `OrderID` und das `isDelivered` Feld den Wert true haben:

```
db.orders.createIndex(
  {"category": 1, "CustomerId": 1, "OrderId": 1},
  {"unique": true, "partialFilterExpression":
    {"$and": [
      {"OrderId": {"$exists": true}},
      {"isDelivered": {"$eq": false}}
    ]}
  }
)
```

Unterstützte Operatoren

- $eq
- $exists
- $and (nur auf oberster Ebene)
- $gt/$gte/$lt/$lte (Indexscan wird nur verwendet, wenn der in der Abfrage angegebene Filter exakt mit dem partiellen Filterausdruck übereinstimmt) (siehe Einschränkungen)

Abfrage mit einem Teilindex

Die folgenden Abfragemuster sind mit partiellen Indizes möglich:

- Das Abfrageprädikat entspricht exakt dem Filterausdruck für den partiellen Index:

```
db.orders.find({"$and": [
    {"OrderId": {"$exists": true}},
    {"isDelivered": {"$eq": false}}
  ]}).explain()
```

- Das erwartete Ergebnis des Abfragefilters ist eine logische Teilmenge des Teilfilters:

```
db.orders.find({"$and": [
    {"OrderId": {"$exists": true}},
    {"isDelivered": {"$eq": false}},
    {"OrderAmount": {"$eq": "5"}}
  ]}).explain()
```

- Ein Unterprädikat der Abfrage kann in Verbindung mit anderen Indizes verwendet werden:

```
db.orders.createIndex({"anotherIndex":1})
db.orders.find({ "$or": [
      {"$and": [
        {"OrderId": {"$exists": true}},
        {"isDelivered": {"$eq": false}}
      ]},
      {"anotherIndex": {"$eq": 5}}
    ]
  }).explain()
```

> **Note**
>
> Ein Abfrageplaner kann sich dafür entscheiden, einen Sammlungsscan anstelle eines Indexscans zu verwenden, wenn dies effizient ist. Dies ist in der Regel bei sehr kleinen Sammlungen oder Abfragen der Fall, bei denen ein großer Teil einer Sammlung zurückgegeben würde.

Funktionen des partiellen Indexes

Listet Teilindizes auf

Listet Teilindizes auf, bei denen die Operation teilweise FilterExpression verwendet wird`getIndex`. Die in ausgegebene `getIndex` Operation listet beispielsweise Teilindizes mit den Feldern key, name und partialFilterExpressions auf:

```
db.orders.getIndexes()
```

Dieses Beispiel gibt die folgende Ausgabe zurück:

```
[
  {
    "v" : 4,
    "key" : {
      "_id" : 1
    },
    "name" : "_id_",
    "ns" : "ecommerceApp.orders"
  },
  {
    "v" : 4,
    "unique" : true,
    "key" : {
      "category" : 1,
      "" : 1,
      "CustomerId" : 1,
      "OrderId" : 1
    },
    "name" : "category_1_CustID_1_OrderId_1",
    "ns" : "ecommerceApp.orders",
    "partialFilterExpression" : {
      "$and" : [
        {"OrderId": {"$exists": true}},
        {"isDelivered": {"$eq": false}}
      ]
    }
  }
]
```

Mehrere partielle Filterausdrücke für denselben Schlüssel:Reihenfolge

Für dieselben Feldkombinationen (Schlüssel:Reihenfolge) können unterschiedliche Teilindizes erstellt werden. Diese Indizes müssen einen anderen Namen haben.

```
db.orders.createIndex(
  {"OrderId":1},
  {
    name:"firstPartialIndex",
    partialFilterExpression:{"OrderId":{"$exists": true}}
  }
)
```

```
db.orders.createIndex(
  {"OrderId":1},
  {
    name:"secondPartialIndex",
    partialFilterExpression:{"OrderId":{"$gt": 1000}}
  }
)
```

Führen Sie `getIndexes` den Vorgang aus, um alle Indizes in der Sammlung aufzulisten:

```
db.orders.getIndexes()
```

Diese Beispiele geben die folgende Ausgabe zurück:

```
[
  {
    "v" : 4,
    "key" : {
      "_id" : 1
    },
    "name" : "_id_",
    "ns" : "ecommerceApp.orders"
  },
  {
    "v" : 4,
    "key" : {
      "OrderId" : 1
    },
    "name" : "firstPartialIndex",
    "ns" : "ecommerceApp.orders",
    "partialFilterExpression" : {"OrderId":{"$exists": true}}
  },
  {
```

```
    "v" : 4,
    "key" : {
      "OrderId" : 1
    },
    "name" : "secondPartialIndex",
    "ns" : "ecommerceApp.orders",
    "partialFilterExpression" : {"OrderId":{"$gt": 1000}}
  }
]
```

> **Important**
>
> Indexnamen müssen unterschiedlich sein und dürfen nur nach Namen gelöscht werden.

Indizes mit partiellen Eigenschaften und TTL-Eigenschaften

Sie können auch Indizes mit partiellen Eigenschaften und TTL-Eigenschaften erstellen, indem Sie bei der Indexerstellung beide `partialFilterExpression` `expireAfterSeconds` Optionen angeben. Auf diese Weise können Sie besser kontrollieren, welche Dokumente jetzt aus einer Sammlung entfernt werden.

Beispielsweise verfügen Sie möglicherweise über einen TTL-Index, der Dokumente identifiziert, die nach einem bestimmten Zeitraum gelöscht werden sollen. Mit der Option „Teilindex“ können Sie jetzt zusätzliche Bedingungen dafür festlegen, wann Dokumente gelöscht werden sollen:

```
db.orders.createIndex(
    { "OrderTimestamp": 1 },
    {
        expireAfterSeconds: 3600 ,
        partialFilterExpression: { "isDelivered": { $eq: true } }
    }
)
```

Dieses Beispiel gibt die folgende Ausgabe zurück:

```
{
        "createdCollectionAutomatically" : false,
        "numIndexesBefore" : 1,
        "numIndexesAfter" : 2,
```

```
        "ok" : 1,
        "operationTime" : Timestamp(1234567890, 1)
}
```

Führen Sie den `getIndexes` Vorgang aus, um die in der Sammlung vorhandenen Indizes aufzulisten:

```
db.orders.getIndexes()
[
    {
        "v" : 4,
        "key" : {
            "_id" : 1
        },
        "name" : "_id_",
        "ns" : "test.orders"
    }
```

Dieses Beispiel gibt die folgende Ausgabe zurück:

```
[
    {
        "v": 4,
        "key": {
            "_id": 1
        },
        "name": "_id_",
        "ns": "ecommerceApp.orders"
    },
    {
        "v": 4,
        "key": {
            "OrderTimestamp": 1
        },
        "name": "OrderTimestamp_1",
        "ns": "ecommerceApp.orders",
        "partialFilterExpression": {
            "isDelivered": {
                "$eq": true
            }
        },
        "expireAfterSeconds": 3600
    }
```

```
]
```

Einschränkungen des partiellen Indexes

Für die Funktion „Teilindex“ gelten die folgenden Einschränkungen:

- Ungleichheitsabfragen in Amazon DocumentDB verwenden nur dann einen Teilindex, wenn das Abfragefilterprädikat genau dem entspricht `partialFilterExpression` und denselben Datentyp hat.

  > **Note**
  >
  > `$hint`Kann im obigen Fall sogar nicht verwendet werden, um IXSCAN zu erzwingen.

  Im folgenden Beispiel `partialFilterExpression` wird das nur angewendet, `field1` aber nicht`field2`:

  ```
  db.orders.createIndex(
    {"OrderAmount": 1},
    {"partialFilterExpression": { OrderAmount : {"$gt" : 5}}}
  )

  db.orders.find({OrderAmount : {"$gt" : 5}}) // Will use partial index
  db.orders.find({OrderAmount : {"$gt" : 6}}) // Will not use partial index
  db.orders.find({OrderAmount : {"$gt" : Decimal128(5.00)}}) // Will not use partial
   index
  ```

- A `partialFilterExpression` mit Array-Operatoren werden nicht unterstützt. Der folgende Vorgang generiert einen Fehler:

  ```
  db.orders.createIndex(
    {"CustomerId":1},
    {'partialFilterExpression': {'OrderId': {'$eq': [1000, 1001, 1002]}}}
  )
  ```

- Die folgenden Operatoren werden in einem FilterExpression Teilfeld nicht unterstützt:
  - `$all`(Array-Operator)
  - $mod(Array-Operator)
  - `$or`

- `$xor`
- `$not`
- `$nor`

- Der Datentyp des Filterausdrucks und des Filters sollten identisch sein.

Textsuche mit Amazon DocumentDB durchführen

Die native Volltextsuchfunktion von Amazon DocumentDB (Text Index v1) ermöglicht Ihnen die Textsuche in großen Textdatensätzen mithilfe spezieller Textindizes. In diesem Abschnitt werden die Funktionen der Textindex-Funktion beschrieben und Schritte zur Erstellung und Verwendung von Textindizes in Amazon DocumentDB bereitgestellt. Einschränkungen bei der Textsuche sind ebenfalls aufgeführt.

Topics

- Unterstützte Funktionen
- Verwenden des Amazon DocumentDB-Textindex
- Unterschiede zu MongoDB
- Bewährte Verfahren und Richtlinien
- Textindex V2
- Einschränkungen

Unterstützte Funktionen

Die Amazon DocumentDB-Textsuche unterstützt die folgenden MongoDB-API-kompatiblen Funktionen:

- Erstellen Sie Textindizes für ein einzelnes Feld.
- Erstellen Sie zusammengesetzte Textindizes, die mehr als ein Textfeld enthalten.
- Führen Sie Suchen mit einem Wort oder mehreren Wörtern durch.
- Kontrollieren Sie die Suchergebnisse mithilfe von Gewichtungen.
- Sortieren Sie die Suchergebnisse nach Punktezahl.
- Verwenden Sie den Textindex in der Aggregationspipeline.
- Suchen Sie nach einer exakten Phrase.

Verwenden des Amazon DocumentDB-Textindex

Um einen Textindex für ein Feld zu erstellen, das Zeichenkettendaten enthält, geben Sie die Zeichenfolge „Text“ wie unten dargestellt an:

Index für ein einzelnes Feld:

```
db.test.createIndex({"comments": "text"})
```

Dieser Index unterstützt Textsuchabfragen im Zeichenfolgenfeld „Kommentare“ in der angegebenen Sammlung.

Erstellen Sie einen zusammengesetzten Textindex für mehr als ein Zeichenkettenfeld:

```
db.test.createIndex({"comments": "text", "title":"text"})
```

Dieser Index unterstützt Textsuchabfragen in den Zeichenfolgenfeldern „Kommentare“ und „Titel“ in der angegebenen Sammlung. Sie können bis zu 30 Felder angeben, wenn Sie einen zusammengesetzten Textindex erstellen. Nach der Erstellung werden mit Ihren Textsuchabfragen alle indizierten Felder abgefragt.

> **Note**
>
> Für jede Sammlung ist nur ein Textindex zulässig.

Einen Textindex in einer Amazon DocumentDB-Sammlung auflisten

Sie können ihn für Ihre Sammlung verwenden`getIndexes()`, um Indizes, einschließlich Textindizes, zu identifizieren und zu beschreiben, wie im folgenden Beispiel gezeigt:

```
rs0:PRIMARY> db.test.getIndexes()
[
   {
      "v" : 4,
      "key" : {
         "_id" : 1
      },
      "name" : "_id_",
      "ns" : "test.test"
```

```
   },
   {
      "v" : 1,
      "key" : {
         "_fts" : "text",
         "_ftsx" : 1
      },
      "name" : "contents_text",
      "ns" : "test.test",
      "default_language" : "english",
      "weights" : {
         "comments" : 1
      },
      "textIndexVersion" : 1
   }
]
```

Sobald Sie einen Index erstellt haben, beginnen Sie mit dem Einfügen von Daten in Ihre Amazon DocumentDB-Sammlung.

```
db.test.insertMany([{"_id": 1, "star_rating": 4, "comments": "apple is red"},
                    {"_id": 2, "star_rating": 5, "comments": "pie is delicious"},
                    {"_id": 3, "star_rating": 3, "comments": "apples, oranges - healthy
 fruit"},
                    {"_id": 4, "star_rating": 2, "comments": "bake the apple pie in the
 oven"},
                    {"_id": 5, "star_rating": 5, "comments": "interesting couch"},
                    {"_id": 6, "star_rating": 5, "comments": "interested in couch for
 sale, year 2022"}])
```

Textsuchabfragen ausführen

Führen Sie eine Textsuchabfrage mit einem Wort aus

Sie müssen die `$search` Operatoren `$text` und verwenden, um Textsuchen durchzuführen. Im folgenden Beispiel werden alle Dokumente zurückgegeben, in denen Ihr indiziertes Textfeld die Zeichenfolge „apple“ oder „apple“ in anderen Formaten wie „apples“ enthält:

```
db.test.find({$text: {$search: "apple"}})
```

Ausgabe:

Die Ausgabe dieses Befehls sieht ungefähr so aus:

```
{ "_id" : 1, "star_rating" : 4, "comments" : "apple is red" }
{ "_id" : 3, "star_rating" : 3, "comments" : "apples, oranges - healthy fruit" }
{ "_id" : 4, "star_rating" : 2, "comments" : "bake the apple pie in the oven" }
```

Führen Sie eine Textsuche mit mehreren Wörtern durch

Sie können auch Textsuchen mit mehreren Wörtern in Ihren Amazon DocumentDB DocumentDB-Daten durchführen. Der folgende Befehl gibt Dokumente zurück, deren indiziertes Textfeld „Apfel“ oder „Kuchen“ enthält:

```
db.test.find({$text: {$search: "apple pie"}})
```

Ausgabe:

Die Ausgabe dieses Befehls sieht ungefähr so aus:

```
{ "_id" : 1, "star_rating" : 4, "comments" : "apple is red" }
{ "_id" : 2, "star_rating" : 5, "comments" : "pie is delicious" }
{ "_id" : 3, "star_rating" : 3, "comments" : "apples, oranges - healthy fruit" }
{ "_id" : 4, "star_rating" : 2, "comments" : "bake the apple pie in the oven" }
```

Führen Sie eine Textsuche mit mehreren Wörtern durch

Verwenden Sie für eine Phrasensuche mit mehreren Wörtern dieses Beispiel:

```
db.test.find({$text: {$search: "\"apple pie\""}})
```

Ausgabe:

Der obige Befehl gibt Dokumente zurück, deren indiziertes Textfeld genau den Ausdruck „Apfelkuchen“ enthält. Die Ausgabe dieses Befehls sieht ungefähr so aus:

```
{ "_id" : 4, "star_rating" : 2, "comments" : "bake the apple pie in the oven" }
```

Führen Sie eine Textsuche mit Filtern aus

Sie können die Textsuche auch mit anderen Abfrageoperatoren kombinieren, um Ergebnisse nach zusätzlichen Kriterien zu filtern:

```
db.test.find({$and: [{star_rating: 5}, {$text: {$search: "interest"}}]})
```

Ausgabe:

Der obige Befehl gibt Dokumente zurück, deren indiziertes Textfeld eine beliebige Form von „Interesse“ und ein „Star-Rating“ gleich 5 enthält. Die Ausgabe dieses Befehls sieht ungefähr so aus:

```
{ "_id" : 5, "star_rating" : 5, "comments" : "interesting couch" }
{ "_id" : 6, "star_rating" : 5, "comments" : "interested in couch for sale, year
 2022" }
```

Beschränken Sie die Anzahl der Dokumente, die bei einer Textsuche zurückgegeben werden

Sie können die Anzahl der zurückgegebenen Dokumente einschränken, indem Sie Folgendes verwenden`limit`:

```
db.test.find({$and: [{star_rating: 5}, {$text: {$search: "couch"}}]}).limit(1)
```

Ausgabe:

Der obige Befehl gibt ein Ergebnis zurück, das den Kriterien des Filters entspricht:

```
{ "_id" : 5, "star_rating" : 5, "comments" : "interesting couch" }
```

Sortiert die Ergebnisse nach der Textpunktzahl

Im folgenden Beispiel werden die Ergebnisse der Textsuche nach der Textpunktzahl sortiert:

```
db.test.find({$text: {$search: "apple"}}, {score: {$meta: "textScore"}}).sort({score:
 {$meta: "textScore"}})
```

Ausgabe:

Der obige Befehl gibt Dokumente zurück, deren indiziertes Textfeld „apple“ oder „apple“ in anderen Formaten wie „apples“ enthält, und sortiert das Ergebnis danach, wie relevant das Dokument für den Suchbegriff ist. Die Ausgabe dieses Befehls sieht ungefähr so aus:

```
{ "_id" : 1, "star_rating" : 4, "comments" : "apple is red", "score" :
 0.6079270860936958 }
```

```
{ "_id" : 3, "star_rating" : 3, "comments" : "apples, oranges - healthy fruit",
 "score" : 0.6079270860936958 }
{ "_id" : 4, "star_rating" : 2, "comments" : "bake the apple pie in the oven",
 "score" : 0.6079270860936958 }
```

`$text`und `$search` werden auch für `delete` Befehle `aggregate`,`count`,`findAndModify`,`update`, und unterstützt.

Aggregationsoperatoren

Aggregationspipeline mit **`$match`**

```
db.test.aggregate(
   [{ $match: { $text: { $search: "apple pie" } } }]
)
```

Ausgabe:

Der obige Befehl gibt die folgenden Ergebnisse zurück:

```
{ "_id" : 1, "star_rating" : 4, "comments" : "apple is red" }
{ "_id" : 3, "star_rating" : 3, "comments" : "apples, oranges - healthy fruit" }
{ "_id" : 4, "star_rating" : 2, "comments" : "bake the apple pie in the oven" }
{ "_id" : 2, "star_rating" : 5, "comments" : "pie is delicious" }
```

Eine Kombination anderer Aggregationsoperatoren

```
db.test.aggregate(
   [
      { $match: { $text: { $search: "apple pie" } } },
      { $sort: { score: { $meta: "textScore" } } },
      { $project: { score: { $meta: "textScore" } } }
   ]
)
```

Ausgabe:

Der obige Befehl gibt die folgenden Ergebnisse zurück:

```
{ "_id" : 4, "score" : 0.6079270860936958 }
```

```
{ "_id" : 1, "score" : 0.3039635430468479 }
{ "_id" : 2, "score" : 0.3039635430468479 }
{ "_id" : 3, "score" : 0.3039635430468479 }
```

Geben Sie mehrere Felder an, wenn Sie einen Textindex erstellen

Sie können bis zu drei Feldern in Ihrem Verbundtextindex Gewichtungen zuweisen. Die Standardgewichtung, die einem Feld in einem Textindex zugewiesen wird, ist eins (1). Das Gewicht ist ein optionaler Parameter und muss im Bereich von 1 bis 100000 liegen.

```
db.test.createIndex(
   {
     "firstname": "text",
     "lastname": "text",
     ...
   },
   {
     weights: {
       "firstname": 5,
       "lastname":10,
       ...
     },
     name: "name_text_index"
   }
 )
```

Unterschiede zu MongoDB

Die Textindex-Funktion von Amazon DocumentDB verwendet einen umgekehrten Index mit einem Term-Frequenz-Algorithmus. Textindizes sind standardmäßig dünn gesät. Aufgrund von Unterschieden in der Parsing-Logik, Tokenisierungstrennzeichen und anderen kann es sein, dass dieselbe Ergebnismenge wie MongoDB nicht für denselben Datensatz oder dieselbe Abfrageform zurückgegeben wird.

Es bestehen die folgenden zusätzlichen Unterschiede zwischen dem Amazon DocumentDB-Textindex und MongoDB:

- Zusammengesetzte Indizes, die Nicht-Text-Indizes verwenden, werden nicht unterstützt.
- Amazon DocumentDB-Textindizes unterscheiden nicht zwischen Groß- und Kleinschreibung.
- Für den Textindex wird nur die englische Sprache unterstützt.

- Die Textindizierung von Array-Feldern (oder Feldern mit mehreren Schlüsseln) wird nicht unterstützt. Wenn Sie beispielsweise einen Textindex für „a“ mit dem Dokument {„a“: [„apple“, „pie“]} erstellen, schlägt fehl.
- Die Indexierung von Platzhaltertext wird nicht unterstützt.
- Eindeutige Textindizes werden nicht unterstützt.
- Das Ausschließen eines Begriffs wird nicht unterstützt.

Bewährte Verfahren und Richtlinien

- Für eine optimale Leistung bei Textsuchabfragen, bei denen nach Textwerten sortiert wird, wird empfohlen, den Textindex vor dem Laden von Daten zu erstellen.
- Textindizes benötigen zusätzlichen Speicherplatz für eine optimierte interne Kopie der indizierten Daten. Dies hat zusätzliche Kosten zur Folge.

Textindex V2

Amazon DocumentDB 8.0 führt eine neue Version des Textindex (V2) ein, die den zugrunde liegenden Textsuchparser ändert, um mehr Kompatibilität mit der MongoDB zu erreichen.

Zusätzlich zu den Funktionen der V1-Textindizes bieten V2-Textindizes auch die folgende Unterstützung:

- Der Planer verschiebt die $match-Phasen nach Möglichkeit früher in der Pipeline und reduziert so die Anzahl der Dokumente, die in nachfolgenden Phasen verarbeitet werden.
- Die Tokenisierung von Sonderzeichen in Textfeldern wie E-Mails, URLs und Dateipfaden wurde verbessert. V2 kann einzelne Token innerhalb dieser Zeichenketten analysieren und zuordnen, während V1 dies nicht konnte.

```
rs0:PRIMARY> db.coll.createIndex({ "a": "text" });
rs0:PRIMARY> db.coll.find()
{ "_id" : 1, "a" : "jane.doe_1234@company.com" }
{ "_id" : 2, "a" : "janedoe@company.com" }
{ "_id" : 3, "a" : "/home/user/company/thesis.pdf" }
{ "_id" : 4, "a" : "/home/user/path/jane.pdf" }
{ "_id" : 5, "a" : "http://www.company.com/path" }
{ "_id" : 6, "a" : "https://company.com/path/../home" }
```

```
// Sample query
rs0:PRIMARY> db.coll.find({ $text: { $search: "jane" } });

// V1 text index – no results
None

// V2 text index – matches tokens within emails and file paths
{ "_id" : 1, "a" : "jane.doe_1234@company.com" }
{ "_id" : 4, "a" : "/home/user/path/jane.pdf" }
```

Einschränkungen

Für die Textsuche gelten in Amazon DocumentDB die folgenden Einschränkungen:

- Textindizes speichern Lexeme und ihre Positionsinformationen. Die Gesamtgröße aller Lexeme und ihrer Positionsinformationen in einem einzigen Dokument ist auf 1 MB begrenzt.

Indizes

Themen

- Indexverwaltung
- Indextypen
- Indexeigenschaften

Indexverwaltung

In diesem Abschnitt werden Themen zur Indexverwaltung für Amazon DocumentDB behandelt.

Themen

- Indexerstellung
- Verwaltung von Indizes
- Bewährte Methoden für die Arbeit mit Indizes

Indexerstellung

Für die Erstellung von Indizes in Amazon DocumentDB müssen eine Reihe von Entscheidungen getroffen werden:

- Wie schnell muss es abgeschlossen werden?
- Kann auf die Sammlung nicht zugegriffen werden, während der Build ausgeführt wird?
- Wie viel Rechenleistung einer Instanz kann dem Build zugewiesen werden?
- Welche Art von Index sollte erstellt werden?

Dieser Abschnitt hilft Ihnen bei der Beantwortung dieser Fragen und enthält die Befehle und Überwachungsbeispiele, um einen Amazon DocumentDB DocumentDB-Index für Ihre instanzbasierte Clustersammlung zu erstellen.

Richtlinien

Die folgenden Richtlinien enthalten grundlegende Grenzwerte und Kompromisse bei der Konfiguration bei der Erstellung neuer Indizes:

- Unterstützung für Amazon DocumentDB DocumentDB-Versionen — Während die Single-Worker-Indizierung in allen Amazon DocumentDB DocumentDB-Versionen unterstützt wird, wird die Multi-Worker-Indizierung nur in den Amazon DocumentDB DocumentDB-Versionen 4.0 und 5.0 unterstützt.
- Leistungseinbußen — Eine Erhöhung der Anzahl der Worker bei der Indexerstellung erhöht die CPU-Auslastung und die Lese-I/O auf der primären Instance Ihrer Amazon DocumentDB DocumentDB-Datenbank. Die Ressourcen, die für die Erstellung eines neuen Indexes benötigt werden, stehen Ihrem laufenden Workload nicht zur Verfügung.
- Elastische Cluster — Parallele Indizierung wird auf elastischen Amazon DocumentDB-Clustern nicht unterstützt.
- Maximale Anzahl an Workern — Die maximale Anzahl von Workern, die Sie konfigurieren können, hängt von der Größe Ihrer primären Instance in Ihrem Datenbank-Cluster ab. Das ist die Hälfte der Gesamtzahl der vCPUs auf der primären Instance Ihres Datenbank-Clusters. Sie können beispielsweise maximal 32 Worker auf einer db.r6g.16xlarge-Instance mit 64 vCPUs ausführen.

> **Note**
>
> Die parallele Indexerstellung wird auf Instances 2xlarge und höher unterstützt.

- Mindestanzahl an Workern — Die Mindestanzahl an Workern, die Sie konfigurieren können, ist eins. Die Standardeinstellung für die Indexerstellung auf instanzbasierten Clustern ist zwei Worker. Sie können die Anzahl der Worker jedoch auf einen reduzieren, indem Sie die Option „Worker-Threads“ verwenden. Dadurch wird der Prozess mit einem einzigen Worker ausgeführt.
- Indexkomprimierung — Amazon DocumentDB unterstützt keine Indexkomprimierung. Die Datengrößen für Indizes sind möglicherweise größer als bei Verwendung anderer Optionen.
- Indizierung mehrerer Sammlungen — Die Hälfte der vCPUs auf der primären Instance Ihres Datenbank-Clusters kann für konfigurierte Worker verwendet werden, die Indexerstellung für mehrere Sammlungen durchführen.
- Indextypen — Eine Liste der unterstützten Indextypen auf Amazon DocumentDB finden Indextypen Sie unter.

Typen der Indexerstellung

Die vier Arten von Indexerstellungen sind:

- Vordergrund: Die Indexerstellung im Vordergrund blockiert alle anderen Datenbankoperationen in der Sammlung, für die der Index erstellt wurde, bis die Indexerstellung abgeschlossen ist. Der Amazon DocumentDB DocumentDB-Vordergrundaufbau besteht aus fünf Phasen.
- Vordergrund (einzigartig): Index-Builds im Vordergrund für ein einzelnes Dokument (eindeutig) blockieren andere Datenbankoperationen wie normale Vordergrund-Builds. Im Gegensatz zum Standard-Build im Vordergrund verwendet der Build für Unique eine zusätzliche Stufe (Sortierung von Schlüsseln 2), um nach doppelten Schlüsseln zu suchen. Der (einzigartige) Build im Vordergrund besteht aus sechs Stufen.
- Hintergrund: Durch die Indexerstellung im Hintergrund können andere Datenbankoperationen im Vordergrund ausgeführt werden, während der Index erstellt wird. Der Amazon DocumentDB DocumentDB-Hintergrundaufbau besteht aus acht Phasen.
- Hintergrund (einzigartig): Bei Index-Builds für ein einzelnes Dokument (eindeutig) können andere Datenbankoperationen während der Indexerstellung im Vordergrund ausgeführt werden. Im Gegensatz zum grundlegenden Hintergrundbuild verwendet der Unique-Build eine zusätzliche Phase (Sortierung von Schlüsseln 2), um nach doppelten Schlüsseln zu suchen. Der (einzigartige) Background-Build besteht aus neun Stufen.

Der Standard-Index-Erstellungstyp ist Vordergrund.

Um einen Index im Hintergrund zu erstellen, fügen Sie beim Erstellen des Indexes den Parameter „background“: true hinzu.

Erste Schritte

Verwenden Sie den Befehl CreateIndexes, um die Indexerstellung für eine Sammlung zu starten. Standardmäßig führt der Befehl zwei parallel Worker aus, wodurch die Geschwindigkeit des Indexerstellungsprozesses um das Zweifache erhöht wird.

Der folgende Befehlsprozess zeigt beispielsweise, wie ein Index für das Feld „user_name“ in einem Dokument erstellt und die Geschwindigkeit des Indizierungsvorgangs auf vier Worker erhöht wird:

1. Erstellen Sie Indizes im Hintergrund mithilfe von zwei parallel Workern auf dem Cluster:

```
db.runCommand({"createIndexes":"test","indexes":[{"key": {"user_name":1},
 "name":"username_idx", "background":true }]})
```

2. Um die Geschwindigkeit des Indexerstellungsprozesses zu optimieren, können Sie die Anzahl der Worker mithilfe der Option „worker threads“ („workers“:<number>) im Befehl db.RunCommand createIndexes angeben.

   Erhöhen Sie die Geschwindigkeit des Prozesses auf vier parallel Mitarbeiter:

```
db.runCommand({"createIndexes":"test","indexes":[{"key": {"user_name":1},
 "name":"username_idx", "workers":4}]})
```

> **Note**
>
> Je höher die Anzahl der Mitarbeiter, desto schneller schreitet die Indexerstellung voran. Je höher jedoch die Anzahl der Worker steigt, desto höher steigt die Auslastung der vCPUs und der Lese-I/O Ihrer primären Instance. Stellen Sie sicher, dass Ihr Cluster ausreichend bereitgestellt ist, um die erhöhte Belastung zu bewältigen, ohne andere Workloads zu beeinträchtigen.

Status des Indizierungsfortschritts

Bei der Indexerstellung werden Sammlungen initialisiert, gescannt, Schlüssel sortiert und schließlich Schlüssel mithilfe eines Indexgenerators eingefügt. Der Prozess besteht aus bis zu sechs Phasen, wenn Sie ihn im Vordergrund ausführen, und bis zu neun Phasen, wenn Sie ihn im Hintergrund ausführen. Sie können Statusmetriken wie die prozentuale Fertigstellung, die Gesamtzahl der gescannten Speicherblöcke, die sortierten Schlüssel und die eingefügten Schlüssel Schritt für Schritt anzeigen.

Überwachen Sie den Fortschritt des Indizierungsprozesses mithilfe des Befehls db.currentOp () in der Mongo-Shell. Ein 100-prozentiger Abschluss der letzten Phase zeigt, dass alle Indizes erfolgreich erstellt wurden:

```
db.currentOp({"command.createIndexes": { $exists : true } })
```

> **Note**
>
> Das Anzeigen des Fortschrittsstatus der Indizierung wird nur in Amazon DocumentDB 5.0 unterstützt.

Phasen der Indexerstellung

Stage	Vordergrund	Vordergrund (einzigartig)	Hintergrund	Hintergrund (einzigartig)
Initialisieren	1	1	1	1
Gebäudeindex: initialisieren	2	2	2	2
Gebäudeindex: Sammlung wird gescannt	3	3	3	3
Gebäudeindex: Schlüssel sortieren 1	4	4	4	4
Gebäudeindex: Sortieren von Schlüsseln 2		5		5
Gebäudeindex: Schlüssel einfügen	5	6	5	6
validieren: Index scannen			6	7
validieren: Tupel sortieren			7	8

Stage	Vordergrund	Vordergrund (einzigartig)	Hintergrund	Hintergrund (einzigartig)
validieren: Sammlung scannen			8	9

- initialisieren — CreateIndex bereitet den Index Builder vor. Diese Phase sollte sehr kurz sein.
- Index erstellen: Initialisieren — Der Index Builder bereitet die Erstellung des Indexes vor. Diese Phase sollte sehr kurz sein.
- Index erstellen: Sammlung scannen — Der Index Builder führt einen Sammlungsscan durch, um Indexschlüssel zu sammeln. Die Maßeinheit ist „Blöcke“.

> **Note**
>
> Wenn mehr als ein Worker für den Indexaufbau konfiguriert ist, wird dieser in dieser Phase angezeigt. Die Phase „Erfassung des Scannens“ ist die einzige Phase, in der während der Indexerstellung mehrere Worker verwendet werden. In allen anderen Phasen wird ein einziger Worker angezeigt.

- Index erstellen: Schlüssel sortieren 1 — Der Indexgenerator sortiert die gesammelten Indexschlüssel. Die Maßeinheit ist „Schlüssel“.
- Index erstellen: Schlüssel sortieren 2 — Der Index Builder sortiert die gesammelten Indexschlüssel, die toten Tupeln entsprechen. Diese Phase ist nur für die Erstellung eines eindeutigen Indexes vorgesehen. Die Maßeinheit ist „Schlüssel“.
- Index erstellen: Schlüssel einfügen — Der Index Builder fügt Indexschlüssel in den neuen Index ein. Die Maßeinheit ist „Schlüssel“.
- validieren: Index scannen — CreateIndex durchsucht den Index nach Schlüsseln, die validiert werden müssen. Die Maßeinheit ist „Blöcke“.
- validieren: Tupel sortieren — CreateIndex sortiert die Ausgabe der Indexscanphase.
- validieren: Sammlung scannen — CreateIndex scannt die Sammlung, um die Indexschlüssel zu validieren, die in den beiden vorherigen Phasen gefunden wurden. Die Maßeinheit ist „Blöcke“.

Beispiel für die Ausgabe einer Indexerstellung

Im folgenden Ausgabebeispiel (Indexerstellung im Vordergrund) wird der Status der Indexerstellung angezeigt. Das Feld „msg“ fasst den Baufortschritt zusammen, indem es die Phase und den Prozentsatz der Fertigstellung des Builds angibt. Das Feld „Arbeiter“ gibt die Anzahl der Arbeiter an, die in dieser Phase der Indexerstellung eingesetzt wurden. Das Feld „Fortschritt“ zeigt die tatsächlichen Zahlen, die zur Berechnung des Prozentsatzes der Fertigstellung verwendet wurden.

> **Note**
>
> Die Felder IndexBuildName „current“, „msg“ und „progress“ werden in Amazon DocumentDB Version 4.0 nicht unterstützt.

```
{
    "inprog" : [{
    …
        "command": {
            "createIndexes": "test",
            "indexes": [{
                "v": 2,
                "key": {
                    "user_name": 1
                },
                "name": "user_name_1"
            }],
            "lsid": {
                "id": UUID("094d0fba-8f41-4373-82c3-7c4c7b5ff13b")
            },
            "$db": "test"
        },
        "currentIndexBuildName": user_name_1,
        "msg": "Index Build: building index number_1, stage 6/6 building index:
 656860/1003520 (keys) 65%",
        "workers": 1,
        "progress": {
            "done": 656861,
            "total": 1003520
        },
    …
    ],
```

```
    "ok" : 1
}
```

Ressourcen zur Fehlerbehebung

In den folgenden Ressourcen finden Sie Informationen zur Behebung von Problemen bei der Indexerstellung:

- Die Indexerstellung schlägt fehl
- Latenzprobleme bei der Indexerstellung im Hintergrund und schlägt fehl

Verwaltung von Indizes

Indexblähung

Amazon DocumentDB verwendet Multi-Version Concurrency Control (MVCC) zur Verwaltung gleichzeitiger Transaktionen. Wenn Dokumente gelöscht oder aktualisiert werden, verbleiben ihre vorherigen Versionen als „tote“ Versionen in Sammlungen und Indizes. Durch den Garbage-Collection-Prozess wird automatisch Speicherplatz aus diesen toten Versionen für future Operationen zurückgewonnen.

Ein aufgeblähter Index tritt auf, wenn die Indizes einer Sammlung aufgrund der Anhäufung toter oder veralteter Indexeinträge oder der Fragmentierung innerhalb der Seiten größer werden. Der angegebene Prozentsatz entspricht der Menge an Indexspeicher, die von future Indexeinträgen verwendet werden kann. Diese Aufblähung beansprucht Speicherplatz sowohl im Puffercache als auch im Speicher. Wenn Sie den Bloat entfernen möchten, müssen Sie die Indizes neu erstellen.

Beispiel: Führen Sie den folgenden Befehl aus, um den ungenutzten Speicherplatz für Ihren Index zu ermitteln:

```
db.coll.aggregate({$indexStats:{}});
```

Das Ergebnis sieht in etwa so aus:

```
{
```

```
    "name" : "_id_",
    "key" : {
        "_id" : 1
    },
    "host" : "devbox-test.localhost.a2z.com:27317",
    "size" : NumberLong(827392),
    "accesses" : {
        "ops" : NumberLong(40000),
        "docsRead" : NumberLong(46049),
        "since" : ISODate("2025-04-03T21:44:51.251Z")
    },
    "cacheStats" : {
        "blksRead" : NumberLong(264),
        "blksHit" : NumberLong(140190),
        "hitRatio" : 99.8121
    },
    "unusedStorageSize" : {
        "unusedSizeBytes" : 409600,
        "unusedSizePercent" : 49.51
    }
}
```

Mit dem Befehl ReIndex können Sie Indizes ohne Ausfallzeiten neu erstellen, wofür die gesamte Sammlung gescannt werden muss. Siehe Indexverwaltung mit ReIndex.

Indexverwaltung mit ReIndex

ReIndex ist ein Befehl, mit dem ein Index neu erstellt wird. Er wird normalerweise verwendet, wenn ein Index beschädigt oder ineffizient geworden ist. Im Laufe der Zeit können Indizes aufgrund vieler Aktualisierungen, Einfügungen oder Löschungen ungenutzten Speicherplatz ansammeln, was zu Leistungseinbußen führt. Eine Neuindizierung hilft dabei, diesen ungenutzten Speicherplatz zu entfernen und die Effizienz des Index wiederherzustellen.

Richtlinien für den reIndex

- ReIndex wird nur auf Amazon DocumentDB 5.0 und höher unterstützt
- ReIndex läuft immer im Hintergrund.
- Amazon DocumentDB unterstützt die Neuindizierung eines einzelnen Indexes im Hintergrund, sodass mehrere Worker verwendet werden können. Der alte Index kann für Abfragen verwendet werden, wenn der Reindex-Prozess ausgeführt wird.

- Amazon DocumentDB unterstützt die Indexierung von Fortschrittsberichten über currentOp. Sie können Index-Erstellungsphasen sehen, die den Index-Erstellungsphasen ähneln, die während der Indexerstellung angezeigt wurden. Der einzige Unterschied besteht darin, dass ReIndex immer acht Stufen hat, unabhängig davon, ob es einzigartig ist oder nicht. Es gibt keine Phase „Index erstellen: Schlüssel sortieren 2“.
- ReIndex kann gleichzeitig mit jedem Befehl ausgeführt werden, mit Ausnahme von indexbezogenen Befehlen für dieselbe Sammlung: createIndexes, DropIndexes, CollMod und RenameCollection.
- ReIndex wird derzeit nicht für Text-, Geodaten-, Vektor- und Teilindizes unterstützt.

Build reIndex indizieren

Verwenden Sie den folgenden Befehl, um Ihren Index neu zu erstellen:

```
db.runCommand({ reIndex: "collection-name", index: "index-name"})
```

Optional können Sie auch die Anzahl der Mitarbeiter steuern, die dem Neuaufbauprozess zugewiesen sind:

```
db.runCommand({ reIndex: "collection-name", index: "index-name", workers: number })
```

Spezifische Informationen zur Verwaltung von Indizes mit Java finden Sie unter Indexverwaltung in Amazon DocumentDB mit Java.

Bewährte Methoden für die Arbeit mit Indizes

Indizes erstellen

Wenn Sie Daten in Amazon DocumentDB importieren, sollten Sie Ihre Indizes erstellen, bevor Sie große Datensätze importieren. Sie können das Amazon DocumentDB Index Tool verwenden, um Indizes aus einer laufenden MongoDB-Instance oder einem Mongodump-Verzeichnis zu extrahieren und diese Indizes in einem Amazon DocumentDB-Cluster zu erstellen. Weitere Hinweise zu Migrationen finden Sie unter Zu DocumentDB migrieren.

Index-Selektivität

Wir empfehlen Ihnen, die Erstellung von Indizes auf Felder zu beschränken, bei denen die Anzahl der Duplikatwerte weniger als 1 % der Gesamtzahl der Dokumente in der Sammlung beträgt. Wenn Ihre Sammlung beispielsweise 100.000 Dokumente enthält, erstellen Sie nur Indizes für Felder, in denen derselbe Wert 1.000 Mal oder weniger vorkommt.

Wenn Sie einen Index mit einer hohen Anzahl von Einzelwerten (d. h. einer hohen Kardinalität) auswählen, wird sichergestellt, dass Filtervorgänge eine geringe Anzahl von Dokumenten zurückgeben, wodurch eine gute Leistung bei Indexscans erzielt wird. Ein Beispiel für einen Index hoher Kardinalität ist ein einzigartiger Index, der garantiert, dass Gleichheitsprädikate höchstens ein einziges Dokument zurückgeben. Beispiele für niedrige Kardinalität sind ein Index über ein boolesches Feld und ein Index über einen Wochentag. Aufgrund ihrer schlechten Leistung ist es unwahrscheinlich, dass Indizes mit niedriger Kardinalität vom Abfrageoptimierer der Datenbank ausgewählt werden. Gleichzeitig verbrauchen Indizes mit niedriger Kardinalität weiterhin Ressourcen wie Festplattenspeicher und. I/Os Als Faustregel gilt, dass Sie Indizes für Felder verwenden sollten, bei denen die typische Wertehäufigkeit 1 % der Gesamtsammlungsgröße oder weniger beträgt.

