



Guida per gli sviluppatori

Amazon DocumentDB



Amazon DocumentDB: Guida per gli sviluppatori

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

I marchi e l'immagine commerciale di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in una qualsiasi modalità che possa causare confusione tra i clienti o in una qualsiasi modalità che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà delle rispettive aziende, che possono o meno essere associate, collegate o sponsorizzate da Amazon.

Table of Contents

Cos'è Amazon DocumentDB	1
Panoramica	1
Cluster	3
Istanze	4
Regioni e zone di disponibilità	6
Regioni	6
Zone di disponibilità	7
Prezzi	9
Versione di prova gratuita	10
Monitoraggio	10
Interfacce	10
AWS Management Console	10
AWS CLI	10
Shell Mongo	11
Driver MongoDB	11
Fasi successive	11
Come funziona	11
Endpoint Amazon DocumentDB	13
Supporto per TLS	17
Archiviazione Amazon DocumentDB	17
Replica Amazon DocumentDB	18
Affidabilità di Amazon DocumentDB	18
Opzioni per le preferenze di lettura	20
Eliminazioni TTL	24
Risorse fatturabili	25
Cos'è un database di documenti?	28
Casi d'uso	28
Comprensione dei documenti	29
Utilizzo dei documenti	35
Guida introduttiva	48
Prerequisiti	49
Fase 1: Creare un AWS Cloud9 ambiente	50
Fase 2: creazione di un gruppo di sicurezza	51
Fase 3: creare un cluster Amazon DocumentDB	54

Passaggio 4: installa la shell mongo	56
Fase 5: Connettiti al tuo cluster Amazon DocumentDB	57
Fase 6: Inserimento e interrogazione dei dati	59
Fase 7: Esplora	61
Quick Start con AWS CloudFormation	62
Prerequisiti	63
Autorizzazioni IAM richieste	63
Coppia di chiavi Amazon EC2	65
Avvio di uno stack Amazon DocumentDB AWS CloudFormation	65
Accesso al cluster Amazon DocumentDB	70
Protezione da cessazione ed eliminazione	71
Compatibilità con MongoDB	72
Compatibilità con MongoDB 5.0	72
Novità di Amazon DocumentDB 5.0	72
Inizia a usare Amazon DocumentDB 5.0	73
Aggiornamento o migrazione ad Amazon DocumentDB 4.0	74
Differenze funzionali	74
Compatibilità con MongoDB 4.0	75
Caratteristiche di Amazon DocumentDB 4.0	76
Inizia a usare Amazon DocumentDB 4.0	77
Aggiornamento o migrazione ad Amazon DocumentDB 4.0	77
Differenze funzionali	78
Transazioni	79
Requisiti	79
Best practice	79
Restrizioni	80
Monitoraggio e diagnostica	81
Livello di isolamento della transazione	82
Casi d'uso	82
Transazioni con più rendiconti	82
Transazioni di raccolta multipla	84
Esempi di API di transazione per l'API di callback	86
Esempi di API di transazione per l'API principale	86
Comandi supportati	119
Funzionalità non supportate	120
Sessioni	120

Consistenza causale	121
Scritture ritrattabili	122
Errori di transazione	122
Best practice	124
Linee guida operative di base	124
Dimensione delle istanze	125
Utilizzo degli indici	127
Creazione degli indici	127
Selettività dell'indice	127
Impatto degli indici sulla scrittura dei dati	128
Identificazione degli indici mancanti	128
Identificazione degli indici non utilizzati	128
Best practice di sicurezza	129
Ottimizzazione dei costi	129
Utilizzo di parametri per identificare problemi a livello di prestazioni	130
Visualizzazione dei parametri relativi alle prestazioni	130
Impostazione di una sveglia CloudWatch	131
Valutazione dei parametri relativi alle prestazioni	131
Ottimizzazione di query	133
Carichi di lavoro di serie temporali e TTL	133
Migrazioni	134
Utilizzo di gruppi di parametri di cluster	134
Query di pipeline di aggregazione	134
batchInsert e batchUpdate	134
Differenze funzionali con MongoDB	135
Vantaggi funzionali di Amazon DocumentDB	135
Transazioni implicite	135
Differenze funzionali aggiornate	136
Indicizzazione di matrici	137
Indici multi-chiave	138
Caratteri null nelle stringhe	139
Controllo accessi basato sui ruoli	139
Indicizzazione \$regex	139
Proiezione per documenti annidati	140
Differenze funzionali con MongoDB	140
Operatore \$vectorSearch	141

OpCountersCommand	141
Raccolte e database di amministrazione	141
cursormaxTimeMS	141
explain()	141
Restrizioni per i nomi dei campi	142
Creazione degli indici	142
Ricerca con chiave vuota nel percorso	143
API, operazioni e tipi di dati di MongoDB	143
mongodumpe mongorestore Utilità	143
Ordinamento dei risultati	144
Scritture ripetibili	144
Indici Sparse	145
Utilizzo di \$elemMatch all'interno di un'espressione \$all	145
\$ne,\$nin,\$nor, \$not\$exists, e indicizzazione \$elemMatch	146
\$lookup	146
API, operazioni e tipi di dati di MongoDB supportati	151
Comandi del database	151
Comandi amministrativi	152
Aggregazione	153
Autenticazione	154
Comandi di diagnostica	154
Operazioni di query e scrittura	155
Comandi di gestione di ruoli	156
Comandi delle sessioni	157
Gestione degli utenti	157
Comandi di sharding	158
Operatori per query e proiezioni	160
Operatori per matrice	160
Operatori bit per bit	160
Operatore per commenti	161
Operatori di confronto	161
Operatori per elementi	162
Operatori per query di valutazione	162
Operatori logici	162
Operatori per proiezioni	163
Operatori per aggiornamenti	163

Operatori per matrice	163
Operatori bit per bit	164
Operatori per campi	164
Modificatori per aggiornamenti	165
Dati geospaziali	165
Specificatori di geometria	165
Selettori di query	166
Metodi per cursori	166
Operatori per pipeline di aggregazione	168
Espressioni per accumulatori	169
Operatori aritmetici	170
Operatori per matrice	171
Operatori booleani	172
Operatori di confronto	172
Operatori per espressioni condizionali	172
Operatori per tipi di dati	173
Operatore di dimensione dei dati	173
Operatori per date	173
Operatore letterale	174
Operatori di unione	174
Operatore naturale	175
Operatori su set	175
Operatori per fasi	175
Operatori di stringa	177
Variabili di sistema	178
Operatore per ricerca testo	179
Operatori di conversione dei tipi	179
Operatori per variabili	180
Operatori vari	180
Tipi di dati	180
Indici e proprietà indice	181
Indici	182
Proprietà indice	182
AI generativa	183
SageMaker Tela	183
Come creare modelli ML senza codice con Canvas SageMaker	183

Configurazione del dominio e del profilo utente SageMaker	184
Configurazione delle autorizzazioni di accesso IAM per Amazon DocumentDB e Canvas SageMaker	184
Creazione di utenti e ruoli del database per Canvas SageMaker	185
Regioni disponibili	185
Ricerca vettoriale	186
Inserimento di vettori	186
Creazione di un indice vettoriale	187
Ottenere una definizione dell'indice	192
Interrogazione dei vettori	193
Caratteristiche e limitazioni	197
Best practice	199
Migrazione ad Amazon DocumentDB	200
Migrazione tra versioni	200
Fase 1: abilitare Change Streams	201
Fase 2: modifica la durata di conservazione di Change Streams	201
Fase 3: Migrazione degli indici	202
Fase 4: Creare un'istanza di AWS DMS replica	203
Fase 5: Creare un AWS DMS endpoint di origine	206
Passaggio 6: creare un endpoint di AWS DMS destinazione	208
Passaggio 7: Creare ed eseguire un'attività di migrazione	210
Fase 8: Modifica dell'endpoint dell'applicazione nel cluster Amazon DocumentDB di destinazione	212
Strumenti di migrazione	212
AWS Database Migration Service	212
Utility della riga di comando	213
Individuazione	213
Pianificazione: requisiti del cluster Amazon DocumentDB	217
Approcci per la migrazione	220
Offline	220
Online	222
Ibrido	223
Origini della migrazione	225
Connettività per la migrazione	226
Test in corso	228
Considerazioni sul test del piano di migrazione	229

Test delle performance	232
Verifica del failover	232
Risorse aggiuntive	233
Playbook sulla migrazione	233
Processo di migrazione	233
Risorse aggiuntive	238
Aggiornamento della versione di Amazon DocumentDB Engine	239
Prerequisiti e limitazioni	240
Procedure consigliate per gli aggiornamenti immediati delle versioni principali	243
Testa sul posto gli aggiornamenti delle versioni principali utilizzando cluster clonati	243
Prima di un aggiornamento immediato della versione principale	243
Durante un aggiornamento immediato della versione principale	245
Dopo un aggiornamento immediato della versione principale	246
Esecuzione di un aggiornamento immediato della versione principale	248
Risoluzione dei problemi relativi all'aggiornamento di una versione principale in corso	251
Differenze tra i cluster aggiornati da Amazon DocumentDB da 3.6/4.0 a 5.0 e i nuovi cluster Amazon DocumentDB 5.0	251
Sicurezza	253
Protezione dei dati	254
Crittografia lato client a livello di campo lato client a	255
Crittografia dei dati inattivi	263
Crittografia dei dati in transito	268
Gestione delle chiavi	279
Identity and Access Management	279
Destinatari	280
Autenticazione con identità	281
Gestione dell'accesso con policy	284
Come funziona Amazon DocumentDB con IAM	287
Esempi di policy basate su identità	295
Risoluzione dei problemi	298
Gestione delle autorizzazioni di accesso alle risorse Amazon DocumentDB	300
Utilizzo di policy basate su identità (policy IAM)	306
AWS politiche gestite per Amazon DocumentDB	310
Riferimento per le autorizzazioni dell'API Amazon DocumentDB	328
Gestione degli utenti Amazon DocumentDB	337
Principale eserviceadmin utente	337

Creazione di utenti aggiuntivi	338
Rotazione automaticamente delle password	340
Controllo accessi basato sui ruoli	341
Concetti RBAC	342
Guida introduttiva ai ruoli integrati RBAC	344
Guida introduttiva ai ruoli RBAC definiti dall'utente	347
Connessione ad Amazon DocumentDB come utente	352
Comandi comuni	353
Differenze funzionali	358
Limiti	359
Accesso al database mediante il controllo degli accessi basato sui ruoli	359
Registrazione e monitoraggio	364
Aggiornamento dei certificati	364
Aggiornamento dell'applicazione e del cluster Amazon DocumentDB	365
Risoluzione dei problemi	369
Domande frequenti	369
Aggiornamento dei certificati — GovCloud (US-West)	376
Aggiornamento dell'applicazione e del cluster Amazon DocumentDB	365
Risoluzione dei problemi	369
Domande frequenti	369
Convalida della conformità	387
Resilienza	388
Sicurezza dell'infrastruttura	389
Best practice di sicurezza	390
Audit degli eventi	391
Eventi supportati	392
Abilitazione dell'audit	397
Disabilitazione dell'audit	404
Accesso agli eventi di audit	406
Backup e ripristino	408
Backup e ripristino: concetti	409
Informazioni sull'utilizzo dello storage di backup	411
Dump, ripristino, importazione ed esportazione di dati	412
mongodump	413
mongoexport	414
mongoexport	414

mongoimport	415
Tutorial	415
Considerazioni sulle snapshot del cluster	418
Storage di backup	419
Finestra di backup	419
Periodo di retention dei backup	421
Copiare Cluster Snapshot Encryption	421
Confronto tra snapshot automatiche e manuali	422
Creazione di una snapshot del cluster manuale	424
Copia di una snapshot del cluster	427
Copia di snapshot condivise	428
Copiare istantanee da una parte all'altra Regioni AWS	428
Limitazioni	428
Gestione della crittografia	429
Considerazioni sui gruppi di parametri	429
Copia di una snapshot del cluster	429
Condivisione di uno snapshot di un cluster	437
Condivisione di uno snapshot crittografato	437
Condivisione di una snapshot	441
Ripristino da una snapshot del cluster	442
Ripristino a un punto temporale specifico	450
Eliminazione di una snapshot del cluster	456
Gestione di Amazon DocumentDB	459
Panoramica sulle attività operative	459
Aggiunta di una replica a un cluster Amazon DocumentDB	460
Descrizione di cluster e istanze	461
Creazione di una snapshot del cluster	463
Ripristino da una snapshot	464
Rimozione di un'istanza da un cluster	465
Eliminazione di un cluster	465
Cluster globali	466
Cos'è un cluster globale?	466
In che modo sono utili i cluster globali?	466
Quali sono gli attuali limiti dei cluster globali?	467
Quick Start Guide	468
Gestione di cluster globali	484

Connessione di cluster globali	492
Monitoraggio dei cluster globali	492
Ripristino di emergenza	493
Gestione dei cluster	496
Comprendere i cluster	496
Impostazioni del cluster	499
Configurazioni di storage in cluster	502
Determinazione dello stato di un cluster	505
Ciclo di vita del cluster	506
Scalabilità dei cluster	549
Clonazione di un volume per un cluster	552
Comprendere la tolleranza agli errori del cluster	565
Gestione delle istanze	567
Gestione delle classi delle istanze	567
Determinazione dello stato di un'istanza	577
Ciclo di vita dell'istanza	577
Gestione di gruppi di sottoreti	601
Creazione di un gruppo di sottoreti	602
Descrizione di un gruppo di sottoreti	608
Modifica di un gruppo di sottoreti	611
Eliminazione di un gruppo di sottoreti	614
Alta disponibilità e replica	615
Dimensionamento della lettura	616
Elevata disponibilità	616
Aggiunta di repliche di	618
Failover	618
Ritardo di replica	623
Gestione degli indici	624
Creazione di indici Amazon DocumentDB	624
Gestione della compressione dei documenti	630
Linee guida	630
Attivazione della compressione dei documenti	630
Monitoraggio della compressione dei documenti	631
Gestione delle collezioni esistenti	632
Gestione degli eventi DB DB	632
Visualizzazione delle categorie di eventi DB DB	633

Visualizzazione Amazon DocumentDB	635
Scelta di regioni e zone di disponibilità	638
Disponibilità nelle regioni	639
Gestione dei gruppi di parametri del cluster	641
Descrizione dei gruppi di parametri del cluster	641
Creazione di gruppi di parametri del cluster	648
Modifica dei gruppi di parametri del cluster	651
Modifica dei cluster per utilizzare gruppi di parametri di cluster personalizzati	656
Copia dei gruppi di parametri del cluster	657
Reimpostazione dei gruppi di parametri del cluster	660
Eliminazione di gruppi di parametri del cluster	662
Riferimento ai parametri del cluster	665
Informazioni sugli endpoint	681
Ricerca degli endpoint del cluster	681
Ricerca di un endpoint dell'istanza	684
Connessione agli endpoint	687
Informazioni sugli ARN di Amazon DocumentDB	689
Costruzione di un ARN	689
Ricerca di un ARN	692
Tagging di risorse	694
Panoramica sui tag delle risorse di	695
Vincoli per i tag	696
Aggiunta o aggiornamento dei tag	696
Come elencare i tag	698
Rimozione tag	699
Manutenzione di Amazon DocumentDB	701
Determinazione delle operazioni di manutenzione in attesa	702
Determinazione delle azioni di manutenzione in sospeso	703
Applicazione degli aggiornamenti dei motori	705
Aggiornamenti avviati dall'utente	709
Gestione delle finestre di manutenzione	710
Aggiornamenti del sistema operativo	712
Comprendere i ruoli collegati ai servizi	716
Autorizzazioni del ruolo collegato ai servizi	716
Creazione di un ruolo collegato ai servizi	718
Modifica di un ruolo collegato ai servizi	718

Eliminazione del ruolo collegato ai servizi	719
Regioni supportate per i ruoli collegati ai servizi di Amazon DocumentDB	720
Utilizzo dei cluster elastici di Amazon DocumentDB	721
Casi d'uso del cluster elastico	721
Profili utente	722
Gestione dei contenuti e record storici	722
Vantaggi dei cluster elastici	722
AWS integrazione dei servizi	722
Disponibilità di regioni e versioni	723
Disponibilità nelle regioni	723
Disponibilità della versione	723
Limitazioni	724
Gestione elastica dei cluster	724
Operazioni di interrogazione e scrittura	724
Gestione della raccolta e dell'indice	725
Amministrazione e diagnostica	725
Funzionalità di attivazione	725
Come funziona	725
Sharding elastico dei cluster di Amazon DocumentDB	726
Migrazione elastica dei cluster	730
Scalabilità elastica dei cluster	730
Affidabilità elastica del cluster	730
Archiviazione e disponibilità di cluster elastici	730
Differenze funzionali tra Amazon DocumentDB 4.0 e cluster elastici	731
Inizia a usare	732
Configurazione	733
Fase 1: Creare un cluster elastico	734
Fase 2: Creare un ambiente AWS Cloud9	741
Passaggio 3: installa la shell mongo	744
Fase 4: Connect al nuovo cluster elastico	745
Fase 5: Condividi la tua raccolta; inserisci e interroga i dati	746
Best practice	748
Scelta delle chiavi di	748
Gestione delle connessioni	749
Raccolte non condivise	749
Dimdelle	749

Mon	750
Gestione dei cluster elastici	750
Modifica delle configurazioni dei cluster elastici	751
Monitoraggio di un cluster elastico	754
Eliminazione di un cluster elastico	758
Gestione delle istantanee dei cluster elastici	760
Arresto e avvio di un cluster elastico	775
Crittografia dei dati memorizzati	780
In che modo i cluster elastici di Amazon DocumentDB utilizzano le sovvenzioni in AWS	
KMS	782
Creazione di una chiave gestita dal cliente	782
Monitoraggio delle chiavi di crittografia per i cluster elastici Amazon DocumentDB	784
Ulteriori informazioni	789
Ruoli collegati ai servizi	790
Autorizzazioni di ruolo collegate ai servizi per i cluster elastici	790
Monitoraggio Amazon DocumentDB	794
Monitoraggio dello stato di un cluster	795
Valori dello stato del cluster	796
Monitoraggio dello stato di un cluster	797
Monitoraggio dello stato di un'istanza	799
Valori di stato delle istanze	800
Monitoraggio dello stato dell'istanza utilizzandoAWS Management Console oAWS CLI	802
Valori dello stato di integrità dell'istanza	804
Monitoraggio dello stato di integrità dell'istanza utilizzando ilAWS Management Console	805
Visualizzazione dei suggerimenti Amazon DocumentDB	806
Abbonamenti a eventi	809
Sottoscrizione agli eventi	810
Gestione delle sottoscrizioni	813
Categorie e messaggi	817
Monitoraggio di Amazon DocumentDB con CloudWatch	820
Parametri di Amazon DocumentDB	821
Visualizzazione CloudWatch Dati	834
Dimensioni Amazon DocumentDB	840
Monitoraggio degli opcounter	840
Monitoraggio delle connessioni al database	841
Registrazione delle chiamate API di Amazon CloudTrail	841

Informazioni su Amazon DocumentDB in CloudTrail	841
Operazioni di profiling	842
Operazioni supportate	843
Restrizioni	844
Abilitazione del profiler	844
Disabilitazione del profiler	849
Disabilitazione dell'esportazione dei log del profiler	850
Accesso ai log del profiler	852
Query comuni	852
Monitoraggio con Performance Insights	853
Concetti di Performance Insights	854
Abilitazione e disattivazione di Performance Insights	858
Configurazione delle policy di accesso per Performance Insights	861
Per analizzare il parametro utilizzando il pannello di controllo di Performance Insights	866
Recupero dei parametri con l'API Performance Insights	884
CloudWatch Metriche Amazon per Performance Insights	899
Performance Insights per le contrometriche	901
Sviluppo con Amazon DocumentDB	904
Connessione a livello di programmazione	904
Determinazione del valore <code>tls</code>	905
Connessione con TLS abilitato	907
Connessione con TLS disabilitato	921
Utilizzo dei flussi di modifica	929
Operazioni supportate	930
Fatturazione	931
Restrizioni	931
Abilitazione dei flussi di modifica	931
Esempio	933
Ricerca di un documento completo	936
Ripresa di un flusso di modifiche	937
Ripresa di un flusso di modifiche <code>constartAtOperationTime</code>	938
Transazioni nei flussi di modifica	940
Modifica della durata di conservazione del registro del flusso di modifica	940
Usando AWS Lambda con Change Streams	944
Restrizioni	945
Utilizzo della convalida dello schema JSON	945

Creazione e utilizzo della convalida dello schema JSON	945
Parole chiave supportate	954
Limitazioni	955
Connessione come set di repliche	955
Utilizzo delle connessioni del cluster	958
Pool di connessione multipli	959
Riepilogo	960
Connessione dall'esterno di un Amazon VPC	960
Connect tramite Studio 3T	962
Prerequisiti	962
Connect con Studio 3T	962
Connect usando DataGrip	973
Prerequisiti	973
Connect usando DataGrip	974
DataGrip caratteristiche	980
Connect tramite Amazon EC2	981
Prerequisiti	981
Connect Amazon EC2 automaticamente	983
Connect Amazon EC2 manualmente	1006
Connect tramite il driver JDBC	1023
Nozioni di base	1024
Connect da Tableau Desktop	1025
Connect da DbVisualizer	1029
Generazione automatica di schemi JDBC	1031
Support SQL e limitazioni	1040
Risoluzione dei problemi	1041
Connect tramite driver ODBC	1041
Nozioni di base	1041
Configurazione del driver ODBC in Windows	1043
Connect da Microsoft Excel	1048
Connect da Microsoft Power BI	1050
Generazione automatica di schemi	1056
Supporto SQL e limitazioni	1057
Risoluzione dei problemi	1057
Quote e limiti	1058
Tipi di istanze supportati	1058

Regioni supportate	1060
Quote regionali	1061
Limiti di aggregazione	1064
Limiti del cluster	1064
Limiti di istanze	1066
Vincoli per la denominazione	1069
Vincoli TTL	1071
Limiti elastici del cluster	1071
Limiti degli shard del cluster elastico	1072
Limiti di CPU, memoria, connessione e cursore del cluster elastico per shard	1072
Esecuzione di query	1074
Interrogazione di documenti	1074
Recupero di tutti i documenti	1075
Valori di campo corrispondenti	1075
Documenti incorporati	1075
Valori dei campi nei documenti incorporati	1076
Corrispondenza a un array	1076
Valori corrispondenti in una matrice	1076
Utilizzo degli operatori	1077
Piano di query	1077
Piano di query	1077
Cache del piano di query	1079
Spiega i risultati	1079
Fase di scansione e filtro	1080
Intersezione dell'indice	1081
Unione dell'indice	1082
Intersezione/unione di indici multipli	1083
Indice composto	1083
Fase di ordinamento	1084
Fase a gironi	1084
Dati geospaziali	1084
Panoramica	1
Indicizzazione e archiviazione di dati geospaziali	1085
Esecuzione di query su dati geospaziali	1087
Limitazioni	1091
Indice parziale	1091

Crea un indice parziale	1091
Operatori supportati	1091
Interrogazione utilizzando un indice parziale	1092
Funzionalità di indicizzazione parziale	1093
Limitazioni parziali dell'indice	1097
Ricerca testuale	1098
Funzionalità supportate	1098
Utilizzo dell'indice di testo di Amazon DocumentDB	1099
Differenze con MongoDB	1104
Migliori pratiche e linee guida	1105
Limitazioni	1105
Risoluzione dei problemi	1106
Problemi di connessione	1106
Impossibile connettersi a un endpoint Amazon DocumentDB	1106
Test della connessione a un'istanza Amazon DocumentDB	1111
Connessione a un endpoint non valido	1112
Creazione dell'indice	1113
La compilazione dell'indice non riesce	1113
Problemi di latenza e errori di compilazione dell'indice in background	1114
Prestazioni e utilizzo delle risorse	1114
Visualizza le statistiche di inserimento, aggiornamento ed eliminazione	1115
Analizza le prestazioni della cache	1116
Trovare e terminare le query bloccate o con esecuzione prolungata	1118
Visualizzare un piano di query e ottimizzare una query	1119
Come posso visualizzare un piano di query in cluster elastici?	1121
Creare l'elenco di tutte le operazioni in esecuzione su un'istanza	1124
Sapere quando una query sta avanzando	1126
Determinare il motivo per cui un sistema viene improvvisamente eseguito lentamente	1129
Determinare la causa dell'utilizzo elevato della CPU	1131
Trova i cursori aperti su un'istanza	1132
Visualizza la versione corrente del motore di Amazon DocumentDB	1132
Analizza l'utilizzo degli indici e identifica gli indici non utilizzati	1133
Identifica gli indici mancanti	1135
Riepilogo delle domande utili	1137
Documentazione di riferimento sulle API per la gestione delle risorse	1139
Azioni	1139

Amazon DocumentDB (with MongoDB compatibility)	1142
Cluster elastici Amazon DocumentDB	1321
Tipi di dati	1384
Amazon DocumentDB (with MongoDB compatibility)	1386
Cluster elastici Amazon DocumentDB	1466
Errori comuni	1481
Parametri comuni	1482
Note di rilascio	1485
3 aprile 2024	1486
Nuove funzionalità	1487
Correzioni di bug e altre modifiche	1487
22 febbraio 2024	1488
Nuove funzionalità	1488
30 gennaio 2024	1488
Nuove funzionalità	1488
10 gennaio 2024	1489
Nuove funzionalità	1489
Correzioni di bug e altre modifiche	1490
20 dicembre 2023	1490
Altre modifiche	1490
13 dicembre 2023	1490
Nuove funzionalità	1490
29 novembre 2023	1491
Nuove funzionalità	1491
21 novembre 2023	1491
Nuove funzionalità	1491
17 novembre 2023	1491
Nuove funzionalità	1491
Correzioni di bug e altre modifiche	1491
6 novembre 2023	1492
Nuove funzionalità	1492
Correzioni di bug e altre modifiche	1492
20 ottobre 2023	1492
Altre modifiche	1492
25 settembre 2023	1493
Nuove funzionalità	1493

20 settembre 2023	1493
Nuove funzionalità	1493
15 settembre 2023	1493
Nuove funzionalità	1493
11 settembre 2023	1493
Nuove funzionalità	1493
3 agosto 2023	1494
Nuove funzionalità	1494
13 luglio 2023	1494
Nuove funzionalità	1494
Correzioni di bug e altre modifiche	1494
7 giugno 2023	1495
Correzioni di bug e altre modifiche	1495
10 maggio 2023	1495
Correzioni di bug e altre modifiche	1495
4 aprile 2023	1495
Correzioni di bug e altre modifiche	1495
22 marzo 2023	1496
Nuove funzionalità	1496
1 marzo 2023	1496
Nuove funzionalità	1496
27 febbraio 2023	1497
Correzioni di bug e altre modifiche	1497
2 febbraio 2023	1497
Correzioni di bug e altre modifiche	1497
30 novembre 2022	1498
Nuove funzionalità	1498
9 agosto 2022	1498
Nuove funzionalità	1498
Correzioni di bug e altre modifiche	1498
25 luglio 2022	1499
Nuove funzionalità	1499
27 giugno 2022	1499
Nuove funzionalità	1499
29 aprile 2022	1499
Nuove funzionalità	1499

7 aprile 2022	1499
Nuove funzionalità	1499
16 marzo 2022	1500
Nuove funzionalità	1500
8 febbraio 2022	1500
Nuove funzionalità	1500
24 gennaio 2022	1500
Nuove funzionalità	1500
21 gennaio 2022	1501
Nuove funzionalità	1501
25 ottobre 2021	1501
Nuove funzionalità	1501
Correzioni di bug e altre modifiche	1502
24 giugno 2021	1502
Nuove funzionalità	1502
4 maggio 2021	1502
Nuove funzionalità	1502
Correzioni di bug e altre modifiche	1503
15 gennaio 2021	1503
Nuove funzionalità	1503
9 novembre 2020	1504
Nuove funzionalità	1504
Correzioni di bug e altre modifiche	1505
30 ottobre 2020	1506
Nuove funzionalità	1506
Correzioni di bug e altre modifiche	1506
22 settembre 2020	1507
Nuove funzionalità	1507
Correzioni di bug e altre modifiche	1507
10 luglio 2020	1507
Nuove funzionalità	1507
Correzioni di bug e altre modifiche	1507
30 giugno 2020	1508
Nuove funzionalità	1508
Correzioni di bug e altre modifiche	1508
Cronologia dei documenti	1509

..... mdxxi

Cos'è Amazon DocumentDB (con compatibilità con MongoDB)

Amazon DocumentDB (con compatibilità con MongoDB) è un servizio di database veloce, affidabile e completamente gestito. Amazon DocumentDB semplifica la configurazione, il funzionamento e la scalabilità di database compatibili con MongoDB nel cloud. Con Amazon DocumentDB, puoi eseguire lo stesso codice applicativo e utilizzare gli stessi driver e strumenti che usi con MongoDB.

Prima di utilizzare Amazon DocumentDB, è necessario esaminare i concetti e le funzionalità descritti in [Come funziona](#). Successivamente, completa la procedura in [Guida introduttiva](#).

Argomenti

- [Panoramica di Amazon DocumentDB](#)
- [Cluster](#)
- [Istanze](#)
- [Regioni e zone di disponibilità](#)
- [Prezzi di Amazon DocumentDB](#)
- [Monitoraggio](#)
- [Interfacce](#)
- [Fasi successive](#)
- [Amazon DocumentDB: come funziona](#)
- [Cos'è un database di documenti?](#)

Panoramica di Amazon DocumentDB

Di seguito sono riportate alcune funzionalità di alto livello di Amazon DocumentDB:

- Amazon DocumentDB supporta due tipi di cluster: cluster basati su istanze e cluster elastici. I cluster elastici supportano carichi di lavoro con milioni di letture/scritture al secondo e petabyte di capacità di storage. Per ulteriori informazioni sui cluster elastici, consulta [Utilizzo dei cluster elastici di Amazon DocumentDB](#). Il contenuto seguente si riferisce ai cluster basati su istanze di Amazon DocumentDB.
- Amazon DocumentDB aumenta automaticamente le dimensioni del volume di storage in base alle esigenze di storage del database. Il volume di storage aumenta con incrementi di 10 GB, fino a un

massimo di 128 TiB. Non è necessario assegnare risorse di storage aggiuntive al cluster per far fronte alla crescita futura.