Darüber hinaus wird empfohlen, nur Indizes für Felder zu erstellen, die häufig als Filter verwendet werden, und regelmäßig nach nicht verwendeten Indizes zu suchen. Weitere Informationen finden Sie unter the section called “Analysieren Sie die Indexnutzung und identifizieren Sie ungenutzte Indizes”.

Auswirkung von Indizes auf das Schreiben von Daten

Zwar können Indizes die Abfrageleistung verbessern, da nicht jedes Dokument in einer Sammlung gescannt werden muss, diese Verbesserung erfordert jedoch einen Kompromiss. Für jeden Index einer Sammlung muss die Datenbank jedes Mal, wenn ein Dokument eingefügt, aktualisiert oder gelöscht wird, die Sammlung aktualisieren und die Felder in jeden der Indizes für die Sammlung schreiben. Wenn eine Sammlung beispielsweise über neun Indizes verfügt, muss die Datenbank zehn Schreibvorgänge durchführen, bevor die Operation dem Kunden bestätigt wird. Somit führt jeder zusätzliche Index zu zusätzlicher Schreiblatenz und zu einer Erhöhung des insgesamt genutzten Speichers. I/Os

Cluster-Instances müssen über eine angemessene Größe verfügen, um den gesamten Arbeitsspeicher zu erhalten. Dadurch wird vermieden, dass Indexseiten kontinuierlich vom Speichervolumen gelesen werden müssen, was sich negativ auf die Leistung auswirkt und höhere I/O Kosten verursacht. Weitere Informationen finden Sie unter Instanzgröße.

Um eine optimale Leistung zu erzielen, sollten Sie die Anzahl der Indizes in Ihren Sammlungen minimieren und nur die Indizes hinzufügen, die zur Verbesserung der Leistung bei häufigen Abfragen erforderlich sind. Bei variierenden Workloads gilt als gute Richtschnur, die Anzahl der Indizes pro Sammlung auf fünf oder weniger zu beschränken.

Identifizieren fehlender Indizes

Die Identifizierung fehlender Indizes ist eine bewährte Methode, die wir empfehlen, regelmäßig durchzuführen. Weitere Informationen finden Sie unter the section called “Identifizieren Sie fehlende Indizes”.

Identifizieren ungenutzter Indizes

Da das Identifizieren und Löschen fehlender Indizes eine bewährte Vorgehensweise ist, empfiehlt sich eine regelmäßige Durchführung. Weitere Informationen finden Sie unter the section called “Analysieren Sie die Indexnutzung und identifizieren Sie ungenutzte Indizes”.

Indextypen

Themen

- Indizes für einzelne Felder
- Zusammengesetzte Indizes
- Multi-key Indizes
- Textindizes
- Geospatiale Indizes
- Vektor-Indizes

Indizes für einzelne Felder

Einzelfeldindizes speichern Informationen aus jedem einzelnen Feld in einer Sammlung von Dokumenten. Standardmäßig haben alle Sammlungen einen Index für das `_id` Feld. Sie können zusätzliche Indizes hinzufügen, um wichtige Abfragen und Operationen zu beschleunigen.

Indizes für einzelne Felder sind in folgenden Fällen von Vorteil:

- Ihre Anwendung fragt häufig Dokumente ab oder filtert sie anhand der Werte eines bestimmten Felds.

- Sie müssen Dokumente effizient nach einem bestimmten Feld sortieren.
- Sie möchten sicherstellen, dass ein bestimmtes Feld in allen Dokumenten einer Sammlung eindeutig ist, indem Sie einen eindeutigen Index erstellen.

Unterstützte Indexeigenschaften

Option	3.6	4,0	5.0	8.0	Elastischer Cluster
name	Ja	Ja	Ja	Ja	Ja
einzigartig	Ja	Ja	Ja	Ja	Ja
spärlich *	Ja	Ja	Ja	Ja	Ja
teilweise * FilterExpression	Nein	Nein	Ja	Ja	Nein
ablaufen AfterSeconds	Ja	Ja	Ja	Ja	Ja

* Die `partialFilterExpression` Optionen `sparse` und können nicht zusammen in derselben Indexdefinition verwendet werden. Wenn Sie versuchen, einen Index mit diesen Optionen zu erstellen, schlägt dies mit dem folgenden Fehler fehl:

```
Error in specification: cannot mix partialFilterExpression and sparse options
```

Einen Index für ein einzelnes Feld erstellen

Verwenden Sie die `createIndex()` Methode, um einen einzelnen Feldindex zu erstellen. Die Syntax lautet:`db.collection.createIndex(<key>, <options>)`.

Der `key` Parameter ist ein JSON-Dokument, das das Feld und die Index-Sortierreihenfolge angibt:

```
{
  "<field>": <1 (ascending)|-1 (descending)>
```

```
}
```

Der `options` Parameter ist ein JSON-Dokument, das die Optionen für den Index angibt:

```
{
  "name": "<name>",
  "unique": <true | false>,
  "sparse": <true | false>,
  "partialFilterExpression": <filter expression>,
  "expireAfterSeconds": <seconds before expiry>
}
```

Beispiele für die Erstellung von Einzelfeldindizes finden Sie unter Indexeigenschaften.

Zusammengesetzte Indizes

Zusammengesetzte Indizes speichern Informationen aus zwei oder mehr Feldern in einer Sammlung von Dokumenten und ermöglichen so Abfragen im ersten Feld oder in beliebigen Präfixfeldern. Diese Indizes optimieren die Leistung für Abfragen, die nach mehreren Feldern gleichzeitig filtern oder Filter mit Sortiervorgängen kombinieren. Sie eignen sich auch für Abfragen mit einer einzigen Bedingung in den indizierten Feldern ganz links. Die Datenbank nutzt diese Indexeinträge, um passende Dokumente effizient zu finden, ohne die Sammlung vollständig scannen zu müssen.

Zusammengesetzte Feldindizes sind nützlich, wenn:

- Sie müssen nach mehreren Feldern gleichzeitig filtern.
- Sie müssen das Filtern mit Sortiervorgängen kombinieren.

Unterstützte Indexeigenschaften

Option	3.6	4,0	5.0	8.0	Elastischer Cluster
name	Ja	Ja	Ja	Ja	Ja
einzigartig	Ja	Ja	Ja	Ja	Ja
spärlich *	Ja	Ja	Ja	Ja	Ja

Option	3.6	4,0	5.0	8.0	Elastischer Cluster
teilweise * FilterExpression	Nein	Nein	Ja	Ja	Nein

* Die `partialFilterExpression` Optionen `sparse` und können nicht zusammen in derselben Indexdefinition verwendet werden. Wenn Sie versuchen, einen Index mit diesen Optionen zu erstellen, schlägt dies mit dem folgenden Fehler fehl:

```
Error in specification: cannot mix partialFilterExpression and sparse options
```

Einen zusammengesetzten Index erstellen

Verwenden Sie die `createIndex()` Methode, um einen zusammengesetzten Index zu erstellen. Die Syntax der Methode lautet: `db.collection.createIndex(<keys>, <options>)`

Der `keys` Parameter ist ein JSON-Dokument, das die Felder und die Index-Sortierreihenfolge angibt:

```
{
  "<field 1>": <1 (ascending)|-1 (descending)>,
  "<field 2>": <1 (ascending)|-1 (descending)>,
  ...
}
```

Beachten Sie, dass in einem zusammengesetzten Index nur ein Feld ein Array sein kann. Wenn Sie versuchen, einen zusammengesetzten Index für zwei oder mehr Array-Felder zu erstellen, schlägt dies mit dem folgenden Fehler fehl:

```
multiple fields of compound index cannot be arrays
```

Der `options` Parameter ist ein JSON-Dokument, das die Optionen für den Index angibt:

```
{
  "name": "<name>",
  "unique": <true | false>,
```

```
  "sparse": <true | false>,
  "partialFilterExpression": <filter expression>
}
```

Beispiele für die Erstellung zusammengesetzter Indizes finden Sie unter Indexeigenschaften.

Multi-key Indizes

Für Felder, die einen Array-Wert haben, ermöglicht Ihnen ein Multi-Key-Index, einen Indexschlüssel für jedes Element im Array zu erstellen. Durch die Indizierung eines Arrays wird ein Indexeintrag für jedes Element des Arrays erstellt.

Multi-key Indizes sind nützlich, wenn Ihre Anwendung häufig Dokumente anhand von Werten in Arrays abfragt oder filtert.

Unterstützte Indexeigenschaften

Option	3.6	4,0	5.0	8.0	Elastischer Cluster
name	Ja	Ja	Ja	Ja	Ja
einzigartig	Ja	Ja	Ja	Ja	Ja
spärlich *	Ja	Ja	Ja	Ja	Ja
teilweise * FilterExpression	Nein	Nein	Ja	Ja	Nein
ablaufen AfterSeconds	Ja	Ja	Ja	Ja	Ja

* Die `partialFilterExpression` Optionen `sparse` und können nicht zusammen in derselben Indexdefinition verwendet werden. Wenn Sie versuchen, einen Index mit diesen Optionen zu erstellen, schlägt dies mit dem folgenden Fehler fehl:

```
Error in specification: cannot mix partialFilterExpression and sparse options
```

Einen Index mit mehreren Schlüsseln erstellen

Verwenden Sie die `createIndex()` Methode, um einen Index mit mehreren Schlüsseln zu erstellen. Die Syntax der Methode lautet: `db.collection.createIndex(<key>, <options>)`

Der `key` Parameter ist ein JSON-Dokument, das das Feld und die Index-Sortierreihenfolge angibt:

```
{
  "<field>": <1 (ascending)|-1 (descending)>
}
```

Der `options` Parameter ist ein JSON-Dokument, das die Optionen für den Index angibt:

```
{
  "name": "<name>",
  "unique": <true | false>,
  "sparse": <true | false>,
  "partialFilterExpression": <filter expression>,
  "expireAfterSeconds": <seconds before expiry>
}
```

Im folgenden Beispiel wird ein Index mit mehreren Schlüsseln für das `categories` Feld erstellt, das in aufsteigender Reihenfolge nach dem Namen sortiert ist: `book_categories`

```
db.collection.createIndex(
  {
    "categories": 1
  },
  {
    "name": "book_categories"
  }
)
```

Beispiele für die Erstellung von Indizes mit mehreren Schlüsseln finden Sie unter Indexeigenschaften.

Textindizes

Textindizes sind nützlich bei der Suche nach Wörtern oder Ausdrücken in Textfeldern in Dokumenten, sodass Sie Volltextsuchfunktionen ausführen können. Sie können Einzelfeld-Textindizes oder zusammengesetzte Textindizes mit mehr als einem Textfeld erstellen. Sie können jedoch nur einen

Textindex pro Sammlung haben. Weitere Informationen finden Sie unter Nutzen Sie das Potenzial der Amazon DocumentDB-Textsuche mit realen Anwendungsfällen.

Unterstützte Indexeigenschaften

Option	3.6	4,0	5.0	8.0	Elastischer Cluster
name	Nein	Nein	Ja	Ja	Nein

Einen Textindex erstellen

Verwenden Sie die `createIndex()` Methode, um einen Textindex zu erstellen. Die Syntax der Methode lautet: `db.collection.createIndex(<keys>, <options>)`

Der `keys` Parameter ist ein JSON-Dokument, das die Felder und den Textindextyp angibt:

```
{
  "<field 1>": "text",
  "<field 2>": "text"
}
```

Der `options` Parameter ist ein JSON-Dokument, das den Namen des Indexes angibt:

```
{
  "name": "<name>"
}
```

Beispiele für die Erstellung von Textindizes finden Sie unter Indexeigenschaften.

Geospatiale Indizes

Geodatenindizes sind spezielle Indextypen, mit denen Geodaten, die in einer Sammlung von Dokumenten gespeichert sind, effizient abgefragt und verwaltet werden können. Amazon DocumentDB unterstützt 2dSphere-Indizes, die speziell für die Verarbeitung von Geodaten auf einer Kugel (wie der Erde) entwickelt wurden. Dies ermöglicht genaue Berechnungen und Abfragen auf der Grundlage sphärischer Geometrie.

Geodatenindizes sind nützlich, wenn Ihre Anwendungen standortbezogene Abfragen ausführen müssen, z. B.:

- Suche nach Sehenswürdigkeiten in der Nähe,
- Feststellen, ob ein Standort in ein bestimmtes Gebiet fällt
- Berechnung von Entfernungen zwischen Standorten

Unterstützte Indexeigenschaften

Option	3.6	4,0	5.0	8.0	Elastischer Cluster
name	Ja	Ja	Ja	Ja	Ja

Einen Geodatenindex erstellen

Verwenden Sie die `createIndex()` Methode, um einen Geodatenindex zu erstellen. Die Syntax der Methode lautet: `db.collection.createIndex(<key>, <options>)`

Der `key` Parameter ist ein JSON-Dokument, das das Feld und den 2dSphere-Indextyp angibt:

```
{
  "<field>": "2dsphere"
}
```

Der `options` Parameter ist ein JSON-Dokument, das die Optionen für den Index angibt:

```
{
  "name": "<name>"
}
```

Beispiele für die Erstellung von Geoindizes finden Sie unter Indexeigenschaften.

Vektor-Indizes

Vektorindizes sind spezielle Indextypen, mit denen Vektordaten, die in einer Sammlung von Dokumenten gespeichert sind, effizient abgefragt und verwaltet werden können. Amazon

DocumentDB unterstützt die Indizes Hierarchical Navigable Small World (HNSW) und Inverted File with Flat Compression (IVFFlat).

Weitere Informationen finden Sie unter Vektorsuche für Amazon DocumentDB.

Vektorindizes sind vorteilhaft für maschinelles Lernen und generative KI-Anwendungsfälle, wie z. B.:

- Semantische Suche
- Produktempfehlung
- Personalisierung
- Chatbots
- Aufdeckung von Betrug
- Erkennung von Anomalien

Unterstützte Indexeigenschaften

Option	3.6	4,0	5.0	8.0	Elastischer Cluster
name	Nein	Nein	Ja	Ja	Nein

Einen Vektorindex erstellen

Verwenden Sie den Befehl createIndex mit der `runCommand()` Methode, um einen Vektorindex zu erstellen. Die Syntax lautet wie folgt:

```
db.runCommand({
  "createIndexes": "<collection>",
  "indexes": [{
    "key": {
      "<field>": "vector"
    },
    "name": "<name>",
    "vectorOptions": {
      "type": "<hnsw> | <ivfflat>",
      "dimensions": <number of dimensions>,
      "similarity": "<euclidean>|<cosine>|<dotProduct>",
```

```
      "lists": <number_of_lists> [applicable for IVFFlat],
      "m": <max number of connections> [applicable for HNSW],
      "efConstruction": <size of the dynamic list for index build> [applicable for
 HNSW]
    }
  }]
})
```

Der Schlüsselparameter ist ein JSON-Dokument, das den Feld- und Vektorindextyp angibt:

```
{
  "<field>": "vector"
}
```

Beispiele für die Erstellung von Vektorindizes finden Sie unter Indexeigenschaften.

Indexeigenschaften

Indexeigenschaften definieren das Verhalten und die Eigenschaften von Indizes in Amazon DocumentDB. Wenn Sie diese Eigenschaften verstehen, können Sie effiziente Indizes entwerfen, die den spezifischen Anforderungen Ihrer Anwendung entsprechen.

Topics

- Index-Eigenschaft: Name
- Index-Eigenschaft: einzigartig
- Index-Eigenschaft: spärlich
- Index-Eigenschaft: teilweise FilterExpression
- Index-Eigenschaft: expire AfterSeconds

Index-Eigenschaft: Name

Unterstützte Indextypen

Option	3.6	4,0	5.0	8.0	Elastischer Cluster
einzelnes Feld	Ja	Ja	Ja	Ja	Ja
compound	Ja	Ja	Ja	Ja	Ja
mehrere Schlüssel	Ja	Ja	Ja	Ja	Ja
text	Nein	Nein	Ja	Ja	Nein
Geodaten	Ja	Ja	Ja	Ja	Ja
Vektor	Nein	Nein	Ja	Ja	Nein

Verwenden Sie die Option name, um einen optionalen Namen für den Index anzugeben.

In allen Beispielen wird das folgende Beispieldokument verwendet:

```
{
  "productId": "PROD133726",
  "sku": "SKU24224",
  "name": "Basic Printer",
  "manufacturer": "The Manufacturer",
  "tags": [ "printer", "basic", "electronics", "business" ],
  "barcodes": [ "542364671", "886330670", "437445606" ],
  "reviews": [
    {
      "review_date": ISODate('2024-01-19T21:37:10.585Z'),
      ...
    }
  ],
  "material": "Polycarbonate",
  "color": "Space Gray",
```

```
  "supplier": {
    "supplierId": "SUP4",
    "location": {
      "type": "Point",
      "coordinates": [ -71.0589, 42.3601 ]
    }
  },
  "productEmbedding": [
    -0.019320633663838058,
    0.019672111388113596
  ],
  "lastUpdated": ISODate('2025-10-20T21:37:10.585Z')
}
```

Einzelnes Feld

```
db.collection.createIndex(
  {
    "productId": 1
  },
  {
    "name": "single_field_index"
  }
)
```

Zusammengesetzt

```
db.collection.createIndex(
  {
    "productId": 1,
    "manufacturer": 1
  },
  {
    "name": "compound_index"
  }
)
```

Multi-key

```
db.collection.createIndex(
  {
```

```
    "tags": 1
  },
  {
    "name": "multikey_index"
  }
)
```

Text

```
db.collection.createIndex(
  {
    "name": "text"
  },
  {
    "name": "text_index"
  }
)
```

Geodaten

```
db.collection.createIndex(
  {
    "supplier.location": "2dsphere"
  },
  {
    "name": "geospatial_index"
  }
)
```

Vektor

```
db.runCommand({
  "createIndexes": "collection",
  "indexes": [{
    "key": {
      "productEmbedding": "vector"
    },
    "name": "hnsw_index",
    "vectorOptions": {
      "type": "hnsw",
      "dimensions": 2,
```

```
      "similarity": "euclidean",
      "m": 16,
      "efConstruction": 64
    }
  }]
})
```

Index-Eigenschaft: einzigartig

Unterstützte Indextypen

Option	3.6	4,0	5.0	8.0	Elastischer Cluster
einzelnes Feld	Ja	Ja	Ja	Ja	Ja
compound	Ja	Ja	Ja	Ja	Ja
mehrere Schlüssel	Ja	Ja	Ja	Ja	Ja

Verwenden Sie die Option „Eindeutig“, um sicherzustellen, dass die Felder in allen Dokumenten einer Sammlung eindeutig sind.

Beispiele

Die folgenden Beispiele zeigen, wie eindeutige Indizes für das folgende Beispieldokument erstellt werden:

```
{
  "productId": "PROD133726",
  "sku": "SKU24224",
  "name": "Basic Printer",
  "manufacturer": "The Manufacturer",
  "tags": [ "printer", "basic", "electronics", "business" ],
  "barcodes": [ "542364671", "886330670", "437445606" ],
  "reviews": [
    {
```

```
      "review_date": ISODate('2024-01-19T21:37:10.585Z'),
      ...
    }
  ],
  "material": "Polycarbonate",
  "color": "Space Gray",
  "supplier": {
    "supplierId": "SUP4",
    "location": {
      "type": "Point",
      "coordinates": [ -71.0589, 42.3601 ]
    }
  },
  "productEmbedding": [
    -0.019320633663838058,
    0.019672111388113596
  ],
  "lastUpdated": ISODate('2025-10-20T21:37:10.585Z')
}
```

einzelnes Feld

Erstellen Sie einen eindeutigen Einzelfeldindex für ProductID, um sicherzustellen, dass dieselbe ProductID nicht in mehr als einem Dokument vorhanden ist:

```
db.collection.createIndex(
  {
    "productId": 1
  },
  {
    name: "productId_unique",
    unique: true
  }
)
```

Verbindung

Erstellen Sie einen eindeutigen zusammengesetzten Index für SKU und Hersteller, um sicherzustellen, dass dieselbe Kombination aus SKU und Hersteller nicht in mehr als einem Dokument vorkommt:

```
db.collection.createIndex(
```

```
  {
    "sku": 1,
    "manufacturer": 1
  },
  {
    name: "sku_and_manufacturer_unique",
    unique: true
  }
)
```

mehrere Schlüssel

Erstellen Sie einen eindeutigen Index mit mehreren Schlüsseln für Barcodes, um sicherzustellen, dass kein Wert im Barcode-Array in mehr als einem Dokument vorkommt:

```
db.collection.createIndex(
  {
    "barcodes": 1
  },
  {
    name: "barcodes_unique",
    unique: true
  }
)
```

Durch die Indizierung eines Arrays wird für jedes Element des Arrays ein Indexeintrag erstellt. Wenn ein Array beispielsweise 50 Elemente enthält, hat es 50 Indexeinträge. Aus diesem Grund erzwingen eindeutige Indizes mit mehreren Schlüsseln die Eindeutigkeit aller einzelnen Elemente. Die folgenden Dokumente verstoßen beispielsweise gegen die Eindeutigkeitsbeschränkung für den Feldindex des Wertearrays:

```
{ "values": [ 1, 2, 3] }
{ "values": [ 3, 2 ] }   --> 3 and 2 already exist
{ "values": [ 1 ] }      --> 1 already exists
```

Beachten Sie das folgende Verhalten bei eindeutigen Indizes:

1. Wenn Sie einen eindeutigen Index für bestehende Daten erstellen, in dem zwei (oder mehr) Dokumente dieselben Werte für die indizierten Felder haben, schlägt die Indexerstellung mit dem folgenden Fehler fehl: `could not create unique index: <collection> index: <index name>`

2. Wenn Sie ein Dokument einfügen, bei dem der Wert des indizierten Felds mit dem Wert dieses Felds in einem anderen Dokument übereinstimmt, schlägt das Einfügen fehl und es wird der folgende Fehler angezeigt: `E11000 duplicate key error collection: <collection> index: <index name>`
3. Wenn Sie ein vorhandenes Dokument so aktualisieren, dass der neue Wert des indizierten Felds mit dem Wert dieses Felds in einem anderen Dokument übereinstimmt, schlägt die Aktualisierung mit dem folgenden Fehler fehl: `E11000 duplicate key error collection: <collection> index: <index name>`
4. Wenn das indizierte Feld in einem Dokument fehlt, wird der Wert als Null behandelt. Indexerstellungen, Einfügungen und Aktualisierungen schlagen wie oben beschrieben fehl, wenn das indizierte Feld in zwei (oder mehr) Dokumenten fehlt.

Index-Eigenschaft: spärlich

Unterstützte Indextypen

Option	3.6	4,0	5.0	8.0	Elastischer Cluster
einzelnes Feld	Ja	Ja	Ja	Ja	Ja
compound	Ja	Ja	Ja	Ja	Ja
mehrere Schlüssel	Ja	Ja	Ja	Ja	Ja

Verwenden Sie die Sparse-Option, um die Indizierung von Dokumenten zu überspringen, bei denen die indizierten Felder fehlen, wodurch die Indexgröße reduziert und Speicherplatz gespart wird. Da die Indexgröße kleiner ist, sind die Abfragen, die sie verwenden, effizienter. Damit eine Abfrage einen dünn besetzten Index verwendet, müssen Sie die $exists-Klausel für die indizierten Felder verwenden. Wenn Sie die $exists-Klausel weglassen, verwendet Amazon DocumentDB den Sparse-Index nicht.

Beispiele

Die folgenden Beispiele zeigen, wie man Sparse-Indizes für das folgende Beispieldokument erstellt:

```
{
  "productId": "PROD133726",
  "sku": "SKU24224",
  "name": "Basic Printer",
  "manufacturer": "The Manufacturer",
  "tags": [ "printer", "basic", "electronics", "business" ],
  "barcodes": [ "542364671", "886330670", "437445606" ],
  "reviews": [
    {
      "review_date": ISODate('2024-01-19T21:37:10.585Z'),
      ...
    }
  ],
  "material": "Polycarbonate",
  "color": "Space Gray",
  "supplier": {
    "supplierId": "SUP4",
    "location": {
      "type": "Point",
      "coordinates": [ -71.0589, 42.3601 ]
    }
  },
  "productEmbedding": [
    -0.019320633663838058,
    0.019672111388113596
  ],
  "lastUpdated": ISODate('2025-10-20T21:37:10.585Z')
}
```

Beachten Sie, dass die Felder Rezensionen, Material und Farben nicht in allen Dokumenten vorhanden sind.

einzelnes Feld

Erstellen Sie einen spärlichen Einzelfeldindex für das Materialfeld:

```
db.collection.createIndex(
  {
    "material": 1
  },
  {
    "name": "material_sparse",
    "sparse": true
```

```
  }
)
```

Dieser Index wird verwendet, um alle Produkte zu finden, die einen Wert für Material haben:

```
db.collection.find({
  "material": {
    $exists: true
  }
})
```

Verbindung

Erstellen Sie einen spärlichen zusammengesetzten Index für die Material- und Farbfelder:

```
db.collection.createIndex(
  {
    "material": 1,
    "color": 1
  },
  {
    "name": "material_and_color_sparse",
    "sparse": true
  }
)
```

Dieser Index wird verwendet, um alle Produkte zu finden, die eine beliebige Kombination von Material- und Farbwerten aufweisen:

```
db.collection.find({
  "material": {
    $exists: true
  }
})

db.collection.find({
  "color": {
    $exists: true
  }
})
```

```
db.collection.find({
  $and: [
    {
      "material": {
        $exists: true
      }
    },
    {
      "color": {
        $exists:true
      }
    }
  ]
})

db.collection.find({
  $and: [
    {
      "color": {
        $exists: true
      }
    },
    {
      "material": {
        $exists:true
      }
    }
  ]
})
```

mehrere Tasten

Erstellen Sie einen spärlichen Index mit mehreren Schlüsseln für das Bewertungs-Array:

```
db.collection.createIndex(
  {
    "reviews": 1
  },
  {
    "name": "reviews_sparse",
    "sparse": true
  }
)
```

Dieser Index wird verwendet, um alle Produkte zu finden, die über ein Bewertungs-Array verfügen:

```
db.collection.find({
  "reviews": {
    $exists: true
  }
})
```

Index-Eigenschaft: teilweise FilterExpression

Unterstützte Indextypen

Option	3.6	4,0	5.0	8.0	Elastischer Cluster
einzelnes Feld	Nein	Nein	Ja	Ja	Nein
compound	Nein	Nein	Ja	Ja	Nein
mehrere Schlüssel	Nein	Nein	Ja	Ja	Nein
Geodaten	Nein	Nein	Nein	Nein	Nein

Verwenden Sie die FilterExpression Option partiell, um einen Teilindex zu erstellen, der nur Dokumente enthält, die eine bestimmte Filterbedingung erfüllen. Auf diese Weise können Sie effizientere Indizes erstellen, indem Sie nur eine Teilmenge der Dokumente in einer Sammlung indizieren, anstatt alle Dokumente zu indizieren, wodurch die Indexgröße reduziert und Speicherplatz gespart wird. Da die Indexgröße kleiner ist, sind die Abfragen, die sie verwenden, effizienter. Amazon DocumentDB verwendet den Teilindex in den folgenden Szenarien:

- Das Abfrageprädikat entspricht exakt dem Filterausdruck für den partiellen Index.
- Das erwartete Ergebnis des Abfragefilters ist eine logische Teilmenge des Teilfilters.
- Ein Unterprädikat der Abfrage kann in Verbindung mit anderen Indizes verwendet werden.

Weitere Informationen finden Sie unter Teilweiser Index.

Beispiele

Die folgenden Beispiele zeigen, wie Teilindizes für das folgende Beispieldokument erstellt werden:

```
{
  "productId": "PROD133726",
  "sku": "SKU24224",
  "name": "Basic Printer",
  "manufacturer": "The Manufacturer",
  "tags": [ "printer", "basic", "electronics", "business" ],
  "barcodes": [ "542364671", "886330670", "437445606" ],
  "reviews": [
    {
      "review_date": ISODate('2024-01-19T21:37:10.585Z'),
      ...
    }
  ],
  "material": "Polycarbonate",
  "color": "Space Gray",
  "supplier": {
    "supplierId": "SUP4",
    "location": {
      "type": "Point",
      "coordinates": [ -71.0589, 42.3601 ]
    }
  },
  "productEmbedding": [
    -0.019320633663838058,
    0.019672111388113596
  ],
  "lastUpdated": ISODate('2025-10-20T21:37:10.585Z')
}
```

einzelnes Feld

Erstellen Sie für Produkte mit der Farbe Space Grey einen teilweisen Herstellerindex für ein einzelnes Feld:

```
db.collection.createIndex(
  {
    "manufacturer": 1
  },
  {
```

```
    "name": "manufacturer_space_gray",
    "partialFilterExpression": {
      "color": {
        $eq: "Space Gray"
      }
    }
  }
)
```

Dieser Index wird bei der Suche nach Produkten in der Farbe Space Grey nach Herstellern verwendet:

```
db.collection.find({
  "manufacturer": "The Manufacturer",
  "color": {
    $eq: "Space Gray"
  }
})
```

Verbindung

Erstellen Sie einen partiellen Verbundindex nach Hersteller und Farbe für Produkte, die aus Polycarbonat bestehen:

```
db.collection.createIndex(
  {
    "manufacturer": 1,
    "color": 1
  },
  {
    "name": "manufacturer_and_color_polycarbonate",
    "partialFilterExpression": {
      "material": {
        $eq: "Polycarbonate"
      }
    }
  }
)
```

Dieser Index wird bei der Suche nach Produkten aus Polycarbonat-Material nach Hersteller und Farbe verwendet:

```
db.collection.find({
  "manufacturer": "The Manufacturer",
  "color": "Space Gray",
  "material": {
    $eq: "Polycarbonate"
  }
})
```

mehrere Tasten

Erstellen Sie einen teilweisen Index mit mehreren Schlüsseln für Tags für Produkte, deren Hersteller den Namen The Manufacturer hat:

```
db.collection.createIndex(
  {
    "tags": 1
  },
  {
    "name": "tags_the_manufacturer",
    "partialFilterExpression": {
      "manufacturer": {
        $eq: "The Manufacturer"
      }
    }
  }
)
```

Dieser Index wird bei der Suche nach Produkten verwendet, die mit einem Drucker gekennzeichnet sind und deren Hersteller von The Manufacturer stammt:

```
db.collection.find({
  "tags": "printer",
  "manufacturer": {
    $eq: "The Manufacturer"
  }
})
```

Index-Eigenschaft: expire AfterSeconds

Unterstützte Indextypen

Art des Indexes	3.6	4,0	5.0	8.0	Elastischer Cluster
einzelnes Feld	Ja	Ja	Ja	Ja	Ja
mehrere Schlüssel	Ja	Ja	Ja	Ja	Ja

Verwenden Sie die AfterSeconds Option expire, um einen Time-to-Live-Index (TTL) zu erstellen. TTL-Indizes ermöglichen es Ihnen, Dokumente anhand ihres Alters zu löschen, basierend auf der Timeout-Bedingung für jedes Dokument. Wenn ein Dokument das angegebene TTL-Alter erreicht, wird es aus der Sammlung gelöscht.

Bewährte Methoden für TTL-Löschungen finden Sie unter. TTL- und Zeitreihen-Workloads

Beispiele

Die folgenden Beispiele zeigen, wie TTL-Indizes für das folgende Beispieldokument erstellt werden:

```
{
  "productId": "PROD133726",
  "sku": "SKU24224",
  "name": "Basic Printer",
  "manufacturer": "The Manufacturer",
  "tags": [ "printer", "basic", "electronics", "business" ],
  "barcodes": [ "542364671", "886330670", "437445606" ],
  "reviews": [
    {
      "review_date": ISODate('2024-01-19T21:37:10.585Z'),
      "rating": 4,
      "comment": "Good product"
    },
    {
      "review_date": ISODate('2024-03-15T14:22:33.120Z'),
      "rating": 5,
```

```
      "comment": "Excellent printer"
    },
    {
      "review_date": ISODate('2024-06-08T09:45:18.890Z'),
      "rating": 3,
      "comment": "Average quality"
    }
  ],
  "material": "Polycarbonate",
  "color": "Space Gray",
  "supplier": {
    "supplierId": "SUP4",
    "location": {
      "type": "Point",
      "coordinates": [ -71.0589, 42.3601 ]
    }
  },
  "productEmbedding": [
    -0.019320633663838058,
    0.019672111388113596
  ],
  "lastUpdated": ISODate('2025-10-20T21:37:10.585Z')
}
```

einzelnes Feld

Erstellen Sie einen TTL-Index für LastUpdated, um Dokumente zu löschen, die seit 90 Tagen nicht aktualisiert wurden:

```
db.collection.createIndex(
  {
    "lastUpdated": 1
  },
  {
    "name": "lastUpdated_ttl",
    "expireAfterSeconds": 7776000
  }
)
```

mehrere Schlüssel

Erstellen Sie einen TTL-Index auf reviews.review_date, um Dokumente zu löschen, für die im letzten Jahr keine Bewertungen abgegeben wurden:

```
db.collection.createIndex(
  {
    "reviews.review_date": 1
  },
  {
    "name": "reviews_review_date_ttl",
    "expireAfterSeconds": 31536000
  }
)
```

Beachten Sie, dass alle Elemente im Array überprüft werden, wenn sich der TTL-Index auf ein Array-Feld bezieht. Wenn ein Zeitstempel im Array die Timeout-Bedingung erfüllt, wird das Dokument gelöscht.

Optimierung der Leistung

Dieses Kapitel enthält Anleitungen zur Optimierung der Leistung von Amazon DocumentDB und zur Behebung häufiger Leistungsprobleme.

Themen

- Allgemeine Leistungsprobleme
- Anti-patterns
- Tipps zur Leistungsverbesserung
- Plananalyse abfragen

Allgemeine Leistungsprobleme

In diesem Abschnitt werden allgemeine Leistungsprobleme behandelt, auf die Sie bei Amazon DocumentDB stoßen können, und wie Sie diese lösen können.

Themen

- Hohe CPU-Auslastung
- Verbindungsprobleme mit Amazon DocumentDB
- Abfrage läuft langsam

Hohe CPU-Auslastung

Eine hohe CPU-Auslastung ist eines der Probleme, auf die Sie bei der Arbeit mit Amazon DocumentDB irgendwann stoßen könnten. Dieser Abschnitt bietet Einblicke zur Lösung des Problems.

Identifizierung — Finden Sie das Problem

Eine hohe CPU-Auslastung auf Amazon DocumentDB DocumentDB-Instances führt zu einer Verlangsamung der Anwendungen, da die Latenzen bei allen Datenbankoperationen erhöht werden. Wenn die CPU-Auslastung von Amazon DocumentDB den optimalen Wert überschreitet, verlängern sich die Ausführungszeiten von Abfragen, der Verbindungsaufbau dauert länger und die Reaktionsfähigkeit der Anwendung nimmt ab. CPU-Spitzen auf der primären Instance verlangsamen

Schreibvorgänge, während Spitzenwerte bei Replikaten zu einer höheren Latenz bei Lesevorgängen führen.

Einige der häufigsten Ursachen für eine hohe CPU-Auslastung in Amazon DocumentDB könnten sein:

- Sammlungsscans: Abfragen ohne korrekte Indizes erzwingen vollständige Sammelscans, wodurch übermäßig viel CPU zur Untersuchung jedes Dokuments verbraucht wird.
- Verbindungsspitzen: Ein plötzlicher Anstieg der Anwendungsverbindungen überfordert die für Authentifizierung und Sitzungsverwaltung benötigten CPU-Ressourcen.
- Komplexe Aggregationen: Multi-stage Operationen (Sortieren, Gruppieren, Zusammenfügen) verbrauchen viel CPU, insbesondere bei großen Datensätzen ohne optimierte Indizes.
- Ineffiziente Abfragen: Eine hohe CPU-Auslastung resultiert aus dem Scannen großer Ergebnismengen und Regex-Operationen.
- Write-Heavy Workloads: Häufige Aktualisierungen und Masseneinfügungen belasten die CPU bei der Dokumentenverarbeitung, Indexaktualisierungen und Transaktionsprotokollierung.

Untersuchen — Metriken sammeln

Amazon DocumentDB bietet Überwachung über Amazon CloudWatch. Amazon DocumentDB-Metriken können grob in Metriken auf Cluster- und Instance-Ebene unterteilt werden. Sehen Sie sich bei Ressourcen, die sich auf CPU, Arbeitsspeicher und Verbindungen beziehen, die Metriken auf Instance-Ebene an, da der Ressourcenverbrauch für die Instance spezifisch ist. Identifizieren Sie die Instances (primär oder repliziert), die CPU-Spitzen anzeigen, und notieren Sie sich die Zeiten der Spitzen.

Die CloudWatch Metrik für die CPU-Auslastung für. `CPUUtilization`

Diagnose — Finden Sie die Grundursache

Nachdem Sie die Instanz und den Zeitplan der CPU-Spitze identifiziert haben, müssen Sie als Nächstes die Ursache diagnostizieren, die die CPU-Auslastung erheblich beeinträchtigt. Da es mehrere Gründe gibt, die zu einem CPU-Anstieg führen können, wollen wir zunächst herausfinden, was dazu beiträgt:

Verbindungen: Überprüfen Sie unter anderem folgende CloudWatch `DatabaseConnections` Kennzahlen: Falls es Verbindungsspitzen gibt und diese mit der CPU-Spitzenzeit zusammenfallen, ist

der Anstieg der Verbindungen über einen kurzen Zeitraum wahrscheinlich die Ursache für den CPU-Anstieg. `DatabaseConnectionsMax`

Abfragen: Wenn es nicht die Verbindung ist, könnte eine Abfrage die Ursache sein. Wenn Sie Performance Insights aktiviert haben, rufen Sie die Performance Insights-Konsole für die Instance auf und sehen Sie sich die Abfragen auf der Instance an. Die andere Sache, mit der Sie sich Abfragen ansehen können, stammt aus dem Profiler.

Lösen — Das Problem beheben

Verbindungsbursts: Wenn Verbindungsbursts die Ursache für CPU-Spitzen sind, sollten Sie erwägen, Verbindungen in Ihrer Anwendung wiederzuverwenden oder Verbindungspooling zu implementieren. Weitere Informationen zur Optimierung von Verbindungen mit hohem Verbindungsaufkommen finden Sie unter. the section called “Probleme mit der Verbindung”

Abfrageverteilung: Wenn die CPU-Spitzen durch Leseabfragen auf der primären Instanz verursacht werden, sollten Sie erwägen, Lesevorgänge auf Replikatinstanzen umzuleiten, wenn Ihre Abfrageergebnisse letztendlich konsistent sein können.

Abfrageoptimierungen: Wenn eine Abfrage oder eine Reihe von Abfragen zu einem CPU-Anstieg führen, sollten Sie in Erwägung ziehen, die Abfrage zu optimieren, z. B. einen Index hinzuzufügen, falls die Abfrage keinen verwendet. Weitere Informationen zur Optimierung einer Abfrage finden Sie unter. the section called “Die Abfrage läuft langsam”

Instanzskalierung: Wenn die CPU-Auslastung nach der Optimierung konstant hoch bleibt, sollten Sie auf eine größere Instance-Klasse mit mehr CPU-Kapazität aufrüsten, um Ihre Workload-Anforderungen effektiv zu bewältigen.

Serverlos: Bei unvorhersehbaren Workloads, die zu kurzzeitigen CPU-Spitzen führen, sollten Sie die Verwendung von. Serverloses Verwenden von Amazon DocumentDB Serverlose Instances skalieren Ressourcen automatisch je nach Bedarf, sodass für solche Workloads keine festen Instanzgrößen bereitgestellt werden müssen.

Verbindungsprobleme mit Amazon DocumentDB

Identifizierung — Finde das Problem

Häufige Ursachen

Verbindungsprobleme sind in der Regel auf drei Hauptbereiche zurückzuführen:

Eine Erschöpfung des Verbindungspools tritt auf, wenn eine Anwendung ihre maximal zulässigen Verbindungen zu Amazon DocumentDB erreicht, entweder über die clientseitigen Verbindungs-Pool-Limits oder die serverseitigen Instance-Limits. Dieser Zustand führt zu verminderter Anwendungsleistung, Zeitüberschreitungen und potenziellen Ausfällen, da neue Verbindungsanfragen entweder in die Warteschlange gestellt oder abgelehnt werden.

Eine Authentifizierungsüberlastung tritt auf, wenn Amazon DocumentDB zu viele gleichzeitige Authentifizierungsanfragen erhält, insbesondere bei der Verarbeitung von mehr als 1.000 neuen Verbindungen in einem kurzen Zeitraum. Während der Authentifizierungswartung hält Amazon DocumentDB eine exklusive Sperre für die Sitzungsübersicht fest, sodass nachfolgende Authentifizierungsversuche in die Warteschlange gestellt werden, bis die Wartung abgeschlossen ist.

Konfigurationsprobleme in Amazon DocumentDB sind häufig auf Fehlkonfigurationen in den Netzwerk-, Sicherheits- und Client-Einstellungen zurückzuführen. Dazu gehören beispielsweise falsche Sicherheitsgruppeneinstellungen, falsche VPC-Konfiguration oder SSL/TLS Zertifikatsprobleme. Das Verständnis der richtigen Konfiguration ist für die Aufrechterhaltung eines sicheren und zuverlässigen Datenbankzugriffs unerlässlich.