- Con Amazon DocumentDB, puoi aumentare la velocità di lettura per supportare richieste di applicazioni ad alto volume creando fino a 15 istanze di replica. Le repliche di Amazon DocumentDB condividono lo stesso storage sottostante, riducendo i costi ed evitando la necessità di eseguire scritture sui nodi di replica. Questa funzionalità libera più potenza di elaborazione per soddisfare le richieste di lettura e riduce il tempo di replica, spesso fino a millisecondi a una cifra. È possibile aggiungere repliche in pochi minuti indipendentemente dalle dimensioni del volume di archiviazione. Amazon DocumentDB fornisce anche un endpoint di lettura, in modo che l'applicazione possa connettersi senza dover tenere traccia delle repliche man mano che vengono aggiunte e rimosse.
- Amazon DocumentDB ti consente di aumentare o ridurre le risorse di calcolo e memoria per ciascuna istanza. Le operazioni di dimensionamento delle risorse di calcolo in genere vengono completate in pochi minuti.
- Amazon DocumentDB viene eseguito in Amazon Virtual Private Cloud (Amazon VPC), quindi puoi isolare il database nella tua rete virtuale. Puoi anche configurare le impostazioni del firewall per controllare l'accesso di rete al cluster.
- Amazon DocumentDB monitora continuamente lo stato del cluster. In caso di errore dell'istanza, Amazon DocumentDB riavvia automaticamente l'istanza e i processi associati. Amazon DocumentDB non richiede la riproduzione in caso di crash recovery dei redo log del database, il che riduce notevolmente i tempi di riavvio. Amazon DocumentDB isola inoltre la cache del database dal processo del database, permettendo alla cache di sopravvivere al riavvio dell'istanza.
- In caso di errore dell'istanza, Amazon DocumentDB automatizza il failover su una delle 15 repliche di Amazon DocumentDB create in altre zone di disponibilità. Se non è stata fornita alcuna replica e si verifica un errore, Amazon DocumentDB tenta di creare automaticamente una nuova istanza di Amazon DocumentDB.
- La funzionalità di backup in Amazon DocumentDB consente point-in-time il ripristino del cluster. Questa caratteristica consente di ripristinare il cluster a qualsiasi momento compreso nel periodo di retention, fino agli ultimi 5 minuti. Puoi configurare il periodo di retention dei backup automatico fino a 35 giorni. I backup automatici sono archiviati in Amazon Simple Storage Service (Amazon S3), progettato per una durabilità del 99,99999%. I backup di Amazon DocumentDB sono automatici, incrementali e continui e non hanno alcun impatto sulle prestazioni del cluster.
- Con Amazon DocumentDB, puoi crittografare i tuoi database utilizzando chiavi create e controllate tramite AWS Key Management Service (AWS KMS). In un cluster di database che utilizza la

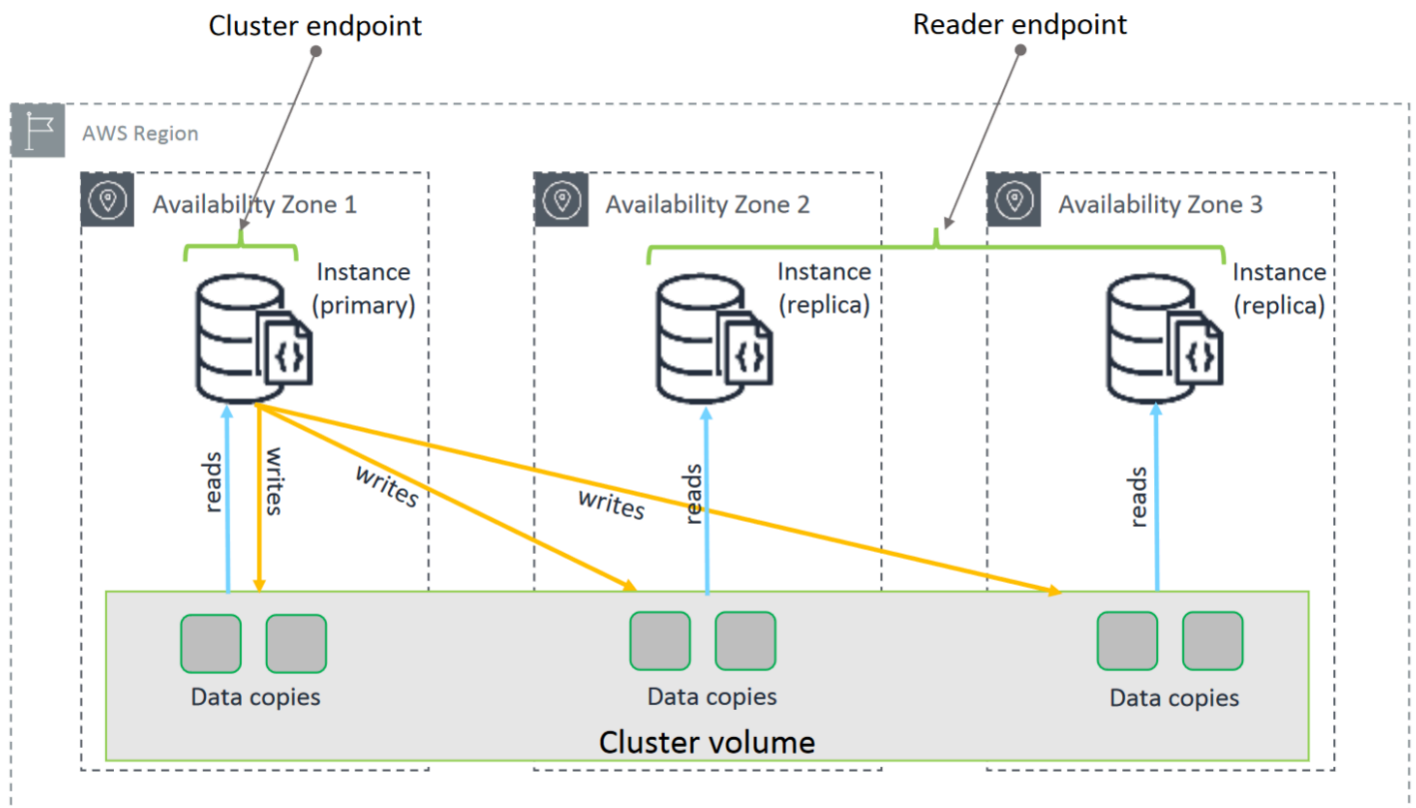
crittografia Amazon DocumentDB, i dati archiviati inattivi nello storage sottostante sono crittografati. Vengono crittografati anche i backup, le snapshot e le repliche automatici nello stesso cluster.

Se non conosci i AWS servizi, utilizza le seguenti risorse per saperne di più:

- AWS offre servizi per l'elaborazione, i database, l'archiviazione, l'analisi e altre funzionalità. Per una panoramica di tutti i AWS servizi, consulta [Cloud Computing con Amazon Web Services](#).
- AWS fornisce una serie di servizi di database. Per indicazioni su quale servizio è più adatto al tuo ambiente, consulta [Databases on AWS](#).

Cluster

Un cluster è composto da 0 a 16 istanze e da un volume di storage del cluster che gestisce i dati per tali istanze. Tutte le operazioni di scrittura vengono eseguite tramite l'istanza primaria. Tutte le istanze (primaria e repliche) supportano le operazioni di lettura. I dati del cluster vengono archiviati nel volume cluster e copiati in tre diverse zone di disponibilità.



I cluster basati su istanze di Amazon DocumentDB 5.0 supportano due configurazioni di storage per un cluster di database: Amazon DocumentDB standard e Amazon DocumentDB con I/O ottimizzato. Per ulteriori informazioni, consulta [Configurazioni di storage in cluster Amazon DocumentDB](#).

Istanze

Un'istanza Amazon DocumentDB è un ambiente di database isolato nel cloud. Un'istanza può contenere più database creati dall'utente. Puoi creare e modificare un'istanza utilizzando AWS Management Console o il AWS CLI.

La capacità di calcolo e di memoria di un'istanza è determinata dalla relativa classe di istanza. Puoi selezionare l'istanza più adatta alle tue esigenze. Se le esigenze cambiano nel corso del tempo, puoi scegliere un'altra classe di istanza. Per le specifiche per la classe di istanza, consulta [Specifiche per la classe di istanza](#).

Le istanze di Amazon DocumentDB vengono eseguite solo nell'ambiente Amazon VPC. Amazon VPC ti offre il controllo del tuo ambiente di rete virtuale: puoi scegliere il tuo intervallo di indirizzi IP, creare sottoreti e configurare il routing e le liste di controllo degli accessi (ACL).

Prima di poter creare istanze di Amazon DocumentDB, devi creare un cluster che contenga le istanze.

Non tutte le classi delle istanze sono supportate in ogni regione. La tabella riportata di seguito specifica quali classi delle istanze sono supportate in ciascuna regione.

Classi di istanze supportate per regione

Regione	R6G	R5	R4	T4G	T3
Stati Uniti orientali (Ohio)	Supportato	Supportato	Supportato	Supportato	Supportato
Stati Uniti orientali (Virginia settentrionale)	Supportato	Supportato	Supportato	Supportato	Supportato
US West (Oregon)	Supportato	Supportato	Supportato	Supportato	Supportato

Regione	R6G	R5	R4	T4G	T3
Sud America (San Paolo)	Supportato o	Supportato o		Supportato o	Supportato o
Asia Pacifico (Hong Kong)	Supportato o	Supportato o		Supportato o	Supportato o
Asia Pacifico (Hyderabad)		Supportato o			Supportato o
Asia Pacifico (Mumbai)	Supportato o	Supportato o		Supportato o	Supportato o
Asia Pacifico (Seul)	Supportato o	Supportato o		Supportato o	Supportato o
Asia Pacifico (Sydney)	Supportato o	Supportato o		Supportato o	Supportato o
Asia Pacifico (Singapore)	Supportato o	Supportato o		Supportato o	Supportato o
Asia Pacifico (Tokyo)	Supportato o	Supportato o		Supportato o	Supportato o
Canada (Centrale)	Supportato o	Supportato o		Supportato o	Supportato o
Europa (Francoforte)	Supportato o	Supportato o		Supportato o	Supportato o
Europa (Irlanda)	Supportato o	Supportato o	Supportato	Supportato o	Supportato o
Europa (Londra)	Supportato o	Supportato o		Supportato o	Supportato o
Europa (Milano)	Supportato o	Supportato o		Supportato o	Supportato o

Regione	R6G	R5	R4	T4G	T3
Europa (Parigi)	Supportato	Supportato		Supportato	Supportato
	o	o		o	o
Medio Oriente (Emirati Arabi Uniti)	Supportato	Supportato		Supportato	Supportato
	o	o		o	o
Regione Cina (Pechino)	Supportato	Supportato		Supportato	Supportato
	o	o		o	o
Cina (Ningxia)	Supportato	Supportato		Supportato	Supportato
	o	o		o	o
AWS GovCloud (Stati Uniti occidentali)	Supportato	Supportato		Supportato	Supportato
	o	o		o	o
AWS GovCloud (Stati Uniti orientali)	Supportato	Supportato		Supportato	Supportato
	o	o		o	o

Regioni e zone di disponibilità

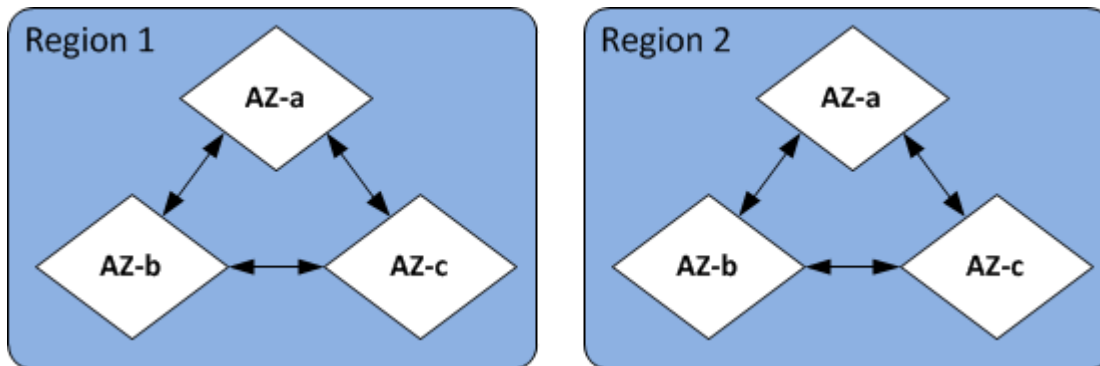
Regioni e zone di disponibilità definiscono le posizioni fisiche del cluster e delle istanze.

Regioni

AWS Le risorse di cloud computing sono ospitate in strutture di data center ad alta disponibilità in diverse aree del mondo (ad esempio, Nord America, Europa o Asia). L'ubicazione di ogni data center è chiamata regione.

Ogni AWS regione è progettata per essere completamente isolata dalle altre AWS regioni. All'interno di ciascuna regione sono presenti più zone di disponibilità. Avviando i nodi in diverse zone di

disponibilità, puoi ottenere la massima tolleranza ai guasti possibile. Il diagramma seguente mostra una panoramica di alto livello del funzionamento delle AWS regioni e delle zone di disponibilità.



Zone di disponibilità

Ogni AWS regione contiene più località distinte chiamate zone di disponibilità. Ogni zona di disponibilità è progettata per essere isolata dagli errori che si verificano in altre zone di disponibilità e per offrire connettività di rete conveniente e a bassa latenza ad altre zone di disponibilità nella stessa regione. Avviando istanze per un determinato cluster in più zone di disponibilità, è possibile proteggere le applicazioni dall'improbabile evento di errore di una zona di disponibilità.

L'architettura Amazon DocumentDB separa storage ed elaborazione. Per il livello di storage, Amazon DocumentDB replica sei copie dei dati in tre AWS zone di disponibilità. Ad esempio, se stai avviando un cluster Amazon DocumentDB in una regione che supporta solo due zone di disponibilità, lo storage dei dati verrà replicato in sei modi su tre zone di disponibilità, ma le tue istanze di calcolo saranno disponibili solo in due zone di disponibilità.

La tabella seguente elenca il numero di zone di disponibilità che è possibile utilizzare in una determinata area Regione AWS per fornire istanze di calcolo per il cluster.

Nome della regione	Regione	Zone di disponibilità (elaborazione)
Stati Uniti orientali (Ohio)	us-east-2	3
Stati Uniti orientali (Virginia settentrionale)	us-east-1	6
US West (Oregon)	us-west-2	4

Nome della regione	Regione	Zone di disponibilità (elaborazione)
Sud America (São Paulo)	sa-east-1	3
Asia Pacifico (Hong Kong)	ap-east-1	3
Asia Pacifico (Hyderabad)	ap-south-2	3
Asia Pacifico (Mumbai)	ap-south-1	3
Asia Pacifico (Seul)	ap-northeast-2	4
Asia Pacifico (Singapore)	ap-southeast-1	3
Asia Pacifico (Sydney)	ap-southeast-2	3
Asia Pacifico (Tokyo)	ap-northeast-1	3
Canada (Centrale)	ca-central-1	3
Regione Cina (Pechino)	cn-north-1	3
Cina (Ningxia)	cn-northwest-1	3
Europa (Francoforte)	eu-central-1	3
Europa (Irlanda)	eu-west-1	3
Europa (Londra)	eu-west-2	3
Europa (Milano)	eu-south-1	3
Europa (Parigi)	eu-west-3	3

Nome della regione	Regione	Zone di disponibilità (elaborazione)
Medio Oriente (Emirati Arabi Uniti)	me-central-1	3
AWS GovCloud (Stati Uniti occidentali)	us-gov-west-1	3
AWS GovCloud (Stati Uniti orientali)	us-gov-east-1	3

Prezzi di Amazon DocumentDB

I cluster Amazon DocumentDB vengono fatturati in base ai seguenti componenti:

- **Ore di istanza (all'ora):** in base alla classe di istanza dell'istanza (ad esempio, db.r5.xlarge). I prezzi sono calcolati in base a una tariffa oraria, mentre le fatture sono calcolate al secondo e mostrano i valori in formato decimale. L'utilizzo di Amazon DocumentDB viene fatturato in incrementi di un secondo, con un minimo di 10 minuti. Per ulteriori informazioni, consulta [Gestione delle classi delle istanze](#).
- **Richieste di I/O (per 1 milione di richieste al mese):** numero totale di richieste di I/O di storage effettuate in un ciclo di fatturazione.
- **Storage di backup (per GiB al mese):** lo storage di backup è lo storage associato ai backup automatici del database e a tutte le istantanee attive del database che sono state scattate. Estendendo il periodo di retention dei backup o creando ulteriori snapshot del database, si aumenta lo storage di backup consumato dal database. Lo storage di backup viene calcolato in GB al mese e non si applica il calcolo al secondo. Per ulteriori informazioni, consulta [Backup e ripristino in Amazon DocumentDB](#).
- **Trasferimento dati (per GB):** trasferimento di dati in entrata e in uscita dall'istanza da o verso Internet o altre regioni. AWS

Per informazioni dettagliate, consulta i prezzi di [Amazon DocumentDB](#).

Versione di prova gratuita

Puoi provare Amazon DocumentDB gratuitamente utilizzando la versione di prova gratuita di 1 mese. Per ulteriori informazioni, consulta la sezione Prova gratuita nei [prezzi di Amazon DocumentDB](#) o consulta le domande frequenti sulla versione di prova gratuita di [Amazon DocumentDB](#).

Monitoraggio

Esistono vari modi per tenere traccia delle prestazioni e dello stato di un'istanza. Puoi utilizzare il CloudWatch servizio Amazon gratuito per monitorare le prestazioni e lo stato di un'istanza. Puoi trovare i grafici delle prestazioni sulla console Amazon DocumentDB. Puoi iscriverti agli eventi di Amazon DocumentDB per ricevere notifiche quando si verificano modifiche con un'istanza, uno snapshot, un gruppo di parametri o un gruppo di sicurezza.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- [Monitoraggio di Amazon DocumentDB con CloudWatch](#)
- [Registrazione delle chiamate API di AmazonAWS CloudTrail](#)

Interfacce

Esistono diversi modi per interagire con Amazon DocumentDB, tra cui il AWS Management Console e il. AWS CLI

AWS Management Console

AWS Management Console È una semplice interfaccia utente basata sul Web. La gestione delle istanze e dei cluster dalla console non richiede alcuna programmazione. [Per accedere alla console Amazon DocumentDB, accedi AWS Management Console e apri la console Amazon DocumentDB all'indirizzo `https://console.aws.amazon.com/docdb`.](#)

AWS CLI

Puoi usare il AWS Command Line Interface (AWS CLI) per gestire i cluster e le istanze di Amazon DocumentDB. Con una configurazione minima, puoi iniziare a utilizzare tutte le funzionalità fornite dalla console Amazon DocumentDB dal tuo programma terminale preferito.

- Per installare AWS CLI, consulta [Installazione dell'interfaccia a riga di AWS comando](#).

- Per iniziare a utilizzare AWS CLI per Amazon DocumentDB, consulta [AWS Command Line Interface Reference for Amazon DocumentDB](#).

Shell Mongo

Per connetterti al tuo cluster per creare, leggere, aggiornare ed eliminare documenti nei tuoi database, puoi usare la mongo shell con Amazon DocumentDB. Per scaricare e installare la shell mongo 4.0, consulta [Passaggio 4: installa la shell mongo](#).

Driver MongoDB

Per sviluppare e scrivere applicazioni su un cluster Amazon DocumentDB, puoi anche utilizzare i driver MongoDB con Amazon DocumentDB.

Fasi successive

Nelle sezioni precedenti sono stati presentati i componenti di base dell'infrastruttura offerti da Amazon DocumentDB. Cosa potrai fare dopo? A seconda delle circostanze, consulta uno dei seguenti argomenti per iniziare:

- Inizia a usare Amazon DocumentDB creando un cluster e un'istanza utilizzando. AWS CloudFormation [Guida rapida all'uso di Amazon DocumentDB AWS CloudFormation](#)
- Inizia a usare Amazon DocumentDB creando un cluster e un'istanza utilizzando le istruzioni contenute nel nostro. [Guida introduttiva](#)
- Inizia a usare Amazon DocumentDB creando un cluster elastico seguendo le istruzioni contenute in. [Inizia a usare i cluster elastici di Amazon DocumentDB](#)
- Esegui la migrazione dell'implementazione di MongoDB ad Amazon DocumentDB utilizzando le indicazioni disponibili all'indirizzo [Migrazione ad Amazon DocumentDB](#)

Amazon DocumentDB: come funziona

Amazon DocumentDB (compatibile con MongoDB) è un servizio di database completamente gestito e compatibile con MongoDB. Con Amazon DocumentDB, puoi eseguire lo stesso codice applicativo e utilizzare gli stessi driver e strumenti che usi con MongoDB. Amazon DocumentDB è compatibile con MongoDB 3.6, 4.0 e 5.0.

Argomenti

- [Endpoint Amazon DocumentDB](#)
- [Supporto per TLS](#)
- [Archiviazione Amazon DocumentDB](#)
- [Replica Amazon DocumentDB](#)
- [Affidabilità di Amazon DocumentDB](#)
- [Opzioni per le preferenze di lettura](#)
- [Eliminazioni TTL](#)
- [Risorse fatturabili](#)

Quando usi Amazon DocumentDB, inizi con la creazione di un cluster. Un cluster è composto da una o più istanze database e da un volume cluster per la gestione dei dati di tali istanze. Un volume cluster Amazon DocumentDB è un volume di storage di database virtuale che si estende su più zone di disponibilità. Ogni zona di disponibilità ha una copia dei dati del cluster.

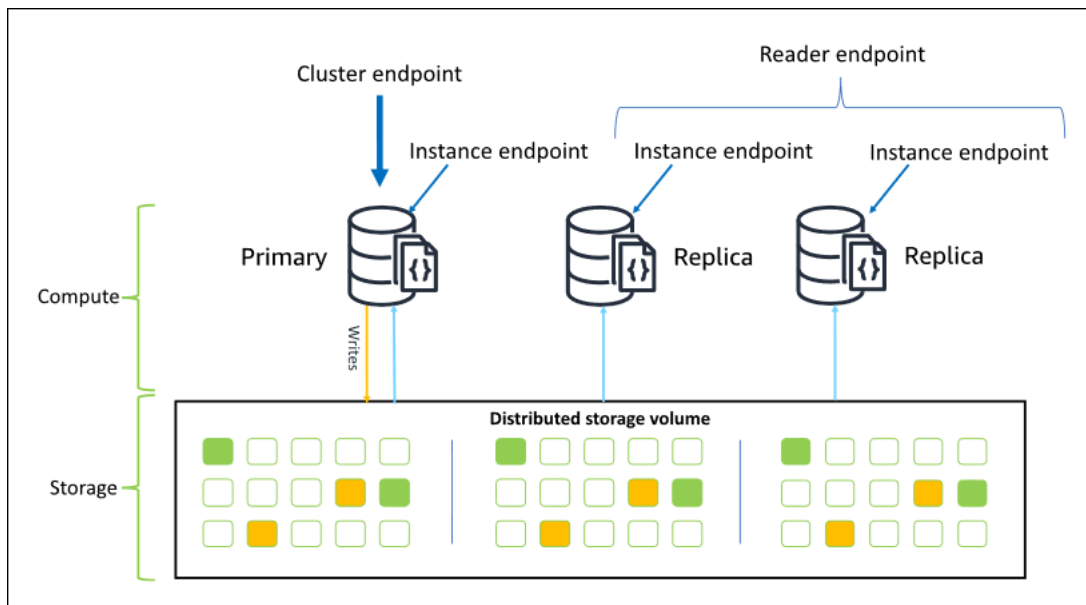
Un cluster Amazon DocumentDB è composto da due componenti:

- **Volume del cluster:** utilizza un servizio di storage nativo del cloud per replicare i dati in sei modi su tre zone di disponibilità, fornendo uno storage altamente durevole e disponibile. Un cluster Amazon DocumentDB ha esattamente un volume cluster, che può archiviare fino a 128 TiB di dati.
- **Istanze:** forniscono la potenza di elaborazione per il database, la scrittura e la lettura dei dati dal volume di storage del cluster. Un cluster Amazon DocumentDB può avere da 0 a 16 istanze.

Le istanze sono utilizzate per uno dei due ruoli:

- **Istanza primaria:** supporta operazioni di lettura e scrittura ed esegue tutte le modifiche ai dati sul volume del cluster. Ogni cluster Amazon DocumentDB ha un'istanza principale.
- **Istanza di replica:** supporta solo operazioni di lettura. Un cluster Amazon DocumentDB può avere fino a 15 repliche oltre all'istanza principale. La presenza di più repliche consente di distribuire i carichi di lavoro di lettura. Inoltre, è sufficiente collocare le repliche in zone di disponibilità separate per aumentare anche la disponibilità del cluster.

Il diagramma seguente illustra la relazione tra il volume del cluster, l'istanza principale e le repliche in un cluster Amazon DocumentDB:



Le istanze cluster non devono appartenere alla stessa classe di istanza e possono essere sottoposte a provisioning e terminate in base alle esigenze. Questa architettura consente di aumentare la capacità di calcolo del cluster in modo indipendente dallo storage.

Quando l'applicazione scrive i dati in un'istanza primaria, questa istanza esegue una scrittura durevole nel volume cluster. Quindi replica lo stato di quella scrittura (non i dati) su ogni replica attiva. Le repliche di Amazon DocumentDB non partecipano all'elaborazione delle scritture e pertanto le repliche di Amazon DocumentDB sono vantaggiose per il ridimensionamento della lettura. Le letture dalle repliche di Amazon DocumentDB alla fine sono coerenti con un ritardo di replica minimo, in genere meno di 100 millisecondi dopo la scrittura dei dati da parte dell'istanza principale. La funzionalità garantisce che le letture dalle repliche vengano lette nell'ordine con cui sono state scritte nell'istanza primaria. Il ritardo della replica varia a seconda della percentuale di variazione dei dati e i periodi con un'intensa attività di scrittura potrebbero aumentare il ritardo della replica. Per ulteriori informazioni, consulta la pagina relativa ai parametri `ReplicationLag` in [Parametri di Amazon DocumentDB](#).

Endpoint Amazon DocumentDB

Amazon DocumentDB offre diverse opzioni di connessione per soddisfare un'ampia gamma di casi d'uso. Per connetterti a un'istanza in un cluster Amazon DocumentDB, devi specificare l'endpoint dell'istanza. Un endpoint è formato da un indirizzo host e da un numero di porta, separati da due punti.

Ti consigliamo di connetterti al cluster utilizzando l'endpoint del cluster e in modalità set di replica (vedi [Connessione ad Amazon DocumentDB come set di repliche](#)), a meno che non hai un caso d'uso specifico per la connessione all'endpoint del lettore o a un endpoint di istanza. Per instradare le richieste alle repliche, scegli un'impostazione di preferenza di lettura del driver che massimizza il dimensionamento della lettura nel rispetto dei requisiti di coerenza di lettura dell'applicazione. La preferenza di lettura `secondaryPreferred` consente la lettura delle repliche e libera l'istanza primaria per eseguire ulteriori operazioni.

I seguenti endpoint sono disponibili da un cluster Amazon DocumentDB.

Endpoint del cluster

L'endpoint del cluster consente la connessione all'istanza primaria corrente del cluster. L'endpoint del cluster può essere utilizzato per le operazioni di lettura e scrittura. Un cluster Amazon DocumentDB ha esattamente un endpoint del cluster.

L'endpoint del cluster fornisce il supporto per il failover per le connessioni in lettura e scrittura al cluster. Se l'istanza primaria corrente del cluster non riesce e il cluster ha almeno una replica di lettura attiva, l'endpoint del cluster reindirizza automaticamente le richieste di connessione a una nuova istanza primaria. Quando ti connetti al cluster Amazon DocumentDB, ti consigliamo di connetterti al cluster utilizzando l'endpoint del cluster e in modalità set di repliche (vedi). [Connessione ad Amazon DocumentDB come set di repliche](#)

Di seguito è riportato un esempio di endpoint del cluster Amazon DocumentDB:

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

Di seguito è riportato un esempio della stringa di connessione che utilizza questo endpoint del cluster:

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

Per ulteriori informazioni sulla ricerca di un endpoint del cluster, consulta [Ricerca degli endpoint del cluster](#).

Endpoint lettore

L'endpoint lettore bilancia il carico delle connessioni di sola lettura in tutte le repliche disponibili nel cluster. Il tentativo di eseguire un'operazione di scrittura con una connessione all'endpoint lettore genera un errore. Un cluster Amazon DocumentDB ha esattamente un endpoint di lettura.

Se il cluster contiene solo un'istanza (primaria), l'endpoint lettore si connette all'istanza primaria. Quando aggiungi un'istanza di replica al tuo cluster Amazon DocumentDB, l'endpoint di lettura apre connessioni di sola lettura alla nuova replica dopo che è attiva.

Di seguito è riportato un esempio di endpoint di lettura per un cluster Amazon DocumentDB:

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

Di seguito è riportato un esempio della stringa di connessione che utilizza un endpoint lettore:

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

L'endpoint lettore bilancia il carico delle connessioni di sola lettura, non delle richieste di lettura. Se alcune connessioni dell'endpoint lettore vengono utilizzate più di altre, le richieste di lettura potrebbero non essere equamente divise tra le istanze nel cluster. Si consiglia di distribuire le richieste collegandosi all'endpoint del cluster come set di repliche e utilizzando l'opzione preferenza di lettura `secondaryPreferred`.

Per ulteriori informazioni sulla ricerca di un endpoint del cluster, consulta [Ricerca degli endpoint del cluster](#).

Endpoint dell'istanza

Un endpoint dell'istanza si connette a un'istanza specifica all'interno del cluster. L'endpoint dell'istanza per l'istanza primaria corrente può essere utilizzato per le operazioni di lettura e scrittura. Tuttavia, il tentativo di eseguire operazioni di scrittura su un endpoint dell'istanza per una replica di lettura genera un errore. Un cluster Amazon DocumentDB ha un endpoint di istanza per istanza attiva.

Un endpoint dell'istanza fornisce il controllo diretto sulle connessioni a una specifica istanza per scenari in cui l'utilizzo di endpoint lettore o del cluster potrebbe non essere appropriato. Un caso d'uso di esempio è il provisioning per un carico di lavoro di analisi di sola lettura periodico. Puoi effettuare il provisioning di un'istanza di `larger-than-normal` replica, connetterti direttamente alla nuova istanza più grande con il relativo endpoint di istanza, eseguire le query di analisi e quindi terminare l'istanza. L'utilizzo dell'endpoint dell'istanza evita che il traffico delle analisi influisca negativamente sulle altre istanze del cluster.

Di seguito è riportato un esempio di endpoint di istanza per una singola istanza in un cluster Amazon DocumentDB:

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

Di seguito è riportato un esempio della stringa di connessione che utilizza questo endpoint dell'istanza:

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

Note

Il ruolo di un'istanza primaria o di replica può variare a causa di un evento di failover. Le applicazioni non devono mai presupporre che un determinato endpoint dell'istanza sia l'istanza primaria. Non è consigliabile connettersi agli endpoint dell'istanza per le applicazioni di produzione. È consigliabile invece connettersi al cluster utilizzando l'endpoint del cluster e in modalità set di repliche (vedi [Connessione ad Amazon DocumentDB come set di repliche](#)). Per un controllo più avanzato sulla priorità di failover delle istanze, consulta [Comprendere la tolleranza agli errori del cluster Amazon DocumentDB](#).

Per ulteriori informazioni sulla ricerca di un endpoint del cluster, consulta [Ricerca di un endpoint dell'istanza](#).

Modalità per i set di repliche

È possibile connettersi all'endpoint del cluster Amazon DocumentDB in modalità set di repliche specificando il nome del set di repliche. `rs0` La connessione con la modalità per i set di repliche consente di specificare le opzioni per Read Concern, Write Concern e Read Preference. Per ulteriori informazioni, consulta [Consistenza di lettura](#).

Di seguito è riportato un esempio della stringa di connessione connessa con la modalità per i set di repliche:

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

Quando ti connetti in modalità set di repliche, il cluster Amazon DocumentDB appare ai driver e ai client come un set di repliche. Le istanze aggiunte e rimosse dal cluster Amazon DocumentDB si riflettono automaticamente nella configurazione del set di repliche.

Ogni cluster Amazon DocumentDB è costituito da un singolo set di repliche con il nome predefinito. `rs0` Il nome del set di repliche non può essere modificato.

La connessione all'endpoint del cluster con la modalità per i set di repliche è il metodo consigliato per l'uso generale.

Note

Tutte le istanze in un cluster Amazon DocumentDB ascoltano le connessioni sulla stessa porta TCP.