Diagnose — Finden Sie die Grundursache

Verbindungspools

Der Verbindungspool wird initialisiert, wenn eine MongoClient Instanz erstellt wird. Jeder Pool verwaltet Verbindungen auf der Grundlage von zwei Schlüsselparametern:

min PoolSize — Mindestanzahl der unterhaltenen Verbindungen

max PoolSize — Maximal zulässige Verbindungen

Wenn eine Anfrage eine Verbindung benötigt:

1. Der Pool sucht nach verfügbaren inaktiven Verbindungen
2. Wenn keine vorhanden sind und die Poolgröße < max istPoolSize, wird eine neue Verbindung erstellt
3. Wenn der Höchstwert erreicht PoolSize ist, wird die Anfrage in eine Warteschlange verschoben
4. Wenn die Warteschlange voll ist oder das Timeout erreicht ist, wird sie ausgelöst MongoWaitQueueFullException

Das Verhalten der Wartewarteschlange wird über diese Parameter gesteuert:

wait QueueTimeout MS - Maximale Wartezeit für die Verbindung

wait QueueSize - Maximale Anzahl von Anfragen in der Warteschlange

Hier ist ein Beispiel für einen problematischen Ansatz für die Verbindung mit Amazon DocumentDB, bei dem jedes Mal ein neuer Pool erstellt wird:

```
for(Request request : requests) {
    MongoClient client = MongoClients.create(settings);
    // Process request
    client.close();
}
```

Folgende wichtige CloudWatch Kennzahlen müssen überwacht werden:

- `DatabaseConnections`- Die Anzahl der Verbindungen (aktiv und inaktiv), die auf einer Instance geöffnet sind, die im Abstand von 1 Minute hergestellt wurden.
- `DatabaseConnectionsMax`- Die maximale Anzahl offener Datenbankverbindungen (aktiv und inaktiv) auf einer Instance in einem Zeitraum von 1 Minute.
- `DatabaseConnectionsLimit`- Die maximale Anzahl gleichzeitiger Datenbankverbindungen (aktiv und inaktiv), die für eine Instance zu einem bestimmten Zeitpunkt zulässig sind.
- `LowMemNumOperationsThrottled`— Die Anzahl der Anfragen, die aufgrund von zu wenig verfügbarem Speicherplatz in einem Zeitraum von 1 Minute gedrosselt wurden.

Limits pro Instance-Klasse finden Sie unter Kontingente und Limits.

Zu den häufigsten Warnsignalen für Probleme mit dem Verbindungspool auf Anwendungsebene gehören:

- Erhöhung der Verbindungsaufnahmezeiten
- Zunehmende Größe der Warteschlange
- Steigende Anzahl von Timeout-Ausnahmen

Überlastung bei der Authentifizierung

Die Verbindung zu Amazon DocumentDB erfolgt nach einem Ablauf, der dem folgenden ähnelt:

Verbindungsanfrage → SSL-Handshake → Authentifizierung → Sitzungserstellung → Verbindung bereit

Bei der Verarbeitung von mehr als 1.000 neuen Verbindungen werden nach Abschluss des SSL-Handshakes weitere Verbindungsanfragen in eine Warteschlange für die Authentifizierung aufgenommen. Bei diesen Überlastungsereignissen erhöhen sich die durchschnittlichen Verbindungszeiten Ihrer Anwendung.

Folgende CloudWatch Kennzahlen müssen unbedingt überwacht werden:

- `DatabaseConnections`- Die Anzahl der Verbindungen (aktiv und inaktiv), die auf einer Instance geöffnet sind, die im Abstand von 1 Minute hergestellt wurden.
- `DatabaseConnectionsMax`- Die maximale Anzahl offener Datenbankverbindungen (aktiv und inaktiv) auf einer Instance in einem Zeitraum von 1 Minute.
- `DatabaseConnectionsLimit`- Die maximale Anzahl gleichzeitiger Datenbankverbindungen (aktiv und inaktiv), die für eine Instance zu einem bestimmten Zeitpunkt zulässig sind.

Probleme mit der Konfiguration

Das häufigste Konfigurationsproblem tritt auf, wenn versucht wird, aus einer Umgebung ohne Zugriff auf die private Netzwerkumgebung eine Verbindung zu einem privaten Amazon DocumentDB-Cluster-Endpunkt herzustellen. Amazon DocumentDB ist nur für Virtual Private Cloud (VPC) verfügbar und unterstützt derzeit keine öffentlichen Endpunkte. Sie können von Ihrem Laptop oder Ihrer lokalen Entwicklungsumgebung außerhalb Ihrer VPC keine direkte Verbindung zu Ihrem Amazon DocumentDB-Cluster herstellen.

Dies wird sich in Fehlern wie den folgenden äußern:

```
Error: couldn't connect to server...
Failed to connect to...
exception: connect failed
connection attempt failed
```

Falsche Sicherheitsgruppenkonfigurationen können ebenfalls zu Verbindungsfehlern führen. Ein Amazon DocumentDB-Cluster wartet standardmäßig auf Verbindungen am TCP-Port 27017. Ihre Anwendung schlägt fehl, wenn versucht wird, eine Verbindung zu einem anderen Port herzustellen als dem, mit dem der Cluster bereitgestellt wurde, oder wenn die Anwendung nicht in der Konfiguration der Eingangssicherheitsgruppe für den Cluster enthalten ist.

Eine falsche Zertifikatsverwaltung kann auch zu Verbindungsproblemen führen. Standardmäßig ist die Verschlüsselung bei der Übertragung für neu erstellte Amazon DocumentDB-Cluster aktiviert. Wenn die Verschlüsselung bei der Übertragung aktiviert ist, sind sichere Verbindungen mit TLS erforderlich, um mithilfe des Zertifikats global-bundle.pem eine Verbindung zum Cluster herzustellen. Wenn Sie versuchen, das falsche Zertifikat zu verwenden, erhalten Sie beispielsweise folgende Fehler:

```
unable to get local issuer certificate
```

Wenn Sie versuchen, eine Verbindung zu einem Cluster mit aktiviertem TLS herzustellen, ohne die TLS-Parameter anzugeben, erhalten Sie folgende Fehler:

```
Server selection timed out after 30000 ms
```

Gelöst — Das Problem beheben

Verbindungspools: Überprüfen Sie das Verbindungspooling, indem Sie die Poolgröße implementieren oder an die Workload-Anforderungen anpassen. Optimale Poolkonfigurationen hängen von Ihrer Arbeitslast und Ihren Anforderungen ab. Sie sollten einen PoolSize Mindestwert einhalten, damit die Kernverbindungen bereit und verfügbar sind, und einen Höchstwert, der WaitTime kurz genug ist, um schnell ausfallen zu können, wenn der Pool erschöpft ist.

Hier ist ein Beispiel dafür, wie Sie einen einzelnen Pool wiederverwenden können, ohne jedes Mal einen neuen zu erstellen:

```
MongoClient client = MongoClients.create(settings);
    for(Request request : requests) {
    // Process request
}
```

Authentifizierungsüberlastung: Verwalten Sie die Authentifizierung, indem Sie einen schrittweisen Verbindungsaufbau implementieren und neue Verbindungen auf jeweils 1.000 beschränken. Verwenden Sie Verbindungspooling, um authentifizierte Verbindungen effektiv wiederzuverwenden. Um eine Überlastung des Amazon DocumentDB-Clusters mit Verbindungen zu vermeiden, implementieren Sie eine Strategie für den Verbindungsaufbau.

```
public class ConnectionManager {
    private static final int BATCH_SIZE = 100;
    private static final int DELAY_MS = 1000;

    public void establishConnections(int totalRequired) {
        int established = 0;
        while (established < totalRequired) {
            int batch = Math.min(BATCH_SIZE, totalRequired - established);
            createConnections(batch);
            Thread.sleep(DELAY_MS);
            established += batch;
        }
    }
}
```

Sie können Ihre Verbindungspool-Einstellungen auch so konfigurieren, dass die Gesamtzahl der zulässigen Verbindungen begrenzt wird.

```
MongoClientSettings settings = MongoClientSettings.builder()
    .applyToConnectionPoolSettings(builder -> {
        builder.maxSize(500)                    // Limit total connections
               .minSize(10)                     // Maintain base connections
               .maxConnectionLifeTime(3600000)  // Rotate connections hourly
    })
    .applyToServerSettings(builder -> {
        builder.heartbeatFrequency(10000)       // Regular server checks
    })
    .build();
```

Konfigurationsprobleme: Stellen Sie sicher, dass Ihre Anwendung Zugriff auf die private VPC und das Subnetz hat, in denen sich Ihre Amazon DocumentDB DocumentDB-Ressourcen befinden. Wenn Sie VPC-Peering verwenden, finden Sie weitere Informationen im Entwicklerhandbuch zur Fehlerbehebung bei einer VPC-Peering-Verbindung. Sie können auch den Knowledge Center-Artikel Wie behebe ich Verbindungsprobleme zwischen dem Internet und Amazon EC2 EC2-Instances in meiner VPC? .

Für die Konfiguration von Sicherheitsgruppen müssen Sie eine Eingangsregel in Ihre Amazon DocumentDB-Sicherheitsgruppe aufnehmen, um Verbindungen von Ihrer Anwendung aus zuzulassen.

```
{
  "SecurityGroupIngress": [
    {
      "IpProtocol": "tcp",
      "FromPort": 27017,
      "ToPort": 27017,
      "SourceSecurityGroupId": "<application-security-group>",
      "Description": "DocumentDB access from application tier"
    }
  ],
  "SecurityGroupEgress": [
    {
      "IpProtocol": "-1",
      "FromPort": -1,
      "ToPort": -1,
      "CidrIp": "0.0.0.0/0"
    }
  ]
}
```

Wenn der Cluster mit TLS-Verschlüsselung konfiguriert ist, laden Sie das TLS-Zertifikat für Amazon Amazon DocumentDB mit dem Namen global-bundle.pem herunter und verwenden Sie es, wenn Sie eine Verbindung zum Cluster herstellen.

```
wget https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem
```

Long-term Lösungen

Die Skalierung von Instanzen kann durch ein Upgrade auf eine größere Instanzklasse oder durch das Hinzufügen von Read Replicas zur Verteilung der Verbindungslast erforderlich sein. Eine ordnungsgemäße Implementierung des Lastenausgleichs gewährleistet eine optimale Ressourcennutzung im gesamten Cluster.

Bei Änderungen an Anwendungen sollte der Schwerpunkt auf der Implementierung einer robusten Verbindungsverwaltung, einer umfassenden Überwachung und der Einhaltung der bewährten Methoden für das Verbindungspooling liegen. Dazu gehören die richtige Fehlerbehandlung und das Management des Verbindungslebenszyklus.

Architekturverbesserungen könnten die Einführung von Amazon DocumentDB Serverless für variable Workloads, die Implementierung einer ausgeklügelten Wiederholungslogik und das Design für Fehlertoleranz beinhalten. Erwägen Sie eine Umstrukturierung der Anwendungsarchitektur, um das Verbindungsmanagement besser handhaben zu können.

Bewährte Methoden

Verbindungspools

Durch die richtige Verwaltung und Überwachung der Verbindungspools können Anwendungen eine stabile Datenbankkonnektivität aufrechterhalten und gleichzeitig Erschöpfungsszenarien verhindern, die sich auf die Zuverlässigkeit und Leistung des Systems auswirken könnten. Konfigurieren Sie geeignete Timeouts und dimensionieren Sie Ihren Pool auf der Grundlage der Eigenschaften Ihres Workloads.

Beispiel für die Einstellung eines Verbindungspools

```
MongoClientSettings settings = MongoClientSettings.builder()
    .applyToConnectionPoolSettings(builder ->
        builder.maxSize(10))
    .applyToConnectionPoolSettings(builder ->
        builder.maxWaitQueueSize(2))
    .applyToConnectionPoolSettings(builder ->
        builder.maxConnectionIdleTime(10, TimeUnit.MINUTES))
    .build();
```

Weitere Informationen finden Sie unter: https://aws.amazon.com/blogs/database/building-resilient-applications-with-amazon-documentdb-with-mongodb-compatibility-part-1-client-configuration/

Überlastung bei der Authentifizierung

Implementieren Sie Verbindungspooling immer mit geeigneten Werten für Parameter, die auf Ihrer Arbeitslast basieren. Verwenden Sie einen schrittweisen Verbindungsaufbau und halten Sie nach Möglichkeit persistente Verbindungen aufrecht. Führen Sie eine ordnungsgemäße Verbindungsbereinigung durch, um sicherzustellen, dass keine ungenutzten Ressourcen verschwendet werden.

Probleme mit der Konfiguration

Stellen Sie sicher, dass Sie das richtige Routing von Ihrer Anwendung zu den Amazon DocumentDB DocumentDB-Ressourcen konfiguriert haben. Verwenden Sie TLS für die Verschlüsselung bei der Übertragung und implementieren Sie den Zugriff mit den geringsten Rechten. Überprüfen Sie Ihre Amazon DocumentDB DocumentDB-Anmeldeinformationen und validieren Sie die Werte der Verbindungszeichenfolgen.

Abfrage läuft langsam

Identifizierung — Finden Sie das Problem

Eine langsam laufende Abfrage ist eine, die die für Ihre Geschäftsanforderungen erwartete Ausführungszeit überschreitet. Die Definition, was eine langsame Abfrage ausmacht, ist je nach Workload unterschiedlich. Sie können langsame Abfragen anhand von Profiler-Protokollen oder Performance Insights identifizieren.

1. Aktivieren Sie den Profiler, falls er nicht bereits aktiviert ist. Profiler-Protokolle werden CloudWatch unter der Protokollgruppe: `/aws/docdb/<cluster-identifier>/profiler` auf Amazon geschrieben. Verwenden Sie CloudWatch Logs Insights, um sie abzufragen.

   Beispiel für eine CloudWatch Log-Analyse-Abfrage, um die 10 langsamsten Abfragen für die Sammlung ecommerce.products abzurufen:

   ```
   filter ns="ecommerce.products" | sort millis desc | limit 10
   ```

2. Verwenden Sie Performance Insights, um teure Abfragen nahezu in Echtzeit zu identifizieren. Aktivieren Sie Performance Insights, falls es noch nicht aktiviert ist.
   a. Öffnen Sie die AWS Konsole, navigieren Sie zu Amazon Amazon DocumentDB, dann zu Performance Insights und wählen Sie Ihre Cluster-Instance aus.
   b. Überprüfen Sie den Zeitplan für DB-Ladevorgänge (AAS) und die häufigsten Abfragen (nach DB-Auslastung). Erweitern Sie einen Abfrage-Digest, um wörtliche untergeordnete Anweisungen anzuzeigen.
   c. Erfassen Sie die Abfragen, die analysiert werden müssen.

> **Note**
>
> Möglicherweise sind nicht alle Abfragen in Performance Insights ineffiziente oder langsame Abfragen.

Untersuchen — Informationen sammeln

1. Der Profiler stellt den Ausführungsplan für die Abfrage und die damit verbundenen wichtigsten Kennzahlen bereit, darunter millis, nreturned und PlanSummary (Indexnutzung):


```
{
    "op": "query",
    "ts": 1721374275673,
    "ns": "test.perf",
    "command": {
        "find": "perf",
        "filter": {
            "threadRunCount": 0
        },
        "$db": "test",
        "lsid": {
            "id": {
                "$binary": "oO2wEtpgQIK+y9KGByYnsw==",
                "$type": "4"
            }
        },
        "$readPreference": {
            "mode": "secondaryPreferred"
        }
    },
    "cursorExhausted": true,
    "nreturned": 0,
    "responseLength": 0,
    "protocol": "op_query",
    "millis": 137,
    "planSummary": "IXSCAN",
    "execStats": {
        "stage": "FETCH",
        "nReturned": "0",
```

```
        "executionTimeMillisEstimate": "100.346",
        "inputStage": {
            "stage": "IXSCAN",
            "nReturned": "0",
            "executionTimeMillisEstimate": "100.342",
            "indexName": "threadRunCount_1"
        }
    },
    "client": "172.31.6.165:43154",
    "appName": "ProdAppTester14",
    "user": "adminuser"
}
```

Um die COLLSCAN-Abfragen zu finden:

```
filter planSummary="COLLSCAN" | sort millis desc | limit 20
```

2. Verwenden Sie Performance Insights, um Trends bei der Abfrageausführung wie Wartezeiten, Auslastung und Ressourcenauswirkungen (z. B. IOPS oder CPU pro Abfrage) in Echtzeit zu analysieren.

   Da Performance Insights den Ausführungsplan für die Abfrage nicht bereitstellt, erfassen Sie die Abfrage und führen Sie explain („executionStats“) für die Abfrage in Ihrem Amazon DocumentDB-Cluster aus:

```
db.ecommerce.products.find().explain("executionStats")
```

3. Korrelieren Sie optional Profiler-Metriken mit Performance Insights-Daten (ordnen Sie z. B. hohe Millionenabfragen im Profiler den häufigsten Abfragen in Performance Insights zu).

Diagnose — Finden Sie die Ursache

In diesem Schritt diagnostizieren Sie den Abfrageplan, um mögliche Optimierungen zu identifizieren. Verwenden Sie das folgende Flow-Symptom → wahrscheinliche Ursache:

- Symptom: PlanSummary: „COLLSCAN“

Ursache: Fehlender oder falscher Index.

- Symptom: Langsame Aggregation mit $group/$sort

  Ursache: Die Aggregationspipeline verarbeitet möglicherweise zu viele Daten im Speicher.

- Symptom: hohe Latenzen, während Performance Insights DB Load gruppiert nach I/O-Wartezeiten anzeigt, obwohl Indizes verwendet werden (PlanSummary: „IXSCAN“).

  Ursache: I/O gebundene Abfragen; Indizes oder Arbeitssatz überschreiten den verfügbaren Puffercache auf der Instance.

- Symptom: PI zeigt CPU-Wartestatus und hohe AAS aufgrund weniger Abfragen

  Ursache: CPU-bound Abfragen (komplexe Aggregationen, $regex).

- Symptom: Viele langsame Abfragen, aber keine zeigt teure PlanSummary

  Ursache: externer Engpass (Netzwerk, Drosselung, Wartungsaufgaben, Anzahl der Abfragen).

Beheben — Das Problem beheben

Wenn Sie Fixes implementieren, validieren Sie immer mit explain („executionStats“) und überwachen Sie Performance Insights DB Load.

1. Zusammenfassung des Plans: „COLL SCAN“
   - Erstellen Sie einen zielgerichteten Index.

     Beispiel: Für häufige Abfragen, die nach {Kategorie, Preis} filtern und nach absteigendem Preis sortieren:

     ```
     db.products.createIndex({ category: 1, price: -1 })
     ```

2. langsame Aggregation mit $group/$sort
   - Setzen Sie $match und $project frühzeitig ein, um zu verhindern, dass Dokumente in $group/$sort landen.
   - Begrenzen Sie die Anzahl der Felder zu Beginn der Pipeline:

     ```
     db.products.explain("executionStats").aggregate([
     ```

```
  { $match: { category: "Electronics", price: { $gt: 0 } } },   // early filter
  { $project: { price: 1, category: 1 } },                     // reduce document
 size
  { $group: { _id: "$category", avgPrice: { $avg: "$price" } } }
])
```

3. hohe Latenzen, während Performance Insights die DB-Auslastung gruppiert nach I/O-Wartezeiten anzeigt
   - Überprüfen Sie, ob BufferCacheHitRatio der Wert niedrig ist oder ob die ReadIOPS auf der Instance hoch sind. Erhöhen Sie den Instanzspeicher (aktualisieren Sie die Instanzklasse, z. B. r6g.large → r6g.xlarge) oder verwenden Sie die NVMe-Instanzklasse.
   - Reduzieren Sie den Platzbedarf im Index.
   - Fügen Sie Read Replicas hinzu, um den Leseverkehr auszulagern (verwenden Sie die ReadPreference-Einstellung, um den Datenverkehr auf Replikaten umzuleiten, wenn die Abfrage tolerant und letztendlich konsistent ist).
4. PI zeigt CPU-Wartezustände an, hohe AAS aufgrund weniger Abfragen
   - Ersetzen Sie teure $regex durch indizierte Präfixsuchen oder $text-Index.
   - Batch-Schreibvorgänge (Einfügen), um die Schreibverstärkung zu reduzieren.

> **Note**
>
> Testen Sie Ihre Änderungen immer in einer niedrigeren Umgebung (außerhalb der Produktionsumgebung), bevor Sie diese Änderungen in die Produktionsumgebung übertragen.

Anti-patterns

In diesem Abschnitt werden gängige Anti-Pattern-Methoden behandelt, die sich negativ auf die Leistung von Amazon DocumentDB auswirken können.

Themen

- Zusammengesetzter Index mit mehr als 3 Attributen
- Abfragen mit langer Laufzeit
- Wenig genutzte und redundante Indizes

- Multi-Key Indizes mit großen Arrays

Zusammengesetzter Index mit mehr als 3 Attributen

-Übersicht

Ein zusammengesetzter oder zusammengesetzter Index verwaltet Verweise auf mehrere Felder innerhalb einer einzigen Indexstruktur. Diese Indizes optimieren die Leistung für Abfragen, die nach mehreren Feldern gleichzeitig filtern oder Filterung mit Sortiervorgängen kombinieren. Sie eignen sich auch für Abfragen mit einer einzigen Bedingung in den indizierten Feldern ganz links. Die Datenbank nutzt diese Indexeinträge, um passende Dokumente effizient zu finden, ohne die Sammlung vollständig scannen zu müssen.

Amazon DocumentDB kann den zusammengesetzten Index verwenden, um Abfragen zu unterstützen, die eine beliebige führende Teilmenge der indizierten Felder enthalten. Dieses Konzept wird als Indexpräfixe bezeichnet. Wenn Sie beispielsweise einen zusammengesetzten Index aktiviert haben`{state: 1, city: 1, zipcode: 1}`, kann Amazon DocumentDB Abfragen effizient verarbeiten, die nur das Feld „state“, die Felder „state“ und „city“ zusammen oder alle drei Felder „state“, „city“ und „zip code“ verwenden. Abfragen müssen jedoch die Felder von links nach rechts verwenden, ohne dass Felder dazwischen übersprungen werden. Das bedeutet, dass Abfragen, die nur das Feld „Stadt“ oder „Postleitzahl“ oder Kombinationen wie „Bundesland“ und „Postleitzahl“ (ohne „Stadt“) verwenden, den Index nicht vollständig nutzen können.

In den meisten realen Szenarien erzielen zusammengesetzte Indizes mit drei oder weniger Attributen in der Regel optimale Leistung und Ressourceneffizienz. Es ist zwar möglich, mehr als 3 Attribute im zusammengesetzten Index zu haben, führt jedoch häufig zu einem erhöhten Ressourcenverbrauch, der die Vorteile überwiegt.

Auswirkungen auf den Cluster

Es ist zwar verlockend, einen Index zu erstellen, der alle Bedingungen in einer Abfrage abdeckt, um eine maximale theoretische Leistung zu erzielen, aber die meisten Datenfilterung erfolgt über die ersten 1—3 Attribute in einem zusammengesetzten Index. Zusätzliche Felder, die diesen Schwellenwert überschreiten, tragen in erster Linie zur Indexgröße und nicht zur sinnvollen Abfrageoptimierung bei.

Speicherplatz und I/O Overhead: Zusammengesetzte Indizes mit vielen Attributen verbrauchen deutlich mehr Speicherplatz als einfachere Alternativen. Die Größe ist direkt proportional zur Anzahl der indizierten Attribute und zur Größe der indizierten Werte selbst.

Speicherbedarf: Der große Speicherbedarf zusammengesetzter Indizes mit vielen Attributen führt zu einem entsprechenden Speicherbedarf, wodurch Ihr Arbeitssatz größer wird und andere häufig aufgerufene Daten aus dem Pufferpool verdrängt werden.

Schreiboperationen: Jede Änderung eines Dokuments, die sich auf mehrere indizierte Felder auswirkt, erfordert die Aktualisierung des gesamten zusammengesetzten Indexeintrags, wodurch der Arbeitsaufwand für den Schreibvorgang vervielfacht wird.

Wie identifiziert man

Überprüfen Sie zunächst alle Indizes in Ihrer Sammlung, um zusammengesetzte Indizes mit mehr als drei Attributen zu identifizieren:

```
// List all indexes for the collection
db.collection.getIndexes()

// Look for indexes with 3+ fields like:

// { "userId": 1, "status": 1, "category": 1, "priority": 1, "region": 1 }
// { "orderId": 1, "customerId": 1, "productId": 1, "timestamp": 1, "warehouse": 1 }
```

Abhilfe

Wenn ein zusammengesetzter Index mit mehr als drei Attributen verwendet wird, identifizieren Sie die Abfragen, die ihn verwenden, und suchen Sie nach Optimierungsmöglichkeiten. Erwägen Sie, diese Indizes durch effizientere Indizes mit drei oder weniger Attributen zu ersetzen. Entfernen Sie nach der Implementierung der neuen Indizes die alten Indizes, die mehr als drei Attribute enthalten.

> **Note**
>
> Stimmen Sie sich stets mit den Stakeholdern ab und überprüfen Sie die Auswirkungen auf die Leistung, bevor Sie Indizes löschen.

Halten Sie sich bei der Erstellung zusammengesetzter Indizes an die ESR-Regel (Equality, Sort, Range).

Equality Sort Range (ESR) -Regel: Diese Reihenfolge maximiert die Indexeffizienz, indem der Datensatz zunächst nach Gleichheitsbedingungen gefiltert wird, dann Sortieroperationen auf die

reduzierte Menge angewendet und schließlich Bereichsscans für die kleinstmögliche Teilmenge durchgeführt werden

- Felder nach Gleichheit (exakte Treffer) anordnen,
- Sortieren (Reihenfolge),
- Bereich (**>**, **<**, $in).

```
// Query pattern
db.orders.find({
  userId: "user123",                    // Equality
  price: { $gte: 50, $lte: 200 }      // Range
}).sort({ createdAt: -1 })             // Sort

// Optimal index following ESR rule
db.orders.createIndex({ userId: 1, createdAt: -1, price: 1 })
//                      Equality   Sort         Range
```

Abfragen mit langer Laufzeit

-Übersicht

Long-running Abfragen können zu clusterweiten Leistungsproblemen führen. Diese Abfragen können den Garbage-Collection-Prozess von Amazon DocumentDB (Multi-Version Concurrency Control, MVCC) stören, was zur Anhäufung von Dokumenten mit alten Versionen und zu Leistungseinbußen im gesamten Cluster führen kann. Amazon DocumentDB implementiert ein 2-stündiges serverseitiges Timeout als Sicherheitsmechanismus, um zu verhindern, dass außer Kontrolle geratene Abfragen auf unbestimmte Zeit Ressourcen verbrauchen.

Was sind Abfragen mit langer Laufzeit:

- Abfragen, die über einen längeren Zeitraum (in der Regel **>** 30 Minuten) ausgeführt werden
- Öffnen Sie Cursor, die stundenlang aktiv bleiben (ein Timeout von 2 Stunden gilt nicht, wenn der Cursor aktiv ist)

Auswirkungen auf den Cluster

Abfragen mit langer Laufzeit können den Garbage-Collection-Prozess beeinträchtigen

- Alte Versionen häufen sich an: Garbage Collector kann alte Dokumentversionen nicht zurückfordern
- Aufblähung von Sammlung und Index: Sammlungs- und Indexeinträge häufen sich im Laufe der Zeit an, die Aufblähung nimmt zu, was zu höheren Speicherkosten führen kann.
- CPU- und Speicherauslastung: Die CPU- und Speicherauslastung steigt aufgrund der ineffizienten Verarbeitung einer erhöhten Anzahl alter Dokumentversionen, Indexeinträge und Transaktions-IDs.

Abfrage mit langer Laufzeit → Blocks-GC → Speicherwachstum → CPU- und Speicherauslastung → Mehr lange Abfragen

Überwachen und erkennen

1. Verwenden Sie den Befehl currentOp, um Abfragen mit langer Laufzeit zu finden.

```
// To find a query running for more than 30 mins
db.adminCommand({
    aggregate: 1,
    pipeline: [
        {$currentOp: {}},
        {$match:
            {$or:
                [{secs_running: {$gt: 1800}},
                 {WaitState: {$exists: true}}]}}],
    cursor: {}
});
```

2. Um Cursor zu finden, die länger als 30 Minuten aktiv sind

```
// To find cursor which is running more than 30 mins
db.adminCommand({
    "currentOp": true,
    "active": true,
    "$all": true
```

```
}).inprog.filter(function(op) {
    return op.desc == "Cursor" &&
           op.secs_running > 1800 &&
           op.active == true;
}).sort((a, b) => b.microsecs_running - a.microsecs_running)
```

3. Überwachung des Fortschritts des Garbage Collectors durch CloudWatch

`LongestRunningGCProcess`— Dauer des längsten aktiven Garbage-Collection-Vorgangs in Sekunden. Wird jede Minute aktualisiert und verfolgt nur aktive Vorgänge, ausgenommen Prozesse, die innerhalb des einminütigen Zeitfensters abgeschlossen werden.

`AvailableMVCCIds`-Ein Zähler, der die Anzahl der verbleibenden Schreiboperationen anzeigt, bevor der Wert Null erreicht wird. Wenn dieser Zähler Null erreicht, wechselt Ihr Cluster in den schreibgeschützten Modus, bis IDs zurückgewonnen und recycelt werden. Der Zähler nimmt mit jedem Schreibvorgang ab und steigt, wenn bei der Garbage-Collection alte MVCC-IDs wiederverwendet werden.

> **Note**
>
> Niedrigere MVCC-IDs und eine längere Garbage-Collection-Dauer sind nicht ausschließlich auf Abfragen mit langer Laufzeit zurückzuführen. Write-intensive Workloads auf Instanzen mit eingeschränkten Ressourcen können auch zu einer verringerten MVCC-ID-Verfügbarkeit und längeren Garbage-Collection-Zyklen führen.

Strategien zur Problembehebung

- Implementieren Sie Abfrage-Timeouts in der Anwendung
- Halten Sie die Cursor nicht für längere Zeit am Leben
- Optimieren Sie die Abfragen für eine bessere Leistung.
- Bevorzugen Sie das Stapeln von Schreibvorgängen

Wenig genutzte und redundante Indizes

-Übersicht

Indizes verbessern die allgemeine Abfrageleistung von Workloads, sind jedoch mit Kosten verbunden. Jeder Index verbraucht Speicherplatz und I/O Ressourcen, und Schreibvorgänge müssen alle Indizes in der Sammlung aktualisieren. Wenn Ihre Datenbank ungenutzte, unzureichend genutzte oder redundante Indizes enthält, führt dies zu einem Overhead für den Cluster, was zu Leistungseinbußen führt. Durch mehrere unnötige Indizes entsteht ein Anti-Pattern, das zu Leistungsproblemen, erhöhten Speicherkosten und höherem Betriebsaufwand führt.

Suboptimale Indizierungsszenarien

- Unbenutzte Indizes: Indizes, die für einmalige Abfragen oder in früheren Produktiterationen erstellt wurden und auf die mit aktuellen Abfragemustern nicht mehr zugegriffen wird. Um ungenutzte Indizes für eine Sammlung zu identifizieren, können Sie IndexStats verwenden. Weitere Informationen finden Sie unter the section called “Analysieren Sie die Indexnutzung und identifizieren Sie ungenutzte Indizes”.
- Redundante Indizes: Mehrere Indizes, die sich überschneidende Schlüsselmuster oder identische Abfragemuster abdecken. Beispiel: Ein Einzelschlüsselindex für Attribut A wird überflüssig, wenn ein zusammengesetzter Index sowohl das Attribut A als auch das Attribut B abdeckt, da der zusammengesetzte Index Abfragen für Attribut A allein verarbeiten kann.
- Over-Indexing: Erstellung von Indizes „für alle Fälle“, ohne die tatsächlichen Abfragemuster oder Leistungsanforderungen zu analysieren.
- Indizes mit niedriger Kardinalität: Indizes für Felder mit wenigen eindeutigen Werten (z. B. boolesche Felder, Statusflags), die nur einen minimalen Nutzen bei der Abfrageoptimierung bieten.

Auswirkungen auf die Cluster-Leistung

- Speicher und I/O: Jeder Index verbraucht Speicherplatz und I/O-Ressourcen und trägt so zu den Gesamtkosten bei. Wenn ein Index ungenutzt oder redundant ist, bedeutet dies unnötige Kosten für Ihren Cluster.
- Eingeschränkte Schreibleistung: Bei Einfüge-, Aktualisierungs- und Löschvorgängen müssen Indizes beibehalten werden, was zu einem Mehraufwand führt, der Ressourcen verbraucht. Ungenutzte oder redundante Indizes führen zu unnötigem Overhead bei diesen Vorgängen.
- Arbeitsspeicher- und CPU-Auslastung: Indizes konkurrieren um den Pufferpool-Speicher und können häufig aufgerufene Daten löschen, wenn der Arbeitssatz nicht in den Instanzspeicher

passt, was zu einem suboptimalen Ergebnis führt. BufferCacheHitRatio Das System verbraucht außerdem CPU-Ressourcen, um die Indexstrukturen aufrechtzuerhalten.

Verfügbare Tools zur Identifizierung von Möglichkeiten zur Indexoptimierung

- Tool zur Indexüberprüfung:
- Tool zur Erkennung der Indexkardinalität

Zusammenstellung des Toolkits:

```
git clone https://github.com/awslabs/amazon-documentdb-tools.git
```

1. Tool zur Indexüberprüfung

Das Tool zur Indexüberprüfung analysiert alle Sammlungen und Indizes, um eine Liste der Indizes und ihrer Verwendungsmuster bereitzustellen, und identifiziert redundante Indizes in Ihrem Amazon DocumentDB-Cluster. Führen Sie dieses Tool für eine umfassende Analyse auf allen Cluster-Instances aus. Weitere Informationen finden Sie unter Index Review Tool.

Verwendung:

```
cd performance/index-review/

python3 index-review.py --server-alias <server-alias> --uri <mongodb-uri>
```

Ausgabedateien

- `{server-alias}-collections.csv`: Collection-level Statistiken
- `{server-alias}-indexes.csv`: Detaillierte Kennzahlen zur Indexnutzung
- `{server-alias}-{timestamp}-index-review.json`: Rohdaten für weitere Analysen

> **Note**
>
> Führen Sie es für jede Instanz im Cluster mit einem unabhängigen Alias aus, um Statistiken für jede Instanz zu generieren, und führen Sie dann das Tool aus, um eine kumulative Analyse zu erhalten

ZB: `python3 index-review.py --files "{server-alias}-{timestamp}-index-review.json, {server-alias}-{timestamp}-index-review.json" --server-alias full-review`

2. Tool zur Erkennung der Indexkardinalität

Dieses Tool identifiziert Indizes mit niedriger Kardinalität, die für die Abfrageleistung ineffizient sind.

Usage

```
cd performance/index-cardinality-detection/

python3 detect-cardinality.py --uri <mongodb-uri>
```

Parameter

- `--threshold`: Prozentsatz des Kardinalitätsschwellenwerts (Standard: 1%)
- `--sample-count`: Anzahl der zu prüfenden Dokumente (Standard: 100.000)
- `--max-collections`: Maximale Anzahl von Sammlungen, die pro Datenbank gescannt werden sollen (Standard: 100)

Weitere Informationen finden Sie unter https://aws.amazon.com/blogs/database/detect-and-fix-low-cardinality-indexes-in-amazon-documentdb/.

Strategien zur Problembehebung

1. Entfernung ungenutzter und redundanter Indizes

```
// Example: Drop unused index
```

```
db.collection.dropIndex("unused_index_name")
```

> **Note**
>
> Indizes sollten niemals gelöscht werden, ohne dies mit allen interessierten Parteien besprochen und die Leistung getestet zu haben.

2. Optimierung des Index mit niedriger Kardinalität

- Verwenden Sie Teilindizes mit Filtern
- Wandeln Sie einzelne Indizes mit niedriger Kardinalität in zusammengesetzte Indizes um

Multi-Key Indizes mit großen Arrays

-Übersicht

Multi-key Mit Indizes in Amazon DocumentDB können Sie Array-Felder effizient abfragen. Diese Indexierungsstrategie sorgt für deutlich geringere Abfragelatenzen bei der Suche innerhalb von Array-Daten und ist somit eine attraktive Option für Anwendungen mit komplexen Datenstrukturen.

Bei der Arbeit mit großen Arrays oder mehreren Array-Feldern innerhalb einer Sammlung ist es jedoch wichtig, die Auswirkungen auf die Ressourcen und die Leistungsmerkmale zu verstehen, um fundierte Architekturentscheidungen treffen zu können. Wenn Sie einen Index für ein Array-Feld erstellen, generiert Amazon DocumentDB individuelle Indexeinträge für jedes Element im Array.

Auswirkungen auf den Cluster

- Speicher- und I/O-Overhead: Multi-key Indizes beanspruchen manchmal Speicherplatz bis zu einem Vielfachen der Basistabelle. Die Größe ist direkt proportional zu den Dokumenten in der Sammlung mit dem indizierten Array-Attribut, der Anzahl der Elemente im Array und der Größe des Elements.
- Speicherverbrauch: Da der Speicherbedarf relativ groß ist, haben diese Indizes einen entsprechenden Speicherbedarf, was zu einem größeren Arbeitssatz führt.
- Schreiboperationen: Multi-key Indizes verursachen während der Schreibvorgänge Mehraufwand. Jedes Array-Element generiert separate Indexeinträge, wodurch der Arbeitsaufwand, der zum Abschließen des Schreibvorgangs erforderlich ist, vervielfacht wird.

Strategien zur Problembehebung

- Erstellen Sie bei Bedarf einen Index mit mehreren Schlüsseln und begrenzen Sie die Anzahl der Felder im Array.
- Beschränken Sie die Anzahl der Multi-Key-Indizes in der Sammlung
- Erwägen Sie, Ihr Datenmodell zu ändern

Tipps zur Leistungsverbesserung

Dieser Abschnitt enthält fünf Strategien zur Leistungsoptimierung für Amazon DocumentDB zur Verbesserung der Anwendungseffizienz und der Abfrageausführung.

1. Verwenden Sie $match als erste Phase in Aggregationspipelines

Platzieren Sie $match immer als erste Stufe für die Filterung in Ihrer Aggregationspipeline, um die Leistung zu maximieren. Amazon DocumentDB nutzt Indizes effektiv, wenn $match die Pipeline leitet, sodass die Datenbank Daten frühzeitig filtern und den Verarbeitungsaufwand reduzieren kann.

```
// Optimized approach
db.orders.aggregate([
  { $match: { status: "active", category: "electronics" } }, // Index utilization
  { $group: { _id: "$category", total: { $sum: "$price" } } },
  { $sort: { total: -1 } }
])
```

Auswirkung: Durch frühzeitiges Filtern wird die Anzahl der Dokumente reduziert, die in nachfolgenden Pipeline-Phasen verarbeitet werden, was zu einer schnelleren Abfrageausführung und einem geringeren Ressourcenverbrauch führt.

2. Verwenden Sie $project in der Aggregationspipeline, um die Größe der Pipeline-Daten zu minimieren

Führen Sie nur wichtige Felder durch die Phasen Ihrer Aggregationspipeline, um die Datengröße zu minimieren und die Leistung zu verbessern. Setzen Sie $project strategisch ein, um nur die Daten einzubeziehen, die Sie benötigen.

```
// Efficient pipeline design
db.orders.aggregate([
  { $match: { orderDate: { $gte: new Date("2024-01-01") } } },
  { $project: { customerId: 1, totalAmount: 1, status: 1 } }, // Only needed fields
  { $group: { _id: "$customerId", totalSpent: { $sum: "$totalAmount" } } }
])
```

Auswirkung: Kleinere Dokumente reduzieren den Speicherverbrauch und verbessern die Effizienz der Pipeline-Verarbeitung, was zu einer insgesamt verbesserten Abfrageleistung führt.

3. Aktivieren Sie die Dokumentenkomprimierung, um die Speicherkosten und Kosten zu I/O senken und die Abfrageleistung zu verbessern

Aktivieren Sie die Dokumentenkomprimierung anhand der Cluster-Parametergruppe, um Speicherkosten und Kosten zu I/O senken und die Abfrageleistung zu steigern. Amazon DocumentDB speichert komprimierte Dokumente sowohl auf der Festplatte als auch im RAM, wodurch der Speicherbedarf und die I/O Kosten reduziert werden.

Auswirkung:

- In den verfügbaren Speicher passen mehr Dokumente
- Schnellerer Datenzugriff mit weniger Festplattenlesevorgängen
- Niedrigere Speicherkosten und I/O Kosten und verbesserte Abfrageleistung

> **Note**
>
> Amazon DocumentDB aktiviert standardmäßig keine Komprimierung für Version 5.0. Sie können die Komprimierung auf Sammlungs- oder Clusterebene für 5.0-Cluster aktivieren. Verwenden Sie das Komprimierungsüberprüfungsprogramm von Amazon DocumentDB, um die Komprimierungsraten für Ihre Sammlungen zu analysieren.
> Für Amazon DocumentDB 8.0 ist die Komprimierung standardmäßig aktiviert.

4. Nutzen Sie Indizes für eine optimale Abfrageleistung

Stellen Sie sicher, dass Ihre Abfragen immer Indizes verwenden, um eine optimale Leistung zu erzielen. Amazon DocumentDB bietet mehrere Indextypen für unterschiedliche Anwendungsfälle.