Supporto per TLS

Per ulteriori dettagli sulla connessione ad Amazon DocumentDB utilizzando Transport Layer Security (TLS), consulta [Crittografia dei dati in transito](#)

Archiviazione Amazon DocumentDB

I dati di Amazon DocumentDB sono archiviati in un volume cluster, che è un singolo volume virtuale che utilizza unità a stato solido (SSD). Un volume cluster è composto da sei copie dei dati, che vengono replicate automaticamente su più zone di disponibilità in un'unica copia. Regione AWS Questa replica contribuisce a garantire l'estrema durata dei tuoi dati e a ridurre il rischio di perdita dei dati. Consente inoltre di assicurare che il cluster non sia più disponibile durante un failover perché le copie dei dati sono già presenti in altre zone di disponibilità. Queste copie possono continuare a servire richieste di dati alle istanze del cluster Amazon DocumentDB.

Fatturazione dello storage dei dati di

Amazon DocumentDB aumenta automaticamente le dimensioni di un volume di cluster all'aumentare della quantità di dati. Un volume di cluster Amazon DocumentDB può crescere fino a una dimensione massima di 128 TiB; tuttavia, ti viene addebitato solo lo spazio utilizzato in un volume cluster Amazon DocumentDB. A partire da Amazon DocumentDB 4.0, quando i dati vengono rimossi, ad esempio eliminando una raccolta o un indice, lo spazio allocato complessivamente diminuisce di una quantità comparabile. In questo modo, puoi ridurre i costi di archiviazione eliminando raccolte, indici e database che non ti servono più. Con Amazon DocumentDB 3.6, quando i dati vengono rimossi, ad esempio eliminando una raccolta o un indice, lo spazio allocato complessivamente rimane lo stesso. Lo spazio libero viene riutilizzato automaticamente quando il volume di dati aumenterà in futuro.

Note

Con Amazon DocumentDB 3.6, i costi di storage si basano sulla «soglia massima» dello storage (la quantità massima allocata per il cluster Amazon DocumentDB in qualsiasi momento). Puoi gestire i costi evitando le pratiche ETL che creano grandi volumi di informazioni temporanee o che caricano grandi volumi di nuovi dati prima di rimuovere i dati più vecchi non necessari. Se la rimozione di dati da un cluster Amazon DocumentDB comporta una notevole quantità di spazio allocato ma inutilizzato, la reimpostazione del limite massimo richiede l'esecuzione di un dump logico dei dati e il ripristino in un nuovo cluster, utilizzando uno strumento come `o. mongodump` e `mongorestore`. La creazione e il ripristino di una snapshot non riduce lo storage allocato perché il livello fisico dello storage sottostante rimane uguale nella snapshot ripristinata.

Note

L'utilizzo di strumenti come `mongodump` e `mongorestore` comporta addebiti di I/O in base alle dimensioni dei dati che vengono letti e scritti nel volume di archiviazione.

[Per informazioni sullo storage dei dati e sui prezzi di I/O di Amazon DocumentDB, consulta le domande frequenti sui prezzi e sui prezzi di Amazon DocumentDB \(compatibile con MongoDB\).](#)

Replica Amazon DocumentDB

In un cluster Amazon DocumentDB, ogni istanza di replica espone un endpoint indipendente. Questi endpoint di replica forniscono l'accesso in sola lettura ai dati del volume cluster. Consentono di calibrare il carico di lavoro in lettura dei dati su più istanze replicate. Inoltre, aiutano a migliorare le prestazioni di lettura dei dati e ad aumentare la disponibilità dei dati nel cluster Amazon DocumentDB. Le repliche di Amazon DocumentDB sono anche obiettivi di failover e vengono promosse rapidamente in caso di guasto dell'istanza principale del cluster Amazon DocumentDB.

Affidabilità di Amazon DocumentDB

Amazon DocumentDB è progettato per essere affidabile, durevole e tollerante ai guasti. (Per migliorare la disponibilità, è necessario configurare il cluster Amazon DocumentDB in modo che abbia più istanze di replica in diverse zone di disponibilità.) Amazon DocumentDB include diverse funzionalità automatiche che lo rendono una soluzione di database affidabile.

Riparazione automatica dello storage

Amazon DocumentDB conserva più copie dei dati in tre zone di disponibilità, riducendo notevolmente la possibilità di perdita dei dati a causa di un errore di storage. Amazon DocumentDB rileva automaticamente gli errori nel volume del cluster. Quando un segmento di un volume del cluster si guasta, Amazon DocumentDB ripara immediatamente il segmento. Utilizza i dati degli altri volumi che costituiscono il volume cluster per garantire che i dati del segmento riparato siano aggiornati. Di conseguenza, Amazon DocumentDB evita la perdita di dati e riduce la necessità di eseguire un point-in-time ripristino per il ripristino dopo un errore di istanza.

Riscaldamento di sopravvivenza della cache

Amazon DocumentDB gestisce la cache delle pagine in un processo separato dal database in modo che la cache delle pagine possa funzionare indipendentemente dal database. Nella remota eventualità di un errore del database, la cache di pagina rimane in memoria. In questo modo il pool di buffer viene riscaldato con lo stato più aggiornato quando il database viene riavviato.

Ripristino in caso di arresto

Amazon DocumentDB è progettato per il ripristino da un crash quasi istantaneo e per continuare a fornire i dati delle applicazioni. Amazon DocumentDB esegue il ripristino da arresto anomalo in modo asincrono su thread paralleli in modo che il database sia aperto e disponibile quasi immediatamente dopo un arresto anomalo.

Governance delle risorse

Amazon DocumentDB protegge le risorse necessarie per eseguire processi critici nel servizio, come i controlli dello stato. A tale scopo, e quando un'istanza è sottoposta a un'elevata pressione della memoria, Amazon DocumentDB limiterà le richieste. Di conseguenza, alcune operazioni potrebbero essere messe in coda per attendere che la pressione della memoria diminuisca. Se la pressione della memoria continua, le operazioni in coda potrebbero scadere. È possibile controllare se le operazioni di limitazione del servizio sono dovute o meno alla scarsa memoria con le seguenti CloudWatch metriche:,,, LowMemThrottleQueueDepth LowMemThrottleMaxQueueDepth LowMemNumOperationsThrottled LowMemNumOperationsTimedOut Per ulteriori informazioni, consulta [Monitoring Amazon DocumentDB with CloudWatch](#) Se riscontri una pressione sostenuta della memoria sulla tua istanza a causa dei LowMem CloudWatch parametri, ti consigliamo di aumentare la scalabilità dell'istanza per fornire memoria aggiuntiva per il carico di lavoro.

Opzioni per le preferenze di lettura

Amazon DocumentDB utilizza un servizio di storage condiviso nativo del cloud che replica i dati sei volte su tre zone di disponibilità per fornire livelli elevati di durabilità. Amazon DocumentDB non si basa sulla replica dei dati su più istanze per ottenere la durabilità. I dati del cluster sono sempre durevoli, sia che contengano una singola istanza che 15.

Durabilità delle scritture

Amazon DocumentDB utilizza un sistema di storage unico, distribuito, tollerante ai guasti e con riparazione automatica. Questo sistema replica sei copie ($V=6$) dei dati in tre AWS zone di disponibilità per fornire disponibilità e durabilità elevate. Durante la scrittura dei dati, Amazon DocumentDB garantisce che tutte le scritture vengano registrate in modo duraturo sulla maggior parte dei nodi prima di confermare la scrittura al client. Se utilizzi un set di repliche MongoDB a tre nodi, l'utilizzo di un problema di scrittura `{w:3, j:true}` di produrrebbe la migliore configurazione possibile rispetto ad Amazon DocumentDB.

Le scritture su un cluster Amazon DocumentDB devono essere elaborate dall'istanza writer del cluster. Il tentativo di scrivere su un lettore genera un errore. Una scrittura riconosciuta da un'istanza primaria di Amazon DocumentDB è durevole e non può essere ripristinata. Amazon DocumentDB è altamente durevole per impostazione predefinita e non supporta un'opzione di scrittura non durevole. Non puoi modificare il livello di durabilità (ovvero Write Concern). Amazon DocumentDB ignora `w=anything` ed è effettivamente `w: 3` e `j: true`. Non puoi ridurlo.

Poiché lo storage e l'elaborazione sono separati nell'architettura Amazon DocumentDB, un cluster con una singola istanza è estremamente durevole. La durabilità è gestita a livello di storage. Di conseguenza, un cluster Amazon DocumentDB con una singola istanza e uno con tre istanze raggiungono lo stesso livello di durabilità. Puoi configurare il cluster per il tuo caso d'uso specifico senza sacrificare la durabilità elevata per i dati.

Le scritture su un cluster Amazon DocumentDB sono atomiche all'interno di un singolo documento.

Amazon DocumentDB non supporta l'`wtimeout` opzione e non restituirà un errore se viene specificato un valore. È garantito che le scritture sull'istanza primaria di Amazon DocumentDB non si blocchino a tempo indeterminato.

Isolamento delle letture

Le letture da un'istanza di Amazon DocumentDB restituiscono solo dati durevoli prima dell'inizio della query. Le letture non restituiscono mai i dati modificati dopo aver avviato l'esecuzione delle query e in nessun caso sono consentite le letture modificate.

Consistenza di lettura

I dati letti da un cluster Amazon DocumentDB sono durevoli e non verranno ripristinati. Puoi modificare la coerenza di lettura per le letture di Amazon DocumentDB specificando la preferenza di lettura per la richiesta o la connessione. Amazon DocumentDB non supporta un'opzione di lettura non durevole.

Le letture dall'istanza principale di un cluster Amazon DocumentDB sono fortemente coerenti in condizioni operative normali e read-after-write sono coerenti. Se si verifica un failover tra la scrittura e la lettura successiva, il sistema è in grado di restituire per breve tempo una lettura non particolarmente coerente. Tutte le letture da una replica di lettura garantiscono coerenza finale e restituiscono i dati nello stesso ordine, spesso con un ritardo di replica inferiore ai 100 ms.

Preferenze di lettura di Amazon DocumentDB

Amazon DocumentDB supporta l'impostazione di un'opzione di preferenza di lettura solo durante la lettura dei dati dall'endpoint del cluster in modalità set di replica. L'impostazione di un'opzione di preferenza di lettura influisce sul modo in cui il client o il driver MongoDB instrada le richieste di lettura alle istanze del cluster Amazon DocumentDB. Puoi impostare le opzioni per le preferenze di lettura per una query specifica oppure come opzione generale nel tuo driver MongoDB. Consulta la documentazione del driver o del client per istruzioni su come impostare un'opzione per le preferenze di lettura.

Se il client o il driver non si connette a un endpoint del cluster Amazon DocumentDB in modalità set di repliche, il risultato della specifica di una preferenza di lettura non è definito.

Amazon DocumentDB non supporta l'impostazione di set di tag come preferenza di lettura.

Opzioni per le preferenze di lettura supportate

- **primary**—Specificare una preferenza di `primary` lettura aiuta a garantire che tutte le letture vengano indirizzate all'istanza primaria del cluster. Se l'istanza primaria non è disponibile, l'operazione di lettura non riesce. Una preferenza di `primary` lettura garantisce read-after-write

coerenza ed è appropriata per i casi d'uso che danno priorità alla read-after-write coerenza rispetto all'elevata disponibilità e al ridimensionamento della lettura.

L'esempio seguente specifica una preferenza di lettura `primary`:

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

- **primaryPreferred**—La specificazione di una preferenza di `primaryPreferred` lettura indirizza le letture all'istanza principale durante il normale funzionamento. Se si verifica un failover dell'istanza primaria, il client indirizza le richieste a una replica. Una preferenza di `primaryPreferred` lettura garantisce read-after-write coerenza durante il normale funzionamento e, infine, letture coerenti durante un evento di failover. Una preferenza di `primaryPreferred` lettura è appropriata per i casi d'uso che danno priorità alla read-after-write coerenza rispetto alla scalabilità di lettura, ma richiedono comunque un'elevata disponibilità.

L'esempio seguente specifica una preferenza di lettura `primaryPreferred`:

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

- **secondary**—La specificazione di una preferenza di `secondary` lettura garantisce che le letture vengano indirizzate solo a una replica, mai all'istanza principale. Se in un cluster non sono presenti istanze di replica, la richiesta di lettura non riesce. Una preferenza di `secondary` lettura produce alla fine letture coerenti ed è appropriata per i casi d'uso che danno priorità al throughput di scrittura dell'istanza principale rispetto all'elevata disponibilità e coerenza. read-after-write

L'esempio seguente specifica una preferenza di lettura `secondary`:

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

- **secondaryPreferred**—La specificazione di una preferenza di `secondaryPreferred` lettura garantisce che le letture vengano indirizzate a una replica di lettura quando una o più repliche sono attive. Se in un cluster non sono presenti istanze di replica attive, la richiesta di lettura viene instradata all'istanza primaria. Una preferenza di lettura `secondaryPreferred` genera letture consistenti finali quando la lettura viene gestita da una replica di lettura. Garantisce read-after-write

coerenza quando la lettura viene gestita dall'istanza principale (esclusi gli eventi di failover). Una preferenza di `secondaryPreferred` lettura è appropriata per i casi d'uso che danno priorità alla scalabilità di lettura e all'elevata disponibilità rispetto alla coerenza. `read-after-write`

L'esempio seguente specifica una preferenza di lettura `secondaryPreferred`:

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

- **nearest**—La specificazione di una `nearest` preferenza di lettura indirizza le letture esclusivamente in base alla latenza misurata tra il client e tutte le istanze nel cluster Amazon DocumentDB. Una preferenza di lettura `nearest` genera letture consistenti finali quando la lettura viene gestita da una replica di lettura. Garantisce `read-after-write` coerenza quando la lettura viene gestita dall'istanza principale (esclusi gli eventi di failover). Una preferenza di `nearest` lettura è appropriata per i casi d'uso che danno priorità al raggiungimento della latenza di lettura più bassa possibile e dell'elevata disponibilità rispetto alla coerenza e al ridimensionamento della lettura. `read-after-write`

L'esempio seguente specifica una preferenza di lettura `nearest`:

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

Elevata disponibilità

Amazon DocumentDB supporta configurazioni di cluster ad alta disponibilità utilizzando le repliche come destinazioni di failover per l'istanza principale. Se l'istanza primaria si guasta, una replica di Amazon DocumentDB viene promossa come nuova istanza primaria, con una breve interruzione durante la quale le richieste di lettura e scrittura effettuate all'istanza primaria hanno esito negativo con un'eccezione.

Se il cluster Amazon DocumentDB non include alcuna replica, l'istanza principale viene ricreata in caso di errore. Tuttavia, promuovere una replica di Amazon DocumentDB è molto più veloce che ricreare l'istanza principale. Pertanto, consigliamo di creare una o più repliche di Amazon DocumentDB come destinazioni di failover.

Le repliche che sono pensate per l'utilizzo come destinazioni di failover devono essere della stessa classe di istanza dell'istanza primaria. Devono essere assegnate in diverse zone di disponibilità dal database primario. Puoi specificare le repliche preferite come destinazioni di failover. Per le best

pratiche sulla configurazione di Amazon DocumentDB per l'alta disponibilità, consulta [Comprendere la tolleranza agli errori del cluster Amazon DocumentDB](#)

Dimensionamento delle letture

Le repliche di Amazon DocumentDB sono ideali per il ridimensionamento della lettura. Sono dedicate completamente alle operazioni di lettura nel volume cluster, ossia le repliche non elaborano le scritture. Le repliche dei dati si verificano all'interno del volume cluster e non tra le istanze. Quindi le risorse di ogni replica sono dedicate all'elaborazione delle query, non a replicare e scrivere dati.

Se l'applicazione richiede più capacità di lettura, puoi aggiungere rapidamente una replica al cluster, in genere in meno di 10 minuti. Se i tuoi requisiti per la capacità di lettura diminuiscono, puoi rimuovere le repliche non necessarie. Con le repliche di Amazon DocumentDB, paghi solo per la capacità di lettura necessaria.

Amazon DocumentDB supporta la scalabilità di lettura lato client tramite l'uso delle opzioni di preferenza di lettura. Per ulteriori informazioni, consulta [Preferenze di lettura di Amazon DocumentDB](#).

Eliminazioni TTL

Le eliminazioni da un'area di indice TTL ottenute tramite un processo in background si basano sul miglior tentativo e non sono garantite all'interno di un determinato periodo di tempo specifico. Fattori come le dimensioni dell'istanza, l'utilizzo di risorse dell'istanza, le dimensioni documento e il throughput complessivo possono influenzare la tempistica di un'eliminazione TTL.

Quando il monitor TTL elimina i documenti, ogni eliminazione comporta costi di IO incrementando l'importo in fattura. Se i costi di throughput e di eliminazioni TTL aumentano, aspettati un aumento degli importi in fattura a causa dell'aumento dell'utilizzo IO.

Quando crei un indice TTL su una raccolta esistente, devi eliminare tutti i documenti scaduti prima di creare l'indice. L'attuale implementazione TTL è ottimizzata per l'eliminazione di una piccola parte dei documenti della raccolta, il che è tipico se il TTL è stato abilitato nella raccolta fin dall'inizio, e può comportare un IOPS più elevato del necessario se è necessario eliminare un numero elevato di documenti contemporaneamente.

Se non desideri creare un indice TTL per eliminare i documenti, puoi invece segmentare i documenti in raccolte in base al tempo e semplicemente eliminare tali raccolte quando i documenti non sono più necessari. Ad esempio, puoi creare una raccolta a settimana e eliminarla senza incorrere in costi di I/O. Questo può essere molto più conveniente rispetto all'utilizzo di un indice TTL.

Risorse fatturabili

Identificazione delle risorse fatturabili di Amazon DocumentDB

Essendo un servizio di database completamente gestito, Amazon DocumentDB addebita costi per istanze, storage, I/O, backup e trasferimento dati. Per ulteriori informazioni, consulta i prezzi di [Amazon DocumentDB \(con compatibilità con MongoDB\)](#).

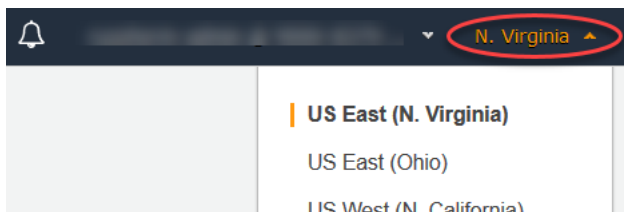
Per scoprire le risorse fatturabili nel tuo account e potenzialmente eliminare le risorse, puoi utilizzare o. AWS Management Console AWS CLI

Utilizzando il AWS Management Console

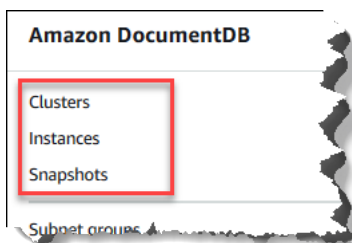
Utilizzando AWS Management Console, puoi scoprire i cluster, le istanze e gli snapshot di Amazon DocumentDB di cui hai effettuato il provisioning per un determinato periodo. Regione AWS

Per individuare cluster, istanze e snapshot

1. [Accedi a e apri AWS Management Console la console Amazon DocumentDB all'indirizzo https://console.aws.amazon.com/docdb.](https://console.aws.amazon.com/docdb)
2. Per scoprire risorse fatturabili in una regione diversa da quella predefinita, nell'angolo in alto a destra dello schermo, scegli Regione AWS quella in cui desideri cercare.



3. Nel riquadro di navigazione, scegliere il tipo di risorse fatturabili di interesse: Clusters (Cluster), Instances (Istanze) o Snapshots (Snapshot).



4. Tutti i cluster, le istanze o le snapshot di cui è stato eseguito il provisioning per la regione sono elencati nel riquadro a destra. Verrà addebitato il costo per i cluster, le istanze e le snapshot.

Utilizzando il AWS CLI

Utilizzando AWS CLI, puoi scoprire i cluster, le istanze e gli snapshot di Amazon DocumentDB di cui hai effettuato il provisioning per un determinato periodo. Regione AWS

Per individuare cluster e istanze

Il codice seguente elenca tutti i cluster e le istanze per la regione specificata. Per eseguire la ricerca di cluster e istanze nella regione predefinita, è possibile omettere il parametro `--region`.

Example

Per Linux, macOS o Unix:

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

Per Windows:

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

L'aspetto dell'output di questa operazione è simile al seguente.

```
"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",
```

Per individuare le snapshot

Il codice seguente elenca tutte le snapshot per la regione specificata. Per eseguire la ricerca di snapshot nella regione predefinita, è possibile omettere il parametro `--region`.

Per Linux, macOS o Unix:

```
aws docdb describe-db-cluster-snapshots \  
  --region us-east-1
```

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

Per Windows:

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

L'aspetto dell'output di questa operazione è simile al seguente.

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

È necessario eliminare solo le snapshot di tipo manual. Le snapshot di tipo Automated vengono eliminate quando si elimina il cluster.

Eliminazione di risorse fatturabili non necessarie

Per eliminare un cluster, è necessario eliminare prima tutte le istanze che esso contiene.

- Per eliminare le istanze, consultare [Eliminazione di un'istanza Amazon DocumentDB](#).

Important

Anche eliminando le istanze in un cluster, lo storage e l'utilizzo di backup di utilizzo associati a tale cluster vengono comunque fatturati. Per interrompere ogni addebito, è necessario eliminare anche il cluster e le snapshot manuali.

- Per eliminare i cluster, consultare [Eliminazione di un cluster Amazon DocumentDB](#).
- Per eliminare le snapshot manuali, consultare [Eliminazione di una snapshot del cluster](#).

Cos'è un database di documenti?

Alcuni sviluppatori non pensano al proprio modello di dati in termini di righe e colonne normalizzate. Tipicamente, nel livello dell'applicazione, i dati sono rappresentati come un documento JSON perché è più intuitivo per gli sviluppatori pensare al proprio modello di dati come a un documento.

La popolarità dei database di documenti è aumentata perché consentono di rendere permanenti i dati in un database utilizzando lo stesso formato del modello di documento utilizzato nel codice dell'applicazione. I database di documenti forniscono API potenti e intuitive per uno sviluppo flessibile e agile.

Argomenti

- [Casi d'uso del database di documenti](#)
- [Comprensione dei documenti](#)
- [Utilizzo dei documenti](#)

Casi d'uso del database di documenti

Il tuo caso d'uso riguarda situazioni in cui hai bisogno di un database di documenti o di altri tipi di database per gestire i dati. I database di documenti sono utili per i carichi di lavoro che richiedono uno schema flessibile per uno sviluppo rapido e iterativo. Di seguito sono elencati alcuni esempi di casi d'uso per i quali i database di documenti possono offrire notevoli vantaggi:

Argomenti

- [Profili utente](#)
- [Big Data in tempo reale](#)
- [Gestione dei contenuti](#)

Profili utente

Poiché i database di documenti si basano su uno schema flessibile, possono archiviare documenti con diversi attributi e valori dei dati. I database di documenti rappresentano una soluzione pratica per i profili online in cui più utenti forniscono tipi di informazioni diversi. Con un database di documenti puoi archiviare ogni profilo utente in modo efficiente archiviando solo gli attributi specifici per il singolo utente.

Supponiamo che un utente decida di aggiungere o rimuovere delle informazioni dal profilo. In questo caso, il documento può essere facilmente sostituito con una versione aggiornata che contiene tutti i dati e gli attributi aggiunti di recente o che omette attributi e dati rimossi di recente. I database di documenti consentono di gestire più facilmente questo livello di individualità e fluidità.

Big Data in tempo reale

Storicamente, la capacità di estrarre informazioni dai dati operativi era ostacolata dal fatto che i database operativi e i database analitici sono stati mantenuti in diversi ambienti, rispettivamente operativi e business/reporting. La possibilità di estrarre informazioni operative in tempo reale è fondamentale in un ambiente aziendale altamente competitivo. Utilizzando i database di documenti, un'azienda può archiviare e gestire i dati operativi da qualsiasi origine e, allo stesso tempo, inviare i dati al motore BI preferito per analizzarli. La presenza di due ambienti non è obbligatoria.

Gestione dei contenuti

Per gestire in modo efficiente i contenuti, devi poterli raccogliere e aggregare da diverse origini e quindi inviarli al cliente. Grazie al loro schema flessibile, i database di documenti sono perfetti per raccogliere e archiviare qualsiasi tipo di dati. Puoi utilizzarli per creare e integrare nuovi tipi di contenuti, inclusi quelli generati dagli utenti, come immagini, commenti e video.

Comprensione dei documenti

I database dei documenti vengono utilizzati per archiviare dati semistrutturati come documento, anziché normalizzare i dati su più tabelle, ognuna con una struttura unica e fissa, come in un database relazionale. I documenti archiviati in un database di documenti utilizzano coppie chiave-valore nidificate per fornire la struttura o lo schema del documento. Tuttavia, nello stesso database di documenti possono essere archiviati diversi tipi di documenti, rispettando così il requisito che prevede l'elaborazione di dati simili in formati diversi. Ad esempio, visto che ogni documento è autodescrittivo, i documenti codificati con JSON per uno store online descritti in questo argomento [Esempio di documenti in un database di documenti](#) possono essere archiviati nello stesso database di documenti.

Argomenti

- [Terminologia SQL rispetto a](#)
- [Documenti semplici](#)
- [Documenti incorporati](#)
- [Esempio di documenti in un database di documenti](#)

- [Informazioni sulla normalizzazione in un database di documenti](#)

Terminologia SQL rispetto a

Nella tabella seguente viene confrontata la terminologia utilizzata dai database di documenti (MongoDB) con quella utilizzata dai database SQL.

SQL	MongoDB
Tabella	Raccolta
Riga	Documento
Colonna	Campo
Chiave primaria	ObjectId
Indice	Indice
Vista	Vista
Oggetto o tabella annidata	Documento incorporato
Array	Array

Documenti semplici

Tutti i documenti in un database di documenti sono autodescrittivi. In questa documentazione utilizziamo documenti con formattazione simile a JSON, anche se puoi utilizzare altri mezzi di codifica.

Un documento semplice ha uno o più campi, tutti allo stesso livello all'interno del documento. In questo esempio i campi SSN, LName, FName, DOB, Street, City, State-Province, PostalCode e Country sono tutti di pari livello all'interno del documento.

```
{
  "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"
}
```

Quando le informazioni vengono organizzate in un documento semplice, ogni campo viene gestito individualmente. Per recuperare l'indirizzo di una persona, devi recuperare `Street`, `City`, `State-Province`, `PostalCode` e `Country` come singoli elementi dati.

Documenti incorporati

Un documento complesso organizza i propri dati creando documenti incorporati nel documento stesso. I documenti incorporati consentono di gestire i dati in gruppi e come singoli elementi, in base alla soluzione più efficace in un determinato caso. Utilizzando l'esempio precedente, puoi incorporare un documento `Address` nel documento principale. In questo modo si otterrà la struttura del documento seguente:

```
{
  "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"
  }
}
```

Ora puoi accedere ai dati nel documento come campi singoli (`"SSN" :`), come documento incorporato (`"Address" :`) o come membro di un documento incorporato (`"Address" : {"Street" :}`).

Esempio di documenti in un database di documenti

Come indicato in precedenza, ogni documento in un database di documenti è autodescrittivo, quindi la struttura dei documenti all'interno di un database di documenti può essere diversa. I due documenti

seguenti, uno relativo a un manuale e l'altro a un periodico, sono strutturalmente differenti. Tuttavia, entrambi possono essere inclusi nello stesso database di documenti.

Di seguito è riportato un documento di esempio per un libro:

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

Di seguito è riportato un documento di esempio per un periodico con due articoli:

```
{
  "_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"  
}
```

Confronta la struttura di questi due documenti. Con un database relazionale, devi avere tabelle separate per "periodico" e "libri" oppure una singola tabella con campi inutilizzati, ad esempio "Pubblicazione", "Numero", "Articoli" e "MI", come valori null. Poiché i database di documenti sono semistrutturati e ogni documento definisce autonomamente la propria struttura, questi due documenti possono coesistere nello stesso database di documenti senza alcun campo null. I database di documenti sono uno strumento efficace per gestire i dati di tipo sparse.

L'utilizzo di un database di documenti consente uno sviluppo rapido e iterativo. Il motivo è che puoi modificare la struttura dei dati di un documento in modo dinamico, senza dover modificare lo schema per l'intera raccolta. I database di documenti sono particolarmente adatti per lo sviluppo agile e gli ambienti che evolvono dinamicamente.

Informazioni sulla normalizzazione in un database di documenti

I database di documenti non sono normalizzati. I dati nel documento possono essere ripetuti in un altro documento. Inoltre, possono esistere delle discrepanze nei dati dei documenti. Ad esempio, considera uno scenario in cui puoi effettuare acquisti in uno store online e tutti i dettagli dei tuoi acquisti vengono archiviati in un singolo documento. Il documento può essere simile al documenti JSON seguente:

```
{  
  "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"
}
```

Tutte le informazioni vengono archiviate sotto forma di documento in una raccolta di transazioni. Successivamente, ti accorgi di aver dimenticato di acquistare un articolo. Accedi di nuovo allo stesso store ed effettui un altro acquisto, che a sua volta viene archiviato come documento nella raccolta di transazioni.

```
{
  "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"
}
```

Notate la ridondanza tra questi due documenti: il vostro nome e l'ID acquirente (e, se avete utilizzato la stessa carta di credito, i dati della vostra carta di credito). Tuttavia, la procedura non presenta problemi perché lo storage è economico e ogni documento registra completamente una singola transazione che può essere recuperata rapidamente con una semplice query chiave-valore che non richiede join.

C'è anche un'apparente discrepanza tra i due documenti, ovvero le informazioni della tua carta di credito. Si tratta di una discrepanza solo apparente perché è probabile che hai semplicemente utilizzato due carte diverse per gli acquisti. Ogni documento contiene tutti i dati corretti per la transazione documentata.

Utilizzo dei documenti

In quanto database di documenti, Amazon DocumentDB semplifica l'archiviazione, la query e l'indicizzazione dei dati JSON. In Amazon DocumentDB, una raccolta è analoga a una tabella in un database relazionale, salvo che ai documenti non è applicato alcuno schema singolo. Le raccolte consentono di raggruppare documenti simili mantenendoli comunque nello stesso database, senza richiedere che siano identici a livello di struttura.

Utilizzando i documenti di esempio delle sezioni precedenti, è probabile che tu disponga di raccolte per `reading_material` e `office_supplies`. È responsabilità del software stabilire a quale raccolta appartenga un documento.

Gli esempi seguenti utilizzano l'API MongoDB per mostrare come aggiungere, eseguire query, aggiornare ed eliminare i documenti.

Argomenti

- [Aggiunta di documenti](#)
- [Esecuzione di query di documenti](#)
- [Aggiornamento dei documenti](#)
- [Eliminazione di documenti](#)

Aggiunta di documenti

In Amazon DocumentDB, viene creato un database quando si aggiunge per la prima volta un documento a una raccolta. In questo esempio, viene creata una raccolta denominata `example` nel database `test`, che è il database predefinito quando ci si connette a un cluster. Poiché la raccolta

viene creata implicitamente quando viene inserito il primo documento, non vi è alcun controllo di errore del nome della raccolta. Di conseguenza, un errore di battitura nel nome della raccolta, ad esempio `eexample` anziché `example`, creerà e aggiungerà il documento alla raccolta `eexample` anziché la raccolta desiderata. Il controllo degli errori deve essere gestito dall'applicazione.

Gli esempi seguenti utilizzano l'API MongoDB per aggiungere documenti.

Argomenti

- [Aggiunta di un singolo documento](#)
- [Aggiunta di più documenti](#)

Aggiunta di un singolo documento

Per aggiungere un singolo documento a una raccolta, utilizza l'operazione `insertOne({})` con il documento da aggiungere alla raccolta.

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

L'aspetto dell'output di questa operazione è simile al seguente (formato JSON).

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

Aggiunta di più documenti

Per aggiungere più documenti a una raccolta, utilizza l'operazione `insertMany([{}, ..., {}])` con un elenco di documenti da aggiungere alla raccolta. Anche se i documenti in questo specifico elenco hanno schemi diversi, ciascuno può essere aggiunto alla stessa raccolta.

```
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,  
        "OrderQty": 36  
      }  
    }  
  ]  
)
```

L'aspetto dell'output di questa operazione è simile al seguente (formato JSON).

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


Esecuzione di query di documenti

A volte, potrebbe essere necessario cercare nell'inventario dello store online, in modo che i clienti possano vedere e acquistare ciò che vendi. Eseguire query su una raccolta è relativamente semplice, sia per le ricerche su tutti i documenti della raccolta che per quelle solo sui documenti che soddisfano un determinato criterio.

Per eseguire una query per i documenti, utilizza l'operazione `find()`. Il comando `find()` ha un parametro per documenti singoli che definisce i criteri da utilizzare nella scelta dei documenti da restituire. L'output di `find()` è un documento formattato su una sola riga di testo senza interruzioni di riga. Per formattare il documento di output per facilitare la lettura, utilizza `find().pretty()`. Tutti gli esempi di questo argomento utilizzano `.pretty()` per formattare l'output.

Utilizza i quattro documenti inseriti nella finestra `example` raccolta nei due esercizi precedenti —`insertOne()` e `insertMany()`.

Argomenti

- [Recupero di tutti i documenti in una raccolta](#)
- [Recupero dei documenti che corrispondono a un valore di campo](#)
- [Recupero di documenti che corrispondono a un documento incorporato](#)
- [Recupero di documenti che corrispondono a un valore di campo in un documento incorporato](#)
- [Recupero dei documenti che corrispondono a una matrice](#)
- [Recupero dei documenti che corrispondono a un valore in una matrice](#)
- [Recupero di documenti usando gli operatori](#)

Recupero di tutti i documenti in una raccolta

Per recuperare tutti i documenti nella raccolta, usa l'operazione `find()` con un documento di query vuoto.

La query seguente restituisce tutti i documenti della raccolta `example`.

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

Recupero dei documenti che corrispondono a un valore di campo

Per recuperare tutti i documenti che corrispondono a un campo e a un valore, usa l'operazione `find()` con un documento di query che identifica i campi e i valori per la corrispondenza.

Usando i documenti precedenti, questa query restituisce tutti i documenti in cui il campo "Item" è uguale a "Pen".

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

Recupero di documenti che corrispondono a un documento incorporato

Per trovare tutti i documenti che corrispondono a un documento incorporato, utilizza l'operazione `find()` con un documento di query che specifica il nome del documento incorporato e tutti i campi e i valori per quel documento incorporato.

Quando si esegue il confronto di un documento incorporato, il documento incorporato del documento deve avere lo stesso nome che ha nella query. Inoltre, i campi e i valori nel documento incorporato devono corrispondere alla query.

La seguente query restituisce solo il documento "Poster Paint". Questo perché "Pen" ha valori diversi per "OnHand" e "MinOnHand" e "Spray Paint" ha un ulteriore campo (`OrderQty`) rispetto al documento di query.

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

Recupero di documenti che corrispondono a un valore di campo in un documento incorporato

Per trovare tutti i documenti che corrispondono a un documento incorporato, utilizza l'operazione `find()` con un documento di query che specifica il nome del documento incorporato e tutti i campi e i valori per quel documento incorporato.

Considerati i documenti precedenti, la seguente query utilizza la "dot notation" (notazione col punto) per specificare il documento incorporato e i campi di interesse. Vengono restituiti tutti i documenti che corrispondono a questi campi, indipendentemente da quali altri campi possono essere presenti nel documento incorporato. La query restituisce "Poster Paint" e "Spray Paint" perché entrambi corrispondono ai campi e ai valori specificati.

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

Recupero dei documenti che corrispondono a una matrice

Per trovare tutti i documenti che corrispondono a una matrice, utilizzare l'operazione `find()` con il nome della matrice richiesta e tutti i valori in quella matrice. La query restituisce tutti i documenti che hanno una matrice con quel nome in cui i valori della matrice sono identici e nello stesso ordine rispetto alla query.

La seguente query restituisce solo "Pen" perché "Poster Paint" ha un ulteriore colore (White) mentre "Spray Paint" ha i colori in un ordine diverso.

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

Recupero dei documenti che corrispondono a un valore in una matrice

Per trovare tutti i documenti che hanno un valore specifico di matrice, utilizza l'operazione `find()` con il nome della matrice e il valore richiesto.

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

L'operazione precedente restituisce tutti e tre i documenti, in quanto ciascuno di essi dispone di una matrice denominata `Colors` e del valore "Red" all'interno della matrice. Se si specifica il valore "White", la query restituisce solo "Poster Paint".

Recupero di documenti usando gli operatori

La seguente query restituisce tutti i documenti in cui il valore `Inventory.OnHand` è inferiore a 50.

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

Per un elenco degli operatori di query supportati, consulta [Operatori per query e proiezioni](#).

Aggiornamento dei documenti

In genere, i documenti non sono statici e vengono aggiornati come parte dei flussi di lavoro dell'applicazione. Gli esempi seguenti mostrano alcune opzioni di aggiornamento dei documenti.

Per aggiornare un documento esistente, utilizza l'operazione `update()`. L'operazione `update()` presenta due parametri del documento. Il primo documento identifica il documento o i documenti da aggiornare. Il secondo documento specifica gli aggiornamenti da eseguire.

Quando si aggiorna un campo esistente, che si tratti di un campo semplice, una matrice o un documento incorporato, è necessario specificare il nome del campo e i relativi valori. Al termine dell'operazione è come se il campo nel documento precedente fosse stato sostituito dal campo e dai valori nuovi.

Argomenti

- [Aggiornamento dei valori di un campo esistente](#)
- [Aggiunta di un nuovo campo](#)
- [Sostituzione di un documento incorporato](#)
- [Inserimento di nuovi campi in un documento incorporato](#)
- [Rimozione di un campo da un documento](#)
- [Rimozione di un campo da più documenti](#)

Aggiornamento dei valori di un campo esistente

Utilizza i seguenti quattro documenti aggiunti in precedenza per le seguenti operazioni di aggiornamento.

```
{
  "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,  
    "OrderQty": 36  
  }  
}
```

Per aggiornare un campo semplice

Per aggiornare un campo semplice, utilizza `update()` con `$set` per specificare il nome del campo e il nuovo valore. L'esempio seguente modifica l'elemento `Item` da "Pen" a "Gel Pen".

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

L'aspetto dei risultati di questa operazione è simile al seguente.

```
{  
  "Item": "Gel Pen",  
  "Colors": ["Red", "Green", "Blue", "Black"],  
  "Inventory": {  
    "OnHand": 244,  
    "MinOnHand": 72  
  }  
}
```

Per aggiornare una matrice

L'esempio seguente sostituisce la matrice esistente di colori con una nuova matrice che comprende `Orange` e rimuove `White` dall'elenco dei colori. Il nuovo elenco di colori è nell'ordine specificato nell'operazione `update()`.

```
db.example.update(  
  { "Colors": ["White", "Orange", "Blue", "Black"] },  
  { $set: { "Colors": ["Orange", "Blue", "Black"] } }
```

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

L'aspetto dei risultati di questa operazione è simile al seguente.

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

Aggiunta di un nuovo campo

Per modificare un documento aggiungendo uno o più nuovi campi, utilizza l'operazione `update()` con un documento di query che identifica il documento in cui inserire i dati e i nuovi campi e valori da inserire utilizzando l'operatore `$set`.

L'esempio seguente aggiunge il campo `UnitPrice` con il valore `3.99` al documento `Spray Paints`. Si noti che il valore `3.99` è numerico e non una stringa.

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

L'aspetto dei risultati di questa operazione è simile al seguente (formato JSON).

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

Sostituzione di un documento incorporato

Per modificare un documento sostituendo un documento incorporato, utilizza l'operazione `update()` con i documenti che identificano il documento incorporato e i nuovi campi e valori utilizzando l'operatore `$set`.

Considerato il seguente documento.

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

Per sostituire un documento incorporato

L'esempio seguente sostituisce l'attuale documento `Date` con uno nuovo che ha solo i campi `Month` e `Day`, mentre `Year` è stato eliminato.

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

L'aspetto dei risultati di questa operazione è simile al seguente.

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

Inserimento di nuovi campi in un documento incorporato

Per aggiungere campi a un documento incorporato

Per modificare un documento aggiungendo uno o più campi nuovi a un documento incorporato, utilizza l'operazione `update()` con i documenti che identificano il documento incorporato e la "dot notation" per specificare il documento incorporato e i nuovi campi e valori da inserire utilizzando l'operatore `$set`.

Considerato il seguente documento, il codice seguente usa la "dot notation" per inserire i campi `Year` e `DoW` nel documento incorporato `Date` e `Words` nel documento padre.

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

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

L'aspetto dei risultati di questa operazione è simile al seguente.

```
{
  "DocName": "Document 1",
  "Date": {
    "Month": 4,
    "Day": 18,
    "Year": 1987,
    "DoW": "Saturday"
  },
  "Words": 2482
}
```

Rimozione di un campo da un documento

Per modificare un documento rimuovendo un campo, utilizza l'operazione `update()` con un documento di query che identifica il documento da cui rimuovere il campo e l'operatore `$unset` per specificare il campo da rimuovere.

L'esempio seguente rimuove il campo `Words` dal documento precedente.

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

L'aspetto dei risultati di questa operazione è simile al seguente.

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

Rimozione di un campo da più documenti

Per modificare un documento rimuovendo un campo da più documenti, utilizza l'operazione `update()` con l'operatore `$unset` e l'opzione `multi` impostata su `true`.

L'esempio seguente rimuove il campo `Inventory` da tutti i documenti della raccolta di esempi. Se un documento non contiene il campo `Inventory`, non viene eseguita alcuna azione. Se `multi: true` viene omissso, l'azione viene eseguita solo nel primo documento che soddisfa il criterio.

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

Eliminazione di documenti

Per rimuovere un documento dal database, utilizza l'operazione `remove()`, specificando il documento da rimuovere. Il codice seguente rimuove "Gel Pen" dalla raccolta `example`.

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

Per rimuovere tutti i documenti dal database, utilizza l'operazione `remove()` con una query vuota, come mostrato di seguito.

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

Inizia a usare Amazon DocumentDB

Esistono molti modi per connettersi e iniziare a usare Amazon DocumentDB. Abbiamo creato questa guida perché riteniamo che questo sia il modo più rapido, semplice e facile per gli utenti di iniziare a utilizzare il nostro potente database di documenti. Questa guida utilizza [AWS Cloud9](#) un terminale basato sul Web per connettersi e interrogare il cluster Amazon DocumentDB utilizzando la shell mongo direttamente da. AWS Management Console I nuovi clienti idonei al piano AWS gratuito possono utilizzare Amazon DocumentDB AWS Cloud9 gratuitamente. Se il tuo AWS Cloud9 ambiente o il tuo cluster Amazon DocumentDB utilizza risorse oltre il livello gratuito, ti vengono addebitate le AWS tariffe normali per tali risorse. Questa guida ti aiuterà a iniziare a usare Amazon DocumentDB in meno di 15 minuti.

Note

Le istruzioni contenute in questa guida riguardano specificamente la creazione e la connessione a cluster basati su istanze Amazon DocumentDB. Se desideri creare e connetterti a cluster elastici di Amazon DocumentDB, consulta. [Inizia a usare i cluster elastici di Amazon DocumentDB](#)

Argomenti

- [Prerequisiti](#)
- [Fase 1: Creare un AWS Cloud9 ambiente](#)
- [Fase 2: creazione di un gruppo di sicurezza](#)
- [Fase 3: creare un cluster Amazon DocumentDB](#)
- [Passaggio 4: installa la shell mongo](#)
- [Fase 5: Connettiti al tuo cluster Amazon DocumentDB](#)
- [Fase 6: Inserimento e interrogazione dei dati](#)
- [Fase 7: Esplora](#)

[Se preferisci connetterti ad Amazon DocumentDB dal tuo computer locale creando una connessione SSH a un'istanza Amazon EC2, consulta le istruzioni Connect with EC2](#)

Prerequisiti

Prima di creare il tuo primo cluster Amazon DocumentDB, devi fare quanto segue:

Crea un account Amazon Web Services (AWS)

Prima di iniziare a utilizzare Amazon DocumentDB, devi disporre di un account Amazon Web Services (AWS). L'account AWS è gratuito. Paghi solo per i servizi e le risorse che utilizzi.

Se non disponi di un Account AWS, completa la procedura seguente per crearne uno.

Per registrarsi a un Account AWS

1. Apri la pagina all'indirizzo <https://portal.aws.amazon.com/billing/signup>.
2. Segui le istruzioni online.

Nel corso della procedura di registrazione riceverai una telefonata, durante la quale sarà necessario inserire un codice di verifica attraverso la tastiera del telefono.

Durante la registrazione di un Account AWS, viene creato un Utente root dell'account AWS. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come best practice di sicurezza, [assegna l'accesso amministrativo a un utente amministrativo](#) e utilizza solo l'utente root per eseguire [attività che richiedono l'accesso di un utente root](#).

Configura le autorizzazioni necessarie AWS Identity and Access Management (IAM).

L'accesso alla gestione delle risorse di Amazon DocumentDB come cluster, istanze e gruppi di parametri del cluster richiede credenziali che AWS possono essere utilizzate per autenticare le richieste. Per ulteriori informazioni, consulta [Identity and Access Management per Amazon DocumentDB](#).

1. Nella barra di ricerca di AWS Management Console, digita IAM e seleziona IAM nel menu a discesa visualizzato.
2. Una volta che sei nella console IAM, seleziona Utenti dal pannello di navigazione.
3. Seleziona il tuo nome utente.
4. Fai clic sul pulsante Aggiungi autorizzazioni.
5. Seleziona Attach existing policies directly (Collega direttamente le policy esistenti).

6. Digita `AmazonDocDBFullAccess` nella barra di ricerca e selezionala quando appare nei risultati della ricerca.
7. Fai clic sul pulsante blu in basso che dice `Avanti: revisione`.
8. Fai clic sul pulsante blu in basso che dice `Aggiungi autorizzazioni`.

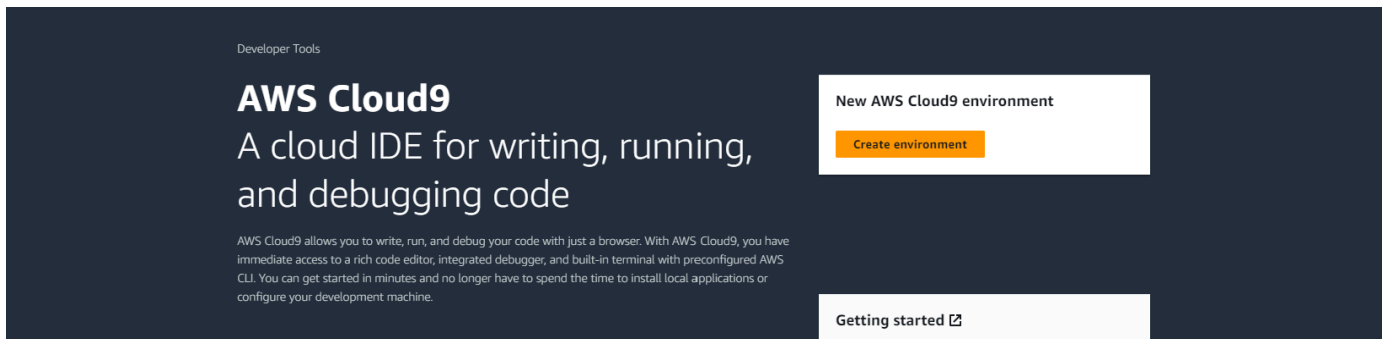
Crea un Amazon Virtual Private Cloud (Amazon VPC)

Questo passaggio è necessario solo se non disponi già di un Amazon VPC predefinito. In caso contrario, completa il passaggio 1 della [Guida introduttiva ad Amazon VPC nella Amazon VPC User Guide](#). Questa operazione richiederà meno di cinque minuti.

Fase 1: Creare un AWS Cloud9 ambiente

AWS Cloud9 fornisce un terminale basato sul Web che puoi utilizzare per connetterti e interrogare il tuo cluster Amazon DocumentDB utilizzando la shell mongo.

1. Da qui AWS Management Console accedi alla AWS Cloud9 console e scegli `Crea ambiente`.



2. Nella sezione `Dettagli` della finestra di dialogo `Crea ambiente`, inserisci `DocumentDBCloud9` il campo `Nome`.

Create environment [Info](#)

Details

Name

 Limit of 60 characters, alphanumeric, and unique per user.

Description - *optional*

 Limit 200 characters.

Environment type [Info](#)
 Determines what the Cloud9 IDE will run on.

New EC2 instance
 Cloud9 creates an EC2 instance in your account. The configuration of your EC2 instance cannot be changed by Cloud9 after creation.

Existing compute
 You have an existing instance or server that you'd like to use.

3. Per le sezioni Nuova istanza EC2, Impostazioni di rete e Tag, lascia l'impostazione predefinita così com'è e fai clic su Crea nella parte inferiore dello schermo.

The following IAM resources will be created in your account

- AWSServiceRoleForAWSCloud9** - AWS Cloud9 creates a service-linked role for you. This allows AWS Cloud9 to call other AWS services on your behalf. You can delete the role from the AWS IAM console once you no longer have any AWS Cloud9 environments. [Learn more](#)
- AWSCloud9SSMAccessRole and AWSCloud9SSMInstanceProfile** - A service role and an instance profile are automatically created if Cloud9 accesses its EC2 instance through AWS Systems Manager. If your environments no longer require EC2 instances that block incoming traffic, you can delete these roles using the AWS IAM console. [Learn more](#)

Cancel **Create**

Il nuovo AWS Cloud9 ambiente viene visualizzato nella tabella Ambienti:

Environments (1)						
Name	Cloud9 IDE	Environment type	Connection	Permission	Owner ARN	
DocumentDBCloud9	Open	EC2 instance	Secure Shell (SSH)	Owner	arn:aws:sts::	Delete View details Open in Cloud9 Create environment

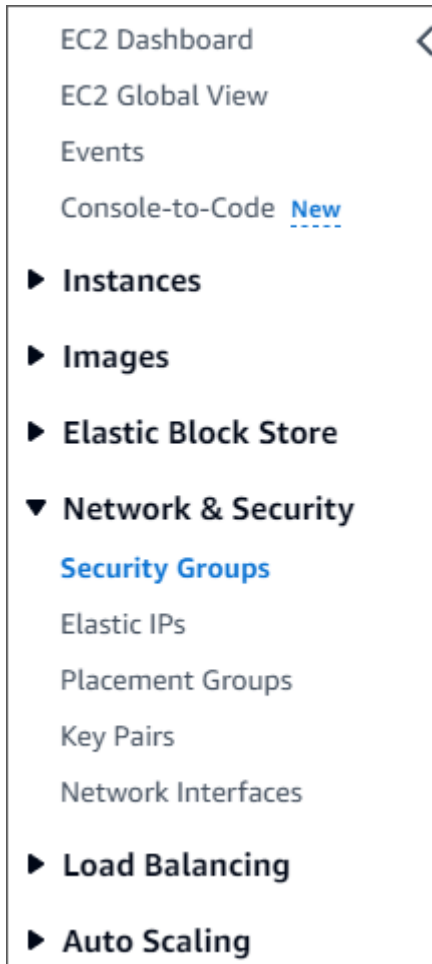
Note

Il provisioning dell'AWS Cloud9 ambiente può richiedere fino a tre minuti.

Fase 2: creazione di un gruppo di sicurezza

Questo gruppo di sicurezza ti consentirà di connetterti al tuo cluster Amazon DocumentDB dal tuo AWS Cloud9 ambiente.

1. Nella [Console di gestione Amazon EC2](#), in Rete e sicurezza, scegli Gruppi di sicurezza.



2. Scegliere Create Security Group (Crea gruppo di sicurezza).

Create security group

3. Nella sezione Dettagli di base:
 - a. In Security group name (Nome gruppo di sicurezza) immettere demoDocDB.
 - b. In Description (Descrizione), inserire una descrizione.
 - c. Per VPC, accetta l'utilizzo del tuo VPC predefinito.

Basic details

Security group name [Info](#)

MyWebServerGroup

Name cannot be edited after creation.

Description [Info](#)

Allows SSH access to developers

VPC [Info](#)

vpc-02c0445657b77542c ▼

4. Nella sezione Regole in entrata, scegliere Aggiungi regola.
 - a. Per Type (Tipo) seleziona Custom TCP Rule (Regola TCP personalizzata).
 - b. Per Port range, inserisci. 27017
 - c. Per Source, scegli il gruppo di sicurezza per l'AWS Cloud9ambiente che hai appena creato. Per visualizzare un elenco dei gruppi di sicurezza disponibili, accedi a Cloud9 al campo Origine nel campo di ricerca a destra. Scegli il gruppo di sicurezza denominato aws-cloud9-*<environment name>*.
 - d. Per Destinazione, scegli Personalizzato. Nel campo accanto, cerca il gruppo di sicurezza che hai appena chiamato demoEC2. Potrebbe essere necessario aggiornare il browser per consentire alla console Amazon EC2 di compilare automaticamente il nome sorgente demoEC2.

Inbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info	Delete	
Custom TCP ▼	TCP	27017	Cust... ▼	Q		Delete
<div style="border: 1px solid #ccc; border-radius: 5px; padding: 5px; display: inline-block;">Add rule</div>						

i Note

La porta 27017 è la porta predefinita per Amazon DocumentDB.

5. Accetta tutte le altre impostazioni predefinite e scegli Crea gruppo di sicurezza.

Create security group

Fase 3: creare un cluster Amazon DocumentDB

In questo passaggio creerai un cluster Amazon DocumentDB utilizzando il gruppo di sicurezza creato nel passaggio precedente.

Note

Le istruzioni in questo passaggio riguardano specificamente la creazione di cluster basati su istanze Amazon DocumentDB. Se desideri creare cluster elastici Amazon DocumentDB, consulta. [Inizia a usare i cluster elastici di Amazon DocumentDB](#)

1. Nella console di gestione Amazon DocumentDB, in Clusters, scegli Crea.

Cluster identifier	Role	Engine version	Region & AZ	Status	Instance health	CPU
docdb-2023-05-15-16-06-42	Regional cluster	5.0.0	us-east-1	available	-	-
docdb-2023-05-15-16-06-42	Primary instance	5.0.0	us-east-1f	available	healthy	8.32%
docdb-2023-05-15-16-06-422	Replica instance	5.0.0	us-east-1c	available	healthy	7.33%
docdb-2023-05-15-16-06-423	Replica instance	5.0.0	us-east-1c	available	healthy	7.80%

2. Nella pagina Crea cluster Amazon DocumentDB, nella sezione Tipo di cluster, scegli Cluster basati su istanze (questa è l'opzione predefinita).

Cluster type

Instance Based Cluster

Instance based cluster can scale your database to millions of reads per second and up to 64TB of storage capacity. With instance based clusters you can choose your instance type based on your requirements.

Elastic Cluster

Elastic clusters can scale your database to millions of reads and writes per second, with petabytes of storage capacity. Elastic clusters support MongoDB compatible sharding APIs. With Elastic Clusters, you do not need to choose, manage or upgrade instances.

3. Nella sezione Configurazione, scegli 1 istanza. La scelta di un'istanza aiuta a ridurre al minimo i costi. Se si trattasse di un sistema di produzione, consigliamo di effettuare il provisioning di tre istanze per l'elevata disponibilità. Puoi lasciare le altre impostazioni nella sezione Configurazione ai valori predefiniti.

Configuration

Cluster identifier [Info](#)
Specify a unique cluster identifier.

docdb-2023-05-19-18-37-37

Engine version
5.0.0

Instance class [Info](#)
db.r6g.large
2 vCPUs 16GiB RAM

Number of instances [Info](#)
1

4. Per la connettività, lascia l'impostazione predefinita di Non connetterti a una risorsa di calcolo EC2.

Connectivity G

Compute resources
Choose whether to set up a connection to a compute resource for this database. Setting up a connection will automatically change connectivity settings so that the compute resource can connect to this database.

Connect to an EC2 compute resource
Set up a connection to an EC2 compute resource for this database.

Don't connect to an EC2 compute resource
Don't set up a connection to a compute resource for this database.

5. Nella sezione Autenticazione, inserisci le credenziali di accesso.

Authentication

Username [Info](#)
Specify an alphanumeric string that defines the login ID for the user.


SampleUser1
Username must start with a letter and contain 1 to 63 characters

Password [Info](#) Confirm password [Info](#)

.....

Password must be at least eight characters long and cannot contain a / (slash), " (double quote) or @ (at symbol).

6. Attiva Mostra impostazioni avanzate.

Show advanced settings  Cancel Create cluster

7. Nella sezione Impostazioni di rete, per i gruppi di sicurezza VPC, scegli DemoDocDB (VPC) se stai creando un cluster di test o demo. Se stai creando un cluster per un sistema di produzione, scegli predefinito (VPC) o se desideri creare un gruppo di sicurezza VPC specifico, consulta [Gruppi](#) di sicurezza nella Amazon Virtual Private Cloud User Guide.

Network settings

Virtual Private Cloud (VPC) [Info](#)
VPC defines the virtual networking environment for this cluster.

vpc-02c0445657b77542c

Only VPCs with a corresponding subnet group are listed. Once a cluster is created, the VPC cannot be changed.

Subnet group [Info](#)
A subnet group is a collection of subnets that are within a VPC.

default

VPC security groups
A security group acts as a virtual firewall for your instance to control inbound and outbound traffic.

Select VPC security groups

default (VPC) X

8. Scegli Create cluster (Crea cluster).

Show advanced settings Cancel Create cluster

Amazon DocumentDB sta ora effettuando il provisioning del cluster, operazione che può richiedere fino a qualche minuto. Puoi connetterti al cluster quando lo stato del cluster e dell'istanza è uguale a **available**

Note

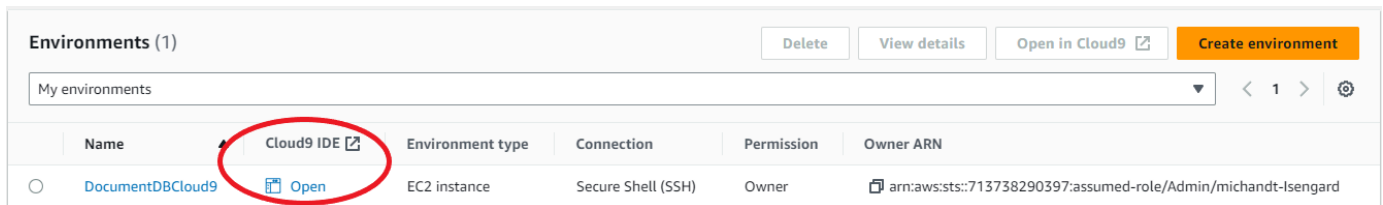
Per informazioni sui valori dello stato del cluster, consulta il [Valori dello stato del cluster](#) capitolo Monitoring Amazon DocumentDB.

Per informazioni sui valori dello stato dell'istanza, consulta il [Valori di stato delle istanze](#) capitolo Monitoring Amazon DocumentDB.

Passaggio 4: installa la shell mongo

Ora installerai la mongo shell nell'AWS Cloud9ambiente che hai creato nel passaggio 1. La mongo shell è un'utilità da riga di comando che puoi utilizzare per connettere e interrogare il tuo cluster Amazon DocumentDB.

1. Se l'AWS Cloud9ambiente è ancora aperto dalla Fase 1, torna a quell'ambiente e passa all'istruzione 3. Se ti sei allontanato dal tuo AWS Cloud9 ambiente, nella console di AWS Cloud9 gestione, in Ambienti, trova l'ambiente denominato DocumentDBCloud9. Scegli Apri nella colonna IDE Cloud9.



Environments (1) Delete View details Open in Cloud9 Create environment

My environments

Name	Cloud9 IDE	Environment type	Connection	Permission	Owner ARN
DocumentDBCloud9	Open	EC2 instance	Secure Shell (SSH)	Owner	arn:aws:sts::713738290397:assumed-role/Admin/michandt-lsengard

- Al prompt dei comandi, create il file del repository con il seguente comando:

```
echo -e "[mongodb-org-4.0] \nname=MongoDB Repository\nbaseurl=https://
repo.mongodb.org/yum/amazon/2013.03/mongodb-org/4.0/x86_64/\ngpgcheck=1 \nenabled=1
\ngpgkey=https://www.mongodb.org/static/pgp/server-4.0.asc" | sudo tee /etc/
yum.repos.d/mongodb-org-4.0.repo
```

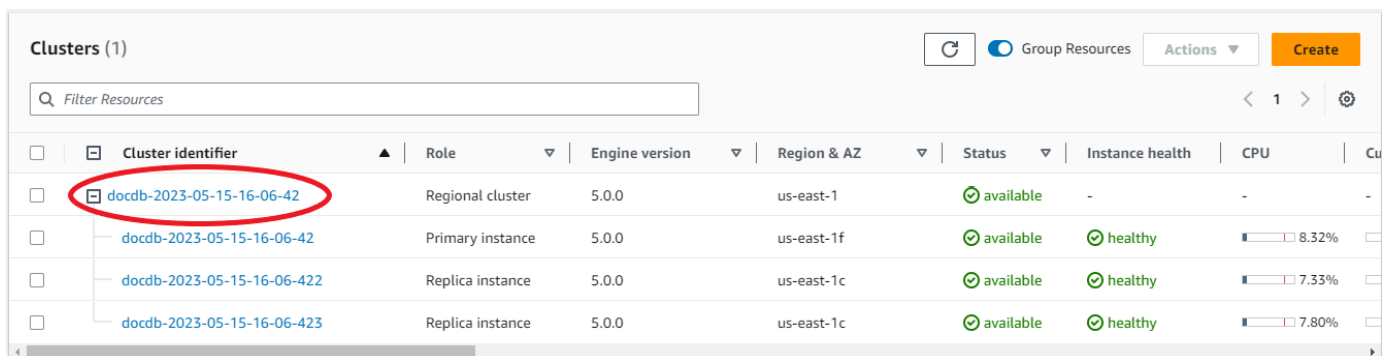
- Quando è completo, installa la shell mongo con il seguente comando:

```
sudo yum install -y mongodb-org-shell
```

Fase 5: Connettiti al tuo cluster Amazon DocumentDB

Ora ti conetterai al tuo cluster Amazon DocumentDB utilizzando la shell mongo che hai installato nella fase 4.

- Nella console di gestione di Amazon DocumentDB, in Clusters, individua il cluster. Scegli il cluster che hai creato facendo clic sull'identificatore del cluster.



Clusters (1) Refresh Group Resources Actions Create

Filter Resources

Cluster identifier	Role	Engine version	Region & AZ	Status	Instance health	CPU
docdb-2023-05-15-16-06-42	Regional cluster	5.0.0	us-east-1	available	-	-
docdb-2023-05-15-16-06-42	Primary instance	5.0.0	us-east-1f	available	healthy	8.32%
docdb-2023-05-15-16-06-422	Replica instance	5.0.0	us-east-1c	available	healthy	7.33%
docdb-2023-05-15-16-06-423	Replica instance	5.0.0	us-east-1c	available	healthy	7.80%

- E nryption-in-transit è abilitato per impostazione predefinita su Amazon DocumentDB. Facoltativamente, puoi disabilitare TLS. Per scaricare il certificato corrente richiesto per l'autenticazione nel cluster, nella scheda Connettività e sicurezza, nella sezione Connect, sotto Scarica il certificato Amazon DocumentDB Certificate Authority (CA) necessario per l'autenticazione nel cluster, copia la stringa di connessione fornita. Torna al tuo AWS Cloud9 ambiente e incolla la stringa di connessione.