Prinzipien der Indexierung:

- Jede Abfrage sollte einen geeigneten Index verwenden
- Amazon DocumentDB bietet mehrere Indextypen
- Zusammengesetzte Indizes bieten die größte Flexibilität, da sie verschiedene Abfrageformen mit einem einzigen Index unterstützen
- Entwerfen Sie Indizes so, dass sie Sortier- und Filtervorgänge gemeinsam unterstützen

Grundlegendes zu Indexpräfixen: Zusammengesetzte Indizes arbeiten mit Indexpräfixen — Amazon DocumentDB kann jede Teilmenge der Indexfelder verwenden, die von links nach rechts geschrieben werden. Der Index erstellt beispielsweise diese verwendbaren Präfixe: `{ category: 1, price: -1, inStock: 1 }`

- `{ category: 1 }`- unterstützt Abfragen, die nur nach Kategorien gefiltert werden
- `{ category: 1, price: -1 }`- unterstützt Abfragen, die nach Kategorie und Preis gefiltert sorting/filtering werden
- `{ category: 1, price: -1, inStock: 1 }`- unterstützt die vollständige zusammengesetzte Abfrage

Abfragen nach Preis, InStock oder InStock allein verwenden diesen Index nicht, da sie nicht mit dem ersten Feld (Kategorie) beginnen.

So identifizieren Sie Abfragen, die keine Indizes verwenden: Verwenden Sie die Methode explain (), um die Abfrageausführung zu analysieren und Abfragen zu identifizieren, die Sammelscans anstelle von Indizes durchführen.

Auswirkung: Abfragen ohne Indexauslastung führen zu Sammlungsscans, was zu einer erhöhten Speicher- und CPU-Auslastung der Instanz und zu einer erhöhten Abfragelatenz führt.

5. Optimieren Sie Datenmodelle auf der Grundlage von Abfragemustern

Passen Sie Ihr Datenmodell an die Art und Weise an, wie Ihre Anwendung Daten abfragt und aktualisiert. Datenmodellierung ist die Grundlage für leistungsstarke Amazon DocumentDB DocumentDB-Anwendungen.

Optimierungsstrategien:

Einbettung aus Gründen der Leistung

- Speichern Sie zusammengehörende Daten zusammen, wenn häufig auf sie zugegriffen wird, als Einheit
- Betten Sie Dokumente ein, die immer zusammen abgerufen werden
- Geeignet für persönliche Beziehungen

```
// Embedded approach for frequently accessed data
{
  _id: ObjectId("..."),
  customerName: "John Doe",
  address: {
    street: "123 Main St",
    city: "Seattle",
    zipCode: "98101"
  },
  recentOrders: [
    { orderId: "ORD001", amount: 99.99, date: "2024-01-15" }
  ]
}
```

Aus Gründen der Flexibilität Referenzierung

- Verwenden Sie Verweise für große oder selten abgerufene Daten
- Empfohlen für Eins-zu-Viele-Beziehungen mit großen Datensätzen
- Beugt aufgeblähten Dokumenten vor und verbessert die Aktualisierungsleistung

Strategie zur Aufteilung von Sammlungen

Wenn nur wenige Felder in großen Dokumenten häufig aktualisiert werden oder wenn große, selten aufgerufene Daten Dokumente überladen, sollten Sie eine Aufteilung von Sammlungen in Betracht ziehen:

- Bewahren Sie häufig aktualisierte Felder in einer separaten, kleineren Sammlung auf
- Speichern Sie statische Daten oder Daten, auf die selten zugegriffen wird, in einer anderen Sammlung
- Verknüpfen Sie sie bei Bedarf mit Referenzen

```
// Before: Large document with mixed access patterns
{
  _id: ObjectId("..."),
  productId: "PROD123",
  name: "Wireless Headphones",        // Frequently accessed
  price: 99.99,                       // Frequently accessed
  inventory: 45,                      // Updated frequently
  lastSold: "2024-01-15",           // Updated frequently
  detailedSpecs: { /* large object */ }, // Infrequently accessed
  manualPDF: "base64...",           // Large, rarely accessed
  reviewHistory: [/* large array */] // Infrequently accessed
}

// After: Split into collections based on access patterns
// products collection (frequently accessed data)
{
  _id: ObjectId("..."),
  productId: "PROD123",
  name: "Wireless Headphones",
  price: 99.99,
  inventory: 45,
  lastSold: "2024-01-15"
}

// product_details collection (infrequently accessed data)
{
  _id: ObjectId("..."),
  productId: "PROD123",           // Reference to products collection
  detailedSpecs: { /* large object */ },
  manualPDF: "base64...",
  reviewHistory: [/* large array */]
```

```
}
```

Leistungssteigerung: Kleinere Dokumente bedeuten schnellere Aktualisierungen, weniger Speicherverbrauch und verbesserte Cache-Effizienz.

Auswirkung: Ineffiziente Datenmodellierung führt zu suboptimalen Abfragen, erhöhten Dokumentengrößen und erhöhtem Speicherverbrauch, was zu einer verminderten Anwendungsleistung und höheren Betriebskosten führt.

Plananalyse abfragen

Die Analyse des Abfrageplans mithilfe von Explain Plan bietet wichtige Einblicke in die Abfrageleistung von Amazon DocumentDB. Der Abfrageplan mit executionStats zeigt wichtige Kennzahlen wie:

- Pro Phase zurückgegebene Dokumente (nReturned)
- Stage-specific Ausführungszeiten (AusführungTimeMillisEstimate)
- Dauer der Planerstellung (PlanungTimeMillis)

Durch die Untersuchung der Ergebnisse des Abfrageplans können Entwickler Ausführungsmuster analysieren, die Indexauslastung bewerten und potenzielle Optimierungsmöglichkeiten in allen Phasen der Abfragepipeline identifizieren.

Um den Abfrageplan zu analysieren, können Sie den Befehl explain () in den folgenden Formaten verwenden.

```
db.runCommand({explain: {query document}, verbosity: "executionStats"})
db.collection.find().explain("executionStats");
```

Im Folgenden finden Sie ein Beispiel für eine Operation:

```
db.collection.find({ companyname: { '$eq': 'ANYCOMPANY' }, isDeleted: { '$eq':
 false } }).sort({"createdAt":1}).limit(2).explain("executionStats");
```

Die Ausgabe dieser Operation sieht in etwa wie folgt aus:

```
{
  queryPlanner: {
    plannerVersion: 2,
    namespace: 'limit_test.test',
    winningPlan: {
      stage: 'LIMIT_SKIP',
      inputStage: {
        stage: 'SORT',
        sortPattern: { createdAt: 1 },
        inputStage: {
          stage: 'IXSCAN',
          indexName: 'companyname_1_createdAt_1_isDeleted_1',
          direction: 'forward',
          indexCond: {
            '$and': [
              { companyname: { '$eq': 'ANYCOMPANY' } },
              { isDeleted: { '$eq': false } }
            ]
          }
        }
      }
    }
  },
  indexFilterSet: false,
  indexFilterApplied: false,
  executionStats: {
    executionSuccess: true,
    executionTimeMillis: '4.186',
    planningTimeMillis: '3.909',
    executionStages: {
      stage: 'LIMIT_SKIP',
      nReturned: '2',
      executionTimeMillisEstimate: '0.199',
      inputStage: {
        stage: 'SORT',
        nReturned: '2',
        executionTimeMillisEstimate: '0.197',
        sortPattern: { createdAt: 1 },
        inputStage: {
          stage: 'IXSCAN',
          nReturned: '34',
```

```
          executionTimeMillisEstimate: '0.151',
          indexName: 'companyname_1_createdAt_1_isDeleted_1',
          direction: 'forward',
          indexCond: {
            '$and': [
              { companyname: { '$eq': 'ANYCOMPANY' } },
              { isDeleted: { '$eq': false } }
            ]
          }
        }
      }
    }
  },
  serverInfo: { host: 'demo-cluster', port: 27017, version: '5.0.0' },
  ok: 1,
  operationTime: Timestamp({ t: 1759915116, i: 1 })
}
```

Im Folgenden finden Sie eine detaillierte Analyse eines Amazon DocumentDB DocumentDB-Abfrageausführungsplans, in dem jede Komponente und ihre Leistungsmerkmale aufgeschlüsselt sind.

Allgemeiner Zeitplan

Die Ausführung TimeMillis stellt die Gesamtzeit dar, die für die Abfrage benötigt wurde, einschließlich der Planungszeit.

Planung TimeMillis stellt die gesamte Planungszeit dar, die für die Abfrage benötigt wurde.

Phasen der Ausführung

Es beschreibt Schritt für Schritt, wie Amazon DocumentDB eine Abfrage ausführt, und zeigt, wie Daten durch verschiedene Operationen fließen.

```
"executionStages": {
    "stage": "[STAGE_NAME]",
    "nReturned": "[NUMBER_OF_DOCS]",
    "executionTimeMillisEstimate": "[TIME]",
    "inputStage": {
        // Nested stages
    }
```

```
}
```

Allgemeine Phasen in einem Abfrageplan

Im Folgenden sind die häufigsten Ausführungsphasen in einem Abfrageplan aufgeführt. In jeder Phase werden Metriken für Ausführung TimeMillisEstimate (Ausführungszeit) und NReturned (Anzahl der Dokumente) zurückgegeben, mit deren Hilfe die Abfrageleistung in jeder Phase bewertet werden kann.

COLLSCAN (Sammlungsscan)

- Scannt die gesamte Sammlung Dokument für Dokument
- nReturned: Gibt alle passenden Dokumente in der Sammlung zurück
- Kann ein teurer Vorgang sein, wenn kein Index verfügbar ist

IXSCAN (Indexscan)

- Verwendet einen Index, um passende Dokumente zu finden
- Zurückgegeben: Nur übereinstimmende Dokumente, die auf dem Index basieren
- Effizienter Betrieb, gegenüber COLLSCAN bevorzugt

SORT

- Sortiert Dokumente anhand bestimmter Felder
- Wenn das Sortierattribut in der Abfrage nicht Teil eines Indexes ist, wird diese Phase explizit angezeigt
- Zurückgegeben: Dieselbe Zahl wie bei den Eingabedokumenten
- Memory-intensive für große Ergebnismengen. Fügen Sie zur Optimierung den Namen des Sortierfeldes einem Index hinzu

LIMIT_SKIP

- Steuert die Anzahl der zurückgegebenen und übersprungenen Dokumente
- Rückgegeben: Limitiert durch den LIMIT-Wert
- Wird für Paginierung oder LIMIT-Operationen verwendet

SUBSCAN

- Führt verschachtelte Abfrageoperationen aus
- Zurückgegeben: Variiert je nach den Ergebnissen der Unterabfrage
- Wird in komplexen Abfragen mit mehreren Phasen verwendet

Phasen mit hoher Ausführungsrate TimeMillisEstimate eignen sich gut für eine Optimierung.

> **Note**
>
> Der ExecutionStats-Parameter unterstützt derzeit keine Aktualisierungs- und Löschbefehle.

Grundlegendes zu DocsExamined in Explain Plan Execution Stats

Wenn Sie eine Abfrage mit ausführen`explain("executionStats")`, bietet Amazon DocumentDB Prüfungsmetriken, anhand derer Sie nachvollziehen können, wie viele Dokumente gescannt wurden, um die Abfrageergebnisse zu erhalten. Diese Metriken sind nützlich, um ineffiziente Abfragepläne zu identifizieren und die Leistung zu optimieren.

> **Note**
>
> Nur in Amazon DocumentDB 8.0.0+ verfügbar.

Felder

Feld	Description	Level
insgesamt DocsExamined	Gesamtzahl der Dokumente, die in allen Ausführungsphasen geprüft wurden.	Top-level execution Stats
Dokumente geprüft	Anzahl der Dokumente, die in einer bestimmten Ausführungsphase geprüft wurden.	Stage-level

Das `docsExamined` Feld erscheint in den folgenden Phasen:

Stage	Description
COLLSCAN	Sammlung scannen. Alle Dokumente in der Sammlung werden geprüft.
ISCAN	Indexscan. Es werden nur Dokumente untersucht, die der Indexbedi ngung entsprechen.
FETCH	Wenn der Optimierer Dokumente in einer separaten Phase von IXSCAN abruft, meldet die FETCH-Phase den Wert DocsExamined. In Indexscan plänen melden die untergeordneten IXSCAN-Stufen nicht den Wert docsExamined. In $lookup-Plänen können sowohl die FETCH-Phase als auch ihre untergeordneten Stufen den Wert DocsExamined melden.

> **Note**
>
> `docsExamined`wird in den Stufen IXONLYSCAN nicht angezeigt, da die Abfrage vollständig aus dem Index beantwortet wird, ohne dass auf Dokumente zugegriffen wird.

In der Ausgabe von Explain Plan executionStats Dokumente anzeigen

Die folgenden Beispiele verwenden eine Sammlung mit 500.000 Dokumenten und veranschaulichen, wie sich die `docsExamined` Änderungen in den verschiedenen Phasen der Abfrageausführung ändern.

Erstellen Sie Beispieldaten:

```
for (let i = 0; i < 500000; i++) {
    db.coll.insertOne({ number: i, arr: [i, [i+1]], value: "test", bool: i % 2 === 
 0 });
}
```

Sammlungsscan (COLLSCAN)

Ohne Index führt Amazon DocumentDB einen vollständigen Sammlungsscan durch.

```
db.coll.find({ "number": { "$lt": 500 } }).explain("executionStats").executionStats
```

Ausgabe:

```
{
    "executionSuccess" : true,
    "nReturned" : "500",
    "executionTimeMillis" : "282.055",
    "planningTimeMillis" : "0.085",
    "totalDocsExamined" : "500000",
    "executionStages" : {
        "stage" : "COLLSCAN",
        "nReturned" : "500",
        "executionTimeMillisEstimate" : "281.915",
        "docsExamined" : "500000",
        "filter" : {
            "number" : {
                "$lt" : 500
            }
        }
    }
}
```

Alle 500.000 Dokumente wurden untersucht und lieferten 500 Ergebnisse. Das Erstellen eines Indexes für das Zahlenfeld verbessert dies.

Indexscan (IXSCAN)

```
db.coll.createIndex({ number: 1 });
db.coll.find({ "number": { "$lt": 5000 } }).explain("executionStats").executionStats
```

Ausgabe:

```
{
    "executionSuccess" : true,
    "nReturned" : "5000",
```

```
    "executionTimeMillis" : "3.047",
    "planningTimeMillis" : "0.296",
    "totalDocsExamined" : "5000",
    "executionStages" : {
        "stage" : "IXSCAN",
        "nReturned" : "5000",
        "executionTimeMillisEstimate" : "2.576",
        "indexName" : "number_1",
        "direction" : "forward",
        "docsExamined" : "5000",
        "indexCond" : {
            "$and" : [
                {
                    "number" : {
                        "$lt" : 5000
                    }
                }
            ]
        }
    }
}
```

Mit dem Index wurden nur 5.000 von 500.000 Dokumenten geprüft und abgerufen, was der zurückgegebenen Zahl entsprach. Durch die Indexbedingung wurden 495.000 Dokumente herausgefiltert, die der Abfrage nicht entsprachen.

Indexscan mit Restfilter

```
db.coll.find({ "number": { "$lt": 5000 }, "arr": { "$gt":
 4000 } }).explain("executionStats").executionStats
```

Ausgabe:

```
{
    "executionSuccess" : true,
    "nReturned" : "999",
    "executionTimeMillis" : "15.367",
    "planningTimeMillis" : "0.115",
    "totalDocsExamined" : "5000",
```

```
    "executionStages" : {
        "stage" : "IXSCAN",
        "nReturned" : "999",
        "executionTimeMillisEstimate" : "15.170",
        "indexName" : "number_1",
        "direction" : "forward",
        "docsExamined" : "5000",
        "indexCond" : {
            "$and" : [
                {
                    "number" : {
                        "$lt" : 5000
                    }
                }
            ]
        },
        "filter" : {
            "arr" : {
                "$gt" : 4000
            }
        }
    }
}
```

Die Indexbedingung entsprach 5.000 von 500.000 Dokumenten, danach `arr` reduzierte der Restfilter das Ergebnis auf 999. Der `docsExamined` Wert 5.000 spiegelt alle Dokumente wider, die nach der Indexbedingung, aber vor der Anwendung des Restfilters untersucht wurden.

Mit IXSCAN abrufen

```
db.coll.find({ "$or": [{ "number": { "$lt": 100000 } }, { "number": { "$gt":
 400000 } }] }).explain("executionStats").executionStats
```

Ausgabe:

```
{
    "executionSuccess" : true,
    "nReturned" : "199999",
    "executionTimeMillis" : "899.801",
```

```
    "planningTimeMillis" : "0.183",
    "totalDocsExamined" : "199999",
    "executionStages" : {
        "stage" : "FETCH",
        "nReturned" : "199999",
        "executionTimeMillisEstimate" : "894.141",
        "docsExamined" : "199999",
        "inputStage" : {
            "stage" : "IXOR",
            "nReturned" : "0",
            "executionTimeMillisEstimate" : "874.897",
            "inputStages" : [
                {
                    "stage" : "IXSCAN",
                    "nReturned" : "100000",
                    "executionTimeMillisEstimate" : "462.208",
                    "indexName" : "number_1",
                    "indexCond" : {
                        "$and" : [
                            {
                                "number" : {
                                    "$lt" : 100000
                                }
                            }
                        ]
                    }
                },
                {
                    "stage" : "IXSCAN",
                    "nReturned" : "99999",
                    "executionTimeMillisEstimate" : "412.684",
                    "indexName" : "number_1",
                    "indexCond" : {
                        "$and" : [
                            {
                                "number" : {
                                    "$gt" : 400000
                                }
                            }
                        ]
                    }
                }
            ]
        }
```

```
    }
}
```

Wenn der Amazon DocumentDB DocumentDB-Optimierer eine Abrufphase zum Abrufen von Dokumenten verwendet, werden in der FETCH-Phase Berichte erstellt. `docsExamined` Die untergeordneten IXSCAN-Stufen erstellen keine Berichte, `docsExamined` da sie nur Indexschlüssel scannen, ohne direkt auf Dokumente zuzugreifen.

FETCH mit aggregierter Suche

```
db.coll.explain("executionStats").aggregate([
    { $match: { "number": { "$lt": 5 } } },
    { $lookup: { from: "coll", pipeline: [{ $match: { "number": { "$lt": 3 } } }], as:
 "sub" } }
]).executionStats
```

Ausgabe:

```
{
    "executionSuccess" : true,
    "nReturned" : "5",
    "executionTimeMillis" : "0.525",
    "planningTimeMillis" : "0.327",
    "totalDocsExamined" : "9",
    "executionStages" : {
        "stage" : "NESTED_LOOP_LOOKUP",
        "nReturned" : "5",
        "executionTimeMillisEstimate" : "0.163",
        "inputStages" : [
            {
                "stage" : "IXSCAN",
                "nReturned" : "5",
                "executionTimeMillisEstimate" : "0.039",
                "indexName" : "number_1",
                "direction" : "forward",
                "docsExamined" : "5",
                "indexCond" : {
                    "$and" : [
```

```
                        {
                            "number" : {
                                "$lt" : 5
                            }
                        }
                    ]
                }
            },
            {
                "stage" : "FETCH",
                "nReturned" : "1",
                "executionTimeMillisEstimate" : "0.009",
                "docsExamined" : "1",
                "inputStage" : {
                    "stage" : "AGGREGATE",
                    "nReturned" : "1",
                    "executionTimeMillisEstimate" : "0.044",
                    "inputStage" : {
                        "stage" : "IXSCAN",
                        "nReturned" : "3",
                        "executionTimeMillisEstimate" : "0.013",
                        "indexName" : "number_1",
                        "direction" : "forward",
                        "docsExamined" : "3",
                        "indexCond" : {
                            "$and" : [
                                {
                                    "number" : {
                                        "$lt" : 3
                                    }
                                }
                            ]
                        }
                    }
                }
            }
        ]
    }
}
```

Der äußere IXSCAN untersuchte 5 Dokumente, die der Zahl < 5 entsprachen. Der innere IXSCAN untersuchte 3 Dokumente, die der Zahl < 3 entsprachen, und in der FETCH-Phase wurde ein

aggregiertes Ergebnis untersucht. Die `totalDocsExamined` Zahl 9 ist die Summe aller Stufen (5 + 3 + 1).

Problembehebung bei Amazon DocumentDB

Die folgenden Abschnitte enthalten Informationen zur Behebung von Problemen, die bei der Verwendung von Amazon DocumentDB (mit MongoDB-Kompatibilität) auftreten können.

Themen

- Fehlerbehebung bei Verbindungsproblemen
- Fehlerbehebung bei Indizes
- Problembehebung bei Leistung und Ressourcennutzung
- Müllabfuhr in Amazon DocumentDB

Fehlerbehebung bei Verbindungsproblemen

Haben Sie Probleme beim Herstellen einer Verbindung? Im Folgenden finden Sie einige gängige Szenarien und wie Sie sie lösen können.

Topics

- Es kann keine Verbindung zu einem Amazon DocumentDB DocumentDB-Endpunkt hergestellt werden
- Testen einer Verbindung zu einer Amazon DocumentDB DocumentDB-Instance
- Verbindung zu einem ungültigen Endpunkt herstellen
- Die Treiberkonfiguration wirkt sich auf die Anzahl der Verbindungen aus

Es kann keine Verbindung zu einem Amazon DocumentDB DocumentDB-Endpunkt hergestellt werden

Wenn Sie versuchen, eine Verbindung zu Amazon DocumentDB herzustellen, wird die folgende Fehlermeldung am häufigsten angezeigt.

```
connecting to: mongodb://docdb-2018-11-08-21-47-27.cluster-ccuszbx3pn5e.us-east-
1.docdb.amazonaws.com:27017/
2018-11-14T14:33:46.451-0800 W NETWORK [thread1] Failed to connect to
172.31.91.193:27017 after 5000ms milliseconds, giving up.
```

```
2018-11-14T14:33:46.452-0800 E QUERY [thread1] Error: couldn't connect to server
docdb-2018-11-08-21-47-27.cluster-ccuszbx3pn5e.us-east-1.docdb.amazonaws.com:27017,
connection attempt failed :
connect@src/mongo/shell/mongo.js:237:13
@(connect):1:6
exception: connect failed
```

Diese Fehlermeldung bedeutet in der Regel, dass Ihr Client (in diesem Beispiel die Mongo-Shell) nicht auf den Amazon DocumentDB DocumentDB-Endpunkt zugreifen kann. Dies kann aus verschiedenen Gründen der Fall sein:

Themen

- Verbindung von öffentlichen Endpunkten aus herstellen
- Regionsübergreifende Verbindungen
- Verbindung von verschiedenen Amazon VPCs aus herstellen
- Die Sicherheitsgruppe blockiert eingehende Verbindungen
- Problem mit den Leseeinstellungen des Java-Mongo-Treibers

Verbindung von öffentlichen Endpunkten aus herstellen

Sie versuchen, direkt von Ihrem Laptop oder Ihrem lokalen Entwicklungscomputer aus eine Verbindung zu einem Amazon DocumentDB-Cluster herzustellen.

Der Versuch, direkt von einem öffentlichen Endpunkt aus, z. B. Ihrem Laptop oder Ihrem lokalen Entwicklungscomputer, eine Verbindung zu einem Amazon DocumentDB-Cluster herzustellen, schlägt fehl. Amazon DocumentDB ist nur für Virtual Private Cloud (VPC) verfügbar und unterstützt derzeit keine öffentlichen Endpunkte. Daher können Sie von Ihrem Laptop oder Ihrer lokalen Entwicklungsumgebung außerhalb Ihrer VPC keine direkte Verbindung zu Ihrem Amazon DocumentDB-Cluster herstellen.

Um von außerhalb einer Amazon VPC eine Verbindung zu einem Amazon DocumentDB-Cluster herzustellen, können Sie einen SSH-Tunnel verwenden. Weitere Informationen finden Sie unter Von außerhalb einer Amazon VPC eine Verbindung zu einem Amazon DocumentDB-Cluster herstellen. Wenn sich Ihre Entwicklungsumgebung in einer anderen Amazon VPC befindet, können Sie außerdem VPC Peering verwenden und von einer anderen Amazon VPC in derselben Region oder einer anderen Region aus eine Verbindung zu Ihrem Amazon DocumentDB-Cluster herstellen.

Regionsübergreifende Verbindungen

Sie versuchen, eine Verbindung zu einem Amazon DocumentDB-Cluster in einer anderen Region herzustellen.

Wenn Sie versuchen, von einer Amazon EC2-Instance in einer anderen Region als der Region des Clusters aus eine Verbindung zu einem Amazon DocumentDB-Cluster herzustellen, z. B. wenn Sie versuchen, von der Region USA West (Oregon) (us-west-2) aus eine Verbindung zu einem Cluster in der Region USA Ost (Nord-Virginia) (us-east-1) herzustellen, schlägt die Verbindung fehl.

Führen Sie den folgenden Befehl aus, um die Region Ihres Amazon DocumentDB-Clusters zu überprüfen. Die Region ist im Endpunkt.

```
aws docdb describe-db-clusters \
   --db-cluster-identifier sample-cluster \
   --query 'DBClusters[*].Endpoint'
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus.

```
[
    "sample-cluster.node.us-east-1.docdb.amazonaws.com"
]
```

Um die Region Ihrer EC2-Instance zu überprüfen, führen Sie den folgenden Befehl aus.

```
 aws ec2 describe-instances \
     --query 'Reservations[*].Instances[*].Placement.AvailabilityZone'
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus.

```
[
    [
        "us-east-1a"
    ]
]
```

Verbindung von verschiedenen Amazon VPCs aus herstellen

Sie versuchen, von einer VPC aus eine Verbindung zu einem Amazon DocumentDB-Cluster herzustellen, die sich von der Amazon VPC unterscheidet, auf der Ihr Cluster bereitgestellt ist.

Wenn sich sowohl Ihr Amazon DocumentDB-Cluster als auch Ihre Amazon EC2 EC2-Instance in derselben AWS-Region, aber nicht in derselben Amazon VPC befinden, können Sie keine direkte Verbindung zu Ihrem Amazon DocumentDB-Cluster herstellen, es sei denn, VPC Peering ist zwischen den beiden Amazon VPCs aktiviert.

Führen Sie den folgenden Befehl aus, um die Amazon VPC Ihrer Amazon DocumentDB-Instance zu verifizieren.

```
aws docdb describe-db-instances \
   --db-instance-identifier sample-instance \
   --query 'DBInstances[*].DBSubnetGroup.VpcId'
```

Führen Sie den folgenden Befehl aus, um die Amazon VPC Ihrer Amazon EC2-Instance zu verifizieren.

```
aws ec2 describe-instances \
   --query 'Reservations[*].Instances[*].VpcId'
```

Die Sicherheitsgruppe blockiert eingehende Verbindungen

Sie versuchen, eine Verbindung zu einem Amazon DocumentDB-Cluster herzustellen, und die Sicherheitsgruppe des Clusters erlaubt keine eingehenden Verbindungen auf dem Port des Clusters (Standardport: 27017).

Angenommen, Ihr Amazon DocumentDB-Cluster und Ihre Amazon EC2 EC2-Instance befinden sich beide in derselben Region und Amazon VPC und verwenden dieselbe Amazon VPC-Sicherheitsgruppe. Wenn Sie keine Verbindung zu Ihrem Amazon DocumentDB-Cluster herstellen können, liegt das wahrscheinlich daran, dass Ihre Sicherheitsgruppe (d. h. die Firewall) für Ihren Cluster keine eingehenden Verbindungen auf dem Port zulässt, den Sie für Ihren Amazon DocumentDB-Cluster ausgewählt haben (Standardport ist 27017).

Führen Sie den folgenden Befehl aus, um den Port für Ihren Amazon DocumentDB-Cluster zu überprüfen.

```
aws docdb describe-db-clusters \
   --db-cluster-identifier sample-cluster \
   --query 'DBClusters[*].[DBClusterIdentifier,Port]'
```

Führen Sie den folgenden Befehl aus, um Ihre Amazon DocumentDB-Sicherheitsgruppe für Ihren Cluster abzurufen.

```
aws docdb describe-db-clusters \
   --db-cluster-identifier sample-cluster \
   --query 'DBClusters[*].[VpcSecurityGroups[*],VpcSecurityGroupId]'
```

Informationen zur Überprüfung der Regeln für eingehende Nachrichten für Ihre Sicherheitsgruppe finden Sie in den folgenden Themen in der Amazon EC2 EC2-Dokumentation:

- Autorisieren von eingehendem Datenverkehr für Ihre Linux-Instances
- Autorisieren von eingehendem Datenverkehr für Ihre Windows-Instances

Problem mit den Leseeinstellungen des Java-Mongo-Treibers

Die Leseeinstellungen der Clients werden nicht berücksichtigt und einige Clients können nach einem Failover nicht in Amazon DocumentDB schreiben, es sei denn, sie starten neu.

Dieses Problem, das erstmals in Java Mongo Driver 3.7.x entdeckt wurde, tritt auf, wenn ein Client mithilfe `MongoClientSettings` und insbesondere beim Verketten der Methode eine Verbindung zu Amazon DocumentDB herstellt. `applyToClusterSettings` Die MongoClient Cluster-Einstellungen können mit verschiedenen Methoden definiert werden, z. B. mit, und. `hosts()` `requiredReplicaSetName()` `mode()`

Wenn der Client in der `hosts()` Methode nur einen Host angibt, wird der Modus auf `ClusterConnectionMode.SINGLE` statt auf gesetzt. `ClusterConnectionMode.MULTIPLE` Dadurch ignoriert der Client die Lesepräferenz und stellt nur eine Verbindung zu dem Server her, der in `hosts()` konfiguriert ist. Selbst wenn die Client-Einstellungen wie unten initialisiert würden, würden alle Lesevorgänge immer noch an den primären statt an den sekundären weitergeleitet.

```
final ServerAddress serverAddress0 = new ServerAddress("cluster-endpoint", 27317));
    final MongoCredential credential = MongoCredential.createCredential("xxx",
            "admin", "xxxx".toCharArray());
    final MongoClientSettings settings = MongoClientSettings.builder()
            .credential(credential)
            .readPreference(ReadPreference.secondaryPreferred())
            .retryWrites(false)
            .applyToSslSettings(builder -> builder
                    .enabled(false))
            .applyToClusterSettings(builder -> builder.hosts(
                            Arrays.asList(serverAddress0
                            ))
                    .requiredReplicaSetName("rs0"))
```

```
            .build();
    MongoClient mongoClient = MongoClients.create(settings);
```

Failover-Fall

Bei Verwendung der oben genannten Client-Verbindungseinstellungen würde der Client bei einem Failover und einer verzögerten Aktualisierung des DNS-Eintrags für den Cluster-Writer-Endpunkt trotzdem versuchen, Schreibvorgänge auf den alten Writer (jetzt Reader nach dem Failover) auszuführen. Dies führt zu einem serverseitigen Fehler (nicht primär), der vom Java-Treiber nicht angemessen behandelt wird (dieser Fehler wird noch untersucht). Somit kann der Client in einem schlechten Zustand belassen werden, bis beispielsweise der Anwendungsserver neu gestartet wird.

Dafür gibt es zwei Abhilfemaßnahmen:

- Bei Clients, die über eine Verbindungszeichenfolge eine Verbindung zu Amazon DocumentDB herstellen, tritt dieses Problem nicht auf, da `ClusterConnectionMode` es `MULTIPLE` bei der Einstellung der Leseeinstellungen auf gesetzt wird.

  ```
  MongoClientURI mongoClientURI = new MongoClientURI("mongodb://usr:pass:cluster-
  endpoint:27317/test?ssl=false&replicaSet=rs0&readpreference=secondaryPreferred");
  MongoClient mongoClient = MongoClients.create(mongoClientURI.getURI());
  ```

  Oder Sie verwenden `MongoClientSettings` Builder mit der `applyConnectionString` Methode.

  ```
  final MongoClientSettings settings = MongoClientSettings.builder()
          .credential(credential)
          .applyConnectionString(new ConnectionString("usr:pass:cluster-endpoint:27317/
  test?ssl=false&replicaSet=rs0&readpreference=secondaryPreferred"))
          .retryWrites(false)
          .applyToSslSettings(builder # builder
                  .enabled(false))
          .build();
  MongoClient mongoClient = MongoClients.create(settings);
  ```

- Explizit gesetzt `ClusterConnectionMode` auf`MULTIPLE`. Dies ist nur erforderlich, wenn `applyToClusterSettings` und verwendet wird`hosts().size() == 1`.

  ```
  final ServerAddress serverAddress0 = new ServerAddress("cluster-endpoint", 27317));
  final MongoCredential credential = MongoCredential.createCredential("xxx","admin",
   "xxxx".toCharArray());
  ```

```
final MongoClientSettings settings = MongoClientSettings.builder()
    .credential(credential)
    .readPreference(ReadPreference.secondaryPreferred())
    .retryWrites(false)
    .applyToSslSettings(builder # builder
    .enabled(false))
    .applyToClusterSettings(builder # builder
                .hosts(Arrays.asList(serverAddress0))
                .requiredReplicaSetName("rs0"))
                .mode(ClusterConnectionMode.MULTIPLE))
    .build();
MongoClient mongoClient = MongoClients.create(settings);
```

Testen einer Verbindung zu einer Amazon DocumentDB DocumentDB-Instance

Sie können Ihre Verbindung zu einem Cluster mit gängigen Linux- oder Windows-Tools testen.

Testen Sie die Verbindung über einen Linux- oder Unix-Terminal, indem Sie folgendes eingeben (ersetzen Sie `cluster-endpoint` durch den Endpunkt und ersetzen Sie `port` durch den Port Ihrer Instance).

```
nc -zv cluster-endpoint port
```

Der folgende Code ist ein Beispiel für eine Beispieloperation und den Rückgabewert:

```
nc -zv docdbTest.d4c7nm7stsfc0.us-west-2.docdb.amazonaws.com 27017

Connection to docdbTest.d4c7nm7stsfc0.us-west-2.docdb.amazonaws.com 27017 port [tcp/*]
 succeeded!
```

Verbindung zu einem ungültigen Endpunkt herstellen

Wenn Sie eine Verbindung zu einem Amazon DocumentDB-Cluster herstellen und einen Cluster-Endpunkt verwenden, der nicht gültig ist, wird ein Fehler ähnlich dem folgenden angezeigt.

```
mongo --ssl \
   --host sample-cluster.node.us-east-1.docdb.amazonaws.com:27017 \
   --sslCAFile global-bundle.pem \
```

```
    --username <user-name> \
    --password <password>
```

Das Ergebnis sieht folgendermaßen aus:

```
MongoDB shell version v3.6
connecting to: mongodb://sample-cluster.node.us-east-1.docdb.amazonaws.com:27017/
2018-11-14T17:21:18.516-0800 I NETWORK [thread1] getaddrinfo("sample-cluster.node.us-
east-1.docdb.amazonaws.com") failed:
nodename nor servname provided, or not known 2018-11-14T17:21:18.537-0800 E QUERY
 [thread1] Error: couldn't initialize
connection to host sample-cluster.node.us-east-1.docdb.amazonaws.com, address is
 invalid :
connect@src/mongo/shell/mongo.js:237:13@(connect):1:6
exception: connect failed
```

Um den gültigen Endpunkt für einen Cluster abzurufen, führen Sie den folgenden Befehl aus:

```
aws docdb describe-db-clusters \
    --db-cluster-identifier sample-cluster \
    --query 'DBClusters[*].[Endpoint,Port]'
```

Um den gültigen Endpunkt für eine Instance abzurufen, führen Sie den folgenden Befehl aus:

```
aws docdb describe-db-instances \
    --db-instance-identifier sample-instance \
    --query 'DBInstances[*].[Endpoint.Address,Endpoint.Port]'
```

Weitere Informationen finden Sie unter Grundlegendes zu Amazon DocumentDB DocumentDB-Endpunkten.

Die Treiberkonfiguration wirkt sich auf die Anzahl der Verbindungen aus

Wenn Sie den Client-Treiber verwenden, um eine Verbindung zu einem Amazon DocumentDB-Cluster herzustellen, müssen Sie den `maxPoolSize` Konfigurationsparameter berücksichtigen. Die `maxPoolSize` Einstellung bestimmt die maximale Anzahl von Verbindungen, die der Client-Treiber in seinem Verbindungspool unterhält.

Fehlerbehebung bei Indizes

Die folgenden Themen erläutern, was zu tun ist, wenn Ihr Index oder Ihr Indexaufbau im Hintergrund fehlschlägt.

Themen

- Die Indexerstellung schlägt fehl
- Latenzprobleme und Fehler bei der Indexerstellung im Hintergrund
- Aufblähung des Datenbankindexes

Die Indexerstellung schlägt fehl

Amazon DocumentDB verwendet lokalen Speicher auf einer Instance als Teil des Indexerstellungsprozesses. Sie können diese Festplattennutzung mithilfe der FreeLocalStorage CloudWatch Metrik () `CloudWatch -> Metrics -> DocDB -> Instance Metrics` überwachen. Wenn ein Indexaufbau den gesamten lokalen Festplattenspeicherplatz verbraucht und fehlschlägt, erhalten Sie eine Fehlermeldung. Wenn Sie Daten zu Amazon DocumentDB migrieren, empfehlen wir Ihnen, zuerst Indizes zu erstellen und dann die Daten einzufügen. Weitere Informationen zu Migrationsstrategien und zum Erstellen von Indizes finden Sie Migration zu Amazon DocumentDB in der Amazon DocumentDB-Dokumentation und im Blog: Migrieren Sie mithilfe der Offline-Methode von MongoDB zu Amazon DocumentDB.

Wenn bei der Erstellung von Indizes auf einem vorhandenen Cluster die Indexerstellung länger dauert als erwartet oder fehlschlägt, empfehlen wir, dass Sie die Instance hochskalieren, um den Index zu erstellen, und dann, nachdem der Index erstellt wurde, wieder herunterskalieren. Amazon DocumentDB ermöglicht Ihnen die schnelle Skalierung von Instance-Größen innerhalb von Minuten mit dem AWS-Managementkonsole oder dem AWS CLI. Weitere Informationen finden Sie unter Instanzklassen verwalten. Bei der sekundengenauen Instance-Preisgestaltung zahlen Sie auf die Sekunde genau nur für die Ressourcen, die Sie verwenden.

Latenzprobleme und Fehler bei der Indexerstellung im Hintergrund

Index-Builds im Hintergrund in Amazon DocumentDB werden erst gestartet, wenn alle Abfragen auf der primären Instance, die vor der Initiierung der Indexerstellung gestartet wurden, vollständig ausgeführt wurden. Wenn es eine lang andauernde Abfrage gibt, werden die Index-Builds im Hintergrund blockiert, bis die Abfrage abgeschlossen ist. Daher kann es länger dauern als erwartet, bis sie abgeschlossen ist. Dies gilt auch dann, wenn Sammlungen leer sind.

Index-Builds im Vordergrund zeigen nicht dasselbe Blockierungsverhalten. Stattdessen wird bei Index-Builds im Vordergrund die Sammlung exklusiv gesperrt, bis die Indexerstellung abgeschlossen ist. Um Indizes für eine leere Sammlung zu erstellen und Blockierungen bei Abfragen mit langer Laufzeit zu vermeiden, empfehlen wir daher, Index-Builds im Vordergrund zu verwenden.

> **Note**
>
> Amazon DocumentDB lässt zu, dass zu einem bestimmten Zeitpunkt nur ein Hintergrundindex für eine Sammlung erstellt wird. Wenn DDL (Data Definition Language) Operationen wie `createIndex()` oder `dropIndex()` während eines Indexaufbaus im HIntergrund in derselben Sammlung auftreten, schlägt der Aufbau des Hintergrundindex fehl.

Aufblähung des Datenbankindexes

Amazon DocumentDB verwendet Multi-Version Concurrency Control (MVCC) zur Verwaltung gleichzeitiger Transaktionen. Wenn Dokumente gelöscht oder aktualisiert werden, verbleiben ihre vorherigen Versionen als „tote“ Versionen in Sammlungen und Indizes. Durch den Garbage-Collection-Prozess wird automatisch Speicherplatz aus diesen toten Versionen für future Operationen zurückgewonnen.

Ein aufgeblähter Index tritt auf, wenn die Indizes einer Sammlung aufgrund der Anhäufung toter oder veralteter Indexeinträge oder der Fragmentierung innerhalb der Seiten größer werden. Der angegebene Prozentsatz entspricht der Menge an Indexspeicher, die von future Indexeinträgen verwendet werden kann. Diese Aufblähung beansprucht Speicherplatz sowohl im Puffer-Cache als auch im Speicher. Wenn Sie den Bloat entfernen möchten, müssen Sie die Indizes neu erstellen.

Example Beispiel

Führen Sie den folgenden Befehl aus, um den ungenutzten Speicherplatz für Ihren Index zu ermitteln:

```
db.coll.aggregate({$indexStats:{}});
```

Das Ergebnis sieht in etwa so aus:

```
{
    "name" : "_id_",
    "key" : {
```

```
        "_id" : 1
    },
    "host" : "devbox-test.localhost.a2z.com:27317",
    "size" : NumberLong(827392),
    "accesses" : {
        "ops" : NumberLong(40000),
        "docsRead" : NumberLong(46049),
        "since" : ISODate("2025-04-03T21:44:51.251Z")
    },
    "cacheStats" : {
        "blksRead" : NumberLong(264),
        "blksHit" : NumberLong(140190),
        "hitRatio" : 99.8121
    },
    "unusedStorageSize" : {
        "unusedSizeBytes" : 409600,
        "unusedSizePercent" : 49.51
    }
}
```

Mit dem `reIndex` Befehl können Sie Indizes ohne Ausfallzeiten neu erstellen. Dazu ist ein Scan der gesamten Sammlung erforderlich. Siehe Indexverwaltung mit `ReIndex`.