Connectivity & security | Instances | Configuration | Monitoring | Events & tags | Maintenance & backups

Connect

Getting Started Guide | Enabling/Disabling TLS | Connecting programmatically

Download the Amazon DocumentDB Certificate Authority (CA) certificate required to authenticate to your cluster [Copy](#)

```
wget https://truststore.pki.rds.amazonaws.com/us-east-1/us-east-1-bundle.pem
```

Connect to this cluster with the mongo shell [Copy](#)

```
mongo --ssl --host docdb-2023-06-02-14-26-22.cluster-cozt4xr9xv9b.us-east-1.docdb.amazonaws.com:27017 --sslCAFile us-east-1-bundle.pem --username testuser --password <insertYourPassword>
```

Connect to this cluster with an application [Copy](#)

```
mongodb://testuser:<insertYourPassword>@docdb-2023-06-02-14-26-22.cluster-cozt4xr9xv9b.us-east-1.docdb.amazonaws.com:27017/?ssl=true&ssl_ca_certs=us-east-1-bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false
```

3. Torna al tuo cluster nella console Amazon DocumentDB, nella scheda Connettività e sicurezza, nella sezione Connect, sotto Connetti a questo cluster con la shell mongo, copia la stringa di connessione fornita. Ometti la copia <insertYourPassword> in modo che ti venga richiesta la password dalla shell mongo quando ti connetti.

Connectivity & security | Instances | Configuration | Monitoring | Events & tags | Maintenance & backups

Connect

Getting Started Guide | Enabling/Disabling TLS | Connecting programmatically

Download the Amazon DocumentDB Certificate Authority (CA) certificate required to authenticate to your cluster [Copy](#)

```
wget https://truststore.pki.rds.amazonaws.com/us-east-1/us-east-1-bundle.pem
```

Connect to this cluster with the mongo shell [Copy](#)

```
mongo --ssl --host docdb-2023-06-02-14-26-22.cluster-cozt4xr9xv9b.us-east-1.docdb.amazonaws.com:27017 --sslCAFile us-east-1-bundle.pem --username testuser --password <insertYourPassword>
```

Connect to this cluster with an application [Copy](#)

```
mongodb://testuser:<insertYourPassword>@docdb-2023-06-02-14-26-22.cluster-cozt4xr9xv9b.us-east-1.docdb.amazonaws.com:27017/?ssl=true&ssl_ca_certs=us-east-1-bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false
```

Torna al tuo AWS Cloud9 ambiente e incolla la stringa di connessione.

Quando inserisci la password e il prompt diventa richiesto, sei connesso correttamente al tuo cluster Amazon `rs0:PRIMARY>` DocumentDB.

Note

Per informazioni sulla risoluzione dei problemi, consulta [Troubleshooting Amazon DocumentDB](#).

Fase 6: Inserimento e interrogazione dei dati

Ora che sei connesso al cluster, puoi eseguire alcune query per acquisire familiarità con l'utilizzo di un database di documenti.

1. Per inserire un singolo documento, inserisci quanto segue:

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

2. Otterrete il seguente risultato:

```
WriteResult({ "nInserted" : 1 })
```

3. Puoi leggere il documento che hai scritto con il `findOne()` comando (perché restituisce solo un singolo documento). Inserisci quanto segue:

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

4. Si ottiene il seguente risultato:

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

5. Per eseguire qualche altra domanda, considera un caso d'uso dei profili di gioco. Innanzitutto, inserisci alcune voci in una raccolta intitolata `profiles`. Inserisci quanto segue:

```
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}
])
```

6. Si ottiene il seguente risultato:

```
{ "acknowledged" : true, "insertedIds" : [ 1, 2, 3, 4 ] }
```

7. Utilizzate il `find()` comando per restituire tutti i documenti nella raccolta dei profili. Inserisci quanto segue:

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

8. Otterrai un output che corrisponderà ai dati che hai digitato nel passaggio 5.
9. Usa una query per un singolo documento usando un filtro. Inserisci quanto segue:

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

10. Dovresti recuperare questo risultato:

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

11. Ora proviamo a trovare un profilo e modificarlo usando il `findAndModify` comando. Daremo all'utente Matt altri dieci punti con il seguente codice:

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

12. Otterrete il seguente risultato (notate che il suo punteggio non è ancora aumentato):

```
{
  "_id" : 1,
  "name" : "Matt",
  "status" : "active",
  "level" : 12,
  "score" : 202
}
```

13. Puoi verificare che il suo punteggio sia cambiato con la seguente domanda:

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

14. Si ottiene il seguente risultato:

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

Fase 7: Esplora

Complimenti! Hai completato con successo la Guida introduttiva ad Amazon DocumentDB.

Qual è il prossimo passo? Scopri come sfruttare appieno questo database con alcune delle sue funzionalità più popolari:

- [Gestione di Amazon DocumentDB](#)
- [Dimensionamento](#)
- [Backup e ripristino](#)

Note

Il cluster creato con questo esercizio introduttivo continuerà a generare costi a meno che non venga eliminato. Per istruzioni, consulta [Eliminazione di un cluster Amazon DocumentDB](#).

Guida rapida all'uso di Amazon DocumentDB AWS CloudFormation

Questa sezione contiene passaggi e altre informazioni per aiutarti a iniziare rapidamente a usare Amazon DocumentDB (con compatibilità con MongoDB) utilizzando [AWS CloudFormation](#). Per informazioni generali su Amazon DocumentDB, consulta [Cos'è Amazon DocumentDB \(con compatibilità con MongoDB\)](#).

Queste istruzioni utilizzano un AWS CloudFormation modello per creare un cluster e delle istanze nel tuo Amazon VPC predefinito. Per istruzioni su come creare queste risorse, consultare [Inizia a usare Amazon DocumentDB](#).

Important

Lo AWS CloudFormation stack creato da questo modello crea più risorse, incluse risorse in Amazon DocumentDB (ad esempio, un cluster e istanze) e Amazon Elastic Compute Cloud (ad esempio, un gruppo di sottoreti).

Alcune di queste risorse non sono gratuite. Per informazioni sui prezzi, consulta i prezzi di [Amazon DocumentDB e i prezzi](#) di [Amazon EC2](#). Al termine, è possibile eliminare lo stack per interrompere gli addebiti.

Questo AWS CloudFormation stack è destinato esclusivamente a scopi didattici. Se utilizzi questo modello per un ambiente di produzione, ti consigliamo di utilizzare politiche e sicurezza IAM più rigorose. Per informazioni sulla protezione delle risorse, consulta [Amazon VPC Security](#) e [Amazon EC2 Network and Security](#).

Argomenti

- [Prerequisiti](#)
- [Avvio di uno stack Amazon DocumentDB AWS CloudFormation](#)
- [Accesso al cluster Amazon DocumentDB](#)
- [Protezione da cessazione ed eliminazione](#)

Prerequisiti

Prima di creare un cluster Amazon DocumentDB, devi disporre di quanto segue:

- Un Amazon VPC predefinito
- Le autorizzazioni IAM richieste

Autorizzazioni IAM richieste

Le seguenti autorizzazioni consentono di creare le risorse per lo stack AWS CloudFormation:

AWSPolitiche gestite

- `AWSCloudFormationReadOnlyAccess`
- `AmazonDocDBFullAccess`

Autorizzazioni aggiuntive per IAM

La policy seguente illustra le autorizzazioni aggiuntive necessarie per creare e rimuovere questo stack AWS CloudFormation.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:GetSSHPublicKey",
        "iam:ListSSHPublicKeys",
        "iam:CreateRole",
        "iam:CreatePolicy",
        "iam:PutRolePolicy",
        "iam:CreateInstanceProfile",
        "iam:AddRoleToInstanceProfile",
        "iam:GetAccountSummary",
        "iam:ListAccountAliases",
        "iam:GetRole",
        "iam:DeleteRole",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteRolePolicy",
```

```

        "iam:DeleteInstanceProfile",
        "cloudformation:*Stack",
        "ec2:DescribeKeyPairs",
        "ec2:*Vpc",
        "ec2:DescribeInternetGateways",
        "ec2:*InternetGateway",
        "ec2:createTags",
        "ec2:*VpcAttribute",
        "ec2:DescribeRouteTables",
        "ec2:*RouteTable",
        "ec2:*Subnet",
        "ec2:*SecurityGroup",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DescribeVpcEndpoints",
        "ec2:*VpcEndpoint",
        "ec2:*SubnetAttribute",
        "ec2:*Route",
        "ec2:*Instances",
        "ec2:DeleteVpcEndpoints"
    ],
    "Resource": "*"
},
{
    "Sid": "iamPassRole",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "iam:PassedToService": "rds.amazonaws.com"
        }
    }
}
]
}

```

Note

Le autorizzazioni in grassetto nella policy precedente sono richieste solo per eliminare uno stack: **iam:DeleteRole**, **iam:RemoveRoleFromInstanceProfile**, **iam:DeleteRolePolicy**, **iam:DeleteInstanceProfile** e

ec2:DeleteVpcEndpoints. Inoltre, ec2:*Vpc concede le autorizzazioni ec2:DeleteVpc.




Coppia di chiavi Amazon EC2





Devi avere una coppia di chiavi e il file PEM disponibili nella regione in cui creerai lo stack AWS CloudFormation. Se devi creare una coppia di chiavi, consulta [Creazione di una coppia di chiavi con Amazon EC2](#) nella Guida per l'utente di Amazon EC2 per istanze Linux.

Avvio di uno stack Amazon DocumentDB AWS CloudFormation

Questa sezione descrive come avviare e configurare uno stack Amazon DocumentDB. AWS CloudFormation

1. Accedi alla AWS Management Console all'indirizzo <https://console.aws.amazon.com/>.
2. La tabella seguente elenca i modelli di stack Amazon DocumentDB per ciascuno di essi. Regione AWS Scegli Launch Stack per il tipo in Regione AWS cui vuoi lanciare lo stack.

Regione	Visualizza modello	Visualizzazione in Designer	Avvia
Stati Uniti orientali (Ohio)	Visualizza modello	Visualizzazione in Designer	
Stati Uniti orientali (Virginia settentrionale)	Visualizza modello	Visualizzazione in Designer	
US West (Oregon)	Visualizza modello	Visualizzazione in Designer	
Asia Pacifico (Mumbai)	Visualizza modello	Visualizzazione in Designer	
Asia Pacifico (Seul)	Visualizza modello	Visualizzazione in Designer	

Regione	Visualizza modello	Visualizzazione in Designer	Avvia
Asia Pacifico (Singapore)	Visualizza modello	Visualizzazione in Designer	
Asia Pacifico (Sydney)	Visualizza modello	Visualizzazione in Designer	
Asia Pacifico (Tokyo)	Visualizza modello	Visualizzazione in Designer	
Canada (Centrale)	Visualizza modello	Visualizzazione in Designer	
Europa (Francoforte)	Visualizza modello	Visualizzazione in Designer	
Europa (Irlanda)	Visualizza modello	Visualizzazione in Designer	
Europa (Londra)	Visualizza modello	Visualizzazione in Designer	
Europa (Parigi)	Visualizza modello	Visualizzazione in Designer	

3. Crea stack: descrive il modello Amazon DocumentDB selezionato. Ogni stack è basato su un modello, un file JSON o YAML, che contiene la configurazione AWS delle risorse che desideri includere nello stack. Poiché hai scelto di avviare uno stack tra i modelli forniti sopra, il modello è già stato configurato per creare uno stack Amazon DocumentDB per Regione AWS lo stack che hai scelto.

Quando avvii uno AWS CloudFormation stack, la [protezione da eliminazione](#) per il tuo cluster Amazon DocumentDB è disabilitata per impostazione predefinita. Se si desidera abilitare la protezione da eliminazione per il cluster, eseguire la procedura seguente. In caso contrario, scegliere Next (Avanti) per continuare con la fase successiva.

Per abilitare la protezione da eliminazione per il tuo cluster Amazon DocumentDB:

1. Scegliere View in Designer (Visualizza in Designer) nell'angolo in basso a destra della pagina Create stack (Crea stack) .
2. Modificare il modello utilizzando l'editor JSON e YAML integrato nella pagina AWS CloudFormation Designer risultante della console. Scorrere fino alla sezione Resources e modificarla per includere DeletionProtection, come segue. Per ulteriori informazioni sull'utilizzo di AWS CloudFormation Designer, consulta [Cos'è AWS 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. Scegliere Create Stack (Crea stack) (



nell'angolo in alto a sinistra della pagina per salvare le modifiche e creare uno stack con queste modifiche abilitate.

4. Dopo aver salvato le modifiche, si verrà reindirizzati alla pagina Create Stack (Crea stack) .

5. Seleziona Successivo per continuare.

4. Specificare i dettagli dello stack: inserisci il nome dello stack e i parametri per il modello. I parametri sono definiti nel modello e consentono di immettere valori personalizzati quando crei o aggiorni uno stack.

- In Stack name (Nome stack), immettere un nome per lo stack o accettare il nome fornito. Il nome dello stack può includere lettere (A—Z e a—z), numeri (0—9) e trattini (—).
- In Parameters (Parametri), immettere i seguenti dettagli:
 - DB ClusterName: inserisci un nome per il tuo cluster Amazon DocumentDB o accetta il nome fornito.

Vincoli per la denominazione del cluster:

- La lunghezza è di [1—63] lettere, numeri o trattini.
- Il primo carattere deve essere una lettera.
- Non può terminare con un trattino o contenere due trattini consecutivi.
- Deve essere unico per tutti i cluster di Amazon RDS, Neptune e Amazon DocumentDB per regione. Account AWS
- DB InstanceClass: dall'elenco a discesa, seleziona la classe di istanza per il tuo cluster Amazon DocumentDB.
- DB InstanceName: inserisci un nome per la tua istanza Amazon DocumentDB o accetta il nome fornito.

Vincoli per la denominazione di un'istanza:

- La lunghezza è di [1—63] lettere, numeri o trattini.
- Il primo carattere deve essere una lettera.
- Non può terminare con un trattino o contenere due trattini consecutivi.
- Deve essere unico per tutte le istanze in Amazon RDS, Neptune e Amazon DocumentDB per regione. Account AWS

- **MasterUser**— Il nome utente dell'account di amministratore del database. **MasterUser** Deve iniziare con una lettera e può contenere solo caratteri alfanumerici.

Scegliere **Next (Avanti)** per salvare le modifiche e continuare.

5. Configura le opzioni dello stack: configura i tag, le autorizzazioni e le opzioni aggiuntive dello stack.
 - **Tag**: specifica le coppie di tag (chiave-valore) da applicare alle risorse dello stack. È possibile aggiungere fino a 50 tag univoci per ogni stack.
 - **Autorizzazioni**: facoltative. Scegli un ruolo IAM per definire in modo esplicito come AWS CloudFormation creare, modificare o eliminare le risorse nello stack. Se non si sceglie un ruolo, AWS CloudFormation utilizza autorizzazioni basate sulle credenziali utente. Prima di specificare un ruolo del servizio, assicurarsi di disporre dell'autorizzazione per passarlo (`iam:PassRole`). L'autorizzazione `iam:PassRole` specifica quali ruolo puoi utilizzare.

Note

Quando specifichi un ruolo del servizio, AWS CloudFormation utilizza sempre quel ruolo per tutte le operazioni eseguite su quello stack. Gli altri utenti che hanno le autorizzazioni per eseguire operazioni su questo stack saranno in grado di utilizzare questo ruolo, anche se non dispongono dell'autorizzazione per passarlo. Se il ruolo include le autorizzazioni di cui l'utente non dovrebbe disporre, puoi riassegnare involontariamente le autorizzazioni di un utente. Assicurarsi che il ruolo garantisca i [privilegi minimi](#).

- **Opzioni avanzate**: puoi impostare le seguenti opzioni avanzate:
 - **Stack policy**: facoltativa. Definisce le risorse che si desidera proteggere da aggiornamenti involontari durante un aggiornamento dello stack. Per impostazione predefinita, durante un aggiornamento dello stack possono essere aggiornate tutte le risorse.

È possibile inserire la policy di stack direttamente come JSON o caricare un file in formato JSON che contenga la policy dello stack. Per ulteriori informazioni, consulta [Impedire gli aggiornamenti delle risorse stack](#).
 - **Configurazione di rollback**: opzionale. Specificate CloudWatch gli allarmi Logs AWS CloudFormation da monitorare durante la creazione e l'aggiornamento dello stack. Se l'operazione supera una soglia di allarme, questa viene ripristinata da AWS CloudFormation.

- Opzioni di notifica: facoltative. Specificare argomenti per Simple Notification System (SNS).
- Opzioni di creazione dello stack: facoltative. Puoi specificare le seguenti opzioni:
 - Rollback in caso di errore: indica se lo stack deve essere ripristinato o meno se la creazione dello stack fallisce.
 - Timeout: il numero di minuti prima del timeout per la creazione di uno stack.
 - Protezione dalla terminazione: impedisce l'eliminazione accidentale dello stack.

Note

AWS CloudFormation la protezione dalla terminazione è diversa dal concetto di protezione dall'eliminazione di Amazon DocumentDB. Per ulteriori informazioni, consulta [Protezione da cessazione ed eliminazione](#).

Seleziona Successivo per continuare.

6. `Revisione<stack-name>`: esamina il modello dello stack, i dettagli e le opzioni di configurazione. È inoltre possibile aprire un quick-create link (collegamento di creazione rapida) nella parte inferiore della pagina per creare stack con le stesse configurazioni di base di questo.
 - Scegliere Create (Crea) per creare lo stack.
 - In alternativa, è possibile scegliere Create change set (Crea set di modifiche). Un set di modifiche è un'anteprima di come verrà configurato questo stack prima che venga creato. Ciò consente di esaminare varie configurazioni prima di eseguire il set di modifiche.

Accesso al cluster Amazon DocumentDB

Una volta completato lo AWS CloudFormation stack, puoi utilizzare un'istanza Amazon EC2 per connetterti al tuo cluster Amazon DocumentDB. Per informazioni sulla connessione a un'istanza Amazon EC2 tramite SSH, consulta [Connect to Your Linux Instance](#) nella Amazon EC2 User Guide for Linux Instances.

Dopo la connessione, consulta le seguenti sezioni, che contengono informazioni sull'uso di Amazon DocumentDB.

- [Passaggio 4: installa la shell mongo](#)
- [Eliminazione di un cluster Amazon DocumentDB](#)

Protezione da cessazione ed eliminazione

È una best practice di Amazon DocumentDB abilitare la protezione da cancellazioni e terminazioni. CloudFormation la protezione dalla terminazione è una funzionalità nettamente diversa dalla funzionalità di protezione dall'eliminazione di Amazon DocumentDB.

- **Protezione dalla terminazione:** puoi evitare che uno stack venga eliminato accidentalmente abilitando la protezione dalla terminazione per il tuo stack. CloudFormation Se un utente tenta di eliminare uno stack con protezione da cessazione abilitata, l'eliminazione ha esito negativo e lo stack rimane invariato. La protezione dalla terminazione è disattivata per impostazione predefinita quando si crea uno stack utilizzando. CloudFormation Puoi abilitare la protezione da cessazione sullo stack quando lo crei. Per ulteriori informazioni consulta [Impostare le opzioni relative allo stack AWS CloudFormation](#).
- **Protezione da eliminazione:** Amazon DocumentDB offre anche la possibilità di abilitare la protezione da eliminazione per un cluster. Se un utente tenta di eliminare un cluster Amazon DocumentDB con la protezione da eliminazione abilitata, l'eliminazione fallisce e il cluster rimane invariato. La protezione da eliminazione, se abilitata, protegge da eliminazioni accidentali da Amazon AWS Management Console DocumentDB AWS CLI e. CloudFormation Per ulteriori informazioni sull'attivazione e la disabilitazione della protezione da eliminazione per un cluster Amazon DocumentDB, consulta. [Deletion protection \(Protezione da eliminazione\)](#)

Compatibilità con MongoDB

Amazon DocumentDB supporta la compatibilità con MongoDB, inclusi MongoDB 4.0 e MongoDB 5.0. La compatibilità con MongoDB significa che la maggior parte delle applicazioni, dei driver e degli strumenti che già utilizzi oggi con i tuoi database MongoDB può essere utilizzata con Amazon DocumentDB con modifiche minime o nulle. Questa sezione descrive tutto ciò che devi sapere sulla compatibilità di Amazon DocumentDB con MongoDB, tra cui nuove funzionalità e caratteristiche, nozioni di base, percorsi di migrazione e differenze funzionali.

Argomenti

- [Compatibilità con MongoDB 5.0](#)
- [Compatibilità con MongoDB 4.0](#)

Compatibilità con MongoDB 5.0

Argomenti

- [Novità di Amazon DocumentDB 5.0](#)
- [Inizia a usare Amazon DocumentDB 5.0](#)
- [Aggiornamento o migrazione ad Amazon DocumentDB 4.0](#)
- [Differenze funzionali](#)

Novità di Amazon DocumentDB 5.0

Amazon DocumentDB 5.0 introduce nuove caratteristiche e funzionalità che includono limiti di storage e crittografia a livello di campo lato client. Il riepilogo seguente presenta alcune delle principali funzionalità introdotte in Amazon DocumentDB 5.0. Per un elenco completo delle nuove funzionalità, consulta la [Note di rilascio](#)

- Limite di storage aumentato a 128 TiB per tutti i cluster Amazon DocumentDB basati su istanze e i cluster elastici basati su shard.
- Introduzione del motore Amazon DocumentDB 5.0 (versione 3.0.775)
 - Supporto per i driver API MongoDB 5.0

- Support per la crittografia a livello di campo (FLE) lato client. Ora puoi crittografare i campi sul lato client prima di scrivere i dati nel cluster Amazon DocumentDB. [Per ulteriori informazioni, consulta Crittografia a livello di campo lato client](#)
- Nuovi operatori di aggregazione: `$dateAdd` `$dateSubtract`
- Supporti per indici con operatore. `$elemMatch` Di conseguenza, le interrogazioni eseguite `$elemMatch` comporteranno scansioni degli indici.

Amazon DocumentDB non supporta tutte le funzionalità di MongoDB 5.0. Quando abbiamo creato Amazon DocumentDB 5.0, abbiamo lavorato a ritroso partendo dalle caratteristiche e dalle funzionalità che i nostri clienti ci chiedevano di sviluppare di più. Continueremo ad aggiungere funzionalità MongoDB 5.0 aggiuntive in base a ciò che i clienti ci chiedono di creare. Per l'elenco più recente delle API supportate, consulta. [API, operazioni e tipi di dati di MongoDB supportati](#)

Inizia a usare Amazon DocumentDB 5.0

Per iniziare a usare Amazon DocumentDB 5.0, consulta la Guida [introduttiva](#). Puoi creare un nuovo cluster Amazon DocumentDB 5.0 utilizzando AWS Management Console o l'AWSSDK, AWS CLI oppure AWS CloudFormation. Quando ci si connette ad Amazon DocumentDB, è necessario utilizzare un driver o un'utilità MongoDB compatibile con MongoDB 5.0 o versioni successive.

Note

Quando si utilizza l'AWSSDK, o AWS CLI/AWS CloudFormation, la versione predefinita del motore è 5.0.0. È necessario specificare esplicitamente il parametro `engineVersion = 4.0.0` per creare un nuovo cluster Amazon DocumentDB 4.0 `engineVersion = 3.6.0` o per creare un nuovo cluster Amazon DocumentDB 3.6. Per un determinato cluster Amazon DocumentDB, puoi determinare la versione del cluster utilizzando AWS CLI to call `describe-db-clusters` o utilizzare la console di gestione Amazon DocumentDB per visualizzare il numero di versione del motore per un determinato cluster.

Amazon DocumentDB 5.0 supporta i processori Amazon EC2 Graviton2 e i tipi di istanza per r6g i cluster t4.medium ed è disponibile in tutte le regioni supportate. Per ulteriori informazioni sui prezzi, consulta la pagina dei prezzi di [Amazon DocumentDB \(con compatibilità con MongoDB\)](#).

Aggiornamento o migrazione ad Amazon DocumentDB 4.0

[Puoi migrare da MongoDB 3.6 o MongoDB 4.0 ad Amazon DocumentDB 5.0 utilizzando le utilità o come, e. AWS DMSmongodumpmongorestoremongoimportmongoexport](#) Per istruzioni su come effettuare la migrazione, consulta. [Aggiornamento del cluster Amazon DocumentDB tramite AWS Database Migration Service](#)

Differenze funzionali

Differenze funzionali tra Amazon DocumentDB 4.0 e 5.0

Con il rilascio di Amazon DocumentDB 5.0, esistono differenze funzionali tra Amazon DocumentDB 3.6 e Amazon DocumentDB 4.0:

- Il ruolo integrato di backup ora supporta. `serverStatus` Azione: gli sviluppatori e le applicazioni con ruolo di backup possono raccogliere statistiche sullo stato del cluster Amazon DocumentDB.
- Il `SecondaryDelaySecs` campo viene sostituito `slaveDelay` in `rep1SetGetConfig` output.
- Il `hello` comando sostituisce `isMaster`: `hello` restituisce un documento che descrive il ruolo di un cluster Amazon DocumentDB.
- Amazon DocumentDB 5.0 ora supporta le scansioni degli indici con l'`$elemMatch` operatore nel primo livello di nesting. Le scansioni dell'indice sono supportate quando il solo filtro di interrogazione ha un livello del `$elemMatch` filtro, ma non sono supportate se è inclusa una query `$elemMatch` annidata.

Ad esempio, in Amazon DocumentDB 5.0, se includi l'`$elemMatch` operatore nel livello annidato, non restituirà un valore come in Amazon DocumentDB 4.0:

```
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 ] } ] ] }

```

- La proiezione «\$» in Amazon DocumentDB 4.0 restituisce tutti i documenti con tutti i campi. Con Amazon DocumentDB 5.0, il find comando con proiezione «\$» restituisce documenti che corrispondono al parametro di query contenente solo il campo corrispondente alla proiezione «\$».
- In Amazon DocumentDB 5.0, i find comandi con \$regex parametri di \$options query restituiscono un errore: «Impossibile impostare le opzioni in entrambi \$regex e\$options».
- Con Amazon DocumentDB 5.0, \$indexOfCP ora restituisce «-1» quando:
 - la sottostringa non si trova nell'espressione stringa, oppure
 - inizio è un numero maggiore di fine, oppure
 - start è un numero maggiore della lunghezza in byte della stringa.
- In Amazon DocumentDB 4.0, \$indexOfCP restituisce «0» quando la posizione iniziale è un numero maggiore della fine o della lunghezza in byte della stringa.
- Con Amazon DocumentDB 5.0, le operazioni di proiezione, ad esempio `_id fields{"_id.nestedField" : 1}`, restituiscono documenti che includono solo il campo proiettato. In Amazon DocumentDB 4.0, invece, i comandi di proiezione di campo annidati non filtrano alcun documento.

Compatibilità con MongoDB 4.0

Argomenti

- [Caratteristiche di Amazon DocumentDB 4.0](#)
- [Inizia a usare Amazon DocumentDB 4.0](#)
- [Aggiornamento o migrazione ad Amazon DocumentDB 4.0](#)
- [Differenze funzionali](#)

Caratteristiche di Amazon DocumentDB 4.0

Amazon DocumentDB 4.0 ha introdotto molte nuove caratteristiche e funzionalità, tra cui transazioni ACID e miglioramenti per modificare i flussi. Il riepilogo seguente mostra alcune delle principali funzionalità introdotte in Amazon DocumentDB 4.0. Per un elenco completo delle funzionalità, consulta la [Note di rilascio](#).

- **Transazioni ACID:** Amazon DocumentDB ora supporta la possibilità di eseguire transazioni su più documenti, dichiarazioni, raccolte e database. Le transazioni semplificano lo sviluppo di applicazioni consentendoti di eseguire operazioni atomiche, consistenti, isolate e durevoli (ACID) su uno o più documenti all'interno di un cluster Amazon DocumentDB. Per ulteriori informazioni, consulta [Transazioni](#).
- **Flussi di modifica:** ora hai la possibilità di aprire un flusso di modifiche a livello di cluster (`client.watch()` o `mongo.watch()`) e di database (`db.watch()`), puoi specificare un cursore `startAtOperationTime` per aprire un cursore del flusso di modifiche e infine puoi estendere il periodo di conservazione del flusso di modifiche a 7 giorni (in precedenza 24 ore). Per ulteriori informazioni, consulta [Utilizzo di Change Streams con Amazon DocumentDB](#).
- **AWS Database Migration Service(AWS DMS):** Ora puoi utilizzarlo AWS DMS per migrare i tuoi carichi di lavoro MongoDB 4.0 su Amazon DocumentDB. AWS DMS ora supporta una fonte MongoDB 4.0, una destinazione Amazon DocumentDB 4.0 e una fonte Amazon DocumentDB 3.6 per eseguire aggiornamenti tra Amazon DocumentDB 3.6 e 4.0. Per ulteriori informazioni, consulta la [documentazione di AWS DMS](#).
- **Prestazioni e indicizzazione:** ora puoi utilizzare un indice con `$lookup`, trovare query con una proiezione che contengono un campo o un campo e il `_id` campo può essere servito direttamente dall'indice e senza bisogno di leggere dalla raccolta (interrogazione coperta), la possibilità di eseguire `hint()` operazioni, ottimizzazioni delle prestazioni e miglioramenti per `$addToSet` ridurre le dimensioni complessive dell'indice. `findAndModify` Per ulteriori informazioni, consulta [Note di rilascio](#).
- **Operatori:** Amazon DocumentDB 4.0 ora supporta una serie di nuovi operatori di aggregazione: `$ifNull`, `$replaceRoot`, `$setIsSubset`, `$setIntersection`, `$setUnion`, `$setEquals`. Puoi vedere tutte le API, le operazioni e i tipi di dati di MongoDB che supportiamo all'indirizzo. [API, operazioni e tipi di dati di MongoDB supportati](#)
- **Controllo degli accessi basato sui ruoli (RBAC):** con entrambi `ListDatabase` i comandi `ListCollection` e ora puoi utilizzare facoltativamente i `authorizedDatabases` parametri `authorizedCollections` e per consentire agli utenti di elencare le raccolte e i database a cui hanno l'autorizzazione ad accedere senza richiedere rispettivamente i ruoli e `listCollections`

`listDatabase` Hai anche la possibilità di eliminare i tuoi cursori senza richiedere il ruolo `KillCursor`

Amazon DocumentDB non supporta tutte le funzionalità di MongoDB 4.0. Quando abbiamo creato Amazon DocumentDB 4.0, abbiamo lavorato a ritroso partendo dalle caratteristiche e dalle capacità che i nostri clienti ci chiedevano di sviluppare di più. Continueremo ad aggiungere funzionalità MongoDB 4.0 aggiuntive in base a ciò che i clienti ci chiedono di creare. Ad esempio, Amazon DocumentDB 4.0 attualmente non supporta gli operatori di conversione dei tipi o gli operatori di stringa introdotti in MongoDB 4.0. Per l'elenco più recente delle API supportate, consulta [API, operazioni e tipi di dati di MongoDB supportati](#)

Inizia a usare Amazon DocumentDB 4.0

Per iniziare a usare Amazon DocumentDB 4.0, consulta la Guida [introduttiva](#). Puoi creare un nuovo cluster Amazon DocumentDB 4.0 utilizzando AWS Management Console o l'AWSSDK, AWS CLI oppure AWS CloudFormation. Quando ci si connette ad Amazon DocumentDB, è necessario utilizzare un driver o un'utilità MongoDB compatibile con MongoDB 4.0 o versioni successive.

Note

Quando si utilizza l'AWSSDK, o AWS CLI/AWS CloudFormation, la versione predefinita del motore è 5.0.0. È necessario specificare esplicitamente il parametro `engineVersion = 4.0.0` per creare un nuovo cluster Amazon DocumentDB 4.0 `engineVersion = 3.6.0` o per creare un nuovo cluster Amazon DocumentDB 3.6. Per un determinato cluster Amazon DocumentDB, puoi determinare la versione del cluster utilizzando AWS CLI to call `describe-db-clusters` o utilizzare la console di gestione Amazon DocumentDB per visualizzare il numero di versione del motore per un determinato cluster.

Amazon DocumentDB 4.0 supporta `r5` e tipi di `t4g.medium` istanza per i cluster ed è disponibile in tutte le regioni supportate. `r6g t3.medium` Non sono previsti costi aggiuntivi per l'utilizzo di Amazon DocumentDB 4.0. Per ulteriori informazioni sui prezzi, consulta la pagina dei prezzi di [Amazon DocumentDB \(con compatibilità con MongoDB\)](#).

Aggiornamento o migrazione ad Amazon DocumentDB 4.0

[Puoi migrare da MongoDB 3.6 o MongoDB 4.0 ad Amazon DocumentDB 4.0 utilizzando o utilità come, e. AWS DMS `mongodump` `mongoexport` `mongoimport` `mongorestore`](#) Allo stesso modo,

puoi utilizzare gli stessi strumenti per l'aggiornamento da Amazon DocumentDB 3.6 ad Amazon DocumentDB 4.0. Per istruzioni su come effettuare la migrazione, consulta. [Aggiornamento del cluster Amazon DocumentDB tramite AWS Database Migration Service](#)

Differenze funzionali

Differenze funzionali tra Amazon DocumentDB 3.6 e 4.0

Con il rilascio di Amazon DocumentDB 4.0, esistono differenze funzionali tra Amazon DocumentDB 3.6 e Amazon DocumentDB 4.0:

- **Proiezione per documenti nidificati:** Amazon DocumentDB 3.6 considera il primo campo di un documento nidificato quando applica una proiezione. Tuttavia, Amazon DocumentDB 4.0 analizzerà i documenti secondari e applicherà la proiezione anche a ciascun documento secondario. Ad esempio: se la proiezione è "a.b.c" : 1, il comportamento in entrambe le versioni è identico. Tuttavia, se la proiezione è {a: {b: {c:1}}}, Amazon DocumentDB 3.6 applicherà la proiezione solo a 'a' e non a 'b' o 'c'.
- **Comportamento per `minKey`, `maxKey`:** In Amazon DocumentDB 4.0, il comportamento per non {x: {\$gt:MaxKey}} restituisce nulla e per {x: {\$lt:MaxKey}} restituisce tutto.
- **Differenze nel confronto tra documenti:** il confronto di valori numerici di diversi tipi (double, int, long) nei documenti secondari (ad esempio, b in {"_id" :1, "a" : {"b":1}}) ora fornisce un output coerente tra i tipi di dati numerici e per ogni livello di un documento.

Differenze funzionali tra Amazon DocumentDB 4.0 e MongoDB 4.0

Di seguito sono riportate le differenze funzionali tra Amazon DocumentDB 4.0 e MongoDB 4.0.

- **Ricerca con chiave vuota nel percorso:** quando una raccolta contiene un documento con una chiave vuota all'interno dell'array (ad esempio {"x" : [{ "" : 10 }, { "b" : 20 }]}) e quando la chiave utilizzata nella query termina con una stringa vuota (ad esempio x.), Amazon DocumentDB restituirà quel documento poiché attraversa tutti i documenti dell'array mentre MongoDB non restituirà quel documento.
- **`$setOnInsert` insieme `$` al percorso:** l'operatore di campo non `$setOnInsert` funzionerà in combinazione con nel percorso `$` in Amazon DocumentDB, che è anche coerente con MongoDB 4.0.

Transazioni

Amazon DocumentDB (con compatibilità MongoDB) ora supporta la compatibilità MongoDB 4.0, transazioni incluse. È possibile eseguire transazioni su più documenti, rendiconti, raccolte e database. Le transazioni semplificano lo sviluppo di applicazioni consentendoti di eseguire operazioni atomiche, coerenti, isolate e durature (ACID) su uno o più documenti all'interno di un cluster Amazon DocumentDB. I casi d'uso più comuni per le transazioni includono l'elaborazione finanziaria, l'evasione e la gestione degli ordini e la creazione di giochi multiplayer.

Non sono previsti costi aggiuntivi per le transazioni. Paghi solo per gli I/O in lettura e scrittura che utilizzi come parte delle transazioni.

Argomenti

- [Requisiti](#)
- [Best practice](#)
- [Restrizioni](#)
- [Monitoraggio e diagnostica](#)
- [Livello di isolamento della transazione](#)
- [Casi d'uso](#)
- [Comandi supportati](#)
- [Funzionalità non supportate](#)
- [Sessioni](#)
- [Errori di transazione](#)

Requisiti

Per utilizzare la caratteristica della transazione, devi soddisfare i seguenti requisiti:

- Devi utilizzare il motore Amazon DocumentDB 4.0.
- È necessario utilizzare un driver compatibile con MongoDB 4.0 o versioni successive.

Best practice

Ecco alcune best practice per ottenere il massimo dalle transazioni con Amazon DocumentDB.

- Effettua o annulla sempre la transazione dopo che è stata completata. Lasciare una transazione in uno stato incompleto limita le risorse del database e può causare conflitti di scrittura.
- Si consiglia di mantenere le transazioni al minor numero di comandi necessari. Se hai transazioni con più estratti conto che possono essere suddivise in più transazioni più piccole, è consigliabile farlo per ridurre la probabilità di un timeout. Cerca sempre di creare transazioni brevi, non letture di lunga durata.

Restrizioni

- Amazon DocumentDB non supporta i cursori all'interno di una transazione.
- Amazon DocumentDB non può creare nuove raccolte in una transazione e non può interrogare/aggiornare raccolte inesistenti.
- I blocchi di scrittura a livello di documento sono soggetti a un timeout di 1 minuto, che non è configurabile dall'utente.
- I comandi di scrittura ritrattabile, `commit retryable` e `retryable abort` non sono supportati in Amazon DocumentDB. Eccezione: Se stai usando mongo shell, non includere il `retryWrites=false` comando in nessuna stringa di codice. Per impostazione predefinita, le scritture ripetibili vengono disabilitate. L'inclusione `retryWrites=false` potrebbe causare errori nei normali comandi di lettura.
- Ogni istanza Amazon DocumentDB ha un limite massimo per il numero di transazioni simultanee aperte sull'istanza contemporaneamente. Per i limiti, vedi [Limiti di istanze](#).
- Per una determinata transazione, la dimensione del registro delle transazioni deve essere inferiore a 32 MB.
- Amazon DocumentDB `count()` supporta una transazione, ma non tutti i driver supportano questa funzionalità. Un'alternativa consiste nell'utilizzare l'`countDocuments()` API, che traduce la query di conteggio in una query di aggregazione lato client.
- Le transazioni hanno un limite di esecuzione di un minuto e le sessioni hanno un timeout di 30 minuti. Se una transazione scade, questa verrà interrotta e qualsiasi comando successivo emesso all'interno della sessione per la transazione esistente genererà il seguente errore:

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

```
} )
```

Monitoraggio e diagnostica

Con il supporto per le transazioni in Amazon DocumentDB 4.0, sono state aggiunte CloudWatch metriche aggiuntive per aiutarti a monitorare le tue transazioni.

Nuove CloudWatch metriche

- `DatabaseTransactions`: il numero di transazioni aperte effettuate in un periodo di un minuto.
- `DatabaseTransactionsAborted`: il numero di transazioni interrotte effettuate in un periodo di un minuto.
- `DatabaseTransactionsMax`: il numero massimo di transazioni aperte in un periodo di un minuto.
- `TransactionsAborted`: il numero di transazioni interrotte su un'istanza in un periodo di un minuto.
- `TransactionsCommitted`: il numero di transazioni effettuate su un'istanza in un periodo di un minuto.
- `TransactionsOpen`: il numero di transazioni aperte su un'istanza eseguite in un periodo di un minuto.
- `TransactionsOpenMax`: il numero massimo di transazioni aperte su un'istanza in un periodo di un minuto.
- `TransactionsStarted`: il numero di transazioni avviate su un'istanza in un periodo di un minuto.

Note

Per ulteriori CloudWatch metriche per Amazon DocumentDB, vai a [Monitoraggio di Amazon DocumentDB con CloudWatch](#).

Inoltre, sono stati aggiunti nuovi campi a `entrancurrentOpIsid` e un nuovo stato per «idle transaction» `eserverStatus`
`transazioni:currentActivecurrentInactivecurrentOpen,totalAborted,totalCommitted,etotalStarted.transactionThreadId`

Livello di isolamento della transazione

Quando si avvia una transazione, è possibile specificare `readConcern` sia il `writeConcern` come mostrato nell'esempio seguente:

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

Per impostazione predefinita `readConcern`, Amazon DocumentDB supporta l'isolamento delle istantanee. Se viene specificato un `readConcern` valore locale, disponibile o maggioritario, Amazon DocumentDB aggiornerà il `readConcern` livello a `snapshot`. Amazon DocumentDB non supporta il `linearizableReadConcern` e specificando un problema di lettura di questo tipo si verificherà un errore.

Infatti `writeConcern`, Amazon DocumentDB supporta la maggioranza per impostazione predefinita e il quorum di scrittura viene raggiunto quando quattro copie dei dati vengono conservate in tre AZ. Se `writeConcern` viene specificato un valore inferiore, Amazon DocumentDB aggiornerà il `writeConcern` valore alla maggioranza. Inoltre, tutte le scritture di Amazon DocumentDB vengono registrate nel diario e l'inserimento nel diario non può essere disabilitato.

Casi d'uso

In questa sezione, esamineremo due casi d'uso per le transazioni: raccolta multipla e raccolta multipla.

Transazioni con più rendiconti

Le transazioni di Amazon DocumentDB sono costituite da più dichiarazioni, il che significa che puoi scrivere una transazione che comprende più dichiarazioni con un `commit` o un `rollback` esplicito. È possibile raggruppare `insert`, `update`, `delete`, e `findAndModify` azioni come un'unica operazione atomica.

Un caso d'uso comune per le transazioni con più rendiconti è una transazione con debito e credito. Ad esempio: devi dei soldi a un amico per i vestiti. Pertanto, devi addebitare (prelevare) \$500 dal tuo account e accreditare \$500 (deposito) sul conto del tuo amico. Per eseguire tale operazione, esegui sia le operazioni di debito che quelle di credito all'interno di un'unica transazione per garantire l'atomicità. In questo modo si evitano scenari in cui 500 USD vengono addebitati sul tuo account, ma non accreditati sull'account del tuo amico. Ecco come si presenterebbe questo caso d'uso:

```
// *** 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();
```

Transazioni di raccolta multipla

Le nostre transazioni sono inoltre a raccolta multipla, il che significa che possono essere utilizzate per eseguire più operazioni all'interno di una singola transazione e su più incassi. Ciò fornisce una visione coerente dei dati e ne mantiene l'integrità. Quando esegui i comandi<> singolarmente, le transazioni sono all-or-nothing esecuzioni, in quanto tutte avranno successo o falliranno tutte.

Ecco un esempio di transazioni di raccolta multipla, che utilizzano lo stesso scenario e gli stessi dati dell'esempio per le transazioni con più rendiconti.

```
// *** 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
```

Esempi di API di transazione per l'API di callback

L'API di callback è disponibile solo per driver 4.2+.

Javascript

Il codice seguente dimostra come utilizzare l'API di transazione Amazon DocumentDB con Javascript.

```
// *** 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

Il codice seguente dimostra come utilizzare l'API di transazione Amazon DocumentDB con Node.js.

```
// 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#

Il codice seguente dimostra come utilizzare l'API di transazione Amazon DocumentDB con C#.

```

// 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

Il codice seguente dimostra come utilizzare l'API di transazione Amazon DocumentDB con Ruby.

```
// 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

Il codice seguente dimostra come utilizzare l'API di transazione Amazon DocumentDB con Go.

```
// 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.NoError(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)
// 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

Il codice seguente dimostra come utilizzare l'API di transazione Amazon DocumentDB con Java.

```

// 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

Il codice seguente dimostra come utilizzare l'API di transazione Amazon DocumentDB con C.

```

// 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

Il codice seguente dimostra come utilizzare l'API di transazione Amazon DocumentDB con Python.

```
// 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
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
```

Esempi di API di transazione per l'API principale

Javascript

Il codice seguente dimostra come utilizzare l'API di transazione Amazon DocumentDB con Javascript.

```
// *** 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#

Il codice seguente dimostra come utilizzare l'API di transazione Amazon DocumentDB con C#.

```

// 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

Il codice seguente dimostra come utilizzare l'API di transazione Amazon DocumentDB con Ruby.

```
# 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})
end
```

```
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
```

Java

Il codice seguente dimostra come utilizzare l'API di transazione Amazon DocumentDB con Java.

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

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

  MongoDBDatabase 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 = MongoClient.create(uri);

    MongoDB database = mongoClient.getDatabase("bank");
    MongoCollection accountColl = database.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.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
observation", e);
        }
        if (!errors.isEmpty()) {
            throw errors.get(0);
        }
        return this;
    }

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

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

```

    }
}

```

C

Il codice seguente dimostra come utilizzare l'API di transazione Amazon DocumentDB con C.

```

// 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

Il codice seguente dimostra come utilizzare l'API di transazione Amazon DocumentDB con Scala.

```

// Scala Core API
def transferMoneyWithRetry(sessionObservable: SingleObservable[ClientSession] ,
database: MongoDBase ): 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()
}
```

Comandi supportati

Comando	Supportato
<code>abortTransaction</code>	Sì
<code>commitTransaction</code>	Sì
<code>endSessions</code>	Sì
<code>killSession</code>	Sì
<code>killAllSession</code>	Sì

Comando	Supportato
<code>killAllSessionsByPattern</code>	No
<code>refreshSessions</code>	No
<code>startSession</code>	Sì

Funzionalità non supportate

Metodi	Fasi o comandi
<code>db.collection.aggregate()</code>	<code>\$collStats</code> <code>\$currentOp</code> <code>\$indexStats</code> <code>\$listSessions</code> <code>\$out</code>
<code>db.collection.count()</code> <code>db.collection.countDocuments()</code>	<code>\$where</code> <code>\$near</code> <code>\$nearSphere</code>
<code>db.collection.insert()</code>	<code>insertn</code> non è supportato se non viene eseguito su una raccolta esistente. Questo metodo è supportato se si rivolge a una raccolta preesistente.

Sessioni

Le sessioni MongoDB sono un framework utilizzato per supportare scritture ripetibili, coerenza causale, transazioni e gestire le operazioni tra i database. Quando viene creata una sessione, il client

genera un identificatore logico di sessione (lsid) che viene utilizzato per etichettare tutte le operazioni all'interno di quella sessione quando si inviano comandi al server.

Amazon DocumentDB supporta l'uso di sessioni per abilitare le transazioni, ma non supporta la coerenza causale o le scritture ripetibili.

Quando si utilizzano transazioni all'interno di Amazon DocumentDB, una transazione verrà avviata dall'interno di una sessione utilizzando l'`session.startTransaction()` API e una sessione supporta una singola transazione alla volta. Allo stesso modo, le transazioni vengono completate utilizzando le API `commit(session.commitTransaction())` o `abort(session.abortTransaction())`.

Consistenza causale

La coerenza causale garantisce che all'interno di una singola sessione client il client osserverà la read-after-write coerenza, le letture e le scritture monoatomiche seguiranno le letture e queste garanzie si applicano a tutte le istanze di un cluster, non solo a quella primaria. Amazon DocumentDB non supporta la consistenza causale e la seguente dichiarazione genererà un errore.

```
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()
```

È possibile disabilitare la coerenza causale all'interno di una sessione. Tieni presente che questa operazione ti consentirà di utilizzare il framework di sessione, ma non fornirà garanzie di coerenza causale per le letture. Quando si utilizza Amazon DocumentDB, le letture dalla versione primaria saranno read-after-write coerenti e le letture delle istanze di replica alla fine saranno coerenti. Le transazioni sono il caso d'uso principale per l'utilizzo delle sessioni.

```
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 }
```

Scritture ritrattabili

Le scritture ritrattabili sono una funzionalità in cui il client tenterà di riprovare le operazioni di scrittura, una volta sola, quando si verificano errori di rete o se il client non è in grado di trovare il primario. In Amazon DocumentDB, le scritture ripetibili non sono supportate e devono essere disabilitate. Puoi disabilitarlo con il comando (`retryWrites=false`) nella stringa di connessione.

Eccezione: Se stai usando mongo shell, non includere il `retryWrites=false` comando in nessuna stringa di codice. Per impostazione predefinita, le scritture ripetibili vengono disabilitate. L'inclusione `retryWrites=false` potrebbe causare errori nei normali comandi di lettura.

Errori di transazione

Quando si utilizzano le transazioni, esistono scenari che possono generare un errore che indica che il numero di transazione non corrisponde a nessuna transazione in corso.

L'errore può essere generato in almeno due scenari diversi:

- After the one-minute transaction timeout.
- After an instance restart (due to patching, crash recovery, etc.), it is possible to receive this error even in cases where the transaction successfully committed. During an instance restart, the database can't tell the difference between a transaction that successfully completed versus a transaction that aborted. In other words, the transaction completion state is ambiguous.

Il modo migliore per gestire questo errore è rendere idempotenti gli aggiornamenti transazionali, ad esempio utilizzando il `$set` mutatore anziché un'operazione di incremento/decremento. Vedi sotto:

```
{ "ok" : 0,
```

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

Best practice per Amazon DocumentDB

Scopri le best practice per lavorare con Amazon DocumentDB (con compatibilità con MongoDB). Questa sezione viene continuamente aggiornata man mano che vengono identificate nuove best practice.

Argomenti

- [Linee guida operative di base](#)
- [Dimensione delle istanze](#)
- [Utilizzo degli indici](#)
- [Best practice di sicurezza](#)
- [Ottimizzazione dei costi](#)
- [Utilizzo di parametri per identificare problemi a livello di prestazioni](#)
- [Carichi di lavoro di serie temporali e TTL](#)
- [Migrazioni](#)
- [Utilizzo di gruppi di parametri di cluster](#)
- [Query di pipeline di aggregazione](#)
- [batchInsert e batchUpdate](#)

Linee guida operative di base

Di seguito sono riportate le linee guida operative di base che tutti dovrebbero seguire quando lavorano con Amazon DocumentDB. L'accordo sul livello di servizio di Amazon DocumentDB richiede il rispetto di queste linee guida.

- Implementa un cluster composto da due o più istanze Amazon DocumentDB in AWS due zone di disponibilità. Per i carichi di lavoro di produzione, consigliamo di implementare un cluster composto da tre o più istanze di Amazon DocumentDB in tre zone di disponibilità.
- Utilizza il servizio nei limiti indicati. Per ulteriori informazioni, consulta [Quote e limiti di Amazon DocumentDB](#).
- Monitora l'utilizzo della memoria, della CPU, delle connessioni e dello storage. Per aiutarti a mantenere le prestazioni e la disponibilità del sistema, configura Amazon in CloudWatch modo che ti avvisi quando i modelli di utilizzo cambiano o quando ti avvicini alla capacità della tua implementazione.

- Incrementa la capacità delle istanze quando stai per raggiungere i limiti della capacità di storage. È necessario eseguire il provisioning delle istanze con risorse di calcolo sufficienti (ad esempio, RAM, CPU) per soddisfare aumenti imprevisti della domanda da parte delle applicazioni.
- Imposta il periodo di retention dei backup per allineare l'obiettivo del punto di ripristino.
- Prova il failover per il cluster per capire quanto tempo impiega il processo per il tuo caso d'uso. Per ulteriori informazioni, consulta [Failover di Amazon DocumentDB](#).
- Connettiti al tuo cluster Amazon DocumentDB con l'endpoint del cluster (vedi [Endpoint Amazon DocumentDB](#)) e in modalità set di repliche (vedi [Connessione ad Amazon DocumentDB come set di repliche](#)) per ridurre al minimo l'impatto di un failover sulla tua applicazione.
- Scegli un'impostazione di preferenza di lettura del driver che massimizza il dimensionamento della lettura nel rispetto dei requisiti di coerenza di lettura dell'applicazione. La preferenza di lettura `secondaryPreferred` consente la lettura delle repliche e libera l'istanza primaria per eseguire ulteriori operazioni. Per ulteriori informazioni, consulta [Opzioni per le preferenze di lettura](#).
- Progetta la tua applicazione per essere resiliente in caso di errori della rete e del database. Usa il meccanismo di errore del driver per distinguere tra errori temporanei ed errori persistenti. Ripeti gli errori temporanei utilizzando un meccanismo di backoff esponenziale quando appropriato. Assicurati che l'applicazione consideri la coerenza dei dati quando implementa una logica di ripetizione.
- Attiva la protezione dell'eliminazione dei cluster per tutti i cluster di produzione o per qualsiasi cluster contenente dati importanti. Prima di eliminare un cluster Amazon DocumentDB, scatta uno snapshot finale. Se stai distribuendo risorse con AWS CloudFormation, abilita la protezione dalla terminazione. Per ulteriori informazioni, consulta [Protezione da cessazione ed eliminazione](#).
- Quando si crea un cluster Amazon DocumentDB, `--engine-version` è un parametro opzionale che utilizza per impostazione predefinita l'ultima versione principale del motore. L'attuale versione principale del motore è la 4.0.0. Quando vengono rilasciate nuove versioni principali del motore, la versione predefinita del motore per `--engine-version` verrà aggiornata in modo da riflettere l'ultima versione principale del motore. Di conseguenza, per i carichi di lavoro di produzione, e in particolare quelli che dipendono da script, automazione o AWS CloudFormation modelli, ti consigliamo di specificare esplicitamente `--engine-version` nella versione principale desiderata.

Dimensione delle istanze

Uno degli aspetti più critici della scelta della dimensione dell'istanza in Amazon DocumentDB è la quantità di RAM per la cache. Amazon DocumentDB riserva un terzo della RAM per i propri servizi,

il che significa che solo due terzi della RAM dell'istanza sono disponibili per la cache. Pertanto, è una best practice di Amazon DocumentDB scegliere un tipo di istanza con RAM sufficiente per contenere il set di lavoro (ad esempio, dati e indici) in memoria. L'uso di istanze di dimensioni adeguate contribuirà a ottimizzare le prestazioni complessive e, potenzialmente, ridurre al minimo i costi di I/O. Puoi utilizzare il [calcolatore di dimensionamento di terze parti di Amazon DocumentDB per stimare la](#) dimensione dell'istanza per un particolare carico di lavoro.

Per determinare se il set di lavoro dell'applicazione si adatta alla memoria, monitora l'BufferCacheHitRatio utilizzo di Amazon CloudWatch per ogni istanza in un cluster sotto carico.

La BufferCacheHitRatio CloudWatch metrica misura la percentuale di dati e indici serviti dalla cache di memoria di un'istanza (rispetto al volume di archiviazione). In generale, il valore di BufferCacheHitRatio dovrebbe essere il più alto possibile, poiché la lettura dei dati dalla memoria del working set è più veloce e più conveniente rispetto alla lettura dal volume di archiviazione. Anche se è consigliabile mantenere il valore BufferCacheHitRatio il più vicino possibile al 100%, il miglior valore ottenibile dipenderà dai modelli di accesso e dai requisiti di prestazione dell'applicazione. Per mantenere il massimo valore BufferCacheHitRatio possibile, si consiglia di eseguire il provisioning delle istanze del cluster con una sufficiente quantità di RAM per poter adattare gli indici e i working set di dati in memoria.

Se i tuoi indici non si adattano alla memoria, vedrai un valore inferiore BufferCacheHitRatio. La lettura continua dal disco comporta costi di I/O aggiuntivi e non è performante come la lettura dalla memoria. Se il rapporto BufferCacheHitRatio è inferiore al previsto, aumentare la dimensione dell'istanza del cluster per fornire più RAM per adattare i dati del working set in memoria. Se il ridimensionamento della classe di istanza si traduce in un aumento drastico di BufferCacheHitRatio, il set di lavoro dell'applicazione non si adattava alla memoria. Continua con l'incremento fino a quando il valore di BufferCacheHitRatio non aumenta più drasticamente dopo un'operazione di dimensionamento. Per ulteriori informazioni sul monitoraggio dei parametri di un'istanza, consulta [Parametri di Amazon DocumentDB](#).

A seconda del carico di lavoro e dei requisiti di latenza, potrebbe essere accettabile che l'applicazione abbia valori BufferCacheHitRatio più elevati durante l'utilizzo della fase costante, ma abbia periodicamente delle riduzioni dei valori BufferCacheHitRatio quando le query analitiche che devono eseguire la scansione di un'intera raccolta vengono eseguite su un'istanza. Questi riduzioni periodiche del valore BufferCacheHitRatio possono manifestarsi come latenza più elevata per le query successive che devono ripopolare i dati del working set dal volume di archiviazione nella cache del buffer. Si consiglia di testare i carichi di lavoro in un ambiente di pre-produzione con un carico di lavoro di produzione rappresentativo al fine di comprendere le

caratteristiche delle prestazioni e il valore **BufferCacheHitRatio** prima di distribuire il carico di lavoro in produzione.

`BufferCacheHitRatio` è un parametro specifici dell'istanza, pertanto istanze diverse all'interno dello stesso cluster possono avere valori `BufferCacheHitRatio` diversi a seconda della modalità di distribuzione delle letture tra le istanze primarie e di replica. Se il carico di lavoro operativo non è in grado di gestire gli aumenti periodici della latenza dal ripopolamento della cache del working set dopo l'esecuzione di query analitiche, ti consigliamo di provare a isolare la cache del buffer del carico di lavoro normale da quella delle query analitiche. Puoi ottenere il completo isolamento di `BufferCacheHitRatio` indirizzando le query operative all'istanza primaria e le query analitiche solo alle istanze di replica. Puoi inoltre ottenere l'isolamento parziale indirizzando le query analitiche a un'istanza di replica specifica, con la consapevolezza che una percentuale di query regolari verrà eseguita anche su tale replica e potrebbe potenzialmente essere influenzata.

I valori appropriati di `BufferCacheHitRatio` dipendono dal caso d'uso e dai requisiti dell'applicazione. Non esiste un valore migliore o un valore minimo per questo parametro; solo tu puoi decidere se il compromesso rappresentato da un valore temporaneamente inferiore di `BufferCacheHitRatio` è accettabile dal punto di vista dei costi e delle prestazioni.

Utilizzo degli indici

Creazione degli indici

Quando si importano dati in Amazon DocumentDB, è necessario creare gli indici prima di importare set di dati di grandi dimensioni. Puoi utilizzare [Amazon DocumentDB Index Tool](#) per estrarre indici da un'istanza o una mongodump directory di MongoDB in esecuzione e creare tali indici in un cluster Amazon DocumentDB. Per ulteriori informazioni sulle migrazioni, consulta [Migrazione ad Amazon DocumentDB](#).

Selettività dell'indice

Si consiglia di limitare la creazione di indici ai campi in cui il numero di valori duplicati è inferiore all'1% del numero totale di documenti nella raccolta. Ad esempio, se la raccolta contiene 100.000 documenti, creare solo indici nei campi in cui lo stesso valore si verifica al massimo 1000 volte.

La scelta di un indice con un numero elevato di valori univoci (ad esempio, un'elevata cardinalità) garantisce che le operazioni di filtro restituiscano un numero ridotto di documenti, ottenendo così buone prestazioni durante le scansioni degli indici. Un esempio di indice ad elevata cardinalità è un indice univoco, che garantisce che i predicati di uguaglianza restituiscano al massimo un singolo

documento. Esempi di bassa cardinalità includono un indice su un campo booleano e un indice nel giorno della settimana. A causa delle scarse prestazioni, è improbabile che gli indici a bassa cardinalità vengano scelti dall'ottimizzatore delle query del database. Allo stesso tempo, indici a bassa cardinalità continuano a consumare risorse come spazio su disco e I/O. Come regola generale, occorre indicare indici su campi in cui la frequenza tipica del valore è l'1% della dimensione totale della raccolta.

Inoltre, è consigliabile creare solo indici su campi comunemente utilizzati come un filtro e cercare regolarmente indici inutilizzati. Per ulteriori informazioni, consulta [In che modo posso analizzare l'utilizzo degli indici e identificare gli indici non utilizzati?](#).

Impatto degli indici sulla scrittura dei dati

Sebbene gli indici possano migliorare le prestazioni delle query evitando la necessità di eseguire la scansione di tutti i documenti di una raccolta, questo miglioramento comporta un compromesso. Per ogni indice di una raccolta, ogni volta che un documento viene inserito, aggiornato o eliminato, il database deve aggiornare la raccolta e scrivere i campi in ciascuno degli indici per la raccolta. Ad esempio, se una raccolta dispone di nove indici, il database deve eseguire dieci scritture prima di riconoscere l'operazione al client. Pertanto, ogni indice aggiuntivo comporta latenza di scrittura aggiuntiva, I/O e aumento dello spazio di storage utilizzato complessivamente.

Le istanze del cluster devono essere dimensionate in modo appropriato per mantenere tutta la memoria del set di lavoro. Ciò evita la necessità di leggere continuamente le pagine degli indici dal volume di archiviazione, il che influisce negativamente sulle prestazioni e genera costi di I/O più elevati. Per ulteriori informazioni, consulta [Dimensione delle istanze](#).

Per ottenere prestazioni ottimali, ridurre al minimo il numero di indici nelle raccolte, aggiungendo solo gli indici necessari per migliorare le prestazioni per le query comuni. Mentre i carichi di lavoro variano, una buona linea guida consiste nel mantenere il numero di indici per raccolta a cinque o meno.

Identificazione degli indici mancanti

Identificare gli indici mancanti è una best practice che consigliamo di eseguire regolarmente. Per ulteriori informazioni, consulta [Come posso identificare gli indici mancanti?](#).

Identificazione degli indici non utilizzati

Identificare e rimuovere gli indici non utilizzati è una best practice che si consiglia di eseguire regolarmente. Per ulteriori informazioni, consulta [In che modo posso analizzare l'utilizzo degli indici e identificare gli indici non utilizzati?](#).

Best practice di sicurezza

Per le best practice di sicurezza, è necessario utilizzare account AWS Identity and Access Management (IAM) per controllare l'accesso alle operazioni API di Amazon DocumentDB, in particolare le operazioni che creano, modificano o eliminano risorse Amazon DocumentDB. Tali risorse includono i cluster, i gruppi di sicurezza e i gruppi di parametri. È inoltre necessario utilizzare IAM per controllare le azioni che eseguono azioni amministrative comuni, come il backup e il ripristino dei cluster. Quando crei ruoli IAM, utilizza il principio del privilegio minimo.

- Applica privilegi minimi con il [controllo accessi basato sui ruoli](#).
- Assegna un account IAM individuale a ogni persona che gestisce le risorse di Amazon DocumentDB. Non utilizzare l'utente Account AWS root per gestire le risorse di Amazon DocumentDB. Crea un utente IAM per tutti, incluso te stesso.
- Concedi a ciascun utente IAM il set minimo di autorizzazioni necessarie per svolgere i propri compiti.
- Utilizza gruppi IAM per gestire in modo efficace le autorizzazioni per più utenti. Per ulteriori informazioni su IAM, consulta la [Guida per l'utente di IAM](#). Per informazioni sulle best practice IAM consulta [Best Practice di IAM](#).
- Ruota periodicamente le credenziali IAM.
- Configura AWS Secrets Manager per ruotare automaticamente i segreti per Amazon DocumentDB. Per ulteriori informazioni, consulta [Rotating Your AWS Secrets Manager Secrets e Rotating Secrets for Amazon DocumentDB](#) nella Secrets AWS Manager User Guide.
- Concedi a ogni utente di Amazon DocumentDB il set minimo di autorizzazioni necessarie per svolgere le proprie mansioni. Per ulteriori informazioni, consulta [Accesso al database tramite il controllo degli accessi basato sui ruoli](#).
- Usa Transport Layer Security (TLS) per crittografare i dati in transito e AWS KMS per crittografare i dati inattivi.

Ottimizzazione dei costi

Le seguenti best practice possono aiutarti a gestire e ridurre al minimo i costi quando usi Amazon DocumentDB. Per informazioni sui prezzi, consulta le domande frequenti sui [prezzi di Amazon DocumentDB \(con compatibilità con MongoDB\)](#) e [Amazon DocumentDB \(con compatibilità con MongoDB\)](#).

- Crea avvisi di fatturazione in corrispondenza delle soglie al 50% e 75% della fattura mensile attesa. Per ulteriori informazioni sulla creazione di avvisi di fatturazione, consulta [Creazione di un allarme di fatturazione](#).
- L'architettura di Amazon DocumentDB separa storage ed elaborazione, quindi anche un cluster a istanza singola è estremamente durevole. Il volume di storage del cluster replica i dati in sei modi su tre zone di disponibilità, garantendo una durabilità estremamente elevata indipendentemente dal numero di istanze nel cluster. Un tipico cluster di produzione dispone di tre o più istanze per fornire la disponibilità elevata. Tuttavia, puoi ottimizzare i costi utilizzando un cluster di sviluppo a istanza singola quando non è richiesta la disponibilità elevata.
- Per scenari di sviluppo e di test, arresta un cluster quando non è più necessario e avvialo quando lo sviluppo riprende. Per ulteriori informazioni, consulta [Arresto e avvio di un cluster Amazon DocumentDB](#).
- Sia TTL sia i flussi di modifica incorrono in I/O quando i dati vengono scritti, letti ed eliminati. Se queste funzionalità sono state abilitate ma non vengono utilizzate nell'applicazione, la disattivazione delle funzionalità può contribuire a ridurre i costi.

Utilizzo di parametri per identificare problemi a livello di prestazioni

Per identificare i problemi di prestazioni causati da risorse insufficienti e altri colli di bottiglia comuni, puoi monitorare i parametri disponibili per il tuo cluster Amazon DocumentDB.

Visualizzazione dei parametri relativi alle prestazioni

Monitora regolarmente i parametri relativi alle prestazioni per osservare i valori medi, massimi e minimi per vari intervalli di tempo. Ciò ti consente di identificare quando le prestazioni subiscono un calo. Puoi anche impostare CloudWatch allarmi Amazon per determinate soglie metriche in modo da essere avvisato se vengono raggiunte.

Per risolvere i problemi relativi alle prestazioni, è importante comprendere le prestazioni di base del sistema. Quando configuri un nuovo cluster e lo esegui con un carico di lavoro tipico, acquisisci il valore medio, massimo e minimo di tutti i parametri relativi alle prestazioni a intervalli diversi (ad esempio, un'ora, 24 ore, una settimana, due settimane). Ciò ti permette di avere un quadro dei valori normali. Ciò aiuta anche a effettuare confronti delle attività durante le ore di punta e non di punta. Puoi quindi utilizzare queste informazioni per identificare quando le prestazioni scendono al di sotto dei livelli standard.

Puoi visualizzare le metriche delle prestazioni utilizzando o. AWS Management Console AWS CLI
Per ulteriori informazioni, consulta [Visualizzazione CloudWatch Dati](#).

Impostazione di una sveglia CloudWatch

Per impostare un CloudWatch allarme, consulta [Using Amazon CloudWatch Alarms](#) nella Amazon CloudWatch User Guide.

Valutazione dei parametri relativi alle prestazioni

Un'istanza ha diverse categorie di parametri. La modalità di determinazione dei valori accettabili dipende dal parametro.

CPU

- Utilizzo della CPU: la percentuale della capacità di elaborazione del computer utilizzata.

Memoria

- Memoria liberabile: quanta RAM è disponibile sull'istanza.
- Utilizzo dello swap: quanto spazio di swap viene utilizzato dall'istanza, in megabyte.

Operazioni di input/output

- IOPS in lettura, IOPS in scrittura: il numero medio di operazioni di lettura o scrittura su disco al secondo.
- Latenza di lettura, latenza di scrittura: il tempo medio per un'operazione di lettura o scrittura in millisecondi.
- Throughput di lettura, velocità effettiva di scrittura: il numero medio di megabyte letti o scritti su disco al secondo.
- Profondità della coda del disco: il numero di operazioni di I/O in attesa di essere scritte o lette dal disco.

Traffico di rete

- Throughput di ricezione in rete, throughput di trasmissione in rete: la velocità del traffico di rete da e verso l'istanza, espressa in megabyte al secondo.

Connessioni database

- Connessioni DB: il numero di sessioni client connesse all'istanza.

In generale, i valori accettabili per i parametri relativi alle prestazioni dipendono dalla baseline e dall'attività dell'applicazione. Indagare le variazioni della baseline coerenti o che rappresentano dei trend.

Di seguito sono riportati alcuni suggerimenti su tipi di parametri specifici:

- Consumo elevato di CPU: potrebbero essere appropriati valori elevati per il consumo di CPU, a condizione che siano in linea con gli obiettivi dell'applicazione (ad esempio velocità effettiva o concorrenza) e siano previsti. Se il consumo della CPU supera costantemente l'80%, valuta la possibilità di aumentare le dimensioni delle istanze.
- Elevato consumo di RAM: se la `FreeableMemory` metrica scende spesso al di sotto del 10% della memoria totale dell'istanza, prendi in considerazione la possibilità di aumentare le istanze. Per ulteriori informazioni su cosa succede quando l'istanza di DocumentDB subisce un'elevata pressione della memoria, consulta [Amazon DocumentDB Resource Governance](#).
- Utilizzo dello swap: questa metrica dovrebbe rimanere pari o prossima allo zero. Se l'utilizzo di swap è significativo, valuta la possibilità di aumentare le dimensioni delle istanze.
- Traffico di rete: per quanto riguarda il traffico di rete, contatta l'amministratore di sistema per capire qual è il throughput previsto per la rete di dominio e la connessione Internet. Indaga il traffico di rete se il throughput è costantemente al di sotto del valore previsto.
- Connessioni al database: valuta la possibilità di limitare le connessioni al database se riscontri un numero elevato di connessioni utente e una riduzione delle prestazioni dell'istanza e dei tempi di risposta. Il numero ideale di connessioni utente per l'istanza dipende dalla classe di istanza e dalla complessità delle operazioni eseguite. In caso di problemi con i parametri relativi alle prestazioni, per migliorare la situazione puoi provare a ottimizzare le query più utilizzate e costose per verificare se ciò riduce la pressione sulle risorse di sistema.

Se le tue query vengono ottimizzate e il problema persiste, valuta la possibilità di aggiornare la classe di istanza di Amazon DocumentDB a una classe con più risorse (CPU, RAM, spazio su disco, larghezza di banda di rete, capacità di I/O) correlate al problema riscontrato.

Ottimizzazione di query

Uno dei modi migliori per migliorare le prestazioni di un cluster consiste nell'ottimizzare le query più comuni e a uso più intensivo di risorse per renderle meno costose da eseguire.

Puoi utilizzare il profiler (vedi [Profilazione delle operazioni di Amazon DocumentDB](#)) per registrare il tempo di esecuzione e i dettagli delle operazioni eseguite nel cluster. Il profiler è utile per monitorare le operazioni più lente sul cluster per aiutare a migliorare le prestazioni delle singole query e le prestazioni complessive del cluster.

Puoi inoltre utilizzare il comando `explain` per informazioni su come analizzare un piano di query per una determinata query. Utilizza queste informazioni per modificare una query o una raccolta sottostante in modo da migliorare le prestazioni della query (ad esempio, aggiungendo un indice).

Carichi di lavoro di serie temporali e TTL

L'eliminazione del documento risultante dalla scadenza dell'indice TTL è un processo di best effort. L'eliminazione dei documenti entro un termine specifico non è garantita. Fattori come la dimensione dell'istanza, l'utilizzo delle risorse dell'istanza, la dimensione del documento, il throughput complessivo, il numero di indici e il fatto che gli indici e il working set si adattino o meno nella memoria possono influenzare i tempi di eliminazione dei documenti scaduti dal processo TTL.

Quando il monitor TTL elimina i documenti, ogni eliminazione comporta costi di IO incrementando l'importo in fattura. Se la velocità effettiva e la velocità di eliminazione TTL aumentano, dovresti aspettarti una fattura più elevata a causa dell'aumento dell'utilizzo di I/O. Tuttavia, se non crei un indice TTL per eliminare i documenti, ma li segmenti in raccolte in base al tempo e li elimini semplicemente quando non sono più necessari, non dovrai sostenere alcun costo di I/O. Questo può essere molto più conveniente rispetto all'utilizzo di un indice TTL.

Per i carichi di lavoro delle serie temporali, è possibile considerare la creazione di raccolte in sequenza anziché di un indice TTL, poiché le raccolte in sequenza possono rappresentare un modo più performante per eliminare i dati e ridurre l'utilizzo di I/O. Se si dispone di raccolte di grandi dimensioni (in particolare di raccolte superiori a 1 TB) o costi di eliminazione TTL rappresentano un problema, si consiglia di ripartire i documenti in raccolte in base al tempo e di eliminare le raccolte quando i documenti non sono più necessari. Puoi creare una raccolta al giorno o alla settimana, a seconda della frequenza di inserimento dei dati. Anche se i requisiti variano a seconda dell'applicazione, una buona regola generale è quella di avere raccolte più piccole piuttosto che alcune raccolte di grandi dimensioni. L'eliminazione di queste raccolte non comporta costi di IO e può risultare significativamente più conveniente rispetto all'utilizzo di un indice TTL.

Migrazioni

Come best practice, durante la migrazione dei dati su Amazon DocumentDB, consigliamo di creare gli indici in Amazon DocumentDB prima di migrare i dati. Creando per primi gli indici, si riduce il tempo complessivo e si aumenta la velocità della migrazione. A tale scopo, puoi utilizzare Amazon DocumentDB [Index Tool](#). Per ulteriori informazioni sulle migrazioni, consulta la guida alla migrazione di [Amazon DocumentDB](#).

Consigliamo inoltre, prima di migrare il database di produzione, di testare completamente l'applicazione su Amazon DocumentDB, prendendo in considerazione funzionalità, prestazioni, operazioni e costi.

Utilizzo di gruppi di parametri di cluster

È consigliabile provare le modifiche apportate al gruppo di parametri di cluster su un cluster di test prima di applicarle ai cluster di produzione. Per ulteriori informazioni sul backup di un cluster, consulta [Backup e ripristino in Amazon DocumentDB](#).

Query di pipeline di aggregazione

Quando crei una query di pipeline di aggregazione con più fasi e valuti solo un sottoinsieme dei dati nella query, utilizza la fase `$match` come prima fase o all'inizio della pipeline. Utilizzando prima `$match` ridurrai il numero di fasi successive dei documenti all'interno della query di pipeline di aggregazione che sarà necessario elaborare, migliorando così le prestazioni della query.

batchInsert e batchUpdate

Quando si esegue una frequenza elevata di `batchUpdate` operazioni simultanee `batchInsert` e/o e la quantità di `FreeableMemory` (CloudWatch Metric) scende a zero sull'istanza principale, è possibile ridurre la concomitanza dell'inserimento in batch o del carico di lavoro di aggiornamento oppure, se non è possibile ridurre la concorrenza del carico di lavoro, aumentare la dimensione dell'istanza per aumentare la quantità di `FreeableMemory`.

Differenze funzionali: Amazon DocumentDB e MongoDB

Di seguito sono riportate le differenze funzionali tra Amazon DocumentDB (con compatibilità con MongoDB) e MongoDB.

Argomenti

- [Vantaggi funzionali di Amazon DocumentDB](#)
- [Differenze funzionali aggiornate](#)
- [Differenze funzionali con MongoDB](#)

Vantaggi funzionali di Amazon DocumentDB

Transazioni implicite

In Amazon DocumentDB, tutte le istruzioni CRUD (`findAndModify`, `updateinsert`, `delete`) garantiscono atomicità e coerenza, anche per le operazioni che modificano più documenti. Con il lancio di Amazon DocumentDB 4.0, sono ora supportate le transazioni esplicite che forniscono proprietà ACID per operazioni con più istruzioni e raccolte multiple. Per ulteriori informazioni sull'utilizzo delle transazioni in Amazon DocumentDB, consulta [Transazioni](#)

Di seguito sono riportati alcuni esempi di operazioni in Amazon DocumentDB che modificano più documenti che soddisfano comportamenti sia atomici che coerenti.