Problembehebung bei Leistung und Ressourcennutzung

Dieser Abschnitt enthält Fragen und Lösungen für häufig auftretende Diagnoseprobleme in Amazon DocumentDB DocumentDB-Bereitstellungen. Die bereitgestellten Beispiele verwenden die mongo-Shell und gelten für eine einzelne Instance. Informationen zum Suchen nach einem Instance-Endpunkt finden Sie unter Grundlegendes zu Amazon DocumentDB DocumentDB-Endpunkten.

Themen

- Wie ermittle ich die Anzahl der Einfüge-, Aktualisierungs- und Löschvorgänge, die für meine Sammlung über die Mongo-API ausgeführt wurden?
- Wie analysiere ich die Cache-Leistung?
- Wie finde und beende ich langsame und blockierte Abfragen?
- Wie kann ich mir einen Abfrageplan ansehen und eine Abfrage optimieren?
- Wie kann ich mir einen Abfrageplan in elastischen Clustern ansehen?
- Wie liste ich alle laufenden Operationen für eine Instance auf?

- Woher weiß ich, wann eine Abfrage Fortschritte macht?
- Wie stelle ich fest, warum ein System plötzlich langsam läuft?
- Wie ermittle ich die Ursache für eine hohe CPU-Auslastung auf einer oder mehreren Cluster-Instances?
- Wie ermittle ich die offenen Cursor auf einer Instance?
- Wie finde ich die aktuelle Version der Amazon DocumentDB DocumentDB-Engine heraus?
- Wie analysiere ich die Indexnutzung und identifiziere ungenutzte Indizes?
- Wie identifiziere ich fehlende Indizes?
- Wie stelle ich fest, dass die Datenbanksammlung überlastet ist?
- Zusammenfassung nützlicher Abfragen

Wie ermittle ich die Anzahl der Einfüge-, Aktualisierungs- und Löschvorgänge, die für meine Sammlung über die Mongo-API ausgeführt wurden?

Um die Anzahl der Einfüge-, Aktualisierungs- und Löschvorgänge anzuzeigen, die für eine bestimmte Sammlung ausgeführt wurden, führen Sie den folgenden Befehl für diese Sammlung aus:

```
db.collection.stats()
```

Die Ausgabe dieses Befehls beschreibt unter seinem `opCounters` Feld Folgendes:

- num DocsIns — Die Anzahl der Dokumente, die in diese Sammlung eingefügt wurden. Dazu gehören Dokumente, die mit den `insertMany` Befehlen `insert` und eingefügt wurden, sowie Dokumente, die mit einem Upsert eingefügt wurden.
- num DocsUpd — Die Anzahl der Dokumente, die in dieser Sammlung aktualisiert wurden. Dazu gehören Dokumente, die mit den `findAndModify` Befehlen `update` und aktualisiert wurden.
- num DocsDel — Die Anzahl der Dokumente, die aus dieser Sammlung gelöscht wurden. Dazu gehören Dokumente`deleteOne`, die mit den `findAndModify` Befehlen`deleteMany`,`remove`, und gelöscht wurden.
- LastReset — Der Zeitpunkt, zu dem diese Zähler zuletzt zurückgesetzt wurden. Die mit diesem Befehl bereitgestellten Statistiken werden zurückgesetzt, wenn starting/stopping der Cluster oder die Instanz skaliert up/down wird.

Ein Beispiel für die Ausgabe von running `db.collection.stats()` ist unten dargestellt.

```
{
    "ns" : "db.test",
    "count" : ...,
    "size" : ...,
    "avgObjSize" : ...,
    "storageSize" : ...,
    "capped" : false,
    "nindexes" : ...,
    "totalIndexSize" : ...,
    "indexSizes" : {
        "_id_" : ...,
        "x_1" : ...
    },
    "collScans" : ...,
    "idxScans" : ...,
    "opCounter" : {
        "numDocsIns" : ...,
        "numDocsUpd" : ...,
        "numDocsDel" : ...
    },
    "cacheStats" : {
        "collBlksHit" : ...,
        "collBlksRead" : ..,
        "collHitRatio" : ...,
        "idxBlksHit" : ...,
        "idxBlksRead" : ...,
        "idxHitRatio" : ...
    },
    "lastReset" : "2022-09-02 19:41:40.471473+00",
    "ok" : 1,
    "operationTime" : Timestamp(1662159707, 1)
}
```

Dieser Statistikbefehl sollte verwendet werden, wenn sammlungsspezifische Zähler für Einfüge-, Aktualisierungs- und Löschvorgänge über die Mongo-API angezeigt werden. Eine andere Möglichkeit, sammlungsspezifische Betriebszähler anzuzeigen, besteht darin, die DML-Überwachung zu aktivieren. Die Anzahl der Einfüge-, Aktualisierungs- und Löschvorgänge für alle Sammlungen in Zeitintervallen von einer Minute kann in einminütigen Zeitintervallen eingesehen werden. Überwachen von Amazon DocumentDB mit CloudWatch

Wie analysiere ich die Cache-Leistung?

Die Analyse der Cache-Leistung kann Aufschluss über die Effizienz des Datenabrufs und die Systemleistung geben und basiert darauf, wie viele Daten von der Festplatte im Vergleich zum Cache gelesen werden. Wir stellen Cache-Statistiken über die Anzahl der Cache-Treffer (aus dem Cache gelesene Daten) und Cache-Fehlschläge (Daten, die nicht im Cache gefunden und von der Festplatte gelesen wurden) zur Verfügung, um einen Einblick in die Cache-Leistung zu geben. Die Cache-Statistiken für eine bestimmte Sammlung können gefunden werden, indem Sie den folgenden Befehl für diese Sammlung ausführen:

```
db.collection.stats()
```

Die Werte im `cacheStats` Feld in der Ausgabe dieses Befehls liefern Cache-Statistiken für die Sammlung sowie die gesamten Cache-Statistiken für die Indizes, die für die Sammlung erstellt wurden. Diese Statistiken sind unten aufgeführt:

- **`collBlksHit`**- Die Anzahl der Blöcke, die während der Operationen an dieser Sammlung aus dem Cache gelesen wurden.
- **`collBlksRead`**- Die Anzahl der Blöcke, die bei Vorgängen an dieser Sammlung von der Festplatte gelesen wurden (Cache-Fehlschläge).
- **`collHitRatio`**— Die Cache-Trefferquote für diese Sammlung (`100 * [collBlksHit / (collBlksHit + collBlksRead)]`).
- **`idxBlksHit`**- Die Anzahl der Blöcke, die für jeden Index, der für diese Sammlung erstellt wurde, aus dem Cache gelesen wurden.
- **`idxBlksRead`**- Die Anzahl der von der Festplatte gelesenen Blöcke (Cache-Fehlschläge) für jeden Index, der für diese Sammlung erstellt wurde.
- **`idxHitRatio`**— Die Cache-Trefferquote für die für diese Sammlung erstellten Indizes (`100 * [idxBlksHit / (idxBlksHit + idxBlksRead)]`).
- **`lastReset`**- Der Zeitpunkt, zu dem diese Statistiken zuletzt zurückgesetzt wurden. Die von bereitgestellten Statistiken `db.collection.stats()` werden zurückgesetzt, wenn starting/stopping der Cluster oder up/down die Instanz skaliert wird.

Eine Aufschlüsselung der `idxBlksRead` Felder `idxBlksHit` und für jeden Index finden Sie auch mit dem `indexStats` Befehl. Indexspezifische Cache-Statistiken finden Sie, indem Sie den folgenden Befehl ausführen:

```
db.collection.aggregate([{$indexStats:{}}]).pretty()
```

Für jeden Index finden Sie die folgenden Cache-Statistiken unter dem `cacheStats` Feld:

- **`blksHit`**- Die Anzahl der Blöcke, die für diesen Index aus dem Cache gelesen wurden.
- **`blksRead`**- Die Anzahl der Blöcke, die für diesen Index von der Festplatte gelesen wurden.
- **`blksHitRatio`**- Die auf vier Dezimalstellen gerundete Cache-Trefferquote, berechnet von`100 * [blksHit / (blksHit + blksRead)]`.

Wie finde und beende ich langsame und blockierte Abfragen?

Benutzerabfragen können aufgrund eines nicht optimalen Abfrageplans langsam ausgeführt oder aufgrund von Ressourcenkonflikten blockiert werden.

Zum Suchen nach Abfragen, die aufgrund eines nicht optimalen Abfrageplans verlangsamt oder aufgrund von Ressourcenkonflikten blockiert werden, verwenden Sie den Befehl `currentOp`. Sie können den Befehl filtern, um die Liste der relevanten Abfragen einzugrenzen. Mit der langsamen Abfrage muss `opid` verknüpft sein, um sie beenden zu können.

Die folgende Abfrage verwendet den Befehl `currentOp`, um alle Abfragen aufzulisten, die blockiert oder länger als 10 Sekunden ausgeführt werden.

```
db.adminCommand({
    aggregate: 1,
    pipeline: [
        {$currentOp: {}},
        {$match:
            {$or: [
                {secs_running: {$gt: 10}},
                {WaitState: {$exists: true}}]}},
        {$project: {_id:0, opid: 1, secs_running: 1}}],
    cursor: {}
});
```

Als Nächstes können Sie die Abfrage einschränken, um die `opid` von länger als 10 Sekunden ausgeführten Abfragen zu finden und diese zu beenden.

So finden und beenden Sie eine Abfrage, die länger als 10 Sekunden läuft:

1. Suchen Sie die `opid` der Abfrage.

```
db.adminCommand({
    aggregate: 1,
    pipeline: [
        {$currentOp: {}},
        {$match:
            {$or:
                [{secs_running: {$gt: 10}},
                 {WaitState: {$exists: true}}]}}],
    cursor: {}
});
```

   Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus (JSON-Format).

```
{
    "waitedMS" : NumberLong(0),
    "cursor" : {
        "firstBatch" : [
            {
                "opid" : 24646,
                "secs_running" : 12
            }
        ],
        "id" : NumberLong(0),
        "ns" : "admin.$cmd"
    },
    "ok" : 1
}
```

2. Beenden Sie die Abfrage mit der Operation `killOp`.

```
db.adminCommand({killOp: 1, op: 24646});
```

Wie kann ich mir einen Abfrageplan ansehen und eine Abfrage optimieren?

Wenn eine Abfrage langsam ausgeführt wird, erfordert die Abfrageausführung möglicherweise den vollständigen Scan der Sammlung, um die relevanten Dokumente auszuwählen. Manchmal kann

die Abfrage schneller ausgeführt werden, wenn geeignete Indizes erstellt werden. Mit dem Befehl `explain` erkennen Sie dieses Szenario und können die Felder für die Indizes auswählen.

> **Note**
>
> Amazon DocumentDB emuliert die MongoDB 3.6-API auf einer speziell entwickelten Datenbank-Engine, die ein verteiltes, fehlertolerantes, selbstheilendes Speichersystem verwendet. Daher `explain()` können sich die Abfragepläne und die Ausgabe von zwischen Amazon DocumentDB und MongoDB unterscheiden. Kunden, die die Kontrolle über ihren Abfrageplan wünschen, können den `$hint`-Operator verwenden, um die Auswahl eines bevorzugten Indexes zu erzwingen.

Führen Sie die Abfrage, die Sie verbessern möchten, unter dem Befehl `explain` wie folgt aus.

```
db.runCommand({explain: {<query document>}})
```

Im Folgenden finden Sie eine Beispieloperation.

```
db.runCommand({explain:{
    aggregate: "sample-document",
    pipeline: [{$match: {x: {$eq: 1}}}],
    cursor: {batchSize: 1}}
});
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus (JSON-Format).

```
{
    "queryPlanner" : {
        "plannerVersion" : 1,
        "namespace" : "db.test",
        "winningPlan" : {
            "stage" : "COLLSCAN"
        }
    },
    "serverInfo" : {
        "host" : "...",
        "port" : ...,
        "version" : "..."
    },
```

```
    "ok" : 1
}
```

Die Ausgabe oben zeigt an, dass in der Phase `$match` die gesamte Sammlung gescannt werden muss, um zu prüfen, ob das Feld `"x"` in jedem Dokument gleich 1 ist. Wenn die Sammlung zahlreiche Dokumente enthält, wird der Scan der Sammlung sehr langsam ausgeführt. Damit ist auch die Gesamtleistung der Abfrage sehr niedrig. Das Vorhandensein von `"COLLSCAN"` in der Ausgabe des Befehls `explain` zeigt daher an, dass die Abfrageleistung durch die Erstellung geeigneter Indizes verbessert werden kann.

In diesem Beispiel prüft die Abfrage, ob das Feld `"x"` in allen Dokumenten gleich 1 ist. Das Erstellen eines Indexes für das Feld `"x"` ermöglicht der Abfrage, einen vollständigen Scan der Sammlung zu vermeiden und den Index zu verwenden, um die relevanten Dokumente schneller zurückzugeben.

Nach dem Erstellen eines Indexes für das Feld `"x"` sieht die `explain`-Ausgabe wie folgt aus.

```
{
    "queryPlanner" : {
         "plannerVersion" : 1,
         "namespace" : "db.test",
         "winningPlan" : {
             "stage" : "IXSCAN",
             "indexName" : "x_1",
             "direction" : "forward"
         }
    },
    "serverInfo" : {
        "host" : "...",
        "port" : ...,
        "version" : "..."
    },
    "ok" : 1
}
```

Das Erstellen eines Indexes für das Feld `"x"` ermöglicht der Stufe `$match` die Verwendung eines Index, um die Anzahl der Dokumente zu reduzieren, in denen das Prädikat `"x = 1"` ausgewertet werden muss.

Bei kleinen Sammlungen kann der Amazon DocumentDB DocumentDB-Abfrageprozessor entscheiden, keinen Index zu verwenden, wenn die Leistungssteigerung vernachlässigbar ist.

Wie kann ich mir einen Abfrageplan in elastischen Clustern ansehen?

Verwenden Sie den `explain` Befehl, um einen Abfrageplan in elastischen Clustern zu untersuchen. Im Folgenden finden Sie einen `explain` Beispielvorgang für eine Suchabfrage, die auf eine Sharded-Sammlung abzielt:

```
db.runCommand(
   {
     explain: { find: "cities", filter: {"name": "Seoul"}}
   }
)
```

> **Note**
>
> Amazon DocumentDB emuliert MongoDB auf einer speziell entwickelten Datenbank-Engine. Daher `explain()` können sich die Abfragepläne und die Ausgabe von zwischen Amazon DocumentDB und MongoDB unterscheiden. Sie können den Abfrageplan mithilfe des `$hint` Operators steuern, um die Auswahl eines bevorzugten Indexes zu erzwingen.

Die Ausgabe dieses Vorgangs könnte etwa wie folgt aussehen (JSON-Format):

```
{
  "queryPlanner" : {
    "elasticPlannerVersion" : 1,
    "winningPlan" : {
      "stage" : "SINGLE_SHARD",
      "shards" : [
        {
          "plannerVersion" : 1,
          "namespace" : "population.cities",
          "winningPlan" : {
            "stage" : "SHARD_MERGE",
            "shards" : [
              {
                "shardName" : "f2cf5cfd-fe9c-40ca-b4e5-298ca0d11111",
                "plannerVersion" : 1,
                "namespace" : "population.cities",
                "winningPlan" : {
                  "stage" : "PARTITION_MERGE",
                  "inputStages" : [
```

```
                    {
                      "stage" : "COLLSCAN",
                      "partitionCount" : 21
                    }
                  ]
                }
              },
              {
                "shardName" : "8f3f80e2-f96c-446e-8e9d-aab8c7f22222",
                "plannerVersion" : 1,
                "namespace" : "population.cities",
                "winningPlan" : {
                  "stage" : "PARTITION_MERGE",
                  "inputStages" : [
                    {
                      "stage" : "COLLSCAN",
                      "partitionCount" : 21
                    }
                  ]
                }
              },
              {
                "shardName" : "32c5a06f-1b2b-4af1-8849-d7c4a033333",
                "plannerVersion" : 1,
                "namespace" : "population.cities",
                "winningPlan" : {
                  "stage" : "PARTITION_MERGE",
                  "inputStages" : [
                    {
                      "stage" : "COLLSCAN",
                      "partitionCount" : 22
                    }
                  ]
                }
              }
            ]
          },
          "shardName" : "32c5a06f-1b2b-4af1-8849-d7c4a0f3fb58"
        }
      ]
    }
  },
  "serverInfo" : {
    "host" : "example-4788267630.us-east-1.docdb-elastic.amazonaws.com:27017",
```

```
    "version" : "5.0.0"
  },
  "ok" : 1,
  "operationTime" : Timestamp(1695097923, 1)
}
```

Die vorherige Ausgabe zeigt den Abfrageplan für die `find` Abfrage in einem Cluster mit drei Shards. Jeder Shard hat mehrere Datenpartitionen, die unterschiedliche Eingabestufen haben können. In diesem Beispiel wird ein „COLLSCAN“ (ein Sammlungsscan) auf allen Partitionen ausgeführt, bevor die Ergebnisse in der Phase“ PARTITION_MERGE „innerhalb jedes Shards zusammengeführt werden. Die Ergebnisse aller Shards werden dann in der Phase“ SHARD_MERGE „zusammengeführt, bevor sie an den Client zurückgesendet werden.

Wie liste ich alle laufenden Operationen für eine Instance auf?

Als Benutzer oder Hauptbenutzer möchten Sie zu Diagnose- und Fehlerbehebungszwecken häufig alle aktuellen Operationen auflisten, die auf einer Instanz ausgeführt werden. (Weitere Informationen zum Verwalten von Benutzern finden Sie unter Amazon DocumentDB DocumentDB-Benutzer verwalten.)

Mit der `mongo` Shell können Sie die folgende Abfrage verwenden, um alle laufenden Operationen auf einer Amazon DocumentDB DocumentDB-Instance aufzulisten.

```
db.adminCommand({currentOp: 1, $all: 1});
```

Die Abfrage gibt die vollständige Liste aller Benutzerabfragen und internen Systemaufgaben zurück, die zurzeit auf der Instance ausgeführt werden.

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus (JSON-Format).

```
{
    "inprog" : [
        {
            "desc" : "INTERNAL"
        },
        {
            "desc" : "TTLMonitor",
            "active" : false
        },
        {
            "client" : ...,
```

```
            "desc" : "Conn",
            "active" : true,
            "killPending" : false,
            "opid" : 195,
            "ns" : "admin.$cmd",
            "command" : {
                "currentOp" : 1,
                "$all" : 1
            },
            "op" : "command",
            "$db" : "admin",
            "secs_running" : 0,
            "microsecs_running" : NumberLong(68),
            "clientMetaData" : {
            "application" : {
                "name" : "MongoDB Shell"
            },
            "driver" : {
                ...
            },
            "os" : {
                ...
            }
         }
      },
      {
         "desc": "GARBAGE_COLLECTION",
         "garbageCollection": {
            "databaseName": "testdb",
            "collectionName": "testCollectionA"
         },
         "secs_running": 3,
         "microsecs_running": NumberLong(3123456)
      },
      {
         "desc": "GARBAGE_COLLECTION",
         "garbageCollection": {
            "databaseName": "testdb",
            "collectionName": "testCollectionB"
         },
         "secs_running": 4,
         "microsecs_running": NumberLong(4123456)
      }
   ],
```

```
    "ok" : 1
}
```

Die folgenden Werte sind gültige Werte für das Feld `"desc"`:

- **`INTERNAL`**— Interne Systemaufgaben wie die Cursorbereinigung oder Aufgaben zur Bereinigung veralteter Benutzer.
- **`TTLMonitor`**— Der Time to Live (TTL) -Monitor-Thread. Der Ausführungsstatus wird im Feld `"active"` dargestellt.
- **`GARBAGE_COLLECTION`**— Der interne Garbage-Collector-Thread.
- **`CONN`**— Die Benutzerabfrage.
- **`CURSOR`**— Die Operation ist ein inaktiver Cursor, der darauf wartet, dass der Benutzer den Befehl „GetMore“ aufruft, um den nächsten Stapel von Ergebnissen zu erhalten. In diesem Zustand verbraucht der Cursor Speicher, verbraucht aber keine Rechenleistung.

In der obigen Ausgabe werden auch alle Benutzerabfragen im System aufgeführt. Jede Benutzerabfrage wird im Kontext einer Datenbank und einer Sammlung ausgeführt. Die Kombination dieser beiden Komponenten wird als Namespace bezeichnet. Der Namespace jeder Benutzerabfrage ist im Feld `"ns"` verfügbar.

Manchmal müssen Sie alle Benutzerabfragen auflisten, die in einem bestimmten Namespace ausgeführt werden. Daher muss die vorherige Ausgabe anhand des Felds `"ns"` gefiltert werden. Im Folgenden finden Sie eine Beispielabfrage für eine gefilterte Ausgabe. Die Abfrage listet alle Benutzerabfragen auf, die zurzeit in der Datenbank `"db"` und in der Sammlung `"test"` ausgeführt werden (d. h. im Namespace `"db.test"`).

```
db.adminCommand({aggregate: 1,
    pipeline: [{$currentOp: {allUsers: true, idleConnections: true}},
               {$match: {ns: {$eq: "db.test"}}}],
    cursor: {}
});
```

Als Hauptbenutzer des Systems können Sie die Abfragen aller Benutzer und auch alle internen Systemaufgaben sehen. Alle anderen Benutzer können nur ihre jeweiligen Abfragen anzeigen.

Wenn die Gesamtzahl der Abfragen und internen Systemaufgaben die Standard-Batch-Cursor-Größe überschreitet, generiert die mongo-Shell automatisch das Iterator-Objekt `'it'`, um den Rest der

Ergebnisse anzuzeigen. Führen Sie den Befehl `'it'` so lange aus, bis alle Ergebnisse angezeigt wurden.

Woher weiß ich, wann eine Abfrage Fortschritte macht?

Benutzerabfragen können aufgrund eines nicht optimalen Abfrageplans langsam ausgeführt oder aufgrund von Ressourcenkonflikten blockiert werden. Das Debuggen solcher Abfragen ist ein mehrstufiger Prozess, in dem möglicherweise mehrmals dieselben Schritte ausgeführt werden müssen.

Im ersten Debugging-Schritt werden alle langsamen oder blockierten Abfragen aufgeführt. Die folgende Abfrage listet alle Benutzerabfragen auf, die länger als 10 Sekunden ausgeführt wurden oder auf Ressourcen warten.

```
db.adminCommand({aggregate: 1,
                 pipeline: [{$currentOp: {}},
                            {$match: {$or: [{secs_running: {$gt: 10}},
                                            {WaitState: {$exists: true}}]}},
                            {$project: {_id:0,
                                        opid: 1,
                                        secs_running: 1,
                                        WaitState: 1,
                                        blockedOn: 1,
                                        command: 1}}],
                 cursor: {}
                });
```

Wiederholen Sie die vorherige Abfrage regelmäßig, um zu ermitteln, ob sich die Liste der Abfragen ändert, und die langsamen oder blockierten Abfragen zu identifizieren.

Wenn das Ausgabedokument der betreffenden Abfrage das Feld `WaitState` enthält, zeigt dies an, dass die Abfrage aufgrund von Ressourcenkonflikten langsam ist oder blockiert wird. Der Ressourcenkonflikt kann entweder auf I/O interne Systemaufgaben oder andere Benutzeranfragen zurückzuführen sein.

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus (JSON-Format).

```
{
    "waitedMS" : NumberLong(0),
    "cursor" : {
        "firstBatch" : [
```

```
            {
                "opid" : 201,
                "command" : {
                    "aggregate" : ...
                },
                "secs_running" : 208,
                "WaitState" : "IO"
            }
        ],
        "id" : NumberLong(0),
        "ns" : "admin.$cmd"
    },
    "ok" : 1
}
```

I/O kann ein Engpass sein, wenn viele Abfragen in verschiedenen Sammlungen gleichzeitig auf derselben Instanz ausgeführt werden, oder wenn die Instanzgröße für den Datensatz, für den die Abfrage ausgeführt wird, zu klein ist. Wenn es sich bei den Abfragen um schreibgeschützte Abfragen handelt, können Sie der eben beschriebenen Situation durch Aufteilung der Abfragen für die einzelnen Sammlungen auf separate Replikate abhelfen. Wenn in verschiedenen Sammlungen gleichzeitig Updates ausgeführt werden oder die Instance zu klein für den Datensatz ist, können Sie die Instance aufwärts skalieren.

Wenn der Ressourcenkonflikt auf Abfragen anderer Benutzer zurückzuführen ist, zeigt das Feld `"blockedOn"` im Ausgabedokument die `"opid"` der Abfrage an, die sich auf die Abfrage auswirkt. Folgen Sie mithilfe der `"opid"` der Kette der Felder `"WaitState"` und `"blockedOn"` aller Abfragen, um die Abfrage an der Ende der Kette zu finden.

Wenn es sich bei der Aufgabe am Ende der Kette um eine interne Aufgabe handelt, kann das Problem nur behoben werden, indem die Abfrage beendet und später erneut ausgeführt wird.

Im Folgenden finden Sie eine Beispielausgabe, in der die Suchabfrage auf einer Sammlungssperre blockiert wird, die im Besitz einer anderen Aufgabe ist.

```
{
    "inprog" : [
        {
            "client" : "...",
            "desc" : "Conn",
            "active" : true,
            "killPending" : false,
            "opid" : 75,
```

```
            "ns" : "...",
            "command" : {
                "find" : "...",
                "filter" : {

                }
            },
            "op" : "query",
            "$db" : "test",
            "secs_running" : 9,
            "microsecs_running" : NumberLong(9449440),
            "threadId" : 24773,
            "clientMetaData" : {
                "application" : {
                   "name" : "MongoDB Shell"
                },
                "driver" : {
                    ...
                },
                "os" : {
                    ...
                }
            },
            "WaitState" : "CollectionLock",
            "blockedOn" : "INTERNAL"
        },
        {
            "desc" : "INTERNAL"
        },
        {
            "client" : "...",
            ...
            "command" : {
                "currentOp" : 1
            },
            ...
        }
    ],
    "ok" : 1
}
```

Wenn "`WaitState`" die Werte "`Latch`", "`SystemLock`", "`BufferLock`", "`BackgroundActivity`" oder "`Other`" hat, wird der Ressourcenkonflikt von internen

Systemaufgaben verursacht. Wenn die Situation lange andauert, besteht die einzige Abhilfe darin, die Abfrage zu beenden und später erneut auszuführen.

Wie stelle ich fest, warum ein System plötzlich langsam läuft?

Im Folgenden finden Sie einige häufige Gründe für die Verlangsamung von Systemen:

- Übermäßige Ressourcenkonflikte zwischen gleichzeitigen Abfragen
- Zunahme der Anzahl der aktiven gleichzeitigen Abfragen im Laufe der Zeit
- Interne Systemaufgaben wie `"GARBAGE_COLLECTION"`

Wenn Sie die Systemnutzung im Laufe der Zeit überwachen möchten, führen Sie in regelmäßigen Abständen die folgende `"currentOp"`-Abfrage aus, und geben Sie die Ergebnisse in einem externen Speicher aus. Die Abfrage zählt die Anzahl der Abfragen und Operationen in jedem Namespace im System. Sie können anschließend die Systemnutzungsergebnisse analysieren, um die Systemlast zu verstehen und entsprechende Maßnahmen zu ergreifen.

```
db.adminCommand({aggregate: 1,
                 pipeline: [{$currentOp: {allUsers: true, idleConnections: true}},
                            {$group: {_id: {desc: "$desc", ns: "$ns", WaitState:
 "$WaitState"}, count: {$sum: 1}}}],
                 cursor: {}
                });
```

Diese Abfrage gibt eine Aggregation aller in den einzelnen Namespaces ausgeführten Abfragen, alle internen Systemaufgaben und die eindeutige Anzahl der Wartezustände (wenn vorhanden) pro Namespace zurück.

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus (JSON-Format).

```
{
    "waitedMS" : NumberLong(0),
    "cursor" : {
        "firstBatch" : [
            {
                "_id" : {
                    "desc" : "Conn",
                    "ns" : "db.test",
                    "WaitState" : "CollectionLock"
                },
```

```
                "count" : 2
            },
            {
                "_id" : {
                    "desc" : "Conn",
                    "ns" : "admin.$cmd"
                },
                "count" : 1
            },
            {
                "_id" : {
                    "desc" : "TTLMonitor"
                },
                "count" : 1
            }
        ],
        "id" : NumberLong(0),
        "ns" : "admin.$cmd"
    },
    "ok" : 1
}
```

In der oben gezeigten Ausgabe werden zwei Benutzerabfragen im Namespace `"db.test"` durch eine Sammlungssperre blockiert: 1 Abfrage in Namespace `"admin.$cmd"` und eine interne `"TTLMonitor"`-Aufgabe.

Wenn die Ausgabe viele Abfragen mit blockierenden Wartezuständen anzeigt, finden Sie Informationen unter Wie finde und beende ich langsame und blockierte Abfragen?.

Wie ermittle ich die Ursache für eine hohe CPU-Auslastung auf einer oder mehreren Cluster-Instances?

In den folgenden Abschnitten finden Sie Informationen, die Ihnen möglicherweise helfen, die Ursache für die hohe CPU-Nutzung einer Instance zu ermitteln. Die Ergebnisse sind vom Workload abhängig.

- Informationen dazu, wie Sie ermitteln, warum eine Instance plötzlich langsam ausgeführt wird, finden Sie unter Wie stelle ich fest, warum ein System plötzlich langsam läuft?.
- Informationen zum Identifizieren und Beenden langsamer Abfragen auf einer bestimmten Instance finden Sie unter Wie finde und beende ich langsame und blockierte Abfragen?.
- Informationen dazu, wie Sie ermitteln, ob eine Abfrage fortschreitet, finden Sie unter Woher weiß ich, wann eine Abfrage Fortschritte macht?.

- Informationen dazu, warum die Ausführung einer Abfrage lange dauert, finden Sie unter Wie kann ich mir einen Abfrageplan ansehen und eine Abfrage optimieren?.
- Informationen dazu, wie Sie langsame Abfragen über die Zeit nachverfolgen, finden Sie unter Profilierung von Amazon DocumentDB DocumentDB-Vorgängen.

Abhängig vom Grund für die hohe CPU-Nutzung Ihrer Instance können Sie einen oder mehrere der folgenden Schritte ausführen.

- Wenn die primäre Instance eine hohe CPU-Nutzung aufweist, die Replikat-Instances jedoch nicht, sollten Sie den Datenverkehr für Lesevorgänge über die Client-Leseeinstellungen auf mehrere Replikate verteilen (z. B. `secondaryPreferred`). Weitere Informationen finden Sie unter Als Replikatsatz eine Verbindung zu Amazon DocumentDB herstellen.

  Die Verwendung von Replikaten für Lesevorgänge kann zu einer besseren Nutzung der Cluster-Ressourcen führen, da die primäre Instance eine größere Menge an Schreibdatenverkehr verarbeiten kann. Lesevorgänge aus -Replikaten sind Eventually Consistent.
- Wenn die hohe CPU-Nutzung durch Schreib-Workloads verursacht wird, können Sie durch die Skalierung der Cluster-Instances auf einen größeren Instance-Typ die Anzahl der CPU-Kerne erhöhen, die für den Workload verfügbar sind. Weitere Informationen erhalten Sie unter Verwaltung von Amazon DocumentDB DocumentDB-Instances und Spezifikationen der Instanzklasse.
- Wenn alle Cluster-Instances eine hohe CPU-Nutzung aufweisen und der Workload Replikate für Lesevorgänge verwendet, erhöht das Hinzufügen weiterer Replikate zum Cluster die Zahl der für Lesevorgänge verfügbaren Ressourcen. Weitere Informationen finden Sie unter Hinzufügen einer Amazon DocumentDB DocumentDB-Instance zu einem Cluster.

Wie ermittle ich die offenen Cursor auf einer Instance?

Wenn Sie mit einer Amazon DocumentDB DocumentDB-Instance verbunden sind, können Sie den Befehl verwenden, `db.runCommand("listCursors")` um die geöffneten Cursor auf dieser Instance aufzulisten. Es gibt ein Limit von bis zu 4.560 aktiven Cursorn, die zu einem bestimmten Zeitpunkt auf einer bestimmten Amazon DocumentDB DocumentDB-Instance geöffnet sind, je nach Instance-Typ. Es wird allgemein empfohlen, Cursor zu schließen, die nicht mehr verwendet werden, da Cursor Ressourcen auf einer Instance verwenden und eine Obergrenze haben. Spezifische Grenzwerte finden Sie unterAmazon DocumentDB Kontingente und Beschränkungen.

```
db.runCommand("listCursors")
```

Wie finde ich die aktuelle Version der Amazon DocumentDB DocumentDB-Engine heraus?

Führen Sie den folgenden Befehl aus, um Ihre aktuelle Amazon DocumentDB DocumentDB-Engine-Version zu ermitteln.

```
db.runCommand({getEngineVersion: 1})
```

Die Ausgabe dieser Operation sieht in etwa folgendermaßen aus (JSON-Format).

```
{ "engineVersion" : "2.x.x", "ok" : 1 }
```

> **Note**
>
> Die Engine-Version für Amazon DocumentDB 3.6 ist 1.x.x, die Engine-Version für Amazon DocumentDB 4.0 ist 2.x.x, die Engine-Version für Amazon DocumentDB 5.0 ist 3.x.x und die Engine-Version für Amazon DocumentDB 8.0 ist 4.x.x.

Wie analysiere ich die Indexnutzung und identifiziere ungenutzte Indizes?

Zum Identifizieren der Indizes für eine bestimmte Sammlung führen Sie den folgenden Befehl aus:

```
db.collection.getIndexes()
```

Um zu analysieren, wie viele Indizes bei Vorgängen an den Sammlungen verwendet werden, können die `indexStats` Befehle `collStats` und verwendet werden. Führen Sie den folgenden Befehl aus, um die Gesamtzahl der mit Indizes (Indexscans) durchgeführten Scans mit der Anzahl der ohne Index durchgeführten Scans (Sammlungsscans) zu vergleichen:

```
db.collection.stats()
```

Die Ausgabe für diesen Befehl umfasst die folgenden Werte:

- **`idxScans`**- Die Anzahl der Scans, die für diese Sammlung mithilfe eines Indexes durchgeführt wurden.

- **`collScans`**- Die Anzahl der Scans, die für diese Sammlung ohne Verwendung eines Indexes durchgeführt wurden. Bei diesen Scans hätten die Dokumente in der Sammlung nacheinander durchsucht werden müssen.
- **`lastReset`**- Der Zeitpunkt, zu dem diese Zähler zuletzt zurückgesetzt wurden. Die mit diesem Befehl bereitgestellten Statistiken werden beim Clustern oder Skalieren starting/stopping up/down der Instanz zurückgesetzt.

Eine Aufschlüsselung, wie häufig die einzelnen Indizes verwendet werden, finden Sie in der Ausgabe des folgenden Befehls. Es hat sich bewährt, ungenutzte Indizes regelmäßig zu identifizieren und zu entfernen, um die Leistung zu verbessern und die Kosten zu senken, da dadurch unnötige Rechenleistung, Speicherung und Nutzung I/Os zur Verwaltung der Indizes vermieden werden.

```
db.collection.aggregate([{$indexStats:{}}]).pretty()
```

Die Ausgabe dieses Befehls enthält die folgenden Werte für jeden Index, der in der Sammlung erstellt wurde:

- **`ops`**- Die Anzahl der Operationen, die den Index verwendet haben. Wenn Ihre Workload über einen ausreichend langen Zeitraum ausgeführt wurde und Sie sicher sind, dass sich Ihre Workload in einem konstanten Zustand befindet, würde ein `ops`-Wert von Null anzeigen, dass der Index überhaupt nicht verwendet wird.
- **`numDocsRead`**- Die Anzahl der Dokumente, die bei Vorgängen gelesen wurden, die diesen Index verwenden.
- **`since`**— Die Zeit, seit Amazon DocumentDB mit der Erfassung von Statistiken zur Indexnutzung begonnen hat. Dies ist in der Regel der Wert seit dem letzten Datenbankneustart oder der letzten Wartungsaktion.
- **`size`**- Die Größe dieses Indexes in Byte.

Das folgende Beispiel ist eine Beispielausgabe aus der Ausführung des obigen Befehls:

```
{
    "name" : "_id_",
    "key" : {
        "_id" : 1
    },
    "host" : "example-host.com:12345",
    "size" : NumberLong(...),
```

```
    "accesses" : {
        "ops" : NumberLong(...),
        "docsRead" : NumberLong(...),
        "since" : ISODate("...")
    },
    "cacheStats" : {
        "blksRead" : NumberLong(...),
        "blksHit" : NumberLong(...),
        "hitRatio" : ...
    }
}
{
    "name" : "x_1",
    "key" : {
        "x" : 1
    },
    "host" : "example-host.com:12345",
    "size" : NumberLong(...),
    "accesses" : {
        "ops" : NumberLong(...),
        "docsRead" : NumberLong(...),
        "since" : ISODate("...")
    },
    "cacheStats" : {
        "blksRead" : NumberLong(...),
        "blksHit" : NumberLong(...),
        "hitRatio" : ...
    }
}
```

Um die Gesamtindexgröße für eine Sammlung zu ermitteln, führen Sie den folgenden Befehl aus:

```
db.collection.stats()
```

Führen Sie den folgenden Befehl aus, um einen nicht verwendeten Index zu löschen:

```
db.collection.dropIndex("indexName")
```

Wie identifiziere ich fehlende Indizes?

Sie können den Amazon DocumentDB DocumentDB-Profiler verwenden, um langsame Abfragen zu protokollieren. Eine Abfrage, die wiederholt im Protokoll über langsame Abfragen erscheint,

kann darauf hinweisen, dass ein zusätzlicher Index erforderlich ist, um diese Abfrageleistung zu verbessern.

Sie können Möglichkeiten für hilfreiche Indizes identifizieren, indem Sie nach Abfragen mit langer Laufzeit suchen, die über eine oder mehrere Phasen verfügen, die mindestens eine `COLLSCAN` Phase ausführen. Das bedeutet, dass in der Abfragephase jedes Dokument in der Sammlung gelesen werden muss, um eine Antwort auf die Abfrage zu geben.

Das folgende Beispiel zeigt eine Abfrage zu einer Sammlung von Taxifahrten, die auf einer großen Sammlung ausgeführt wurden.

```
db.rides.count({"fare.totalAmount":{$gt:10.0}}))
```

Um dieses Beispiel auszuführen, musste die Abfrage einen Sammlungsscan durchführen (d. h. jedes einzelne Dokument in der Sammlung lesen), da es keinen Index für das `fare.totalAmount`-Feld gibt. Die Ausgabe des Amazon DocumentDB DocumentDB-Profilers für diese Abfrage sieht in etwa wie folgt aus:

```
{
    ...
    "cursorExhausted": true,
    "nreturned": 0,
    "responseLength": 0,
    "protocol": "op_query",
    "millis": 300679,
    "planSummary": "COLLSCAN",
    "execStats": {
        "stage": "COLLSCAN",
        "nReturned": "0",
        "executionTimeMillisEstimate": "300678.042"
    },
    "client": "172.31.5.63:53878",
    "appName": "MongoDB Shell",
    "user": "example"
}
```

Um die Abfrage in diesem Beispiel zu beschleunigen, möchten Sie einen Index auf `fare.totalAmount` erstellen, wie unten gezeigt.

```
db.rides.createIndex( {"fare.totalAmount": 1}, {background: true} )
```

> **Note**
>
> Indizes, die im Vordergrund erstellt werden (d. h. wenn die Option `{background:true}` beim Erstellen des Index nicht angegeben wurde), erhalten eine exklusive Schreibsperre, die Anwendungen daran hindert, Daten so lange in die Sammlung zu schreiben, bis der Indexaufbau abgeschlossen ist. Beachten Sie diese mögliche Auswirkung beim Erstellen von Indizes für Produktions-Cluster. Beim Erstellen von Indizes empfehlen wir die Einstellung `{background:true}`.

Im Allgemeinen möchten Sie Indizes für Felder mit hoher Kardinalität erstellen (z. B. eine große Anzahl eindeutiger Werte). Das Erstellen eines Index für ein Feld mit geringer Kardinalität kann zu einem großen Index führen, der nicht verwendet wird. Der Amazon DocumentDB DocumentDB-Abfrageoptimierer berücksichtigt bei der Erstellung eines Abfrageplans die Gesamtgröße der Sammlung und die Selektivität der Indizes. Manchmal wird der Abfrageprozessor einen `COLLSCAN` auswählen, selbst wenn ein Index vorhanden ist. Dies geschieht, wenn der Abfrageprozessor schätzt, dass die Verwendung des Index keinen Leistungsvorteil gegenüber dem Scannen der gesamten Sammlung bringt. Wenn Sie den Abfrageprozessor zwingen möchten, einen bestimmten Index zu verwenden, können Sie den `hint()`-Operator wie unten gezeigt verwenden.