```
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 ]
})
```

Le singole operazioni che compongono operazioni di massa come `updateMany` e `deleteMany` sono atomiche, ma la totalità dell'operazione di massa non è atomica. Ad esempio, la totalità dell'operazione `insertMany` è atomica se le singole operazioni di inserimento vengono eseguite correttamente senza errori. Se si verifica un errore con un'operazione `insertMany`, ogni singola istruzione `insert` all'interno dell'operazione `insertMany` verrà eseguita come operazione atomica. Se sono necessarie proprietà ACID per e `deleteMany` operazioni `insertManyupdateMany`, si consiglia di utilizzare una transazione.

Differenze funzionali aggiornate

Amazon DocumentDB continua a migliorare la compatibilità con MongoDB sfruttando a ritroso le funzionalità che i nostri clienti ci chiedono di sviluppare. Questa sezione contiene le differenze funzionali che abbiamo rimosso in Amazon DocumentDB per semplificare le migrazioni e la creazione di applicazioni per i nostri clienti.

Argomenti

- [Indicizzazione di matrici](#)

- [Indici multi-chiave](#)
- [Caratteri null nelle stringhe](#)
- [Controllo accessi basato sui ruoli](#)
- [Indicizzazione \\$regex](#)
- [Proiezione per documenti annidati](#)

Indicizzazione di matrici

A partire dal 23 aprile 2020, Amazon DocumentDB ora supporta la capacità di indicizzare array di dimensioni superiori a 2.048 byte. Il limite per un singolo elemento in un array rimane comunque di 2.048 byte, il che è coerente con MongoDB.

Se si sta creando un nuovo indice, non è necessaria alcuna operazione per sfruttare le funzionalità migliorate. Se si dispone di un indice esistente, è possibile sfruttare le funzionalità migliorate rilasciando l'indice e quindi ricreandolo. La versione dell'indice corrente con le funzionalità migliorate è "v" : 3.

Note

Per i cluster di produzione, il rilascio dell'indice potrebbe influenzare le prestazioni dell'applicazione. Si consiglia di eseguire innanzitutto una verifica e di procedere con cautela quando si apportano modifiche a un sistema di produzione. Inoltre, il tempo necessario per ricreare l'indice sarà una funzione della dimensione complessiva dei dati della raccolta.

È possibile eseguire una query per la versione degli indici utilizzando il seguente comando.

```
db.collection.getIndexes()
```

L'aspetto dell'output di questa operazione è simile al seguente. In questo output, la versione dell'indice è "v" : 3, che è quella più recente.

```
[
  {
    "v" : 3,
    "key" : {
      "_id" : 1
```

```
    },
    "name" : "_id_",
    "ns" : "test.test"
  }
]
```

Indici multi-chiave

A partire dal 23 aprile 2020, Amazon DocumentDB ora supporta la possibilità di creare un indice composto con più chiavi nello stesso array.

Se si sta creando un nuovo indice, non è necessaria alcuna operazione per sfruttare le funzionalità migliorate. Se si dispone di un indice esistente, è possibile sfruttare le funzionalità migliorate rilasciando l'indice e quindi ricreandolo. La versione dell'indice corrente con le funzionalità migliorate è "v" : 3.

Note

Per i cluster di produzione, il rilascio dell'indice potrebbe influenzare le prestazioni dell'applicazione. Si consiglia di eseguire innanzitutto una verifica e di procedere con cautela quando si apportano modifiche a un sistema di produzione. Inoltre, il tempo necessario per ricreare l'indice sarà una funzione della dimensione complessiva dei dati della raccolta.

È possibile eseguire una query per la versione degli indici utilizzando il seguente comando.

```
db.collection.getIndexes()
```

L'aspetto dell'output di questa operazione è simile al seguente. In questo output, la versione dell'indice è "v" : 3, che è quella più recente.

```
[
  {
    "v" : 3,
    "key" : {
      "_id" : 1
    },
    "name" : "_id_",
    "ns" : "test.test"
  }
]
```

]

Caratteri null nelle stringhe

A partire dal 22 giugno 2020, Amazon DocumentDB ora supporta i caratteri null ('`\0`') nelle stringhe.

Controllo accessi basato sui ruoli

A partire dal 26 marzo 2020, Amazon DocumentDB supporta il controllo degli accessi basato sui ruoli (RBAC) per i ruoli integrati. Per ulteriori informazioni, vedi [Controllo accessi basato sui ruoli](#).

Indicizzazione `$regex`

A partire dal 22 giugno 2020, Amazon DocumentDB ora supporta la possibilità per `$regex` gli operatori di utilizzare un indice.

Per utilizzare un indice con l'operatore `$regex`, è necessario utilizzare il comando `hint()`. Quando si utilizza `hint()`, è necessario specificare il nome del campo in cui si sta applicando `$regex`. Ad esempio, se si dispone di un indice nel campo `product` con il nome dell'indice come `p_1`, `db.foo.find({product: /^x.*$/}).hint({product:1})` utilizzerà l'indice `p_1`, ma `db.foo.find({product: /^x.*$/}).hint("p_1")` non utilizzerà l'indice. È possibile verificare se viene scelto un indice utilizzando il comando `explain()` o utilizzando il profiler per la registrazione di query lente. Ad esempio, `db.foo.find({product: /^x.*$/}).hint("p_1").explain()`.

Note

Il metodo `hint()` può essere utilizzato solo con un indice alla volta.

L'utilizzo di un indice per una query `$regex` è ottimizzato per le query regex che utilizzano un prefisso e non specificano le opzioni regex `I`, `m` o `o`.

Quando si utilizza un indice con `$regex`, si consiglia di creare un indice in campi altamente selettivi in cui il numero di valori duplicati è inferiore all'1% del numero totale di documenti nella raccolta. Ad esempio, se la raccolta contiene 100.000 documenti, creare solo indici nei campi in cui lo stesso valore si verifica al massimo 1000 volte.

Proiezione per documenti annidati

Esiste una differenza funzionale con `$project` l'operatore tra Amazon DocumentDB e MongoDB nella versione 3.6 che è stata risolta in Amazon DocumentDB 4.0 ma non sarà supportata in Amazon DocumentDB 3.6.

Amazon DocumentDB 3.6 considera solo il primo campo di un documento annidato quando applica una proiezione, mentre MongoDB 3.6 analizzerà i documenti secondari e applicherà la proiezione anche a ciascun documento secondario.

Ad esempio: se la proiezione è "a.b.c" : 1, il comportamento funziona come previsto sia in Amazon DocumentDB che in MongoDB. Tuttavia, se la proiezione è {a: {b: {c:1}}}, Amazon DocumentDB 3.6 applicherà la proiezione a solo a e non a o. b c In Amazon DocumentDB 4.0, la proiezione {a: {b: {c:1}}} verrà applicata a a, b e c

Differenze funzionali con MongoDB

Argomenti

- [Operatore \\$vectorSearch](#)
- [OpCountersCommand](#)
- [Raccolte e database di amministrazione](#)
- [cursorMaxTimeMS](#)
- [explain\(\)](#)
- [Restrizioni per i nomi dei campi](#)
- [Creazione degli indici](#)
- [Ricerca con chiave vuota nel percorso](#)
- [API, operazioni e tipi di dati di MongoDB](#)
- [mongodump mongorestore Utilità](#)
- [Ordinamento dei risultati](#)
- [Scritture ripetibili](#)
- [Indici Sparse](#)
- [Utilizzo di \\$elemMatch all'interno di un'espressione \\$all](#)
- [\\$ne,\\$nin,\\$nor, \\$not\\$exists, e indicizzazione \\$elemMatch](#)
- [\\$lookup](#)

Operatore `$vectorSearch`

Amazon DocumentDB non supporta `$vectorSearch` come operatore indipendente. Supportiamo invece, `vectorSearch` all'interno dell'`$searchoperator`. Per ulteriori informazioni, consulta [Ricerca vettoriale per Amazon DocumentDB](#).

OpCountersCommand

Il `OpCountersCommand` comportamento di Amazon DocumentDB si discosta da quello di MongoDB nel modo seguente: `opcounters.command`

- MongoDB `opcounters.command` conta tutti i comandi tranne inserimento, aggiornamento ed eliminazione, mentre Amazon DocumentDB esclude `OpCountersCommand` anche il comando `find`
- Amazon DocumentDB conta i comandi interni (ad esempio `getCloudWatchMetricsV2`) verso `OpCountersCommand`

Raccolte e database di amministrazione

Amazon DocumentDB non supporta rispettivamente l'amministratore o il database locale né MongoDB o le raccolte `system.*startup_log`

`cursor.maxTimeMS`

In Amazon DocumentDB, `cursor.maxTimeMS` reimposta il contatore per ogni richiesta. `getMore` Pertanto, se `maxTimeMS` viene specificato un valore di 3000 MS, la query impiega 2800 MS e ogni `getMore` richiesta successiva impiega 300 MS, quindi il cursore non scadrà. Il cursore scade solo quando una singola operazione, la query o una singola richiesta, richiede più di quanto specificato. `getMore maxTimeMS` Inoltre, lo sweeper che controlla il tempo di esecuzione del cursore viene eseguito con una granularità di cinque (5) minuti.

`explain()`

Amazon DocumentDB emula l'API MongoDB 4.0 su un motore di database appositamente progettato che utilizza un sistema di storage distribuito, con tolleranza ai guasti e riparazione automatica. Di conseguenza, i piani di interrogazione e l'output di `explain()` possono differire tra Amazon DocumentDB e MongoDB. I clienti che desiderano il controllo sul piano di query possono utilizzare l'operatore `$hint` per applicare la selezione di un indice preferito.

Restrizioni per i nomi dei campi

Amazon DocumentDB non supporta i punti «.» nel nome del campo di un documento, ad esempio, `db.foo.insert({'x.1':1})`

Amazon DocumentDB inoltre non supporta il prefisso \$ nei nomi dei campi.

Ad esempio, prova il seguente comando in Amazon DocumentDB o MongoDB:

```
rs0:PRIMARY> db.foo.insert({"a":{"$a":1}})
```

MongoDB restituirà quanto segue:

```
WriteResult({ "nInserted" : 1 })
```

Amazon DocumentDB restituirà un errore:

```
WriteResult({
  "nInserted" : 0,
  "writeError" : {
    "code" : 2,
    "errmsg" : "Document can't have $ prefix field names: $a"
  }
})
```

Note

Esiste un'eccezione a questa differenza funzionale. I seguenti nomi di campo che iniziano con il prefisso \$ sono stati inseriti nella whitelist e possono essere utilizzati con successo in Amazon DocumentDB: \$id, \$ref e \$db.

Creazione degli indici

Amazon DocumentDB consente la creazione di un solo indice alla volta su una raccolta. In primo piano o sullo sfondo. Se operazioni come `createIndex()` o `dropIndex()` si verificano nella stessa raccolta quando è in corso una creazione di indice, l'operazione appena tentata avrà esito negativo.

Per impostazione predefinita, le compilazioni degli indici in Amazon DocumentDB e MongoDB versione 4.0 vengono eseguite in background. MongoDB versione 4.2 e successive ignorano l'opzione di creazione dell'indice in background se specificata in `CreateIndexes` o nei relativi helper della shell e. `createIndex()` `createIndexes()`

Un indice Time to Live (TTL) inizia a far scadere i documenti dopo il completamento della creazione dell'indice.

Ricerca con chiave vuota nel percorso

Quando cerchi una chiave che include una stringa vuota come parte del percorso (ad esempio `x.x..b`) e l'oggetto ha un percorso chiave di stringa vuoto (ad esempio `{ "x" : [{ "" : 10 }, { "b" : 20 }] }`) all'interno di un array, Amazon DocumentDB restituirà risultati diversi rispetto a quelli che si otterrebbero eseguendo la stessa ricerca in MongoDB.

In MongoDB, la ricerca del percorso della chiave vuota all'interno dell'array funziona come previsto quando la chiave stringa vuota non si trova alla fine della ricerca del percorso. Tuttavia, quando la chiave stringa vuota si trova alla fine della ricerca del percorso, non esamina l'array.

Tuttavia, in Amazon DocumentDB, viene letto solo il primo elemento all'interno dell'array, perché `getArrayIndexFromKeyString` converte una stringa vuota in `0`, quindi la ricerca della chiave di stringa viene considerata come una ricerca dell'indice dell'array.

API, operazioni e tipi di dati di MongoDB

Amazon DocumentDB è compatibile con le API MongoDB 3.6 e 4.0. Per un up-to-date elenco delle funzionalità supportate, consulta [API, operazioni e tipi di dati di MongoDB supportati](#)

mongodump mongorestore Utilità

Amazon DocumentDB non supporta un database di amministrazione e quindi non esegue il dump o il ripristino del database di amministrazione quando si utilizzano le `mongodump` utilità o `mongorestore`. Quando crei un nuovo database in Amazon DocumentDB utilizzando `mongorestore`, devi ricreare i ruoli utente oltre all'operazione di ripristino.

Note

Consigliamo MongoDB Database Tools fino alla versione 100.6.1 inclusa per Amazon DocumentDB. [Puoi accedere ai download di MongoDB Database Tools qui.](#)

Ordinamento dei risultati

Amazon DocumentDB non garantisce l'ordinamento implicito dei set di risultati. Per garantire l'ordinamento di un set di risultati, specifica in modo esplicito un ordinamento utilizzando `sort()`.

L'esempio seguente ordina gli elementi della raccolta dell'inventario in ordine decrescente in base al campo del magazzino.

```
db.inventory.find().sort({ stock: -1 })
```

Quando si utilizza la fase di `$sort` aggregazione, l'ordinamento non viene mantenuto a meno che la `$sort` fase non sia l'ultima fase della pipeline di aggregazione. Quando si utilizza la fase di `$sort` aggregazione in combinazione con la fase di `$group` aggregazione, la fase di `$sort` aggregazione viene applicata solo agli accumulatori e `$first` `$last`. In Amazon DocumentDB 4.0, è stato aggiunto il supporto `$push` per rispettare l'ordinamento della fase precedente `$sort`.

Scritture ripetibili

A partire dai driver compatibili MongoDB 4.2, le scritture ripetibili sono abilitate per impostazione predefinita. Tuttavia, Amazon DocumentDB attualmente non supporta scritture riutilizzabili. La differenza funzionale si manifesterà in un messaggio di errore simile al seguente.

```
{"ok":0,"errmsg":"Unrecognized field: 'txnNumber',"code":9,"name":"MongoError"}
```

Le scritture riutilizzabili possono essere disabilitate tramite la stringa di connessione (ad esempio)

```
MongoClient("mongodb://my.mongodb.cluster/db?retryWrites=false"))
```

o l'argomento della parola chiave del MongoClient costruttore (ad esempio,.

```
MongoClient("mongodb://my.mongodb.cluster/db", retryWrites=False))
```

Di seguito è riportato un esempio Python che disabilita le scritture ripetibili nella stringa di connessione.

```
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)
```

Indici Sparse

Per utilizzare un indice Sparse creato in una query, devi utilizzare la clausola `$exists` nei campi che coprono l'indice. Se ometti `$exists`, Amazon DocumentDB non utilizza l'indice sparso.

Di seguito è riportato un esempio.

```
db.inventory.count({ "stock": { $exists: true } })
```

Per gli indici sparsi e a più chiavi, Amazon DocumentDB non supporta un vincolo di chiave univoco se la ricerca di un documento produce un insieme di valori e manca solo un sottoinsieme dei campi indicizzati. Ad esempio, `createIndex({"a.b" : 1 }, { unique : true, sparse : true })` non è supportato, dato che l'input di `"a" : [{ "b" : 2 }, { "c" : 1 }]`, come `"a.c"` è memorizzato nell'indice.

Utilizzo di `$elemMatch` all'interno di un'espressione `$all`

Amazon DocumentDB attualmente non supporta l'uso dell'operatore `$elemMatch` all'interno di un'espressione `$all`. Come soluzione alternativa, è possibile utilizzare l'operatore `$and` con `$elemMatch` come segue.

Funzionamento originale:

```
db.col.find({
  qty: {
    $all: [
      { "$elemMatch": { part: "xyz", qty: { $lt: 11 } } } },
      { "$elemMatch": { num: 40, size: "XL" } }
    ]
  }
})
```

Funzionamento aggiornato:

```
db.col.find({
  $and: [
    { qty: { "$elemMatch": { part: "xyz", qty: { $lt: 11 } } } } },
    { qty: { "$elemMatch": { qty: 40, size: "XL" } } }
  ]
})
```

```
})
```

\$ne, \$nin, \$nor, \$not\$exists, e indicizzazione \$elemMatch

Amazon DocumentDB attualmente non supporta la possibilità di utilizzare gli indici con gli operatori `$ne`, `$nin`, `$nor`, `$not`, `$exists` e `$distinct`. Di conseguenza, l'utilizzo di questi operatori comporterà scansioni delle raccolte. L'esecuzione di un filtro o di una corrispondenza prima di utilizzare uno di questi operatori ridurrà la quantità di dati da scansionare e quindi potrà migliorare le prestazioni.

Amazon DocumentDB ha aggiunto il supporto per le scansioni degli indici con l'operatore `$elemMatch` in Amazon DocumentDB 5.0 e cluster elastici. Le scansioni degli indici sono supportate quando il solo filtro di interrogazione ha un livello del `$elemMatch` filtro, ma non sono supportate se è inclusa una query annidata. `$elemMatch`

`$elemMatch` forma di query che supporta le scansioni degli indici in Amazon DocumentDB 5.0:

```
db.foo.find( { "a": { $elemMatch: { "b": "xyz", "c": "abc" } } })
```

`$elemMatch` forma di query che non supporta le scansioni degli indici in Amazon DocumentDB 5.0:

```
db.foo.find( { "a": { $elemMatch: { "b": { $elemMatch: { "d": "xyz", "e": "abc" } } } } })
```

\$lookup

Amazon DocumentDB supporta la possibilità di eseguire corrispondenze di uguaglianza (ad esempio, left outer join) ma non supporta sottoquery non correlate.

Utilizzo di un indice con **\$lookup**

Ora puoi utilizzare un indice con lo `$lookup` stage operator. In base al caso d'uso, esistono diversi algoritmi di indicizzazione che è possibile utilizzare per ottimizzare le prestazioni. Questa sezione spiegherà i diversi algoritmi di indicizzazione `$lookup` e ti aiuterà a scegliere quello migliore per il tuo carico di lavoro.

Per impostazione predefinita, Amazon DocumentDB utilizza l'algoritmo hash quando `allowDiskUse: false` viene utilizzato e sort merge quando viene utilizzato. `allowDiskUse: true`

In alcuni casi d'uso, può essere consigliabile forzare l'ottimizzatore di query a utilizzare un algoritmo diverso. Di seguito sono riportati i diversi algoritmi di indicizzazione che l'operatore di `$lookup` aggregazione può utilizzare:

- **Ciclo annidato:** un piano a ciclo annidato è in genere utile per un carico di lavoro se la raccolta esterna è <1 GB e il campo della raccolta esterna ha un indice. Se viene utilizzato l'algoritmo a ciclo annidato, il piano di spiegazione mostrerà lo stage come. `NESTED_LOOP_LOOKUP`
- **Ordinamento e unione:** un piano di ordinamento e unione è in genere utile per un carico di lavoro se la raccolta esterna non dispone di un indice sul campo utilizzato nella ricerca e il set di dati di lavoro non si adatta alla memoria. Se viene utilizzato l'algoritmo di ordinamento e unione, il piano di spiegazione mostrerà lo stage come. `SORT_LOOKUP`
- **Hash:** un piano hash è in genere utile per un carico di lavoro se la raccolta esterna è < 1 GB e il set di dati di lavoro si adatta alla memoria. Se viene utilizzato l'algoritmo hash, il piano di spiegazione mostrerà lo stage come. `HASH_LOOKUP`

È possibile identificare l'algoritmo di indicizzazione utilizzato per l'`$lookup` operatore utilizzando `explain` nella query. Di seguito è riportato un esempio.