```
db.collection.find().hint("indexName")
```

Wie stelle ich fest, dass die Datenbanksammlung überlastet ist?

Eine Aufblähung von Sammlungen tritt auf, wenn die Größe einer Sammlung aufgrund der Anhäufung toter oder veralteter Dokumente oder der Fragmentierung innerhalb von Datenbankseiten zunimmt. Der angegebene Prozentsatz entspricht der Menge an Dokumentenspeicher, die von future Dokumenten verwendet werden kann. Diese Aufblähung beansprucht Speicherplatz sowohl im Puffercache als auch im Speicher. Um diese Aufblähung zu beseitigen, müssen Sammlungen während eines Wartungsfensters dump/restore entweder über einen Migrations-Loopback und einen Switchover neu geladen werden.

Example Beispiel

Führen Sie den folgenden Befehl aus, um den ungenutzten Speicherplatz für Ihre Sammlung zu ermitteln:

```
db.runCommand({collStats:'coll'})
```

Das Ergebnis sieht in etwa so aus:

```
{
        "ns" : "test.coll",
        "count" : 7500,
        "size" : 23250,
        "avgObjSize" : 31,
        "storageSize" : 106496,
        "unusedStorageSize" : {
                "unusedBytes" : 16384,
                "unusedPercent" : 25.12
        },
        "compression" : {
                "enable" : false
        },
        "capped" : false,
        "nindexes" : 1,
        "totalIndexSize" : 57344,
        "indexSizes" : {
                "_id_" : 57344
        },
        "collScans" : 4,
        "idxScans" : 10000,
        "opCounter" : {
                "numDocsIns" : 1000,
                "numDocsUpd" : 0,
                "numDocsDel" : 250
        },
        "cacheStats" : {
                "collBlksHit" : 3570,
                "collBlksRead" : 8,
                "collHitRatio" : 99.7765,
                "idxBlksHit" : 12293,
                "idxBlksRead" : 6,
                "idxHitRatio" : 99.9513
        },
        "lastReset" : "2024-12-18 00:30:21.552019+00",
        "ok" : 1,
        "operationTime" : Timestamp(1734632375, 1)
}
```

Zusammenfassung nützlicher Abfragen

Die folgenden Abfragen können für die Überwachung der Leistung und der Ressourcennutzung in Amazon DocumentDB nützlich sein.

- Verwenden Sie den folgenden Befehl, um Statistiken über eine bestimmte Sammlung anzuzeigen, einschließlich Betriebszähler, Cache-Statistiken, Zugriffsstatistiken und Größenstatistiken:

```
db.collection.stats()
```

- Verwenden Sie den folgenden Befehl, um Statistiken zu jedem Index anzuzeigen, der für eine Sammlung erstellt wurde, einschließlich der Größe des Indexes, indexspezifischer Cache-Statistiken und Statistiken zur Indexnutzung:

```
db.collection.aggregate([{$indexStats:{}}]).pretty()
```

- Verwenden Sie die folgende Abfrage, um alle Aktivitäten aufzulisten.

```
db.adminCommand({currentOp: 1, $all: 1});
```

- Der folgende Code listet alle langsamen oder blockierten Abfragen auf.

```
db.adminCommand({aggregate: 1,
                 pipeline: [{$currentOp: {}},
                            {$match: {$or: [{secs_running: {$gt: 10}},
                                            {WaitState: {$exists: true}}]}},
                            {$project: {_id:0,
                                        opid: 1,
                                        secs_running: 1,
                                        WaitState: 1,
                                        blockedOn: 1,
                                        command: 1}}],
                 cursor: {}
                });
```

- Der folgende Code beendet eine Abfrage.

```
db.adminCommand({killOp: 1, op: <opid of running or blocked query>});
```

- Verwenden Sie den folgenden Code, um eine aggregierte Ansicht des Systemstatus zu erhalten.

```
db.adminCommand({aggregate: 1,
                 pipeline: [{$currentOp: {allUsers: true, idleConnections: true}},
                            {$group: {_id: {desc: "$desc", ns: "$ns", WaitState:
 "$WaitState"}, count: {$sum: 1}}}],
                 cursor: {}
                });
```

Müllabfuhr in Amazon DocumentDB

Amazon DocumentDB implementiert eine MVCC-Datenbankarchitektur (Multi-Version Concurrency Control), die für jeden Aktualisierungsvorgang neue Versionen von Dokument- und Indexeinträgen erstellt. Diese Architektur ermöglicht die Isolierung von Transaktionen und verhindert so, dass die Änderungen einer Transaktion in einer anderen erscheinen.

Topics

- Grundlegendes zur Müllabfuhr in Amazon DocumentDB
- Prozess der Müllabfuhr
- Speicherarchitektur und erweiterter Speicher
- Überwachung der Müllabfuhr
- Beispiel für eine CollStats-Ausgabe
- Häufig gestellte Fragen

Grundlegendes zur Müllabfuhr in Amazon DocumentDB

Garbage Collection (GC) ist ein automatisierter Hintergrundprozess, der eine optimale Systemleistung und Verfügbarkeit in Amazon DocumentDB gewährleistet. Wie viele moderne Datenbanken erstellt auch die MVCC-Architektur von Amazon DocumentDB mit jeder Aktualisierung neue Dokument- und Indexversionen. Jeder Schreibvorgang verbraucht eine eindeutige MVCC-ID aus einem endlichen Zähler. Diese IDs identifizieren, zu welcher Transaktion eine Dokumentversion gehört und ob sie festgeschrieben oder zurückgesetzt wurde. Im Laufe der Zeit häufen sich diese alten Versionen und ihre MVCC-IDs an, sodass eine Bereinigung erforderlich ist, um Leistungseinbußen vorzubeugen.

Funktionen der Müllabfuhr

Der Müllsammler erfüllt drei wesentliche Funktionen:

- Gewinnt Speicherplatz zurück — Es entfernt veraltete Dokument- und Indexversionen, die für aktive Abfragen nicht mehr benötigt werden, und gibt so Speicherplatz für future Schreibvorgänge frei.
- Beugt einem MVCC-ID-Überlauf vor — Es verhindert einen MVCC-ID-Überlauf, indem der endliche Zähler der MVCC-IDs verwaltet wird. Ohne diese Verwaltung würde der Zähler irgendwann sein Limit erreichen und die Datenbank in einen temporären Nur-Lese-Modus zwingen, bis die IDs wiederverwendet werden.
- Beibehaltung der Abfrageleistung — Es sorgt für eine optimale Abfrageleistung, indem veraltete Dokumentversionen entfernt werden, die sich andernfalls ansammeln und die Abfrageverarbeitung verlangsamen würden.

Prozess der Müllabfuhr

Der GC-Prozess wird pro Sammlung ausgeführt und es können mehrere Prozesse gleichzeitig in verschiedenen Sammlungen ausgeführt werden. Der Prozess besteht aus vier aufeinanderfolgenden Phasen:

1. Identifizierung — Das System identifiziert Dokument- und Indexversionen, auf die in aktiven Transaktionen oder Abfragen nicht mehr verwiesen wird.
2. Laden des Speichers — Alte Dokumente und Indexeinträge werden in den Speicher geladen, sofern sie nicht bereits vorhanden sind.
3. Löschen — Veraltete Versionen werden dauerhaft gelöscht, um Speicherplatz zurückzugewinnen.
4. MVCC-ID-Recycling — Das System recycelt MVCC-IDs aus gelöschten Versionen für neue Operationen.

Wenn die Garbage-Collection die Verarbeitung alter Dokumentversionen abgeschlossen hat, werden die ältesten MVCC-IDs aus dem System entfernt. Diese Bereinigung ist entscheidend, um einen MVCC-ID-Überlauf zu verhindern, indem MVCC-IDs wiederverwendet werden, sodass sie für neue Schreibvorgänge im gesamten Cluster verfügbar sind. Ohne diesen Recyclingprozess würde das System irgendwann seinen begrenzten MVCC-ID-Zähler erschöpfen und in einen schreibgeschützten Zustand übergehen.

Planung der Müllabfuhr

Die Müllabfuhr wird in regelmäßigen Abständen automatisch im Hintergrund ausgeführt. Das Timing und die Frequenz passen sich dynamisch an die Systemlast, die verfügbaren Ressourcen, das Schreibvolumen und den MVCC-ID-Verbrauch an. Bei hoher Schreibaktivität wird der GC-Prozess häufiger ausgeführt, um die erhöhte Anzahl von Dokumentversionen zu bewältigen.

Speicherarchitektur und erweiterter Speicher

Amazon DocumentDB verwendet eine ausgeklügelte Speicherarchitektur, die den Dokumentenspeicher in zwei unterschiedliche Segmente unterteilt:

Basisspeichersegment

Das Basisspeichersegment enthält die primären Dokumentdaten und Metadaten. In diesem Segment wird Folgendes gespeichert:

- Dokumentinhalt, der in die Standardseitengröße (8 KB) passt.
- Metadaten und Strukturinformationen des Dokuments.
- Primärindizes und ihre Einträge.
- Collection-level Statistik und Konfiguration.

Erweitertes Speichersegment

Das erweiterte Speichersegment verwendet einen speziellen Objektspeicher für große Dokumente, der für die Verarbeitung von Dokumenten konzipiert ist, die die Standardspeicherseitengröße überschreiten. Dieses Segment bietet:

- Effizienter Umgang mit großen Dokumenten — Dokumente, die den Basisspeicherschwellenwert überschreiten, werden automatisch in das erweiterte Speichersegment verschoben.
- Optimiertes Speicherlayout — Das Segment verwendet ein anderes Speicherformat, das für große Objekte optimiert ist, wodurch die Fragmentierung reduziert und die Zugriffsmuster verbessert werden.
- Unabhängige Speicherbereinigung — Das erweiterte Speichersegment verfügt über einen eigenen Speicherbereinigungsprozess, der unabhängig von der Bereinigung des Basisspeichers ausgeführt werden kann.
- Transparenter Zugriff — Anwendungen greifen problemlos auf große Dokumente zu, ohne wissen zu müssen, welches Speichersegment die Daten enthält.

Das erweiterte Speichersegment ist besonders vorteilhaft für:

- Sammlungen mit Dokumenten, die große eingebettete Arrays enthalten.
- Dokumente mit umfangreichen verschachtelten Strukturen.
- Sammlungen, die Binärdaten oder große Textfelder speichern.
- Anwendungen mit gemischten Dokumentengrößen, bei denen einige Dokumente die durchschnittliche Größe deutlich überschreiten.

Überwachung der Müllabfuhr

Metriken auf Clusterebene

`AvailableMVCCIds`

- Standort — Amazon CloudWatch
- Beschreibung — Ein Zähler, der die Anzahl der verbleibenden Schreibvorgänge anzeigt, die ab einer Höchstgrenze von 1,8 Milliarden verfügbar sind. Wenn dieser Zähler Null erreicht, wechselt Ihr Cluster in den schreibgeschützten Modus, bis IDs zurückgewonnen und recycelt werden. Der Zähler nimmt mit jedem Schreibvorgang ab und steigt, wenn bei der Garbage-Collection alte MVCC-IDs wiederverwendet werden.
- Empfehlung — Stellen Sie einen Alarm ein, wenn der Wert unter 1,3 Milliarden fällt. Diese Frühwarnung ermöglicht es Ihnen, empfohlene Maßnahmen zu ergreifen, die später besprochen werden.

`LongestActiveGCRuntime`

- Standort — Amazon CloudWatch
- Beschreibung — Dauer des längsten aktiven Müllsammelvorgangs in Sekunden. Wird jede Minute aktualisiert und verfolgt nur aktive Vorgänge, ausgenommen Prozesse, die innerhalb des Zeitfensters von einer Minute abgeschlossen werden.
- Empfehlung: Vergleichen Sie mit `gcRuntimeStats` historischen Daten, um ungewöhnliches Verhalten bei der Speicherbereinigung zu ermitteln, z. B. längere Laufzeiten bei Massenlöschungen.

Kennzahlen auf Erfassungsebene

`MVCCIDStats: MVCCIdScale`

- Standort — Datenbankbefehl CollStats
- Beschreibung — Misst das Alter der MVCC-ID auf einer Skala von 0 bis 1, wobei 1 das maximale Alter angibt, bevor ein Cluster in den schreibgeschützten Zustand übergeht. Verwenden Sie diese Metrik zusammen`AvailableMVCCIds`, um Sammlungen zu identifizieren, die die ältesten MVCC-IDs enthalten, die den Cluster altern lassen.
- Empfehlung — Behalten Sie für jede Sammlung Werte unter 0,3 bei.

`gcRuntimeStats`

- Standort — Datenbankbefehl CollStats
- Beschreibung — Stellt eine zweimonatige Historie von Messdaten zur Garbage-Collection bereit, einschließlich der Gesamtzahl der Durchläufe, der durchschnittlichen Dauer und der Höchstdauer. Schließt nur Müllabfuhr ein, die länger als fünf Minuten dauern, um aussagekräftige Statistiken zu gewährleisten.

`storageSizeStats`

- Standort — Datenbankbefehl CollStats
- Beschreibung — Bietet eine detaillierte Aufschlüsselung der Speichernutzung in verschiedenen Speichersegmenten:
  - `storageSegmentBase`— Speicher, der vom Basisspeichersegment für Standarddokumente verwendet wird
  - `storageSegmentExtended`— Speicher, der vom erweiterten Speichersegment für große Dokumente verwendet wird
- Nutzung — Hilft bei der Identifizierung von Sammlungen mit sehr großem Dokumentenbestand und hilft dabei, die Speicherverteilungsmuster zu verstehen.

`unusedStorageSize`(Sammlungsebene)

- Standort — Datenbankbefehl CollStats

- Beschreibung — Schätzt den ungenutzten Speicherplatz in einer Sammlung auf der Grundlage von Stichprobenstatistiken. Es umfasst Speicherplatz aus gelöschten Dokumenten und leeren Segmenten. Die Metrik bietet sowohl kombinierte Gesamtwerte als auch Aufschlüsselungen pro Segment:
  - Kombiniert `unusedBytes` und für `unusedPercent` alle Speichersegmente
  - `storageSegmentBase`— Ungenutzter Speicherplatz speziell im Basisspeichersegment
  - `storageSegmentExtended`— Ungenutzter Speicherplatz speziell im erweiterten Speichersegment

`documentFragmentStats`

- Standort — Datenbankbefehl CollStats
- Beschreibung — Stellt detaillierte Informationen über Dokumentfragmente und tote Daten in Sammlungen bereit. Dokumentfragmente stellen die internen Speichereinheiten dar, die von der Datenbank-Engine verwendet werden, und tote Fragmente weisen auf Daten hin, auf die nicht mehr zugegriffen werden kann, die aber noch nicht zurückgewonnen wurden. Diese Metrik beinhaltet:
  - `totalDocFragmentsCount`— Gesamtzahl der Dokumentfragmente in der Sammlung
  - `deadDocFragmentsCount`— Anzahl der Fragmente, die tote (unzugängliche) Daten enthalten
  - `deadDocFragmentsPercent`— Prozentsatz der Fragmente, die tote Daten enthalten
  - `deadDocFragmentBytes`— Geschätzter Byteverbrauch durch tote Dokumentfragmente
  - Per-segment Aufschlüsselung für `storageSegmentBase` und `storageSegmentExtended`
- Nutzung — Überwachen Sie diese Kennzahl, um sich ein Bild von der Effektivität der Müllabfuhr zu machen und um Sammlungen zu identifizieren, die von Wartungsarbeiten profitieren könnten. Ein hoher Prozentsatz an toten Fragmenten deutet darauf hin, dass die Müllabfuhr möglicherweise ins Hintertreffen gerät oder dass die Sammlung von Optimierungen profitieren würde.

Metriken auf Indexebene

`unusedStorageSize`(Indexebene)

- Standort — Befehl IndexStats für die Datenbank

- Beschreibung — Schätzt den ungenutzten Speicherplatz in einem Index auf der Grundlage von Stichprobenstatistiken. Es beinhaltet Speicherplatz aus veralteten Indexeinträgen und leeren Segmenten.
- Empfehlung — Verwenden Sie den `reIndex` Befehl, um Indizes ohne Ausfallzeiten neu zu erstellen und ungenutzten Speicherplatz zurückzugewinnen. Weitere Informationen finden Sie unter Indizes verwalten.

Beispiel für eine CollStats-Ausgabe

Das folgende Beispiel zeigt eine typische `collStats` Ausgabe mit Metriken zur Garbage-Collection und Speicherung:

```
{
    "ns" : "Mvcc_consumption_test_db.mvcc_test_collection",
    "MVCCIdStats" : {
        "MVCCIdScale" : 0.03
    },
    "gcRuntimeStats" : {
        "numRuns" : 1,
        "historicalAvgRuntime" : 3295,
        "historicalMaxRuntime" : 3295,
        "lastRuntime" : 3295,
        "lastRuntimeStart" : ISODate("2025-06-24T08:47:14Z")
    },
    "documentFragmentStats" : {
        "totalDocFragmentsCount" : 45000000,
        "deadDocFragmentsCount" : 2250000,
        "deadDocFragmentsPercent" : 5.0,
        "deadDocFragmentBytes" : 98304000,
        "storageSegmentBase" : {
            "totalDocFragmentsCount" : 30000000,
            "deadDocFragmentsCount" : 1500000,
            "deadDocFragmentsPercent" : 5.0,
            "deadDocFragmentBytes" : 65536000
        },
        "storageSegmentExtended" : {
            "totalDocFragmentsCount" : 15000000,
            "deadDocFragmentsCount" : 750000,
            "deadDocFragmentsPercent" : 5.0,
            "deadDocFragmentBytes" : 32768000
        }
```

```
    },
    "collScans" : 14,
    "count" : 30000000,
    "size" : 1320000000,
    "avgObjSize" : 44,
    "storageSize" : 6461497344,
    "storageSizeStats" : {
        "storageSegmentBase" : 4307664896,
        "storageSegmentExtended" : 2153832448
    },
    "capped" : false,
    "nindexes" : 2,
    "totalIndexSize" : 9649553408,
    "indexSizes" : {
        "_id_" : 1910661120,
        "c_1" : 7738892288
    },
    "unusedStorageSize" : {
        "unusedBytes" : 4201881600,
        "unusedPercent" : 65.05,
        "storageSegmentBase" : {
            "unusedBytes" : 2801254400,
            "unusedPercent" : 65.05
        },
        "storageSegmentExtended" : {
            "unusedBytes" : 1400627200,
            "unusedPercent" : 65.05
        }
    },
    "cacheStats" : {
        "collBlksHit" : 171659016,
        "collBlksRead" : 754061,
        "collHitRatio" : 99.5627,
        "idxBlksHit" : 692563636,
        "idxBlksRead" : 1177921,
        "idxHitRatio" : 99.8303
    },
    "idxScans" : 41823984,
    "opCounter" : {
        "numDocsIns" : 0,
        "numDocsUpd" : 20911992,
        "numDocsDel" : 0
    },
    "lastReset" : "2025-06-24 05:57:08.219711+00",
```

```
    "ok" : 1,
    "operationTime" : Timestamp(1750968826, 1)
}
```

Häufig gestellte Fragen

Wie erkenne ich, ob die Müllabfuhr nicht effizient funktioniert?

Achten Sie auf diese Warnzeichen, die auf eine ineffiziente Müllabfuhr hinweisen:

- Übermäßiges Aufblähen von Datensammlungen — Stetig steigende `unusedStorageSize` Messwerte bei umfangreichen Schreibvorgängen oder Massenlöschungen, insbesondere bei großen Indizes.
- Hoher Prozentsatz an toten Fragmenten — `documentFragmentStats` zeigt konstant hohe `deadDocFragmentsPercent` Werte (über 10-15%).
- Verminderte Abfragelatenz — Erhöhte Abfragelatenz aufgrund der Anhäufung toter Dokumente.
- Verlängerte GC-Dauer — Die Müllabfuhr dauert länger als der historische Durchschnitt in`gcRuntimeStats`.
- Erhöhte GC-Verarbeitung — Hoch `LongestActiveGCRuntime` bedeutet, dass der Garbage Collector nicht mit den Systemanforderungen Schritt halten kann.

Beeinträchtigt die Garbage-Collection die Leistung meiner Datenbank?

Unter normalen Bedingungen hat die Garbage-Collection nur minimale Auswirkungen auf die Leistung. Wenn die Müllabfuhr jedoch ins Hintertreffen gerät, kann es zu folgenden Problemen kommen:

- Erhöhte Speicherkosten aufgrund angesammelter toter Dokumente.
- Langsamere Abfrageleistung aufgrund veralteter Indexeinträge.
- Temporärer Nur-Lese-Modus, wenn die MVCC-IDs aufgebraucht sind.
- Höherer Ressourcenverbrauch bei intensiven Erfassungsläufen, insbesondere bei kleineren Instanzen.
- Geringere Effizienz bei Operationen mit erweiterten Speichersegmenten für große Dokumente.

Kann ich die Müllabfuhr manuell auslösen?

Nein, die Garbage-Collection in Amazon DocumentDB kann nicht manuell ausgelöst werden. Das System verwaltet die Müllabfuhr im Rahmen seiner internen Wartungsarbeiten automatisch.

Welche Alarme sollte ich als bewährte Methode für den Betrieb einrichten?

Wir empfehlen, die Überwachung sowohl auf Cluster- als auch auf Sammlungsebene einzurichten, um eine optimale Leistung Ihres Amazon DocumentDB-Systems sicherzustellen.

Für die Überwachung auf Clusterebene erstellen Sie zunächst einen CloudWatch Amazon-Alarm für die `AvailableMVCCIds` Metrik mit einem Schwellenwert von 1,3 Milliarden. Auf diese Weise haben Sie ausreichend Zeit, um Maßnahmen zu ergreifen, bevor die Metrik Null erreicht. Ab diesem Zeitpunkt würde Ihr Cluster in den schreibgeschützten Modus wechseln. Denken Sie daran, dass diese Kennzahl je nach Ihren spezifischen Nutzungsmustern schwanken kann. Manche Kunden gehen davon aus, dass sie unter 1,3 Milliarden fällt und sich dann wieder auf über 1,5 Milliarden erholt, sobald die Garbage-Collection ihre Arbeit abgeschlossen hat.

Es ist auch wichtig, die `LongestActiveGCRuntime` Metrik über Amazon zu überwachen CloudWatch. Diese Metrik hilft Ihnen`gcRuntimeStats`, zu verstehen, wie effizient die Speicherbereinigung in Ihrem gesamten System funktioniert.

Konzentrieren Sie sich bei der Überwachung auf Sammlungsebene auf die folgenden wichtigen Kennzahlen:

- `MVCCIdScale`— Achten Sie auf steigende Werte, die darauf hindeuten, dass MVCC-IDs veralten und möglicherweise überarbeitet werden müssen.
- `gcRuntimeStats`— Identifizieren Sie Prozesse zur Müllabfuhr, die ungewöhnlich lange dauern oder sich über mehrere Tage erstrecken.
- `documentFragmentStats`— `deadDocFragmentsPercent` Werte überwachen — konstant hohe Prozentsätze (über 10-15%) können darauf hindeuten, dass die Müllabfuhr hinterherhinkt.
- `storageSizeStats`und `unusedStorageSize` — Verfolgen Sie die Muster der Speichernutzung und identifizieren Sie Sammlungen mit erheblichem ungenutztem Speicherplatz in beiden Speichersegmenten.

Sammlungen mit häufigen Schreibvorgängen erfordern besondere Aufmerksamkeit, da sie mehr Arbeit für den Garbage-Collector bedeuten. Wir empfehlen, diese Metriken bei Sammlungen mit

starker Schreibaktivität häufiger zu überprüfen, um sicherzustellen, dass die Garbage-Collection mit Ihrer Arbeitslast Schritt hält.

Beachten Sie, dass diese Überwachungsempfehlungen als Ausgangspunkt dienen. Wenn Sie mit dem Verhalten Ihres Systems besser vertraut sind, sollten Sie diese Schwellenwerte möglicherweise anpassen, um sie besser an Ihre spezifischen Nutzungsmuster und Anforderungen anzupassen.

Was sollte ich tun, wenn meine **`verfügbaren MVCCIDs`** unter 1,3 Milliarden fallen?

Wenn Ihre `AvailableMVCCIds` Metrik unter 1,3 Milliarden fällt, empfehlen wir, sofort Maßnahmen zu ergreifen, um zu verhindern, dass Ihr Cluster in den schreibgeschützten Modus wechselt. Wir empfehlen, zunächst Ihre Instance-Größe zu vergrößern, um dem Garbage Collector mehr Rechenressourcen zur Verfügung zu stellen. Dies ist unsere wichtigste Empfehlung, da es Ihrer Anwendung ermöglicht, den normalen Betrieb fortzusetzen und gleichzeitig dem Garbage Collector die zusätzliche Leistung zu geben, die er zum Aufholen benötigt.

Wenn eine Skalierung allein die Situation nicht verbessert, empfehlen wir, eine Reduzierung Ihrer Schreibvorgänge in Betracht zu ziehen. Identifizieren Sie anhand der `MVCCIdScale` Metrik, welche spezifischen Sammlungen ältere MVCC-IDs enthalten, die Ihrer Aufmerksamkeit bedürfen. Überwachen Sie außerdem Sammlungen mit einem hohen Prozentsatz `documentFragmentStats` an toten Fragmenten, die möglicherweise zur Ineffizienz der Müllsammlung beitragen.

Sobald Sie diese Sammlungen identifiziert haben, müssen Sie möglicherweise vorübergehend die Schreibvorgänge auf sie reduzieren, damit die Garbage-Collection aufholen kann. Während der Erholungsphase empfehlen wir, die `AvailableMVCCIds` Metrik genau zu beobachten, um sicherzustellen, dass Ihre Maßnahmen die gewünschte Wirkung haben. Ihr Cluster gilt als fehlerfrei, sobald der `AvailableMVCCIds` Wert wieder 1,5 Milliarden oder höher erreicht.

Denken Sie daran, dass es sich bei diesen Schritten um vorbeugende Maßnahmen handelt, mit denen Ihr System wiederhergestellt werden kann, bevor es einen kritischen Zustand erreicht. Je früher Sie Maßnahmen ergreifen, nachdem der Wert unter 1,3 Milliarden gesunken ist, desto wahrscheinlicher ist es, dass Sie jegliche Auswirkungen auf Ihre Schreibvorgänge vermeiden.

Versionshinweise

In diesen Versionshinweisen werden die Funktionen, Verbesserungen und Bugfixes von Amazon DocumentDB beschrieben, geordnet nach Hauptversionen der Engine. In jedem Versionsabschnitt sind die Einträge nach Datum in einem Tabellenformat aufgelistet.

Einzelheiten zur Nummerierung von Engine-Versionen und Patch-Versionen (einschließlich der Zuordnung zwischen Engine-Patch-Versionspräfixen und Amazon DocumentDB DocumentDB-Engine-Versionen) finden Sie unter. Nummerierung der Engine-Versionen

Sie können die aktuelle Patch-Version der Amazon DocumentDB DocumentDB-Engine ermitteln, indem Sie den folgenden Befehl ausführen:

```
db.runCommand({getEngineVersion: 1})
```

Wenn Ihr Cluster nicht auf der neuesten Version der Engine installiert ist, ist es wahrscheinlich, dass noch Wartungsarbeiten verfügbar sind, die Ihre Engine aktualisieren werden. Weitere Informationen finden Sie Wartung von Amazon DocumentDB im Entwicklerhandbuch.

Themen

- Versionshinweise zur Amazon DocumentDB DocumentDB-Engine
- Allgemeine Versionshinweise zu Amazon DocumentDB
- Versionshinweise zu Amazon DocumentDB Elastic Clusters

Versionshinweise zur Amazon DocumentDB DocumentDB-Engine

Versionshinweise für Amazon DocumentDB DocumentDB-Engine-Versionen, geordnet nach Hauptversionen.

Amazon DocumentDB 8.0

Versionshinweise für die Amazon DocumentDB DocumentDB-Engine Version 8.0 (MongoDB 8.0-Kompatibilität).

Date	Versionshinweise
13. Mai 2026	Neues Feature

Date	Versionshinweise
	Amazon DocumentDB serverless ist jetzt für Amazon DocumentDB 8.0 verfügbar. Weitere Informationen finden Sie unter Serverloses Verwenden von Amazon DocumentDB.
6. Mai 2026	Fehlerkorrekturen und andere Änderungen Amazon DocumentDB 8.0 (Modulversion: 4.0.6940) Dieses Update bietet einen optionalen Engine-Patch mit den folgenden Verbesserungen: 1. Es wurde ein Fehler bei der Speicherbereinigung behoben, der in Ausnahmefällen zum Absturz von Lesegeräten führen konnte.
20. April 2026	Neues Feature In-place Ein Major Version Upgrade (MVU) von Amazon DocumentDB 5.0 auf Amazon DocumentDB 8.0 ist jetzt verfügbar. Weitere Informationen finden Sie unter Direktes Upgrade der Hauptversion von Amazon DocumentDB.

Date	Versionshinweise
20. April 2026	Neue Features und Verbesserungen Amazon DocumentDB 8.0 (Engine-Versionen: 4.0.5995, 4.0.6473) Dies ist ein erforderlicher Engine-Patch, der die folgenden neuen Funktionen, Verbesserungen und Korrekturen enthält: 1. `$sortArray` Betreiber in`$project`: • Support für `$sortArray` Operator in der `$project` Phase der Aggregationspipeline für Planner Version 3. Der `$sortArray` Operator sortiert ein Array anhand seiner Elemente (für Skalarwerte) oder eines bestimmten Felds (für Dokumentarrays) und gibt das sortierte Array in aufsteigender (1) oder absteigender () Reihenfolge zurück. `-1` 2. Support für parallel ungeordnete Massenupdates in`bulkWrite()` . 3. Support für`$out`,`$collStats` ,`$indexStats` , `$geoNear` mit Planner v3. Mit Planner V3 unterstützt die `$out` Stage auch das Schreiben in Sammlungen in verschiedenen Datenbanken. 4. Die Aggregationspipeline wird jetzt zusammengeführt `$lookup` und `$unwind` schrittweise ausgeführt, auch wenn die `$unwind` Phase den Parameter enthält. `includeArrayIndex` Bisher wurde diese Optimierung übersprungen, wenn sie vorhanden war. `includeArrayIndex` 5. Leistungsverbesserungen zur Verbesserung des Schreibdurchsatzes für db.r8g.8xlarge- und größere Instances, die auf Konfiguration ausgeführt werden. I/O-Optimized 6. Bereitstellung von Metriken zur Überwachung von Instances. `Connections (active)` Die Beschränkungen finden Sie auf unserer Amazon DocumentDB-Seite Kontingente und Beschränkungen. 7. Verbesserte regionsübergreifende Resilienz von globalen Clustern durch Eliminierung des sekundären Clusters mit Global Survivable Read Only.

Date	Versionshinweise
	8. Support für `$dateToParts` und `$dateFromParts` Aggregationsoperatoren. 9. Command-level Leistungskennzahlen sind jetzt CloudWatch für CRUD-Operationen (`find`,,`insert`,`findAndModify` ,`update`,,`delete`, `aggregate` `count`,`commitTransaction`) `distinct` `getMoreabortTransaction` , Exposing `AvgDuration` und `MaxConcurrent` Dimensionen für eine verbesserte Betriebsüberwachung verfügbar. `P100Duration` 10. Es wurde ein `$replaceRoot` Verhaltensfehler behoben, bei dem `newRoot` Felder, die boolesche Werte von`true`/`false`oder numerische Werte von`0`/enthielten, im `1` Ausgabedokument fehlten. 11. Es wurde ein Fehler behoben`$indexOfArray` , bei dem gültige Abfragen Fehler zurückgaben, die darauf hinwiesen, dass sie ungültig waren. 12. Der Explain-Plan enthält jetzt `docsExamined` Metriken in der `executionStats` Ausgabe. 13. Die Leistung der SASL-Authentifizierung wurde verbessert. 14. Optimierte Dokumentaktualisierungen zur Reduzierung des Speicheraufwands, wenn die Indexwerte unverändert bleiben und Dokumente in bestehende Seiten passen. 15. Support für `bypassDocumentValidation` in`$merge`. Alle Amazon DocumentDB 8.0-Cluster werden während ihres nächsten Wartungsfensters automatisch auf diese Patch-Version aktualisiert.

Date	Versionshinweise
26. März 2026	Neue Features Amazon DocumentDB unterstützt jetzt die neueste Generation von speicheroptimierten Instances, db.r8g, die auf Arm-based AWS Graviton4-Prozessoren basieren und eine um bis zu 30% bessere Leistung als R6G-Instances bieten. Weitere Informationen finden Sie in diesem Handbuch Instanzklassen verwalten

Date	Versionshinweise
11. November 2025	Neue Features Amazon DocumentDB bietet jetzt volle Wire-Protokoll-Kompatibilität mit MongoDB 8.0. Amazon DocumentDB 8.0 verbessert die Abfragele istung, sodass Sie Hochleistungsanwendungen zu geringeren Kosten erstellen können. Amazon DocumentDB 8.0 (Engine-Patch-Version 4.0.4448) • Unterstützung für MongoDB 8.0 API-Treiber hinzugefügt. • Es wurde Unterstützung für Planner Version 3 hinzugefügt, die Leistungsverbesserungen auf Operatoren in der Aggregationsphase ausdehnt und außerdem Optimierungen der Aggregationspipeline und verschiedene Befehle unterstützt. • Support für wörterbuchbasierte Komprimierung durch den Zstandard -Komprimierungsalgorithmus hinzugefügt, wodurch die Komprimie rungsrate um das Fünffache verbessert wurde. • Neue Funktionen hinzugefügt: Amazon DocumentDB 8.0 unterstützt Sortierung und Ansichten. • Unterstützung für neue Aggregationsstufen und Operatoren hinzugefügt: $replaceWith, $vectorSearch, $merge, $set, $unset, $bucket und die 3 neuen Aggregationsoperatoren $pow, $rand, $DateTrunc. • Unterstützung für eine neue Version des Textindexes hinzugefü gt: Der Textindex v2 in Amazon DocumentDB 8.0 führt zusätzliche Token ein und verbessert so die Textsuchfunktionen. • Beinhaltet Verbesserungen bei der Vektorsuche durch parallel Vektorindexerstellung, wodurch die Indexerstellungszeit um das bis zu 30-fache reduziert wird. • Die Unterstützung für TLS 1.0 und TLS 1.1 wurde entfernt. Die TLS-Mindestversion ist jetzt TLS 1.2.

Amazon DocumentDB 5.0

Versionshinweise für die Amazon DocumentDB DocumentDB-Engine Version 5.0 (MongoDB 5.0-Kompatibilität).

Date	Unterversion	Versionshinweise
8. Juni 2026	5.0.1	Neue Nebenversion Amazon DocumentDB 5.0.1 (Modulversion 3.0.21138) Amazon DocumentDB 5.0.1 ist die erste Nebenversion für die Amazon DocumentDB 5.0-Hauptversion. Nebenversionen enthalten Verbesserungen wie neue Funktionen, Sicherheitskorrekturen und Fehlerkorrekturen. Sie können mit einem kleineren Versionsupgrade von 5.0.0 auf 5.0.1 aktualisieren. Weitere Informationen finden Sie unter Upgrade der Nebenversion von Amazon DocumentDB. Diese Nebenversion enthält die folgenden neuen Funktionen und Verbesserungen: 1. Die Metriken auf Sammelebene wurden hinzugefügt `gcRuntimeStats` `documentFragmentStats` , `collstats` um mehr Informationen über den Gesamtstatus des Müllsammelprozesses zu erhalten. `storageSegmentBase` `storageSegmentExtended` Details dazu finden Sie unter Müllabfuhr in Amazon DocumentDB. 2. Support für `$rand` und `$pow` Aggregationsoperatoren. 3. Bereitstellung von Metriken `Connections (active)` zur Überwachung von Instances. Die Beschränkungen finden Sie auf unserer Amazon DocumentDB-Seite Kontingente und Beschränkungen.

Date	Unterversion	Versionshinweise
		4. Support für `$dateToParts` und `$dateFromParts` Aggregationsoperatoren. 5. Command-level Leistungskennzahlen sind jetzt CloudWatch für CRUD-Operationen (`find`,,`insert`,`findAndModify` ,`update`,,`delete`, `aggregate` `count`,`commitTransaction`) `distinct` `getMoreabortTransaction` , Exposing `AvgDuration` und `MaxConcurrent` Dimensionen für eine verbesserte Betriebsüberwachung verfügbar. `P100Duration`
6. Mai 2026	5.0.0	Fehlerkorrekturen und andere Änderungen Amazon DocumentDB 5.0 (Modulversion: 3.0.20421) Diese Version ist für einen erforderlichen Sicherheitspatch vorgesehen.
20. April 2026	5.0.0	Neues Feature In-place Ein Major Version Upgrade (MVU) von Amazon DocumentDB 5.0 auf Amazon DocumentDB 8.0 ist jetzt verfügbar. Weitere Informationen finden Sie unter Direktes Upgrade der Hauptversion von Amazon DocumentDB.

Date	Unterversion	Versionshinweise
13. April 2026	5.0.0	Fehlerkorrekturen und andere Änderungen Amazon DocumentDB 5.0 (Engine-Versionen: 3.0.19917) Dies ist ein erforderlicher Engine-Patch, der die folgenden neuen Funktionen, Verbesserungen und Korrekturen enthält: 1. Es wurde eine DatabaseConnectionsActiveMax Metrik hinzugefügt, die Einblicke in die „Verbindungen (aktiv)“ für Instances bietet. Die Beschränkungen finden Sie auf unserer Amazon DocumentDB-Seite Kontingente und Beschränkungen. 2. Die Leistung der SASL-Authentifizierung wurde verbessert. Alle Amazon DocumentDB 5.0-Cluster werden während ihres nächsten Wartungsfensters automatisch auf diese Patch-Version aktualisiert.

Date	Unterversion	Versionshinweise
22. Oktober 2025	5.0.0	Neue Features Amazon DocumentDB 5.0 (Engine-Patch-Version 3.0.17983) Amazon DocumentDB unterstützt jetzt die neueste Generation von speicheroptimierten Instances, db.r8g, die auf Arm-based AWS Graviton4-Prozessoren basieren und eine um bis zu 30% bessere Leistung als R6G-Instances bieten. Weitere Informationen finden Sie in diesem Handbuch und in diesem Blogbeitrag. Instanzklassen verwalten Neue Features Amazon DocumentDB 5.0 (Engine-Patch-Version 3.0.15902) • Unterstützung für längere Sammlungsnamen hinzugefügt (Namespace-Länge bis zu 255 Zeichen). • Es wurde ein neuer Abfrageplaner eingeführt (Planner Version 2.0). Weitere Informationen finden Sie unter Abfrageplaner v2 in diesem Handbuch. • Es wurden neue Felder `collstats` für „mvccidStats“ und „gcRuntimeStats“ hinzugefügt, die Informationen über den allgemeinen Zustand der Sammlung in Bezug auf Müllabfuhr und veraltete Sammlungen liefern.

Date	Unterversion	Versionshinweise
16. Oktober 2025	5.0.0	Neues Feature Amazon DocumentDB 5.0 (Engine-Patch-Version 3.0.15902) Amazon DocumentDB unterstützt jetzt den Dual-Stack-Modus (IPv4/IPv6), wenn sich Ihr Cluster in einer Virtual Private Cloud (VPC) befindet. Weitere Informationen finden Sie in diesem Blogbeitrag und Amazon VPC und Amazon DocumentDB im Amazon DocumentDB Developer Guide.
15. September 2025	5.0.0	Fehlerkorrekturen und andere Änderungen Amazon DocumentDB 5.0 (Engine-Patch-Version 3.0.17983) Engine-Absturz behoben, wenn Abfragen eine nachfolgende und eine Phase enthielten. `$replaceRoot $lookup`

Date	Unterversion	Versionshinweise
29. Juli 2025	5.0.0	Neue Features Amazon DocumentDB 5.0 (Engine-Patch-Version 3.0.15902) • Unterstützung für den Aggregationsoperator hinzugefügt. `$regexFindAll` • Index-Bloat und sammlungsbasierte Bloat-Metriken wurden eingeführt • Es wurden CloudWatch `AvailableMVCCIds` Metriken hinzugefügt`LongestActiveGCRun time` , die Informationen über den allgemeinen Zustand des Clusters in Bezug auf Müllsammlung und veraltete Sammlungen liefern. • Der `serverStatus` Befehl enthält jetzt ein Feld „nvme_cache“, das die Anzahl der Seiten anzeigt, die auf Instanzen in den NVMe-Cache geschrieben und nicht geschrieben wurden. NVMe-backed • Die Beschränkung der Anzahl der Felder für und wurde aufgehoben `$group` `$project` • Support für die folgenden Zeichenkettenopera toren: `$trim`,`$rtrim`,`$ltrim`,`$regexFin dAll` ,`$replaceOne` , und `$replaceAll` • Support für die folgenden Array-Operatoren: `$first` und `$last` • Support für den folgenden Stage-Operator: `$collStats` Fehlerkorrekturen und andere Änderungen Amazon DocumentDB 5.0 (Engine-Patch-Version 3.0.15902)

Date	Unterversion	Versionshinweise
		Es wurde ein Problem bei der Indexerstellung behoben, das große Sammlungen betraf.
28. Juli 2025	5.0.0	Neue Features Amazon DocumentDB 5.0 (Engine-Patch-Version 3.0.14228) Instanzbasierte Amazon DocumentDB-Cluster unterstützen jetzt Amazon DocumentDB Serverless, eine On-Demand-Konfiguration mit auto-scaling. Weitere Informationen finden Sie unter Serverloses Verwenden von Amazon DocumentDB und in diesem Blogbeitrag „Was ist neu“.
24. März 2025	5.0.0	Neues Feature Amazon DocumentDB 5.0 (Engine-Patch-Version 3.0.11800) Unterstützung für `postBatchResumeToken` In-Change-Streams hinzugefügt. Weitere Informationen finden Sie unter `Wiederaufnahme eines Change-Streams mit PostBatchResumeToken`.

Date	Unterversion	Versionshinweise
15. Januar 2025	5.0.0	Neue Features Amazon DocumentDB 5.0 (Engine-Patch-Version 3.0.11800) Amazon DocumentDB behält jetzt die Leseverfü gbarkeit auch bei Neustarts der Writer-Instance bei. Reader-Instances bearbeiten nun weiterhin Leseanfra gen bei Neustarts der Writer-Instance. Fehlerkorrekturen und andere Änderungen Amazon DocumentDB 5.0 (Engine-Patch-Version 3.0.11800) • Der `killOp` Befehl zur Behandlung eines Sonderfal ls von Masseneinfügungen wurde korrigiert. • Verbesserte I/O-related Netzwerkspeichernutzung auf Amazon DocumentDB DocumentDB-Instances. • Der `count` Befehl für `$text` Filterabfragen wurde korrigiert.
18. Dezember 202	5.0.0	Neue Features Amazon DocumentDB 5.0 (Engine-Patch-Version 3.0.5721) Instanzbasierte Amazon DocumentDB DocumentDB-Cluster unterstützen NVMe-backed jetzt R6GD-Inst ances. Weitere Informationen finden Sie unter „Was ist neu“ NVMe-backed Instanzen -Blogbeitrag.

Date	Unterversion	Versionshinweise
6. November 2024	5.0.0	Neue Features Amazon DocumentDB 5.0 (Engine-Patch-Version 3.0.11051) • Unterstützung für minimale TLS-Versionen `tls1.2+` und `tls1.3+` Cluster-Parameter hinzugefügt. `tls` • Unterstützung für die Zeichen Dollar ($) und Punkt (.) in Feldnamen aktiviert. Informationen zu funktionalen Unterschieden finden Sie unterDollar ($) und Punkt (.) in Feldnamen.

Date	Unterversion	Versionshinweise
17. September 2024	5.0.0	Neue Features Amazon DocumentDB 5.0 (Engine-Patch-Version 3.0.10696) Amazon DocumentDB unterstützt jetzt das Neuerstellen von Indizes mit `reIndex` in. `runCommand` Weitere Informationen finden Sie unter Indexverwaltung mit `ReIndex`. **Note** `reIndex`wird nur auf Amazon DocumentDB 5.0 (Engine Patch Version 3.0.10696 und höher) unterstützt. Fehlerkorrekturen und andere Änderungen Amazon DocumentDB 5.0 (Engine-Patch-Version 3.0.10696) • `$setOnInsert` unterstützt das `_id` Feld jetzt bei Einfügungen, die aus Aktualisierungsvorgängen resultieren. • Es wurde ein Problem behoben, das die Rückgewinnung von Speicherplatz nach einem Upgrade der Hauptversion auf Amazon DocumentDB 5.0 verhindert.

Date	Unterversion	Versionshinweise
22. August 2024	5.0.0	Neues Feature Amazon DocumentDB 5.0 (Alle Engine-Patch-Versionen) Globale Amazon DocumentDB-Cluster unterstützen jetzt Cluster-Switchover und verwaltete Cluster-Failover. Weitere Informationen erhalten Sie unter Durchführen eines Switchovers für einen globalen Amazon DocumentDB-Cluster und Durchführen eines verwalteten Failovers für einen globalen Amazon DocumentDB-Cluster. **Note** Globale Cluster-Switchover und -Failover werden nur auf Amazon DocumentDB 4.0 und 5.0 unterstützt.

<table>
<tr><th>Date</th><th>Unterversion</th><th>Versionshinweise</th></tr>
<tr><td>23. Juli 2024</td><td>5.0.0</td><td>Neue Features

Amazon DocumentDB 5.0 (Engine-Patch-Version 3.0.8126)

• Unterstützung für längere Indexnamen (bis zu 255 Zeichen) hinzugefügt. Weitere Informationen finden Sie unter Benennungseinschränkungen:.
• Das maximale Verbindungslimit wurde um das Zweifache erhöht:

<table>
<tr><th>Instance-Typ</th><th>Ursprüngliches Limit</th><th>Neues Limit</th></tr>
<tr><td>t3.medium</td><td>500</td><td>1000</td></tr>
<tr><td>t4g.medium</td><td>500</td><td>1000</td></tr>
<tr><td>r5.large</td><td>1700</td><td>3400</td></tr>
<tr><td>r5.xlarge</td><td>3500</td><td>7000</td></tr>
<tr><td>r5.2xlarge</td><td>7100</td><td>14200</td></tr>
<tr><td>r5.4xlarge</td><td>14200</td><td>28400</td></tr>
<tr><td>r5.8xlarge</td><td>28400</td><td>60000</td></tr>
<tr><td>r5.12xlarge</td><td>30000</td><td>60000</td></tr>
<tr><td>r5.16xlarge</td><td>30000</td><td>60000</td></tr>
<tr><td>r5.24xlarge</td><td>30000</td><td>60000</td></tr>
<tr><td>r6g.large</td><td>1700</td><td>3400</td></tr>
<tr><td>r6g.xlarge</td><td>3500</td><td>7000</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Date</th><th>Unterversion</th><th>Versionshinweise</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><th>Instance-Typ</th><th>Ursprüngliches Limit</th><th>Neues Limit</th></tr>
<tr><td>r6g.2xlarge</td><td>7100</td><td>14200</td></tr>
<tr><td>r6g.4xlarge</td><td>14200</td><td>28400</td></tr>
<tr><td>r6g.8xlarge</td><td>28400</td><td>60000</td></tr>
<tr><td>r6g.12xlarge</td><td>30000</td><td>60000</td></tr>
<tr><td>r6g.16xlarge</td><td>30000</td><td>60000</td></tr>
</table>
Weitere Informationen finden Sie unter Instance-Limits.
Fehlerkorrekturen und andere Änderungen
Amazon DocumentDB 5.0 (Engine-Patch-Version 3.0.8126)
Die Logik für die Synchronisation <code>CurrentTime</code> und <code>ResumeToken</code> für den Change-Stream auf Lesegeräten wurde verbessert.
</td></tr>
</table>

Date	Unterversion	Versionshinweise

22. Juli 2024	5.0.0	Neue Features
		
		Amazon DocumentDB 5.0 (Engine-Patch-Version 3.0.6742)
		
		• Unterstützung für DML-Audit-Filterung hinzugefügt. Sie können jetzt Filterbedingungen einrichten, um DML-Auditprotokolle anhand ihrer spezifischen Anforderungen herauszufiltern, anstatt jede DML-Abfrage zu protokollieren. Weitere Informationen finden Sie unter DML-Auditereignisse filtern.
		• Unterstützung bei der Dokumentenkomprimierung für Folgendes hinzugefügt:
		  • Einstellung eines Mindestschwellenwerts für die Komprimierung
		  • Aktivierung der Komprimierung für bestehende Sammlungen (gilt für neue Dokumente)
		  • Lassen Sie die Standardkomprimierungseinstellung auf Clusterebene zu
		
		  Weitere Informationen finden Sie unter Verwaltung der Dokumentenkomprimierung auf Sammlungsebene.
		• Unterstützung für die Nutzung von Change-Streams auf Reader-Instances wurde hinzugefügt. Weitere Informationen finden Sie unter Verwendung von Change-Streams auf sekundären Instanzen.

9. Juli 2024	5.0.0	Neues Feature Für Amazon DocumentDB 5.0 (minimale Engine-Patch-Version 3.0.4780) erfordern TLS-CA-Zertifikatsaktualisierungen keinen Systemneustart mehr. Weitere Informationen finden Sie unter Aktualisierung Ihrer Amazon DocumentDB-TLS-Zertifikate.

Date	Unterversion	Versionshinweise
29. Mai 2024	5.0.0	Neue Features Amazon DocumentDB 5.0 (Engine-Patch-Version 3.0.6742) • Unterstützung für Operatoren und hinzugefügt. `$regexMatch` `$regexFind` • Unterstützung hinzugefügt, um die volle Präzision der Audit-Logs bei der Adressierung großer Ganzzahlen zu gewährleisten. Audit-Logs behalten jetzt die exakte numerische Darstellung für alle Zahlen bei, wodurch jeglicher Genauigkeitsverlust vermieden wird.
3. April 2024	5.0.0	Neue Features Amazon DocumentDB 5.0 (Engine-Patch-Version 3.0.5721) • Unterstützung für `bypassDocumentValidation` und detaillierte Fehlermeldungen für hinzugefügt. `$jsonSchema` Mehr über `bypassDocumentValidation` erfahren Sie unter umgehen DocumentValidation. • Unterstützung von `$expr` hinzugefügt. • Unterstützung für unkorrelierte Verknüpfungen hinzugefügt. `$lookup` • Unterstützung für die Beibehaltung von Validierungsregeln in der `$out` Aggregationsphase hinzugefügt.

Date	Unterversion	Versionshinweise
10. Januar 2024	5.0.0	Neue Features Amazon DocumentDB 5.0 (Engine-Patch-Versionen 3.0.4574, 3.0.4780, 3.0.4960) • Unterstützung für HNSW-Vektorindizes hinzugefügt. Weitere Informationen finden Sie unter Vektorsuche für Amazon DocumentDB. • Unterstützung für Teilindizes hinzugefügt. Weitere Informationen finden Sie unter Teilweiser Index. • Unterstützung für GC-Laufzeit für eine Sammlung innerhalb eines `currentOp` Befehls hinzugefügt. • Textindex-Unterstützung für die native Textsuche in Amazon DocumentDB hinzugefügt. Weitere Informationen finden Sie unter Textsuche mit Amazon DocumentDB durchführen. • Unterstützung für `$jsonSchema` Schema-Schlüsselwörtertype,,`allOf`,`oneOf`,`anyOf`,`not`,`maxItems`,`minItems`,`maxProperties` ,`minProperties` ,,`pattern`, `patternProperties` `multipleOf` `dependencies` , und `uniqueItems` hinzugefügt. Weitere Informationen finden Sie unter Verwenden der JSON-Schemavalidierung. • Unterstützung für arithmetische Operatoren `$ceil`,,`$floor`,`$ln`, `$log` `$log10`, `$sqrt`, und `$exp` hinzugefügt. Weitere Informationen finden Sie unter Arithmetische Operatoren. • Unterstützung für den Operator für bedingte Ausdrücke `$switch` hinzugefügt.

Date	Unterversion	Versionshinweise
		• Unterstützung für parallel `IVFFLAT` Vektorindex-Builds hinzugefügt. Die Dokumentation wurde aktualisiert, indem die Beschränkung für die Erstellung parallel `IVFFLAT` Vektorindizes aus dem Entwicklerhandbuch entfernt wurde. Fehlerkorrekturen und andere Änderungen • Beim Aufrufen wurde eine Funktion hinzugefügt, bei der Groß- und Kleinschreibung nicht berücksichtigt wird. `db.runCommand("dbstats")` Amazon DocumentDB 5.0-Kunden mit Engine-Patch-Versionen vor 3.0.4960 oder 2.0.10221 sollten diese neuesten Engine-Patches installieren. • Ein Fehler beim Aufrufen `db.coll.stats()` auf der Mongo-Shell Version 1.7 und höher wurde behoben. Die Dokumentation wurde aktualisiert, indem der Tipp `db.coll.stats()` zur Fehlerbehebung bei Mongo-Shell aus dem Entwicklerhandbuch entfernt wurde.
29. November 202	5.0.0	Neue Features Amazon DocumentDB 5.0 (Engine-Patch-Version 3.0.3727) Unterstützung für die Vektorsuche hinzugefügt. Weitere Informationen finden Sie in diesem Blogbeitrag und Vektorsuche für Amazon DocumentDB im Amazon DocumentDB Developer Guide.

Date	Unterversion	Versionshinweise
21. November 202	5.0.0	Neue Features Amazon DocumentDB 5.0 (Engine-Patch-Version 3.0.3727) Unterstützung für Speicher hinzugefügt. I/O-optimized Weitere Informationen finden Sie Amazon DocumentDB-Cluster-Speicherkonfigurationen im Amazon DocumentDB Developer Guide. Es wurde eine Integration für maschinelles Lernen ohne Code mit SageMaker Canvas hinzugefügt. Weitere Informationen finden Sie No-code maschinelles Lernen mit Amazon SageMaker AI Canvas im Amazon DocumentDB Developer Guide.

Date	Unterversion	Versionshinweise
6. November 2023	5.0.0	Amazon DocumentDB 5.0 (Engine-Patch-Versionen 3.0.3727) Neue Features • Unterstützung für `$jsonSchema` Schema-Schlüsselwörter `maxLength`, `minLength`, `maximum`, `minimum` `exclusiveMaximum`, `exclusiveMinimum` und hinzugefügt. `items` `additionalItems` Beachten Sie, dass die JSON-Schemavalidierung nur in instanzbasierten Clustern unterstützt wird. • Unterstützung für den `$convert` Aggregationspipeline-Operator und seine abgeleiteten Kurzoperatoren `$toBool`, `$toInt`, `$toLong`, `$toDouble`, `$toString` und wurde hinzugefügt. `$toDecimal` `$toObjectId` `$toDate` • Unterstützung für Mengenausdrucksoperatoren `$setDifference`, `$anyElementTrue` und `$allElementTrue` hinzugefügt. Fehlerkorrekturen und andere Änderungen Es wurde ein Problem behoben, bei dem ein Change-Stream-Update von `-NaN` zu nicht angezeigt `NaN` wurde.
15. September 20	5.0.0	Neue Features Amazon DocumentDB 5.0 (Engine-Patch-Version 3.0.3140) Unterstützung für den $jsonSchema-Schema-Validator wurde nur in instanzbasierten Clustern hinzugefügt. Weitere Informationen finden Sie unter Verwenden der JSON-Schemavalidierung.

Date	Unterversion	Versionshinweise
13. Juli 2023	5.0.0	Neue Features Amazon DocumentDB 5.0 (Engine-Patch-Version 3.0.1948) • Unterstützung für die Komprimierung von Dokumenten wurde hinzugefügt. • Unterstützung für parallel Indexerstellungen hinzugefügt. • Unterstützung für den Status der Indexerstellung hinzugefügt. Fehlerkorrekturen und andere Änderungen Amazon DocumentDB 5.0 (Engine-Patch-Version 3.0.1948) • Es wurde ein Authentifizierungsproblem `createCollection` bei elastischen Amazon DocumentDB-Clustern behoben, wenn Benutzer keinen Zugriff auf Systemsammlungen hatten. • Es wurde ein Problem behoben, bei dem Instances in der sekundären Region nicht dieselben Instance-Namen für die primäre Region verwenden konnten.
7. Juni 2023	5.0.0	Fehlerkorrekturen und andere Änderungen Amazon DocumentDB 5.0 • r5- und t3.medium-Instances werden jetzt in Amazon DocumentDB 5.0 unterstützt. • `engineVersion` Die Standardoption befindet sich `5.0.0` im AWS SDK,, und. AWS CLI CloudFormation

Date	Unterversion	Versionshinweise
10. Mai 2023	5.0.0	Fehlerkorrekturen und andere Änderungen Amazon DocumentDB 5.0 (Engine-Patch-Version 3.0.1361) • Unterstützung für `ignoreunknownindex options` im Befehl hinzugefügt. createIndex • Das Hinzufügen interner Überwachungsanfragen zu den Überwachungsprotokollen wurde beendet. • Benutzerdefinierte lokale Variablennamen unterstützen jetzt „_“ (Unterstrich) für Projektionsoperatoren wie `$let` und`$filter`.

Date	Unterversion	Versionshinweise

1. März 2023	5.0.0	Neue Features
		
		Amazon DocumentDB 5.0 (Engine-Patch-Version 3.0.775)
		
		• Amazon DocumentDB 5.0 eingeführt
		  • MongoDB 5.0-Kompatibilität (Unterstützung für MongoDB 5.0-API-Treiber)
		  • Support für Client-side Field Level Encryption (FLE). Sie können jetzt Felder auf der Clientseite verschlüsseln, bevor Sie die Daten in den Amazon DocumentDB-Cluster schreiben. Weitere Informationen finden Sie unter Verschlüsselung auf Feldebene Client-side
		  • Neue Aggregationsoperatoren:`$dateAdd`, `$dateSubtract`
		• Das Speicherlimit wurde für alle instanzbasierten Amazon DocumentDB-Cluster und shard-basierten Elastic-Cluster auf 128 TiB erhöht.
		• Amazon DocumentDB 5.0 unterstützt jetzt Indexscans mit dem `$elemMatch` Operator in der ersten Verschachtelungsebene. Indexscans werden unterstützt, wenn Abfragen nur eine `$elemMatch` Filterebene haben und die verschachtelte `$elemMatch` Abfrage keinen Indexscan unterstützt.
		
		Abfrageform, die den Indexscan unterstützt:
		
		`db.foo.find( { "a": {$elemMatch: { "b": "xyz", "c": "abc"} } })`
		
		Abfrageform, die den Indexscan nicht unterstützt:

Date	Unterversion	Versionshinweise
		`db.foo.find( { "a": {$elemMatch: { "b": {$elemMatch: { "d": "xyz", "e": "abc"} }} } })`

Amazon DocumentDB 4.0

Versionshinweise für die Amazon DocumentDB DocumentDB-Engine Version 4.0 (MongoDB 4.0-Kompatibilität).

Date	Versionshinweise
27. April 2026	Fehlerkorrekturen und andere Änderungen Amazon DocumentDB 4.0 (Modulversion: 2.0.14278) Dies ist ein erforderlicher Engine-Patch, der die folgenden Probleme behebt: 1. Es wurde ein Problem behoben, das in seltenen Fällen dazu führen konnte, dass Point-in-Time Recovery (PITR) und Major Version Upgrades (MVU) nicht mehr reagierten. Alle Amazon DocumentDB 4.0-Cluster werden während ihres nächsten Wartungsfensters automatisch auf diese Patch-Version aktualisiert.
9. März 2026	Fehlerkorrekturen und andere Änderungen Amazon DocumentDB 4.0 (Modulversion: 2.0.14165) Dieses Update bietet einen optionalen Engine-Patch mit den folgenden Verbesserungen: 1. Es wurde eine DatabaseConnectionsActiveMax Metrik hinzugefü gt, die Einblicke in die „Verbindungen (aktiv)“ für Instances bietet.

Date	Versionshinweise
	Die Beschränkungen finden Sie auf unserer Amazon DocumentDB-Seite Kontingente und Beschränkungen. 2. Die Leistung der SASL-Authentifizierung wurde verbessert.
22. Oktober 2025	Neue Features Amazon DocumentDB 4.0 (Engine-Patch-Version 2.0.11747) Es wurden neue Felder `collstats` für „MvccidStats“ und „gcRuntimeStats“ hinzugefügt, die Informationen über den allgemeinen Zustand der Sammlung in Bezug auf Müllabfuhr und veraltete Sammlungen liefern.
16. Oktober 2025	Neues Feature Amazon DocumentDB 4.0 (Engine-Patch-Version 2.0.11747) Amazon DocumentDB unterstützt jetzt den Dual-Stack-Modus (IPv4/IPv6), wenn sich Ihr Cluster in einer Virtual Private Cloud (VPC) befindet. Weitere Informationen finden Sie in diesem Blogbeitrag und Amazon VPC und Amazon DocumentDB im Amazon DocumentDB Developer Guide.

Date	Versionshinweise
29. Juli 2025	Neue Features Amazon DocumentDB 4.0 (Engine-Patch-Version 2.0.11747) • Index-Bloat und sammlungsbasierte Bloat-Metriken wurden eingeführt • Es wurden CloudWatch `AvailableMVCCIds` Metriken hinzugefügt`LongestActiveGCRuntime`, die Informationen über den allgemeinen Zustand des Clusters in Bezug auf Müllsammlung und veraltete Sammlungen liefern. • Support für die folgenden Zeichenkettenoperatoren: `$trim``$rtrim`, und `$ltrim` • Support für den folgenden Stage-Operator: `$collStats` Fehlerkorrekturen und andere Änderungen Amazon DocumentDB 4.0 (Engine-Patch-Version 2.0.11747) Es wurde ein Problem bei der Indexerstellung behoben, das große Sammlungen betraf.
15. Januar 2025	Fehlerkorrekturen und andere Änderungen Amazon DocumentDB 4.0 (Engine-Patch-Version 2.0.11096) • Der `killOp` Befehl zur Behandlung eines Sonderfalls von Masseneinfügungen wurde korrigiert. • Verbesserte I/O-related Netzwerkspeichernutzung auf Amazon DocumentDB DocumentDB-Instances.
6. November 2024	Neue Features Amazon DocumentDB 4.0 (Engine-Patch-Version 2.0.10980) • Unterstützung für minimale TLS-Versionen `tls1.2+` und `tls1.3+` Cluster-Parameter hinzugefügt. `tls`

Date	Versionshinweise
17. September 2024	Fehlerkorrekturen und andere Änderungen Amazon DocumentDB 4.0 (Engine-Patch-Version 2.0.10898) • `$setOnInsert` unterstützt das `_id` Feld jetzt bei Einfügungen, die aus Aktualisierungsvorgängen resultieren. • Es wurde ein Problem behoben, das die Rückgewinnung von Speicherplatz nach einem Upgrade der Hauptversion auf Amazon DocumentDB 5.0 verhindert.
22. August 2024	Neues Feature Amazon DocumentDB 4.0 (Engine-Patch-Version 2.0.5704) Globale Amazon DocumentDB-Cluster unterstützen jetzt Cluster-Switchover und verwaltete Cluster-Failover. Weitere Informationen erhalten Sie unter Durchführen eines Switchovers für einen globalen Amazon DocumentDB-Cluster und Durchführen eines verwalteten Failovers für einen globalen Amazon DocumentDB-Cluster. **Note** Globale Cluster-Switchover und -Failover werden nur auf Amazon DocumentDB 4.0 und 5.0 unterstützt.

<table>
<tr><th>Date</th><th>Versionshinweise</th></tr>
<tr><td>23. Juli 2024</td><td>
Neue Features

Amazon DocumentDB 4.0 (Engine-Patch-Version 2.0.10709)

• Unterstützung für längere Indexnamen (bis zu 255 Zeichen) hinzugefügt. Weitere Informationen finden Sie unter Benennung seinschränkungen:.
• Das maximale Verbindungslimit wurde um das Zweifache erhöht:
<table>
<tr><th>Instance-Typ</th><th>Ursprüngliches Limit</th><th>Neues Limit</th></tr>
<tr><td>t3.medium</td><td>500</td><td>1000</td></tr>
<tr><td>t4g.medium</td><td>500</td><td>1000</td></tr>
<tr><td>r5.large</td><td>1700</td><td>3400</td></tr>
<tr><td>r5.xlarge</td><td>3500</td><td>7000</td></tr>
<tr><td>r5.2xlarge</td><td>7100</td><td>14200</td></tr>
<tr><td>r5.4xlarge</td><td>14200</td><td>28400</td></tr>
<tr><td>r5.8xlarge</td><td>28400</td><td>60000</td></tr>
<tr><td>r5.12xlarge</td><td>30000</td><td>60000</td></tr>
<tr><td>r5.16xlarge</td><td>30000</td><td>60000</td></tr>
<tr><td>r5.24xlarge</td><td>30000</td><td>60000</td></tr>
<tr><td>r6g.large</td><td>1700</td><td>3400</td></tr>
<tr><td>r6g.xlarge</td><td>3500</td><td>7000</td></tr>
<tr><td>r6g.2xlarge</td><td>7100</td><td>14200</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Date</th><th>Versionshinweise</th></tr>
<tr><td></td><td>
<table>
<tr><th>Instance-Typ</th><th>Ursprüngliches Limit</th><th>Neues Limit</th></tr>
<tr><td>r6g.4xlarge</td><td>14200</td><td>28400</td></tr>
<tr><td>r6g.8xlarge</td><td>28400</td><td>60000</td></tr>
<tr><td>r6g.12xlarge</td><td>30000</td><td>60000</td></tr>
<tr><td>r6g.16xlarge</td><td>30000</td><td>60000</td></tr>
</table>
Weitere Informationen finden Sie unter Instance-Limits.
</td></tr>
<tr><td>22. Juli 2024</td><td>Neue Features

Amazon DocumentDB 4.0 (Engine-Patch-Version 2.0.10593)

• Unterstützung für DML-Audit-Filterung hinzugefügt. Sie können jetzt Filterbedingungen einrichten, um DML-Auditprotokolle anhand ihrer spezifischen Anforderungen herauszufiltern, anstatt jede DML-Abfrage zu protokollieren. Weitere Informationen finden Sie unter DML-Auditereignisse filtern.</td></tr>
<tr><td>9. Juli 2024</td><td>Neues Feature

Für Amazon DocumentDB 4.0 (minimale Engine-Patch-Version 2.0.10179) erfordern TLS-CA-Zertifikatsaktualisierungen keinen Systemneustart mehr. Weitere Informationen finden Sie unter Aktualisierung Ihrer Amazon DocumentDB-TLS-Zertifikate.</td></tr>
</table>

Date	Versionshinweise
29. Mai 2024	Neue Features Amazon DocumentDB 4.0 (Engine-Patch-Version 2.0.10593) • Unterstützung hinzugefügt, um die volle Präzision der Audit-Logs bei der Adressierung großer Ganzzahlen zu gewährleisten. Audit-Logs behalten jetzt die exakte numerische Darstellung für alle Zahlen bei, wodurch jeglicher Genauigkeitsverlust vermieden wird.
3. April 2024	Neue Features Amazon DocumentDB 4.0 (Engine-Patch-Version 2.0.10392) • Unterstützung für hinzugefügt. `bypassDocumentValidation` `$jsonSchema` Mehr über `bypassDocumentValidation` erfahren Sie unter umgehen DocumentValidation. • Unterstützung von hinzugefügt`$expr`. • Unterstützung für unkorrelierte Verknüpfungen hinzugefügt. `$lookup` • Unterstützung für die Beibehaltung von Validierungsregeln in der `$out` Aggregationsphase hinzugefügt.

Date	Versionshinweise
10. Januar 2024	Neue Features Amazon DocumentDB 4.0 (Engine-Patch-Versionen 2.0.10124, 2.0.10179, 2.0.10221) • Es wurde eine Unterstützung für GC-Runtime für eine Sammlung innerhalb eines Befehls hinzugefügt. `currentOp` • Unterstützung für `$jsonSchema` Schema-Schlüsselwörtertype,`allOf`,`oneOf`,`anyOf`,`not`,`maxItems`,`minItems`,`maxProperties` ,`minProperties` ,`pattern`,`patternProperties` , `multipleOf` `dependencies` , und hinzugefügt`uniqueItems` . Weitere Informationen finden Sie unter Verwenden der JSON-Schemavalidierung. • Unterstützung für arithmetische Operatoren`$ceil`,,`$floor`,`$ln`, `$log` `$log10`$`sqrt`, und hinzugefügt. `$exp` Weitere Informationen finden Sie unter Arithmetische Operatoren. • Unterstützung für den Operator für bedingte Ausdrücke hinzugefügt. `$switch`
20. Dezember 2023	Weitere Änderungen Unterstützung für direkte Hauptversions-Upgrades in Amazon DocumentDB 4.0 aktiviert. Weitere Informationen finden Sie unter Direktes Upgrade der Hauptversion von Amazon DocumentDB.

Date	Versionshinweise
6. November 2023	Amazon DocumentDB 4.0 (Engine-Patch-Versionen 2.0.9876) Neue Features • Unterstützung für `$jsonSchema` Schema-SchlüsselwörtermaxLength ,,,minLength ,maximum, minimum exclusiveMaximum exclusiveMinimum , items und hinzugefügt. additionalItems Beachten Sie, dass die JSON-Schemavalidierung nur in instanzbasierten Clustern unterstützt wird. • Unterstützung für den `$convert` Aggregationspipeline-Operator und seine abgeleiteten Kurzoperatoren$toBool,,,, $toInt $toLong$toDouble , $toString und wurde hinzugefügt. $toDecimal $toObjectId $toDate • Unterstützung für Mengenausdrucksoperatoren$setDifference ,, und $anyElementTrue hinzugefügt. $allElementTrue Fehlerkorrekturen und andere Änderungen Es wurde ein Problem behoben, bei dem ein Change-Stream-Update von -NaN zu nicht angezeigt NaN wurde.
20. September 2023	Neue Features Unterstützung für direkte Hauptversions-Upgrades in Amazon DocumentDB 4.0 hinzugefügt. Weitere Informationen finden Sie unter Direktes Upgrade der Hauptversion von Amazon DocumentDB.

Date	Versionshinweise
15. September 2023	Neue Features Amazon DocumentDB 4.0 (Engine-Patch-Version 2.0.9686) Unterstützung für den $jsonSchema-Schema-Validator wurde nur in instanzbasierten Clustern hinzugefügt. Weitere Informationen finden Sie unter Verwenden der JSON-Schemavalidierung.
13. Juli 2023	Neue Features Amazon DocumentDB 4.0 (Engine-Patch-Version 2.0.9259) • Unterstützung für parallel Indexerstellungen hinzugefügt. Fehlerkorrekturen und andere Änderungen Amazon DocumentDB 4.0 (Engine-Patch-Version 2.0.9259) • Das Hinzufügen interner Überwachungsanfragen zu den Audit-Pro tokollen wurde beendet.

Date	Versionshinweise
4. April 2023	Fehlerkorrekturen und andere Änderungen Amazon DocumentDB 4.0 (Engine-Patch-Version 2.0.8934) • Das Problem mit der DML-Überwachung, wenn sie während einer laufenden Arbeitslast aktiviert wurde, wurde behoben. • Es wurde ein Problem mit der DML-Überwachung behoben, bei dem aggregierten Befehlen mit einem Hinweis ein Zeichenfolgenwert übergeben wurde. • Es wurde ein Problem behoben, bei dem der `listCollections` Befehl nicht funktionierte, wenn Benutzer mit der Rolle readwrite anydatabase sowohl die Optionen AuthorizedCollections als auch NameOnly auf true gesetzt hatten. • Das Problem, dass numerische Zeichenketten in einem Feldnamen korrekt analysiert wurden, wurde behoben. • Brecht lange laufende Cursor ab, wenn sie sich auf die Garbage-C ollection auswirken. • Benutzerdefinierte lokale Variablennamen unterstützen jetzt „_“ (Unterstrich) für Projektionsoperatoren wie und. `$let` `$filter`
27. Februar 2023	Fehlerkorrekturen und andere Änderungen Amazon DocumentDB 4.0 Unterstützung für AWS Lambda hinzugefügt. Weitere Informationen finden Sie unter Verwendung AWS Lambda mit Change-Streams.

Date	Versionshinweise
09. August 2022	Neue Features 4.0 • Unterstützung für den Decimal128-Datentyp hinzugefügt. Decimal128 ist ein BSON-Datentyp, der in allen Regionen unterstützt wird, in denen DocumentDB verfügbar ist. Weitere Informationen finden Sie unter Data Types. • Unterstützung für die Prüfung von DML-Abfragen mit Amazon CloudWatch Logs hinzugefügt. Amazon DocumentDB kann jetzt DML-Ereignisse (Data Manipulation Language) und DDL-Ereignisse (Data Definition Language) in Amazon Logs aufzeichnen. CloudWatch Weitere Informationen finden Sie in diesem Blog-Beitrag. Fehlerkorrekturen und andere Änderungen 4.0 • Sie können jetzt Ihr eigenes Passwort mit einem eigenen Passwort mit Privilegien ändern. `changeOwnPassword`
25. Juli 2022	Neue Features Amazon DocumentDB 4.0 Sie können jetzt schneller Cluster erstellen, da Sie Klone erstellen können, die dasselbe DocumentDB-Cluster-Volume verwenden und dieselben Daten wie der ursprüngliche Cluster haben. Einzelheiten finden Sie unter Amazon DocumentDB-Cluster verwalten.

Date	Versionshinweise
27. Juni 2022	Neue Features Amazon DocumentDB 4.0 (Engine-Patch-Version 2.0.7509) Amazon DocumentDB passt die Größe Ihrer Datenbank dynamisch auf der Grundlage von Nutzungsmustern an. Durch das Hinzufüge n weiterer Daten wird der Speicherplatz auf bis zu 64 Tebibyte (TiB) erhöht, und durch das Löschen von Daten wird der zugewiesene Speicherplatz verringert.
7. April 2022	Neue Features 4.0 (Engine-Patch-Versionen 2.0.6142 und 2.0.6948) Amazon DocumentDB Performance Insights ist jetzt als Vorschauv ersion verfügbar. Sie können jetzt den Leistungsverlauf von sieben Tagen ohne zusätzliche Kosten in einem sich öffnenden Fenster speichern. Weitere Informationen finden Sie unter Monitoring with Performance Insights.

Date	Versionshinweise

24. Januar 2022	Neue Features
	
	4.0 (Engine-Patch-Version 2.0.5170)
	
	• Amazon DocumentDB bietet jetzt eine kostenlose Testversion. Einzelheiten finden Sie auf der Seite mit der kostenlosen Testversion von Amazon DocumentDB.
	• Sie können jetzt erweiterte Funktionen mit Geospatial-Abfragen verwenden, einschließlich der folgenden APIs:
	  • `$geoWithin`
	  • `$geoIntersects`
	• Unterstützung für die folgenden MongoDB-Operatoren hinzugefügt:
	  • `$mergeObjects`
	  • `$reduce`
	
	Weitere Informationen finden Sie unter Abfragen von Geodaten mit Amazon DocumentDB.

Date	Versionshinweise

21. Januar 2022	Neue Features
	
	Amazon DocumentDB 4.0 (Engine-Patch-Version 2.0.5706)
	
	• Amazon DocumentDB Graviton2-Instances (r6g.large, r6g.2xlarge, r6g.4xlarge, r6g.8xlarge, r6g.12xlarge, r6g.16xlarge und t4g.mediu m) werden jetzt unterstützt.
	
	Neue Features
	
	4.0 (Engine-Patch-Version 2.0.5706)
	
	• Unterstützung für die folgenden MongoDB-APIs hinzugefügt:
	  • `$reduce`
	  • `$mergeObjects`
	  • `$geoWithin`
	  • `$geoIntersects`

Date	Versionshinweise

25. Oktober 2021	Neue Features
	
	4.0 (Engine-Patch-Version 2.0.5704)
	
	• Unterstützung für die folgenden MongoDB-APIs hinzugefügt
	  • `$literal`
	  • `$map`
	  • `$$ROOT`
	• Support für GeoSpatial Abfragefunktionen. Weitere Informationen finden Sie in diesem Blogbeitrag
	• Support für die Zugriffskontrolle mit benutzerdefinierten Rollen. Weitere Informationen finden Sie in diesem Blogbeitrag
	• Amazon DocumentDB JDBC-Treiber zur Aktivierung der Konnektivität von BI-Tools wie Tableau und Abfragetools wie SQL Workbench
	
	Fehlerkorrekturen und andere Änderungen
	
	4.0 (Engine-Patch-Version 2.0.5704)
	
	• Fehlerkorrektur für `$natural` die korrekte Sortierung, wenn ein Explizit zusammen `.sort()` mit `$natural`
	• Bugfix für den Change-Stream, mit dem gearbeitet werden soll `$redact`
	• Bugfix für `$ifNull` das Arbeiten mit einem leeren Array
	• Bugfix für übermäßigen consumption/server Ressourcenabsturz, wenn ein aktuell angemeldeter Benutzer gelöscht oder diesem Benutzer die Rechte für eine laufende Aktivität entzogen wurde
	• Fehlerbehebung bei der Anmeldung und Überprüfung der Rechte `listDatabase listCollection`
	• Fehler behoben: Deduplizierungslogik für Elemente mit mehreren Schlüsseln

Date	Versionshinweise
24. Juni 2021	Neue Features 4.0 (Engine-Patch-Version 2.0.3371) • Die Instanzen r5.8xlarge und r5.16xlarge werden jetzt unterstüt zt. Weitere Informationen finden Sie im Blogbeitrag Amazon DocumentDB unterstützt jetzt r5.8xlarge- und r5.16xlarge-Instances. • Globale Cluster werden jetzt unterstützt, um eine Notfallwi ederherstellung nach regionalen Ausfällen zu ermöglichen und globale Lesevorgänge mit geringer Latenz zu ermöglichen, indem Lesevorgänge vom nächstgelegenen Amazon DocumentDB-Cluster zugelassen werden. Beachten Sie, dass globale Cluster derzeit in den Regionen Südamerika (São Paulo), Europa (Mailand), China (Peking) und China (Ningxia) nicht unterstützt werden.

Date	Versionshinweise
4. Mai 2021	Neue Features 4.0 (Engine-Patch-Version 2.0.3371) • `renameCollection` • `$zip` • `$indexOfArray` • `$reverseArray` • `$natural` • `$hint`Unterstützung für Updates • Index-Scan für `distinct` Fehlerkorrekturen und andere Änderungen 4.0 (Engine-Patch-Version 2.0.3371) • Reduzierter Speicherverbrauch für Abfragen `$in` • Ein Speicherleck in Multikey-Indizes wurde behoben • Der Explain-Plan und die Profiler-Ausgabe für wurden behoben `$out` • Es wurde ein Timeout für Operationen aus dem internen Überwachu ngssystem hinzugefügt, um die Zuverlässigkeit zu verbessern • Es wurde ein Fehler behoben, der sich auf die Abfrageprädikate auswirkte, die an Multikey-Indizes übergeben wurden
15. Januar 2021	Neue Features Amazon DocumentDB 4.0 (Engine-Patch-Version 2.0.722) • Keine

Date	Versionshinweise
9. November 2020	Neue Features Amazon DocumentDB 4.0 (Engine-Patch-Version 2.0.722) • MongoDB 4.0-Kompatibilität • ACID-Transaktionen • Support für `cluster(client.watch()` oder `mongo.watch())` und die `(db.watch())` Change-Streams auf Datenbankebene • Möglichkeit, einen Change-Stream zu starten oder fortzusetzen mit `startAtOperationTime` • Verlängern Sie die Aufbewahrungsfrist für Ihren Change-Stream auf 7 Tage (zuvor 24 Stunden) • AWS DMS Ziel für Amazon DocumentDB 4.0 • CloudWatch Metriken: `TransactionsOpen` `TransactionsOpenMax` , `TransactionsAborted` `TransactionsStarted` , und `TransactionsCommitted` • Neue Felder für Transaktionen in `currentOp` `ServerStatus` , und`profiler`. • Möglichkeit, einen Index in der `$lookup` Aggregationsphase zu verwenden • `find()`Abfragen mit Prognosen können direkt von einem Index aus bedient werden (abgedeckte Abfrage) • Fähigkeit zur Verwendung `hint()` mit `findAndModify` • Leistungsoptimierungen für `$addToSet` den Bediener • Verbesserungen zur Reduzierung der allgemeinen Indexgrößen. • Neue Aggregationsoperatoren:`$ifNull`,`$replaceRoot` ,`$setIsSubset` , `$setInstersection` `$setUnion` , und `$setEquals` • Mit den `ListDatabase` Befehlen `ListCollection` und können Sie nun optional die `authorizedDatabases` Parameter `authorizedCollections` und verwenden, damit Benutzer

Date	Versionshinweise
	die Sammlungen und Datenbanken auflisten können, auf die sie zugreifen dürfen, ohne dass die `listDatabase` Rollen `listCollections` bzw. • Benutzer können auch ihre eigenen Cursor beenden, ohne die `KillCursor` Rolle zu benötigen • Der Vergleich numerischer Typen von Filialdokumenten entspricht jetzt dem Vergleich numerischer Typen von Dokumenten der ersten Ebene. Das Verhalten in Amazon DocumentDB 4.0 ist jetzt mit MongoDB kompatibel. Fehlerkorrekturen und andere Änderungen Amazon DocumentDB 4.0 (Engine-Patch-Version 2.0.722) • `$setOnInsert` erlaubt keine Aktualisierungen mehr, wenn der Positionsoperator verwendet wird. $ Das Verhalten in Amazon DocumentDB 4.0 ist jetzt mit MongoDB kompatibel. • Problem mit `$createCollection` und Set behoben `autoIndex Id` • Projektion für verschachtelte Dokumente • Die Standardeinstellung für den Arbeitsspeicher wurde so geändert, dass sie mit der Größe des Instanzspeichers skaliert • Verbesserungen bei der Müllabfuhr • Suche mit leerem Pfadschlüssel, Verhaltensunterschied bei Mongo • `dateToString` Fehler im Verhalten der Zeitzone behoben • Behoben `$push` (Aggregation), um die Sortierreihenfolge zu respektieren • Ein Fehler im Aggregat `$currentOp` wurde behoben • Problem mit einem `readPreference` Sekundärgerät behoben • Es wurde ein Problem mit der Überprüfung behoben, `$createIn dex` dass es sich um dieselbe Datenbank handelt, in der der Befehl ausgegeben wurde

Date	Versionshinweise
	• Inkonsistentes Verhalten für`minKey`, Suche schlägt fehl `maxKey` • Es wurde ein Problem behoben, bei dem der `$size` Operator nicht mit einem zusammengesetzten Array funktionierte • Problem mit der Negation von `$in` mit Regex behoben • Es wurde ein Problem behoben, bei dem der `$distinct` Befehl für eine Ansicht ausgeführt wurde • Es wurde ein Problem mit Aggregationen und Suchbefehlen behoben, bei denen fehlende Felder unterschiedlich sortiert wurden • Problem behoben`$eq`, bei dem reguläre Ausdrücke den Typ nicht überprüfen • Ein `$currentDate` Fehler im Verhalten bei der Ordinalposition von Zeitstempeln wurde behoben • Die Granularität im Millisekundenbereich wurde behoben für `$currentDate`

Amazon DocumentDB 3.6

Versionshinweise für die Amazon DocumentDB DocumentDB-Engine Version 3.6 (MongoDB 3.6-Kompatibilität).

Date	Versionshinweise
27. April 2026	Neue Features Amazon DocumentDB 3.6 (Engine-Version: 1.0.208692) [in Bearbeitung] Dieses Update bietet einen optionalen Engine-Patch mit den folgenden Verbesserungen: 1. Unterstützung für `startAtOperationTime` In-Change-Streams wurde hinzugefügt.
12. Februar 2026	Fehlerkorrekturen und andere Änderungen

Date	Versionshinweise
	Amazon DocumentDB 3.6 (Modulversion: 1.0.208675) 1. Es wurde eine DatabaseConnectionsActiveMax Metrik hinzugefügt, die Einblicke in die „Verbindungen (aktiv)“ für Instances bietet. Die Beschränkungen finden Sie auf unserer Amazon DocumentDB-Seite Kontingente und Beschränkungen. 2. Die Leistung der SASL-Authentifizierung wurde verbessert. 3. Fehlerkorrektur für den Befehl $indexStats.
20. August 2024	Neues Feature Für Amazon DocumentDB 3.6 (minimale Engine-Patch-Version 1.0.208662) erfordern TLS-CA-Zertifikatsaktualisierungen keinen Systemneustart mehr. Weitere Informationen finden Sie unter Aktualisierung Ihrer Amazon DocumentDB-TLS-Zertifikate.
22. Juli 2024	Neue Features Amazon DocumentDB 3.6 (Engine-Patch-Version 1.0.208662) Die Indexbeschränkungen für db.r5.*- und db.r6.*-Instances in Amazon DocumentDB MVU wurden entfernt. Weitere Informationen finden Sie unter Voraussetzungen. Fehlerkorrekturen und andere Änderungen Amazon DocumentDB 3.6 (Engine-Patch-Version 1.0.208662) Amazon DocumentDB erkennt -NaN jetzt als gültiges JSON-Token.
20. Dezember 2023	Weitere Änderungen Unterstützung für direkte Hauptversions-Upgrades in Amazon DocumentDB 3.6 aktiviert. Weitere Informationen finden Sie unter Direktes Upgrade der Hauptversion von Amazon DocumentDB.

Date	Versionshinweise
17. November 2023	Fehlerkorrekturen und andere Änderungen Amazon DocumentDB 3.6 (Engine-Patch-Version 1.0.208570) Benutzerdefinierte lokale Variablennamen unterstützen jetzt „_“ (Unterstrich) für Projektionsoperatoren wie und. `$let` `$filter`
20. September 2023	Neue Features Unterstützung für direkte Hauptversions-Upgrades in Amazon DocumentDB 3.6 hinzugefügt. Weitere Informationen finden Sie unter Direktes Upgrade der Hauptversion von Amazon DocumentDB.
2. Februar 2023	Fehlerkorrekturen und andere Änderungen Amazon DocumentDB 3.6 (Engine-Patch-Version 1.0.208432) • Es wurde ein Problem mit der DML-Überwachung behoben, wenn sie während einer laufenden Arbeitslast aktiviert wurde. • Es wurde ein Problem mit der DML-Überwachung behoben, bei dem aggregierten Befehlen mit einem Hinweis ein Zeichenfolgenwert übergeben wurde. • Es wurde ein Problem behoben, bei dem der `listCollections` Befehl nicht funktionierte, wenn Benutzer mit der Rolle readwrite anydatabase sowohl die Optionen AuthorizedCollections als auch NameOnly auf true gesetzt hatten. • Das Problem, dass numerische Zeichenketten in einem Feldnamen korrekt analysiert wurden, wurde behoben. • Brecht lange laufende Cursor ab, wenn sie sich auf die Garbage-C ollection auswirken.

Date	Versionshinweise
09. August 2022	Neue Features Amazon DocumentDB 3.6 (Engine-Patch-Version 1.0.208152) • Unterstützung für den Datentyp Decimal128 wurde hinzugefügt. Decimal128 ist ein BSON-Datentyp, der in allen Regionen unterstützt wird, in denen DocumentDB verfügbar ist. Weitere Informationen finden Sie unter Data Types. • Unterstützung für die Prüfung von DML-Abfragen mit Amazon CloudWatch Logs hinzugefügt. Amazon DocumentDB kann jetzt DML-Ereignisse (Data Manipulation Language) und DDL-Ereignisse (Data Definition Language) in Amazon Logs aufzeichnen. CloudWatch Weitere Informationen finden Sie in diesem Blog-Beitrag. Fehlerkorrekturen und andere Änderungen Amazon DocumentDB 3.6 (Engine-Patch-Version 1.0.208152) • Sie können jetzt Ihr eigenes Passwort mit einem eigenen Passwort mit Privilegien ändern. `changeOwnPassword`
7. April 2022	Neue Features Amazon DocumentDB 3.6 (Engine-Patch-Versionen 1.0.207836 und 1.0.208015) Amazon DocumentDB Performance Insights ist jetzt als Vorschauversion verfügbar. Sie können jetzt den Leistungsverlauf von sieben Tagen ohne zusätzliche Kosten in einem sich öffnenden Fenster speichern. Weitere Informationen finden Sie unter Monitoring with Performance Insights.

Date	Versionshinweise

24. Januar 2022	Neue Features
	
	Amazon DocumentDB 3.6 (Engine-Patch-Version 1.0.207684)
	
	• Amazon DocumentDB bietet jetzt eine kostenlose Testversion. Einzelheiten finden Sie auf der Seite mit der kostenlosen Testversion von Amazon DocumentDB.
	• Sie können jetzt erweiterte Funktionen mit Geospatial-Abfragen verwenden, einschließlich der folgenden APIs:
	  • `$geoWithin`
	  • `$geoIntersects`
	• Unterstützung für die folgenden MongoDB-Operatoren hinzugefügt:
	  • `$mergeObjects`
	  • `$reduce`
	
	Weitere Informationen finden Sie unter Abfragen von Geodaten mit Amazon DocumentDB.

21. Januar 2022	Neue Features
	
	Amazon DocumentDB 3.6 (Engine-Patch-Version 1.0.207781)
	
	• Unterstützung für die folgenden MongoDB-APIs hinzugefügt:
	  • `$reduce`
	  • `$mergeObjects`
	  • `$geoWithin`
	  • `$geoIntersects`

Date	Versionshinweise

25. Oktober 2021	Neue Features
	
	Amazon DocumentDB 3.6 (Engine-Patch-Version 1.0.207780)
	
	• Unterstützung für die folgenden MongoDB-APIs hinzugefügt
	  • `$literal`
	  • `$map`
	  • `$$ROOT`
	• Support für GeoSpatial Abfragefunktionen. Weitere Informationen finden Sie in diesem Blogbeitrag
	• Support für die Zugriffskontrolle mit benutzerdefinierten Rollen. Weitere Informationen finden Sie in diesem Blogbeitrag
	• Amazon DocumentDB JDBC-Treiber zur Aktivierung der Konnektivität von BI-Tools wie Tableau und Abfragetools wie SQL Workbench
	
	Fehlerkorrekturen und andere Änderungen
	
	Amazon DocumentDB 3.6 (Engine-Patch-Version 1.0.207780)
	
	• Fehlerkorrektur für `$natural` die korrekte Sortierung, wenn ein Explizit `.sort()` zusammen mit `$natural`
	• Bugfix für den Change-Stream, mit dem gearbeitet werden soll `$redact`
	• Bugfix für `$ifNull` das Arbeiten mit einem leeren Array
	• Bugfix für übermäßigen consumption/server Ressourcenabsturz, wenn ein aktuell angemeldeter Benutzer gelöscht oder diesem Benutzer die Rechte für eine laufende Aktivität entzogen wurde
	• Fehlerbehebung bei der Anmeldung und Überprüfung der Rechte `listDatabase listCollection`
	• Fehler behoben: Deduplizierungslogik für Elemente mit mehreren Schlüsseln

Date	Versionshinweise
24. Juni 2021	Neue Features Amazon DocumentDB 3.6 (Engine-Patch-Version 1.0.207117) • Die Instances r5.8xlarge und r5.16xlarge werden jetzt unterstützt. Weitere Informationen finden Sie im Blogbeitrag Amazon DocumentDB unterstützt jetzt r5.8xlarge- und r5.16xlarge-Instances. • Globale Cluster werden jetzt unterstützt, um eine Notfallwiederherstellung nach regionalen Ausfällen zu ermöglichen und globale Lesevorgänge mit geringer Latenz zu ermöglichen, indem Lesevorgänge vom nächstgelegenen Amazon DocumentDB-Cluster zugelassen werden. Beachten Sie, dass globale Cluster derzeit in den Regionen Südamerika (São Paulo), Europa (Mailand), China (Peking) und China (Ningxia) nicht unterstützt werden.

Date	Versionshinweise
4. Mai 2021	Neue Features Amazon DocumentDB 3.6 (Engine-Patch-Version 1.0.207117) • `renameCollection` • `$zip` • `$indexOfArray` • `$reverseArray` • `$natural` • `$hint`Unterstützung für Updates • Index-Scan für `distinct` Fehlerkorrekturen und andere Änderungen Amazon DocumentDB 3.6 (Engine-Patch-Version 1.0.207117) • Reduzierter Speicherverbrauch für Abfragen `$in` • Ein Speicherleck in Multikey-Indizes wurde behoben • Der Explain-Plan und die Profiler-Ausgabe für wurden behoben `$out` • Es wurde ein Timeout für Operationen aus dem internen Überwachu ngssystem hinzugefügt, um die Zuverlässigkeit zu verbessern • Es wurde ein Fehler behoben, der sich auf die Abfrageprädikate auswirkte, die an Multikey-Indizes übergeben wurden

Date	Versionshinweise
15. Januar 2021	Neue Features Amazon DocumentDB 3.6 (Engine-Patch-Version 1.0.206295) • Fähigkeit, einen Index in der Aggregationsphase zu verwenden `$lookup` • `find()`Abfragen mit Prognosen können direkt von einem Index aus bedient werden (abgedeckte Abfrage) • Fähigkeit zur Verwendung `hint()` mit `findAndModify` • Leistungsoptimierungen für `$addToSet` den Bediener • Verbesserungen zur Reduzierung der allgemeinen Indexgrößen • Neue Aggregationsoperatoren:`$ifNull`,`$replaceRoot` ,`$setIsSubset` , `$setInstersection` `$setUnion` , und `$setEquals` • Benutzer können auch ihre eigenen Cursor beenden, ohne die Rolle zu benötigen `KillCursor`
9. November 2020	Neue Features Amazon DocumentDB 3.6 (Engine-Patch-Version 1.0.206295) • Keine Fehlerkorrekturen und andere Änderungen Amazon DocumentDB 3.6 (Engine-Patch-Version 1.0.206295) • Keine

Date	Versionshinweise
30. Oktober 2020	Neue Features Amazon DocumentDB 3.6 (Engine-Patch-Version 1.0.206295) • Es wurde die Möglichkeit hinzugefügt, einen Change-Stream-Cursor auf Cluster-Ebene (`client.watch()` oder in der Datenbank zu öffnen `mongo.watch()) (db.watch())` • Möglichkeit, die Aufbewahrungsfrist für Change-Streams auf 7 Tage (zuvor 24 Stunden) zu erhöhen Fehlerkorrekturen und andere Änderungen Amazon DocumentDB 3.6 (Engine-Patch-Version 1.0.206295) • Verschiedene allgemeine Verbesserungen der Fallleistung • Eine gezielte Verbesserung der Sicherheit • Es wurde ein Problem behoben, bei dem die Sortierung im zweiten Feld eines zusammengesetzten Indexes übersprungen wurde • Aktiviert den regulären Index für Gleichheit für ein einzelnes Feld eines Indexes mit mehreren Schlüsseln (nicht zusammengesetzt) • Die Bedingung für das Autorisierungsrennen wurde behoben • Es wurde ein Problem behoben, das zu einem seltenen Absturz bei der Garbage-Collection führte • Verbesserung der RBAC-Sicherheit • Metrik hinzugefügt `databaseConnectionsMax` • Leistungsverbesserungen für bestimmte Workloads auf Instanzen `r5.24xlarge`

Date	Versionshinweise
22. September 2020	Neue Features Amazon DocumentDB 3.6 (Engine-Patch-Version 1.0.206295) • `$out`Aggregationsphase • Die maximale Anzahl von Verbindungen und Cursor pro Instanz wurde um das Zehnfache erhöht Fehlerkorrekturen und andere Änderungen Amazon DocumentDB 3.6 (Engine-Patch-Version 1.0.206295) • Keine
10. Juli 2020	Neue Features Amazon DocumentDB 3.6 (Engine-Patch-Version 1.0.206295) • Regionsübergreifende Snapshot-Kopie Fehlerkorrekturen und andere Änderungen Amazon DocumentDB 3.6 (Engine-Patch-Version 1.0.206295) • Keine

Date	Versionshinweise
30. Juni 2020	Neue Features Amazon DocumentDB 3.6 (Engine-Patch-Version 1.0.206295) • Mittlere T3-Instanzen Fehlerkorrekturen und andere Änderungen Amazon DocumentDB 3.6 (Engine-Patch-Version 1.0.206295) • Rückgewinnung von Arbeitsspeicher im Leerlauf für T3-Instances • Verbesserungen bei der Authentifizierung • Verbesserte Leistung der SASL-Authentifizierung • `currentOp` Das Problem beim Überschreiten der maximal möglichen Operationen wurde behoben • `killOps`Problem beim Bulk-Update und Löschen behoben • `$sample`Leistungsverbesserungen mit `$match` • Die Unterstützung für „$$In Cond Case“ in der Redact-Phase wurde behoben • Verschiedene wiederkehrende Ursachen für Abstürze wurden behoben • Verbesserungen beim TTL-Sweeping zur Reduzierung von iOS und Latenz • Optimierte Speichernutzung für `$unwind` • Es wurde ein Fehler behoben, bei dem das Rennen mit Drop-Index angezeigt wurde • Die Rennbedingung bei der gleichzeitigen Indexerstellung wurde behoben • Ein seltener Absturz im `hash_search` Index wurde behoben

Allgemeine Versionshinweise zu Amazon DocumentDB

Allgemeine Service-Updates, einschließlich regionaler Verfügbarkeit, Tool-Integrationen und versionsübergreifender Funktionen.

Date	Versionshinweise
29. April 2026	Neues Feature Amazon DocumentDB ist jetzt in der Region Kanada West (Calgary) verfügbar. Weitere Informationen finden Sie in diesem Blog-Beitrag.
17. April 2026	Neues Feature Eine schnellere Skalierung auf DocumentDB serverless ist jetzt verfügbar .
11. Februar 2026	Neues Feature Amazon DocumentDB ist jetzt in der Region Asien-Pazifik (Melbourne) verfügbar. Weitere Informationen finden Sie in diesem Blog-Beitrag. Amazon DocumentDB ist jetzt in der Region Europa (Zürich) verfügbar. Weitere Informationen finden Sie in diesem Blog-Beitrag.
08. Januar 2026	Neues Feature Amazon DocumentDB ist jetzt in der Region Asien-Pazifik (Jakarta) verfügbar. Weitere Informationen finden Sie in diesem Blog-Beitrag.
13. Oktober 2025	Neues Feature Amazon DocumentDB unterstützt jetzt R6G- und T4G-Instances in der Region Asien-Pazifik (Hyderabad). Weitere Informationen finden Sie unter Unterstützte Instance-Klassen nach Region.
7. Oktober 2025	Neues Feature Amazon DocumentDB ist jetzt in den folgenden Regionen verfügbar:

Date	Versionshinweise
	• Asien-Pazifik (Malaysia) • Asien-Pazifik (Osaka) • Asien-Pazifik (Thailand) • Mexiko (Zentral) Weitere Informationen finden Sie in diesem Blog-Beitrag.
26. September 2025	Neue Features Amazon DocumentDB unterstützt jetzt regionsübergreifendes und kontoübergreifendes Kopieren und Teilen von Snapshots. Weitere Informationen erhalten Sie unter Schnappschüsse werden kopiert AWS-Regionen und Amazon DocumentDB-Cluster-Snapshots teilen.
18. Juni 2025	Neues Feature Amazon DocumentDB ist jetzt in der Region Israel (Tel Aviv) verfügbar.
8. Mai 2025	Neues Feature Amazon DocumentDB ist jetzt in der Region Europa (Stockholm) verfügbar. Weitere Informationen finden Sie in diesem Blog-Beitrag.
2. April 2025	Fehlerkorrekturen und andere Änderungen Ein Fehler bei der Erstellung von Vektorindizes mit Hintergrundindizes wurde behoben.
6. Februar 2025	Neues Feature Amazon DocumentDB ist jetzt in integriert AWS Toolkit for Visual Studio Code. Weitere Informationen finden Sie in diesem Blogbeitrag „Was ist neu“ und im AWS Toolkit for Visual Studio Code Benutzerhandbuch unter Arbeiten mit Amazon DocumentDB im Toolkit.

Date	Versionshinweise
22. Oktober 2024	Neues Feature Amazon DocumentDB unterstützt jetzt Durchsatzmetriken für `StorageNetworkReceiveThroughput` Speichern etzwerke`StorageNetworkTransmitThroughput` , und`StorageNetworkThroughput` . Weitere Informationen finden Sie unter Auswertung der Nutzung von Amazon DocumentDB DocumentDB-Instances anhand von Metriken CloudWatch.
18. September 2024	Neues Feature Amazon DocumentDB ist jetzt in der Region Afrika (Kapstadt) verfügbar. Weitere Informationen finden Sie in diesem Blog-Beitrag. Amazon DocumentDB ist jetzt in der Region Europa (Spanien) verfügbar. Weitere Informationen finden Sie in diesem Blog-Beitrag.
25. Juni 2024	Neues Feature Die Authentifizierung mit AWS IAM-ARNs ist in Amazon DocumentDB DocumentDB-Instance-basierten 5.0-Clustern in allen unterstützten Regionen verfügbar. Weitere Informationen finden Sie unter Authentifizierung mit IAM-Identität.
3. April 2024	Neues Feature Amazon DocumentDB ist jetzt in der Region Naher Osten (VAE) verfügbar. Weitere Informationen finden Sie in diesem Blog-Beitrag. Fehlerkorrekturen und andere Änderungen • Ein Fehler beim Aufrufen `db.coll.stats()` auf der Mongo-Shell Version 1.7 und höher wurde behoben. • Es wurde ein Problem mit Speicherlecks bei Change-Stream-Abfragen behoben, die `$regex` als Teil derselben Aggregationspipeline enthalten.

Date	Versionshinweise
30. Januar 2024	Neue Features Globale Amazon DocumentDB-Cluster Globale Cluster sind jetzt in beiden AWS GovCloud (US) Regionen verfügbar: AWS GovCloud (US-East) und AWS GovCloud (US-West).
13. Dezember 2023	Neue Features Unterstützung für 1-Klick-EC2-Konnektivität hinzugefügt. Weitere Informationen finden Sie unter Stellen Sie mithilfe von Amazon EC2 eine Verbindung her.
17. November 2023	Neue Features Amazon DocumentDB ist jetzt in der Region AWS GovCloud (US-East) verfügbar. Weitere Informationen finden Sie in diesem Blog-Beitrag.
25. September 2023	Neue Features Amazon DocumentDB ist jetzt in der Region Asien-Pazifik (Hongkong) verfügbar. Weitere Informationen finden Sie in diesem Blog-Beitrag.
11. September 2023	Neue Features Amazon DocumentDB ist jetzt in der Region Asien-Pazifik (Hyderabad) verfügbar. Weitere Informationen finden Sie in diesem Blog-Beitrag.
29. April 2022	Neue Features Amazon DocumentDB ist jetzt in der Region China (Peking) verfügbar. Weitere Informationen finden Sie in diesem Blog-Beitrag.
16. März 2022	Neue Features Amazon DocumentDB ist jetzt in der Region Europa (Mailand) verfügbar. Weitere Informationen finden Sie in diesem Blog-Beitrag.

Date	Versionshinweise
8. Februar 2022	Neue Features Amazon DocumentDB R6G- und T4G-Instances sind jetzt im asiatisch-pazifischen Raum, Südamerika und Europa verfügbar. Weitere Informationen finden Sie in diesem Blog-Beitrag.
4. Mai 2021	Neue Features In diesem Blogbeitrag finden Sie alle neuen Funktionen.
9. November 2020	Neue Features Alle neuen Funktionen finden Sie in diesem Blogbeitrag.
30. Oktober 2020	Neue Features Alle neuen Funktionen finden Sie in diesem Blogbeitrag.
22. September 2020	Neue Features Alle neuen Funktionen finden Sie in diesem Blogbeitrag.
10. Juli 2020	Neue Features Alle neuen Funktionen finden Sie in diesem Blogbeitrag.
30. Juni 2020	Neue Features Alle neuen Funktionen finden Sie in diesem Blogbeitrag.

Versionshinweise zu Amazon DocumentDB Elastic Clusters

Versionshinweise für Amazon DocumentDB Elastic Clusters.

Date	Versionshinweise
28. Januar 2025	Neues Feature

Date	Versionshinweise
	Für Konnektivität mit einem Klick ist Amazon DocumentDB jetzt AWS CloudShell für instanzbasierte und elastische Cluster integriert. Weitere Informationen finden Sie in einer oder allen der folgenden Seiten: • Erste Schritte mit Amazon DocumentDB • Erste Schritte mit Amazon DocumentDB Elastic Clusters • Was ist ein neuer Blogbeitrag • Blogbeitrag mit technischen Anleitungen
12. November 2024	Neue Features Elastische Amazon DocumentDB-Cluster unterstützen jetzt Hintergrundindizes.
1. November 2024	Neues Feature Amazon DocumentDB unterstützt jetzt Wartungsaktionen für elastische Cluster. Weitere Informationen finden Sie unter Wartung elastischer Amazon DocumentDB-Cluster.
8. August 2024	Neues Feature Elastische Amazon DocumentDB-Cluster sind jetzt in den Regionen Asien-Pazifik (Hongkong), Kanada (Zentral) und Europa (Paris) verfügbar. Weitere Informationen finden Sie unter Regionale Verfügbarkeit für elastische Cluster.
8. Juli 2024	Neues Feature Elastische Amazon DocumentDB-Cluster sind jetzt in der Region Europa (Mailand) verfügbar. Weitere Informationen finden Sie unter Regionale Verfügbarkeit für elastische Cluster.

Date	Versionshinweise
22. Februar 2024	Neue Features Elastische Amazon DocumentDB-Cluster Elastische Amazon DocumentDB-Cluster unterstützen jetzt die folgenden Funktionen: • Lesbare sekundäre Shard-Instance-Replikate — weitere Informationen finden Sie in Schritt 5b von. Schritt 1: Erstellen Sie einen elastischen Cluster • Start/stop Cluster — weitere Informationen finden Sie unter. Stoppen und Starten eines elastischen Amazon DocumentDB-Clusters • Konfigurierbare Shard-Instanzen — weitere Informationen finden Sie in Schritt 5b vonSchritt 1: Erstellen Sie einen elastischen Cluster. • Automatische Backups für Snapshots — weitere Informationen finden Sie unter. Verwaltung eines automatischen Backups eines Elastic Cluster-Snapshots • Snapshot kopieren — weitere Informationen finden Sie unterEinen Elastic Cluster-Snapshot wird kopiert.
30. Januar 2024	Neue Features Elastische Amazon DocumentDB-Cluster Elastische Amazon DocumentDB-Cluster sind jetzt in den folgenden Regionen verfügbar: • Asien-Pazifik (Mumbai) • Asien-Pazifik (Seoul) • Südamerika (São Paulo) • Europa (London) Weitere Informationen finden Sie unter Elastische Cluster-Region und Versionsverfügbarkeit.

Date	Versionshinweise

3. August 2023	Neue Features
	
	Elastische Amazon DocumentDB-Cluster
	
	• Amazon DocumentDB Elastic-Cluster unterstützen jetzt die folgenden Operationen:
	  • `top`
	  • `collStats`
	  • `hint`
	  • `dataSize`
	
	  Die Unterstützte MongoDB-APIs, Operationen und Datentypen in Amazon DocumentDB vollständige Liste der unterstützten Befehle und Operationen finden Sie unter.
	• Time to Live (TTL) -Indizes werden jetzt unterstützt.
	• Indizes `hints` werden jetzt mit Indexausdrücken unterstützt.

22. März 2023	Neue Features Elastische Amazon DocumentDB-Cluster sind jetzt in den Regionen Asien-Pazifik (Singapur), Asien-Pazifik (Sydney) und Asien-Pazifik (Tokio) verfügbar. Weitere Informationen finden Sie unter Elastische Cluster-Region und Versionsverfügbarkeit.

Date	Versionshinweise
30. November 2022	Neue Features Elastische Amazon DocumentDB-Cluster Amazon DocumentDB Elastic Clusters ist ein neuer Typ von Amazon DocumentDB-Cluster, mit dem Benutzer die MongoDB-Sharding-APIs nutzen können, um ihren Cluster zu skalieren. Elastic Cluster verarbeiten praktisch jede Anzahl von Lese- und Schreibvorgängen mit Petabyte an Speicherkapazität, indem sie die Daten und Rechenleistung auf mehrere zugrunde liegende Recheninstanzen und Volumes verteilen. Weitere Informationen finden Sie unter Verwenden von elastischen Amazon DocumentDB-Clustern.

Dokumentenverlauf für den Amazon DocumentDB Developer Guide

- API-Version: 2014-10-31
- Letzte Aktualisierung der Dokumentation: 27. Mai 2026

In der folgenden Tabelle wird die Dokumentation für diese Version des Amazon DocumentDB Developer Guide beschrieben.

Änderung	Beschreibung	Datum
Neues Amazon DocumentDB DocumentDB-Entwicklerhandbuch	Der Amazon DocumentDB Developer Guide wurde jetzt unter einer neuen URL veröffentlicht. Die API-Referenz ist separat unter Amazon DocumentDB API Reference erhältlich.	27. Mai 2026
AWS verwaltetes Richtlinienupdate — Änderung der Richtlinie	Amazon DocumentDB aktualisiert die Vollzugriffsrichtlinien für elastische Cluster.	11. Februar 2025
AWS verwaltetes Richtlinienupdate — Änderung der Richtlinie	Amazon DocumentDB aktualisiert die Vollzugriffsrichtlinien für elastische Cluster.	21. Februar 2024
AWS verwaltetes Richtlinienupdate — Änderung der Richtlinie	Amazon DocumentDB aktualisiert die Richtlinien für Nur-Lese-Zugriff und Vollzugriff für elastische Cluster.	21. Juni 2023
AWS verwaltetes Richtlinienupdate — neue Richtlinie	Amazon DocumentDB führt eine neue Nur-Lese-Richtlinie für elastische Cluster ein.	08. Juni 2023

AWS verwaltetes Richtlinienupdate — neue Richtlinie	Amazon DocumentDB führt eine neue Vollzugriffsrichtlinie für elastische Cluster ein.	5. Juni 2023
MongoDB 5.0-Kompatibilität	Amazon DocumentDB ist jetzt mit Version 5.0 von MongoDB kompatibel.	1. März 2023
Aktualisierung der Richtlinien	Um die Elastic Cluster-Funktion von Amazon DocumentDB zu unterstützen, AmazonDocDB-ElasticServiceRolePolicy wird die AmazonDocDBConsoleFullAccess Richtlinie aktualisiert und eingeführt.	30. November 2022
Elastische Cluster	Neue Elastic Cluster-Funktion hinzugefügt, die Hash-basierte Partitionierung (Sharding) von Daten im verteilten Speichersystem von Amazon DocumentDB unterstützt.	30. November 2022
Globale Cluster	Es wurde eine Dokumentation zur Verwendung von Global Clusters hinzugefügt.	2. Juni 2021
Abonnements für Veranstaltungen	Dokumentation für Event-Abonnements hinzugefügt.	26. März 2021
Aktualisierungen auf Version 3.6	Dokumentierte Verbesserungen gegenüber Version 3.6 in Bezug auf rollenbasierte Zugriffskontrollen, Aggregationsoperatoren und Leistung.	15. Januar 2021

MongoDB 4.0-Kompatibilität	Amazon DocumentDB ist jetzt mit Version 4.0 von MongoDB kompatibel.	9. November 2020
Leitfäden für die ersten Schritte	Neue Anleitungen für die ersten Schritte mit Amazon DocumentDB mithilfe von Amazon EC2 AWS Cloud9, Robo3T oder Studio3T.	15. August 2020
Zusätzliche Availability Zones werden unterstützt	Amazon DocumentDB hat Unterstützung für eine zusätzliche Availability Zone im asiatisch-pazifischen Raum (Seoul) hinzugefügt (ap-north east-2).	14. Juli 2020
Unterstützung für das Kopieren von Schnappsc hüssen zwischen Regionen hinzugefügt.	Amazon DocumentDB hat Unterstützung für das Kopieren von Cluster-S napshots hinzugefügt. AWS-Regionen Weitere Informationen finden Sie unter Kopieren von Snapshots zwischen Regionen.	10. Juli 2020
Unterstützung für die Instanzkl asse T3 wurde hinzugefügt.	Unterstützung für T3-Instan ce-Typen in allen Regionen hinzugefügt, die Amazon DocumentDB unterstüt zen. Weitere Informationen finden Sie unter Unterstützte Instance-Klassen nach Region und Instance-Klassensp ezifikationen.	30. Juni 2020

Unterstützung für hinzugefügt AWS GovCloud (US).	Amazon DocumentDB ist jetzt in der AWS GovCloud (US) Region (us-gov-west-1) verfügbar.	29. Juni 2020
16 neue Metriken wurden hinzugefügt. CloudWatch	Amazon DocumentDB hat Unterstützung für 16 neue CloudWatch Amazon-Metriken hinzugefügt. Weitere Informationen finden Sie unter Amazon DocumentDB überwachen mit CloudWatch.	23. Juni 2020
Unterstützung für Null-Zeichen und den $regex-Operator wurde hinzugefügt.	Amazon DocumentDB hat Unterstützung für Nullzeichen in Zeichenketten und die Möglichkeit hinzugefügt, einen Index für $regex zu verwenden. Informationen zu den unterstützten MongoDB-APIs und Aggregationspipeline-Funktionen für Amazon DocumentDB finden Sie unter Funktionale Unterschiede zu MongoDB.	22. Juni 2020

Unterstützung für verbesserte Multi-Key-Indexierungsfunktionen hinzugefügt.	Amazon DocumentDB hat Unterstützung für verbesserte Multi-Key-Indexierungsfunktionen hinzugefügt, darunter die Indizierung von Arrays mit mehr als 2.048 Byte und die Möglichkeit, einen zusammengesetzten Multi-Key-Index mit mehreren Schlüsseln im selben Array zu erstellen. Weitere Informationen finden Sie unter Funktionsunterschiede bei MongoDB.	23. April 2020
Unterstützung für den Löschschutz für einen Amazon DocumentDB CloudFormation DocumentDB-Stack hinzugefügt.	Amazon DocumentDB hat Unterstützung für die Aktivierung des Löschschutzes bei der Erstellung eines Amazon DocumentDB CloudFormation DocumentDB-Stacks hinzugefügt.	20. April 2020
Unterstützung für rollenbasierte Zugriffskontrolle hinzugefügt.	Amazon DocumentDB hat Unterstützung für die rollenbasierte Zugriffskontrolle mithilfe integrierter Rollen hinzugefügt.	26. März 2020
Unterstützung für eine zusätzliche Availability Zone in Kanada (Central) (ca-central-1) hinzugefügt.	Amazon DocumentDB ist jetzt in der Region Kanada (Central) (ca-central-1) mit Instances der Klasse R5 und 3 Availability Zones verfügbar.	26. März 2020

Unterstützung für zwei zusätzliche MongoDB-APIs hinzugefügt.	Amazon DocumentDB hat Unterstützung für `$dateFromString` und `executionStats` MongoDB-APIs hinzugefügt.	23. März 2020
Unterstützung für fünf weitere MongoDB-APIs hinzugefügt.	Amazon DocumentDB hat Unterstützung für`$objectToArray` ,, `$arrayToObject` `$slice` `$mod`, und `$range` MongoDB-APIs hinzugefügt.	6. Februar 2020
Unterstützung für Kanada (Central) hinzugefügt.	Amazon DocumentDB ist jetzt in der Region Kanada (Central) (ca-central-1) mit Instances der Klasse R5 verfügbar.	11. Dezember 2019
ChangeStreamLogSizeUnterstützung für hinzugefügt.	Amazon DocumentDB hat Unterstützung `ChangeStreamLogSize` für Cloudwatch-Metriken hinzugefügt.	22. November 2019
Unterstützung für die Region Europa (Paris) hinzugefügt	Amazon DocumentDB ist jetzt in der Region Europa (Paris) (eu-west-3) mit Instances der Klasse R5 verfügbar.	30. Oktober 2019
Unterstützung für die Region Asien-Pazifik (Mumbai) wurde hinzugefügt	Amazon DocumentDB ist jetzt in der Region Asien-Pazifik (Mumbai) (ap-south-1) mit Instances der Klasse R5 verfügbar.	17. Oktober 2019

Unterstützung für drei zusätzliche MongoDB-APIs hinzugefügt	Amazon DocumentDB hat Unterstützung für die APIs `$addFields` `$concatArrays` , und `$lookup` MongoDB hinzugefügt.	16. Oktober 2019
Unterstützung für die Region Asien-Pazifik (Singapur) hinzugefügt	Amazon DocumentDB ist jetzt in der Region Asien-Pazifik (Singapur) (ap-southeast-1) mit Instances der Klasse R5 verfügbar.	14. Oktober 2019
Neues Dokument für die Aktualisierung von TLS-Zertifikaten hinzugefügt	Anweisungen zum Aktualisieren von Zertifizierungsstellenzertifikaten zur Verwendung des neuen Zertifizierungsstellenzertifikats zum Erstellen von TLS-Verbindungen wurden hinzugefügt.	2. Oktober 2019
API-Unterstützung für Zertifikate hinzugefügt	Amazon DocumentDB ist ein neuer Zertifikatsdatentyp für Instances. Weitere Informationen finden Sie unter DBInstance.	1. Oktober 2019
Support für die Erstellung von Abfrageprofilen	Amazon DocumentDB hat die Möglichkeit hinzugefügt, unterstützte Operationen auf den Instances und Datenbanken Ihres Clusters zu profilieren.	19. August 2019

Dritte AZ im asiatisch-pazifischen Raum (Tokio) hinzugefügt	Amazon DocumentDB hat eine dritte Availability Zone (AZ) für Ihre Compute-Instances im asiatisch-pazifischen Raum (Tokio) hinzugefügt.	9. August 2019
Support für zusätzliche Mongo-APIs	Unterstützung für zusätzliche Funktionen der Aggregationspipeline hinzugefügt, zu denen die Aggregationsoperatoren `$in` `$isoWeek` `$isoWeekYear` `$isoDayOfWeek` , , und die `$dateToString` `$addToSet` Aggregationsphase gehören. Amazon DocumentDB hat außerdem Unterstützung für den `top()` Befehl zur Diagnose auf Sammlungsebene und die Möglichkeit hinzugefügt, den `expireAfterSeconds` Parameter für TTL-Indizes mithilfe des Befehls zu ändern. `collMod()`	31. Juli 2019
Unterstützung für Europa (London) hinzugefügt	Amazon DocumentDB ist jetzt in Europa (London) (eu-west-2) mit Instances der Klasse R5 verfügbar.	18. Juli 2019
Codebeispiele wurden hinzugefügt	In R und Ruby wurden Codebeispiele für die programmgesteuerte Verbindung zu Amazon DocumentDB hinzugefügt.	17. Juli 2019

Bewährtes Verfahren hinzugefügt	Es wurde eine Best Practice hinzugefügt, die Ihnen hilft, Ihre Amazon DocumentDB DocumentDB-Kosten zu verwalten.	17. Juli 2019
Support für das Stoppen und Starten eines Clusters	Amazon DocumentDB hat Unterstützung für das Stoppen und Starten von Clustern hinzugefügt, um die Kosten für Entwicklungs- und Testumgebungen zu verwalten.	1. Juli 2019
Support für den Schutz vor Clusterlöschung	Um Ihre Cluster vor versehentlichem Löschen zu schützen, hat Amazon DocumentDB einen Löschschutz hinzugefügt. Weitere Informationen finden Sie in den folgenden Themen: Erstellen eines Amazon DocumentDB-Clusters, Ändern eines Amazon DocumentDB-Clusters, Löschen eines Amazon DocumentDB-Clusters und `DeletionProtection` im API-Thema DBCluster.	1. Juli 2019
Aktualisierung der funktionalen Unterschiede	Implizite Transaktionen wurden den Funktionsunterschieden hinzugefügt.	26. Juni 2019
Hinzufügung funktionaler Unterschiede	Hinweis zur Speicherung und Indexkomprimierung in Amazon DocumentDB hinzugefügt.	13. Juni 2019

Zusätzliche Region wird unterstützt	Amazon DocumentDB ist jetzt im asiatisch-pazifischen Raum (Sydney) (ap-southeast-2) mit Instances der Klasse R5 verfügbar.	5. Juni 2019
Die R5-Instance-Klasse wird in weiteren Regionen unterstützt	Unterstützung für R5-Instance-Klasse für 4 zusätzliche Regionen hinzugefügt: USA Ost (Ohio), USA Ost (Nord-Virginia), USA West (Oregon) und EU (Irland). Mit dieser Änderung werden R5-Instances in allen Regionen unterstützt, die Amazon DocumentDB unterstützen.	17. Mai 2019
Zusätzliche Regionen werden unterstützt	Unterstützung für zwei weitere Regionen, Asien-Pazifik (Tokio) (ap-northeast-1) und Asien-Pazifik (Seoul) (ap-northeast-2), mit R5-Instance-Klassen hinzugefügt. Weitere Informationen finden Sie unter Unterstützte Instance-Klassen nach Region und Instance-Klassen-Spezifikationen.	8. Mai 2019
Weitere Beispiele für Verbindungscodes wurden hinzugefügt	Es wurden Codebeispiele in Java und C# für die Verbindung mit Amazon DocumentDB hinzugefügt.	24. April 2019

Zusätzliche Mongo-API-Unterstützung	Es wurde die Unterstützung von sieben Aggregations-Zeichenfolgenoperatoren (`$indexOfBytes`, `$indexOfCP`, `$strLenBytes`, `$strLenCP`, `$toLower`, `$toUpper`, `$split`), neun Datumszeitoperatoren (`$dayOfYear`, `$dayOfMonth`, `$dayOfWeek`, `$year`, `$month`, `$hour`, `$minute`, `$second`, `$millisecond`) und die Aggregations-Pipeline-Stufe `$sample` hinzugefügt.	4. April 2019
Beispiele für Verbindungscodes wurden hinzugefügt	Es wurden Codebeispiele in Python Node.js, PHP und Go für die Verbindung mit Amazon DocumentDB hinzugefügt.	21. März 2019
Support für die Region Frankfurt und R5-Instances	Unterstützung für die Region Europa (Frankfurt) (eu-central-1) mit R5-Instance-Klassen hinzugefügt. Weitere Informationen finden Sie unter Unterstützte Instance-Klassen nach Region und Instance-Klassen-Spezifikationen.	13. März 2019

Unterstützung von Aggregationspipeline-Operatoren	Es wurde die Unterstützung für neue Aggregations-Zeichenfolgenoperatoren (`$concat`, `$substr`, `$substrBytes` , `$substrCP` , `$strcasecmp`), einen Array-Aggregationsoperator (`$size`), einen Aggregationsgruppen-Akkumulatoroperator (`$push`) und Aggregationsstufen (`$redact` und `$indexStats`) hinzugefügt. Wir haben außerdem die Unterstützung für Positional-Array-Operatoren (`$[]` und `$[<identifier>]`) und `hint()` hinzugefügt.	28. Februar 2019
Motor-Upgrades	Es wurde eine Dokumentation zur Ermittlung ausstehender Cluster-Änderungen und Aktualisierung der Engine Version Ihres Clusters hinzugefügt.	15. Februar 2019
Ereignisse prüfen	Unterstützung für die Prüfung von Datenbankereignissen mit Amazon CloudWatch Logs hinzugefügt.	12. Februar 2019
Schnellstart	Es wurde ein Schnellstart-Thema hinzugefügt, das Ihnen den Einstieg in Amazon DocumentDB erleichtert. CloudFormation	11. Januar 2019

Öffentliche Veröffentlichung	Dies ist die erste öffentliche Version von Amazon DocumentDB (mit MongoDB-Kompatibilität). Diese Version enthält den Entwicklerleitfaden und die integrierte API-Referenz für das Ressourcenmanagement.	9. Januar 2019

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.