```
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
}

```

In alternativa all'utilizzo del `explain()` metodo, è possibile utilizzare il profiler per esaminare l'algoritmo utilizzato con l'utilizzo dell'`$lookup` operatore. Per ulteriori informazioni sul profiler, consulta [Profilazione delle operazioni di Amazon DocumentDB](#)

Utilizzo di un `planHint`

Se desideri forzare l'ottimizzatore di query a utilizzare un algoritmo di indicizzazione diverso con `$lookup`, puoi usare un `planHint`. Per fare ciò, usa il commento nelle opzioni della fase di aggregazione per forzare un piano diverso. Di seguito è riportato un esempio della sintassi del commento:

```

comment : {
  comment : "<string>",

```

```
lookupStage : { planHint : "SORT" | "HASH" | "NESTED_LOOP" }
}
```

Di seguito è riportato un esempio di utilizzo di `planHint` per forzare l'ottimizzatore di query a utilizzare l'algoritmo di HASH indicizzazione:

```
db.foo.aggregate(
  [
    {
      $lookup:
      {
        from: "foo",
        localField: "_id",
        foreignField: "_id",
        as: "joined"
      },
    }
  ],
  {
    comment : "{ \\\"lookupStage\\\" : { \\\"planHint\\\": \\\"HASH\\\" } }"
```

Per verificare qual è l'algoritmo più adatto al proprio carico di lavoro, è possibile utilizzare il `executionStats` parametro del `explain` metodo per misurare il tempo di esecuzione della `$lookup` fase mentre si modifica l'algoritmo di indicizzazione (ad esempio, //). HASH SORT NESTED_LOOP

L'esempio seguente mostra come misurare il tempo `executionStats` di esecuzione dello `$lookup` stadio utilizzando l'algoritmo. SORT

```
db.foo.explain("executionStats").aggregate(
  [
    {
      $lookup:
      {
        from: "foo",
        localField: "_id",
        foreignField: "_id",
        as: "joined"
      },
    }
  ],
  {
```



```
comment : "{ \"lookupStage\" : { \"planHint\": \"SORT\" }}"
```

API, operazioni e tipi di dati di MongoDB supportati

Amazon DocumentDB (compatibile con MongoDB) è un servizio di database di documenti veloce, scalabile, ad alta disponibilità e completamente gestito che supporta i carichi di lavoro MongoDB. Amazon DocumentDB è compatibile con le API MongoDB 3.6, 4.0 e 5.0. In questa sezione sono elencate le funzionalità supportate. Per assistenza nell'utilizzo delle API e dei driver MongoDB, consulta i forum della community di MongoDB. Per ricevere assistenza sull'utilizzo del servizio Amazon DocumentDB, contatta il team di AWS supporto appropriato. Per le differenze funzionali tra Amazon DocumentDB e MongoDB, consulta [Differenze funzionali: Amazon DocumentDB e MongoDB](#)

Gli operatori e i comandi MongoDB solo interni o non applicabili a un servizio completamente gestito non sono supportati e non sono inclusi nell'elenco delle funzionalità supportate.

Abbiamo aggiunto oltre 50 funzionalità aggiuntive dal lancio e continueremo a lavorare procedendo a ritroso dai nostri clienti per fornire le funzionalità necessarie. Per informazioni sui lanci più recenti, consulta [Amazon DocumentDB Announcements](#).

Se c'è una funzionalità non supportata che vorresti che creassimo, faccelo sapere inviando un'e-mail con il tuo AccountID, le funzionalità richieste e il caso d'uso al team di assistenza di [Amazon DocumentDB](#).

Argomenti

- [Comandi del database](#)
- [Operatori per query e proiezioni](#)
- [Operatori per aggiornamenti](#)
- [Dati geospaziali](#)
- [Metodi per cursori](#)
- [Operatori per pipeline di aggregazione](#)
- [Tipi di dati](#)
- [Indici e proprietà indice](#)

Comandi del database

Argomenti

- [Comandi amministrativi](#)
- [Aggregazione](#)
- [Autenticazione](#)
- [Comandi di diagnostica](#)
- [Operazioni di query e scrittura](#)
- [Comandi di gestione di ruoli](#)
- [Comandi delle sessioni](#)
- [Gestione degli utenti](#)
- [Comandi di sharding](#)

Comandi amministrativi

Comando	3.6	4.0	5.0	Cluster elastico
Capped Collections	No	No	No	No
cloneCollectionAsCapped	No	No	No	No
collMod	Parziale	Parziale	Parziale	Sì
CollMod: expireAfterSeconds	Sì	Sì	Sì	No
convertToCapped	No	No	No	No
copydb	No	No	No	No
Creare	Sì	Sì	Sì	Sì
createView	No	No	No	No

Comando	3.6	4.0	5.0	Cluster elastico
createIndexes	Sì	Sì	Sì	Sì
currentOp	Sì	Sì	Sì	Sì
drop	Sì	Sì	Sì	Sì
dropDatabase	Sì	Sì	Sì	Sì
dropIndexes	Sì	Sì	Sì	Sì
filemd5	No	No	No	No
killCursors	Sì	Sì	Sì	Sì
killOp	Sì	Sì	Sì	Sì
Elenco delle collezioni*	Sì	Sì	Sì	Sì
listDatabases	Sì	Sì	Sì	Sì
listIndexes	Sì	Sì	Sì	Sì
reIndex	No	No	No	No
renameCollection	Sì	Sì	Sì	No

* La type chiave nell'opzione di filtro non è supportata.

Aggregazione

Comando	3.6	4.0	5.0	Cluster elastico
aggregate	Sì	Sì	Sì	Sì
count	Sì	Sì	Sì	Sì

Comando	3.6	4.0	5.0	Cluster elastico
distinct	Sì	Sì	Sì	Sì
mapReduce	No	No	No	No

Autenticazione

Comando	3.6	4.0	5.0	Cluster elastico
authenticate	Sì	Sì	Sì	Sì
Logout	Sì	Sì	Sì	Sì

Comandi di diagnostica

Comando	3.6	4.0	5.0	Cluster elastico
buildInfo	Sì	Sì	Sì	Sì
collStats	Sì	Sì	Sì	Sì
connPoolStats	No	No	No	No
connectionStatus	Sì	Sì	Sì	Sì
dataSize	Sì	Sì	Sì	Sì
dbHash	No	No	No	No
dbStats	Sì	Sì	Sì	Sì
explain	Sì	Sì	Sì	Sì
explain: executionStats	Sì	Sì	Sì	Sì
caratteristiche	No	No	No	No

Comando	3.6	4.0	5.0	Cluster elastico
hostInfo	Sì	Sì	Sì	Sì
listCommands	Sì	Sì	Sì	Sì
profiler	Sì	Sì	Sì	No
serverStatus	Sì	Sì	Sì	Sì
top	Sì	Sì	Sì	Sì

Operazioni di query e scrittura

Comando	3.6	4.0	5.0	Cluster elastico
Elimina	Sì	Sì	Sì	Sì
find	Sì	Sì	Sì	Sì
findAndModify	Sì	Sì	Sì	Sì
getLastError	No	No	No	No
getMore	Sì	Sì	Sì	Sì
getPrevError	No	No	No	No
insert	Sì	Sì	Sì	Sì
parallelCollection Scan	No	No	No	No
resetError	No	No	No	No
aggiorna	Sì	Sì	Sì	Sì
Change streams	Sì	Sì	Sì	No
GridFS	No	No	No	No

Comando	3.6	4.0	5.0	Cluster elastico
ReplaceOne	Sì	Sì	Sì	Sì

Comandi di gestione di ruoli

Comando	3.6	4.0	5.0	Cluster elastico
createRole	Sì	Sì	Sì	No
deleteRole	Sì	Sì	Sì	No
getRole	Sì	Sì	Sì	No
listRoles	Sì	Sì	Sì	No
updateRole	Sì	Sì	Sì	No
createRoleFromKey	Sì	Sì	Sì	No
deleteRoleFromKey	Sì	Sì	Sì	No
getRoleFromKey	Sì	Sì	Sì	No
listRolesFromKey	Sì	Sì	Sì	No
updateRoleFromKey	Sì	Sì	Sì	No

Comandi delle sessioni

Comando	3.6	4.0	5.0	Cluster elastico
Transazione interrotta	No	Sì	Sì	No
commitTransaction	No	Sì	Sì	No
Termina le sessioni	No	No	No	No
killAllSessions	No	Sì	Sì	No
killAllSessionsByPattern	No	No	No	No
Uccidi sessioni	No	Sì	Sì	No
Aggiorna le sessioni	No	No	No	No
Avvia sessione	No	Sì	Sì	No

Gestione degli utenti

Comando	3.6	4.0	5.0	Cluster elastico
createUser	Sì	Sì	Sì	Sì
dropAllUsersFromDatabase	Sì	Sì	Sì	Sì
dropUser	Sì	Sì	Sì	Sì

Comando	3.6	4.0	5.0	Cluster elastico
grantRolesToUtente	Sì	Sì	Sì	Sì
revokeRolesFromUtente	Sì	Sì	Sì	Sì
updateUser	Sì	Sì	Sì	Sì
userInfo	Sì	Sì	Sì	Sì

Comandi di sharding

Comando	Cluster elastico
abortReshardCollection	No
Aggiunge Shard	No
addShardToZona	No
balancerCollectionStatus	No
Balancer Start	No
Stato del bilanciatore	No
Balancer Stop	No
checkShardingIndex	No
clearJumboFlag	No
cleanupOrphaned	No
cleanupReshardCollection	No
commitReshardCollection	No

Comando	Cluster elastico
Abilita la condivisione	Sì
flushRouterConfig	No
getShardMap	No
getShardVersion	No
isdbgrid	No
Elenca i frammenti	No
Chiave mediana	No
Sposta Chunk	No
Sposta il primario	No
Unisci blocchi	No
refineCollectionShardChiave	No
Rimuove Shard	No
removeShardFromZona	No
Collezione Reshard	No
setAllowMigrations	No
setShardVersion	No
Collezione Shard	Sì
Stato di condivisione	No
dividi	No
Vettore diviso	No

Comando	Cluster elastico
Annulla lo sharding	No
updateZoneKeyIntervallo	No

Operatori per query e proiezioni

Argomenti

- [Operatori per matrice](#)
- [Operatori bit per bit](#)
- [Operatore per commenti](#)
- [Operatori di confronto](#)
- [Operatori per elementi](#)
- [Operatori per query di valutazione](#)
- [Operatori logici](#)
- [Operatori per proiezioni](#)

Operatori per matrice

Comando	3.6	4.0	5.0	Cluster elastico
\$all	Sì	Sì	Sì	Sì
\$elemMatch	Sì	Sì	Sì	Sì
\$size	Sì	Sì	Sì	Sì

Operatori bit per bit

Comando	3.6	4.0	5.0	Cluster elastico
\$bitsAllSet	Sì	Sì	Sì	Sì

Comando	3.6	4.0	5.0	Cluster elastico
\$bitsAnySet	Sì	Sì	Sì	Sì
\$bitsAllClear	Sì	Sì	Sì	Sì
\$bitsAnyClear	Sì	Sì	Sì	Sì

Operatore per commenti

Comando	3.6	4.0	5.0	Cluster elastico
\$comment	Sì	Sì	Sì	Sì

Operatori di confronto

Comando	3.6	4.0	5.0	Cluster elastico
\$eq	Sì	Sì	Sì	Sì
\$gt	Sì	Sì	Sì	Sì
\$gte	Sì	Sì	Sì	Sì
\$lt	Sì	Sì	Sì	Sì
\$lte	Sì	Sì	Sì	Sì
\$ne	Sì	Sì	Sì	Sì
\$in	Sì	Sì	Sì	Sì
\$nin	Sì	Sì	Sì	Sì

Operatori per elementi

Comando	3.6	4.0	5.0	Cluster elastico
\$exists	Sì	Sì	Sì	Sì
\$type	Sì	Sì	Sì	Sì

Operatori per query di valutazione

Comando	3.6	4.0	5.0	Cluster elastico
\$expr	No	No	No	No
\$jsonSchema	No	Sì	Sì	No
\$mod	Sì	Sì	Sì	Sì
\$regex	Sì	Sì	Sì	Sì
\$text	No	No	Sì	No
\$where	No	No	No	No

Operatori logici

Comando	3.6	4.0	5.0	Cluster elastico
\$or	Sì	Sì	Sì	Sì
\$and	Sì	Sì	Sì	Sì
\$not	Sì	Sì	Sì	Sì
\$nor	Sì	Sì	Sì	Sì

Operatori per proiezioni

Comando	3.6	4.0	5.0	Cluster elastico
\$	Sì	Sì	Sì	Sì
\$elemMatch	Sì	Sì	Sì	Sì
\$meta	No	No	Sì	No
\$slice	Sì	Sì	Sì	Sì

Operatori per aggiornamenti

Argomenti

- [Operatori per matrice](#)
- [Operatori bit per bit](#)
- [Operatori per campi](#)
- [Modificatori per aggiornamenti](#)

Operatori per matrice

Comando	3.6	4.0	5.0	Cluster elastico
\$	Sì	Sì	Sì	Sì
\$[]	Sì	Sì	Sì	Sì
\$[<identifier>]	Sì	Sì	Sì	Sì
\$addToSet	Sì	Sì	Sì	Sì
\$pop	Sì	Sì	Sì	Sì
\$pullAll	Sì	Sì	Sì	Sì
\$pull	Sì	Sì	Sì	Sì

Comando	3.6	4.0	5.0	Cluster elastico
\$push	Sì	Sì	Sì	Sì

Operatori bit per bit

Comando	3.6	4.0	5.0	Cluster elastico
\$bit	Sì	Sì	Sì	Sì

Operatori per campi

Operatore	3.6	4.0	5.0	Cluster elastico
\$inc	Sì	Sì	Sì	Sì
\$mul	Sì	Sì	Sì	Sì
\$rename	Sì	Sì	Sì	Sì
\$setOnInsert	Sì	Sì	Sì	Sì
\$set	Sì	Sì	Sì	Sì
\$unset	Sì	Sì	Sì	Sì
\$min	Sì	Sì	Sì	Sì
\$max	Sì	Sì	Sì	Sì
\$currentDate	Sì	Sì	Sì	Sì

Modificatori per aggiornamenti

Operatore	3.6	4.0	5.0	Cluster elastico
\$each	Sì	Sì	Sì	Sì
\$slice	Sì	Sì	Sì	Sì
\$sort	Sì	Sì	Sì	Sì
\$position	Sì	Sì	Sì	Sì

Dati geospaziali

Specificatori di geometria

Selettori di query	3.6	4.0	5.0	Cluster elastico
\$box	No	No	No	No
\$center	No	No	No	No
\$centerSphere	No	No	No	No
\$nearSphere	Sì	Sì	Sì	No
\$geometry	Sì	Sì	Sì	No
\$maxDistance	Sì	Sì	Sì	No
\$minDistance	Sì	Sì	Sì	No
\$polygon	No	No	No	No
\$uniqueDocs	No	No	No	No

Selettori di query

Comando	3.6	4.0	5.0	Cluster elastico
\$geoIntersects	Sì	Sì	Sì	No
\$geoWithin	Sì	Sì	Sì	No
\$near	No	No	No	No
\$nearSphere	Sì	Sì	Sì	No
\$polygon	No	No	No	No
\$uniqueDocs	No	No	No	No

Metodi per cursori

Comando	3.6	4.0	5.0	Cluster elastico
cursor.batchSize()	Sì	Sì	Sì	Sì
cursor.close()	Sì	Sì	Sì	Sì
cursor.isClosed()	Sì	Sì	Sì	Sì
cursor.collation()	No	No	No	No
cursor.comment()	Sì	Sì	Sì	Sì
cursor.count()	Sì	Sì	Sì	Sì
cursor.explain()	Sì	Sì	Sì	No
cursor.forEach()	Sì	Sì	Sì	Sì
cursor.hasNext()	Sì	Sì	Sì	Sì

Comando	3.6	4.0	5.0	Cluster elastico
<code>cursor.hint()</code>	Sì	Sì	Sì	Sì*
<code>cursor.isExhausted()</code>	Sì	Sì	Sì	No
<code>cursor.itcount()</code>	Sì	Sì	Sì	No
<code>cursor.limit()</code>	Sì	Sì	Sì	No
<code>cursor.map()</code>	Sì	Sì	Sì	No
<code>cursor.maxScan()</code>	Sì	Sì	Sì	No
<code>cursor.maxTimeMS()</code>	Sì	Sì	Sì	No
<code>cursor.max()</code>	No	No	No	No
<code>cursor.min()</code>	No	No	No	No
<code>cursor.next()</code>	Sì	Sì	Sì	Sì
<code>cursor.noCursorTimeout()</code>	No	No	No	No
<code>cursor.objsLeftInBatch()</code>	Sì	Sì	Sì	No
<code>cursor.pretty()</code>	Sì	Sì	Sì	No
<code>cursor.readConcern()</code>	Sì	Sì	Sì	No
<code>cursor.readPref()</code>	Sì	Sì	Sì	No
<code>cursor.returnKey()</code>	No	No	No	No

Comando	3.6	4.0	5.0	Cluster elastico
<code>showRecordId()</code>	No	No	No	No
<code>cursor.size()</code>	Sì	Sì	Sì	No
<code>cursor.skip()</code>	Sì	Sì	Sì	No
<code>cursor.sort()</code>	Sì	Sì	Sì	No
<code>cursor.tailable()</code>	No	No	No	No
<code>cursor.toArray()</code>	Sì	Sì	Sì	No

* L'indice `hint` è supportato con le espressioni di indice. Ad esempio, `db.foo.find().hint({x:1})`.

Operatori per pipeline di aggregazione

Argomenti

- [Espressioni per accumulatori](#)
- [Operatori aritmetici](#)
- [Operatori per matrice](#)
- [Operatori booleani](#)
- [Operatori di confronto](#)
- [Operatori per espressioni condizionali](#)
- [Operatori per tipi di dati](#)
- [Operatore di dimensione dei dati](#)
- [Operatori per date](#)
- [Operatore letterale](#)
- [Operatori di unione](#)
- [Operatore naturale](#)
- [Operatori su set](#)

- [Operatori per fasi](#)
- [Operatori di stringa](#)
- [Variabili di sistema](#)
- [Operatore per ricerca testo](#)
- [Operatori di conversione dei tipi](#)
- [Operatori per variabili](#)
- [Operatori vari](#)

Espressioni per accumulatori

Expression	3.6	4.0	5.0	Cluster elastico
\$sum	Sì	Sì	Sì	Sì
\$avg	Sì	Sì	Sì	Sì
\$first	Sì	Sì	Sì	Sì
\$last	Sì	Sì	Sì	Sì
\$max	Sì	Sì	Sì	Sì
\$min	Sì	Sì	Sì	Sì
\$push	Sì	Sì	Sì	Sì
\$addToSet	Sì	Sì	Sì	Sì
\$stdDevPop	No	No	No	No
\$stdDevSamp	No	No	No	No
\$accumulator	-	-	No	No
\$count	-	-	No	No

Operatori aritmetici

Comando	3.6	4.0	5.0	Cluster elastico
\$abs	Sì	Sì	Sì	Sì
\$add	Sì	Sì	Sì	Sì
\$ceil	No	Sì	Sì	Sì
\$divide	Sì	Sì	Sì	Sì
\$exp	No	Sì	Sì	Sì
\$floor	No	Sì	Sì	Sì
\$ln	No	Sì	Sì	Sì
\$log	No	Sì	Sì	Sì
\$log10	No	Sì	Sì	Sì
\$mod	Sì	Sì	Sì	Sì
\$multiply	Sì	Sì	Sì	Sì
\$pow	No	No	No	No
\$sqrt	No	Sì	Sì	Sì
\$subtract	Sì	Sì	Sì	Sì
\$trunc	No	No	No	No
\$rotondo	-	-	No	No

Operatori per matrice

Comando	3.6	4.0	5.0	Cluster elastico
\$arrayElemAt	Sì	Sì	Sì	Sì
\$arrayToObject	Sì	Sì	Sì	Sì
\$concatArrays	Sì	Sì	Sì	Sì
\$filter	Sì	Sì	Sì	Sì
\$indexOfArray	Sì	Sì	Sì	Sì
\$isArray	Sì	Sì	Sì	Sì
\$objectToArray	Sì	Sì	Sì	Sì
\$range	Sì	Sì	Sì	Sì
\$reverseArray	Sì	Sì	Sì	Sì
\$reduce	Sì	Sì	Sì	Sì
\$size	Sì	Sì	Sì	Sì
\$slice	Sì	Sì	Sì	Sì
\$zip	Sì	Sì	Sì	Sì
\$in	Sì	Sì	Sì	Sì
\$first	-	-	No	No
\$last	-	-	No	No

Operatori booleani

Comando	3.6	4.0	5.0	Cluster elastico
\$and	Sì	Sì	Sì	Sì
\$or	Sì	Sì	Sì	Sì
\$not	Sì	Sì	Sì	Sì

Operatori di confronto

Comando	3.6	4.0	5.0	Cluster elastico
\$cmp	Sì	Sì	Sì	Sì
\$eq	Sì	Sì	Sì	Sì
\$gt	Sì	Sì	Sì	Sì
\$gte	Sì	Sì	Sì	Sì
\$lt	Sì	Sì	Sì	Sì
\$lte	Sì	Sì	Sì	Sì
\$ne	Sì	Sì	Sì	Sì

Operatori per espressioni condizionali

Comando	3.6	4.0	5.0	Cluster elastico
\$cond	Sì	Sì	Sì	Sì
\$ifNull	Sì	Sì	Sì	Sì
\$switch	No	No	No	No

Operatori per tipi di dati

Comando	3.6	4.0	5.0	Cluster elastico
\$type	Sì	Sì	Sì	Sì

Operatore di dimensione dei dati

Comando	3.6	4.0	5.0	Cluster elastico
\$binarySize	-	-	No	No
\$bsonSize	-	-	No	No

Operatori per date

Comando	3.6	4.0	5.0	Cluster elastico
\$dateAdd	No	No	Sì	Sì
\$dateSubtract	No	No	Sì	Sì
\$dayOfYear	Sì	Sì	Sì	Sì
\$dayOfMonth	Sì	Sì	Sì	Sì
\$dayOfWeek	Sì	Sì	Sì	Sì
\$year	Sì	Sì	Sì	Sì
\$month	Sì	Sì	Sì	Sì
\$week	Sì	Sì	Sì	Sì
\$hour	Sì	Sì	Sì	Sì
\$minute	Sì	Sì	Sì	Sì

Comando	3.6	4.0	5.0	Cluster elastico
\$second	Sì	Sì	Sì	Sì
\$millisecond	Sì	Sì	Sì	Sì
\$dateToString	Sì	Sì	Sì	Sì
\$ Settimana isoDayOf	Sì	Sì	Sì	Sì
\$isoWeek	Sì	Sì	Sì	Sì
\$dateFromParts	No	No	No	No
\$dateToParts	No	No	No	No
\$dateFromString	Sì	Sì	Sì	Sì
\$isoWeekYear	Sì	Sì	Sì	Sì
\$ DataTrunc	-	-	No	No
\$dataDiff	-	-	No	No

Operatore letterale

Comando	3.6	4.0	5.0	Cluster elastico
\$literal	Sì	Sì	Sì	Sì

Operatori di unione

Comando	3.6	4.0	5.0	Cluster elastico
\$mergeObjects	Sì	Sì	Sì	Sì

Operatore naturale

Comando	3.6	4.0	5.0	Cluster elastico
\$ naturale	Sì	Sì	Sì	Sì

Operatori su set

Comando	3.6	4.0	5.0	Cluster elastico
\$setEquals	Sì	Sì	Sì	Sì
\$setIntersection	Sì	Sì	Sì	Sì
\$setUnion	Sì	Sì	Sì	Sì
\$setDifference	No	Sì	Sì	Sì
\$setIsSubset	Sì	Sì	Sì	Sì
\$anyElementTrue	No	Sì	Sì	Sì
\$allElementsTrue	No	Sì	Sì	Sì

Operatori per fasi

Comando	3.6	4.0	5.0	Cluster elastico
\$collStats	No	No	No	No
\$project	Sì	Sì	Sì	Sì
\$match	Sì	Sì	Sì	Sì
\$redact	Sì	Sì	Sì	Sì

Comando	3.6	4.0	5.0	Cluster elastico
\$limit	Sì	Sì	Sì	Sì
\$skip	Sì	Sì	Sì	Sì
\$unwind	Sì	Sì	Sì	Sì
\$group	Sì	Sì	Sì	Sì
\$sample	Sì	Sì	Sì	Sì
\$sort	Sì	Sì	Sì	Sì
\$geoNear	Sì	Sì	Sì	No
\$lookup	Sì	Sì	Sì	Sì
\$out	Sì	Sì	Sì	No
\$indexStats	Sì	Sì	Sì	Sì
\$facet	No	No	No	No
\$bucket	No	No	No	No
\$bucketAuto	No	No	No	No
\$sortByCount	No	No	No	No
\$addFields	Sì	Sì	Sì	Sì
\$replaceRoot	Sì	Sì	Sì	Sì
\$count	Sì	Sì	Sì	Sì
\$currentOp	Sì	Sì	Sì	Sì
\$listLoca ISessions	No	No	No	No
\$listSessions	No	No	No	No

Comando	3.6	4.0	5.0	Cluster elastico
\$graphLookup	No	No	No	No
\$merge	-	-	No	No
\$planCacheStats	-	-	No	No
\$setWindowFields	-	-	No	No
\$unionWith	-	-	No	No
\$unset	-	-	No	No

Operatori di stringa

Comando	3.6	4.0	5.0	Cluster elastico
\$concat	Sì	Sì	Sì	Sì
\$indexOfBytes	Sì	Sì	Sì	Sì
\$indexOfCP	Sì	Sì	Sì	Sì
\$ltrim	No	No	No	No
\$rtrim	No	No	No	No
\$split	Sì	Sì	Sì	Sì
\$strcasecmp	Sì	Sì	Sì	Sì
\$strLenBytes	Sì	Sì	Sì	Sì
\$strLenCP	Sì	Sì	Sì	Sì
\$substr	Sì	Sì	Sì	Sì
\$substrBytes	Sì	Sì	Sì	Sì

Comando	3.6	4.0	5.0	Cluster elastico
\$substrCP	Sì	Sì	Sì	Sì
\$toLower	Sì	Sì	Sì	Sì
\$toUpper	Sì	Sì	Sì	Sì
\$trim	No	No	No	No
\$regexFind	-	-	No	No
\$regexFindAll	-	-	No	No
\$RegexMatch	-	-	No	No
\$ sostituisci uno	-	-	No	No
\$ sostituisci tutto	-	-	No	No

Variabili di sistema

Comando	3.6	4.0	5.0	Cluster elastico
\$\$CURRENT	No	No	No	No
\$\$DESCEND	Sì	Sì	Sì	Sì
\$\$KEEP	Sì	Sì	Sì	Sì
\$\$PRUNE	Sì	Sì	Sì	Sì
\$\$REMOVE	No	No	No	No
\$\$ROOT	Sì	Sì	Sì	Sì

Operatore per ricerca testo

Comando	3.6	4.0	5.0	Cluster elastico
\$ricerca	No	No	Sì	No
\$meta	No	No	Sì	No

Operatori di conversione dei tipi

Comando	3.6	4.0	5.0	Cluster elastico
\$ converti	No	Sì	Sì	Sì
\$ a BOOL	No	Sì	Sì	Sì
\$ fino ad oggi	No	Sì	Sì	Sì
\$toDecimal	No	Sì	Sì	Sì
\$ per raddoppiare	No	Sì	Sì	Sì
\$ a INT	No	Sì	Sì	Sì
\$ a Long	No	Sì	Sì	Sì
\$toObjectId	No	Sì	Sì	Sì
\$toString	No	Sì	Sì	Sì
\$isNumber	-	-	No	No

Operatori per variabili

Comando	3.6	4.0	5.0	Cluster elastico
\$map	Sì	Sì	Sì	Sì
\$let	Sì	Sì	Sì	Sì

Operatori vari

Comando	3.6	4.0	5.0	Cluster elastico
\$rand	-	-	No	No
\$sampleRate	-	-	No	No
\$getField	-	-	No	No

Tipi di dati

Comando	3.6	4.0	5.0	Cluster elastico
Doppio	Sì	Sì	Sì	Sì
Stringa	Sì	Sì	Sì	Sì
Oggetto	Sì	Sì	Sì	Sì
Array	Sì	Sì	Sì	Sì
Dati binari	Sì	Sì	Sì	Sì
ObjectId	Sì	Sì	Sì	Sì
Booleano	Sì	Sì	Sì	Sì
Data	Sì	Sì	Sì	Sì

Comando	3.6	4.0	5.0	Cluster elastico
Null	Sì	Sì	Sì	Sì
Numero intero a 32 bit (int)	Sì	Sì	Sì	Sì
Timestamp	Sì	Sì	Sì	Sì
Numero intero a 64 bit (lungo)	Sì	Sì	Sì	Sì
MinKey	Sì	Sì	Sì	Sì
MaxKey	Sì	Sì	Sì	Sì
Decimal128	Sì	Sì	Sì	Sì
Espressione regolare	Sì	Sì	Sì	Sì
JavaScript	No	No	No	No
JavaScript(con ambito)	No	No	No	No
Undefined	No	No	No	No
Symbol	No	No	No	No
DBPointer	No	No	No	No

Indici e proprietà indice

Argomenti

- [Indici](#)
- [Proprietà indice](#)

Indici

Comando	3.6	4.0	5.0	Cluster elastico
Indice con campo singolo	Sì	Sì	Sì	Sì
Indice composto	Sì	Sì	Sì	Sì
Indice con più chiavi	Sì	Sì	Sì	Sì
Indice di testo	No	No	Sì	No
2dsphere	Sì	Sì	Sì	No
Indice 2d	No	No	No	No
Indice con hash	No	No	No	No

Proprietà indice

Comando	3.6	4.0	5.0	Cluster elastico
TTL	Sì	Sì	Sì	Sì
Unique	Sì	Sì	Sì	Sì
Parziale	No	No	Sì	No
Senza distinzione tra maiuscole e minuscole	No	No	No	No
Sparse	Sì	Sì	Sì	Sì
Contesto	Sì	Sì	Sì	No

Intelligenza artificiale generativa di Amazon DocumentDB

Amazon DocumentDB offre funzionalità per consentire ai modelli di apprendimento automatico (ML) e intelligenza artificiale generativa (AI) di lavorare con i dati archiviati in Amazon DocumentDB in tempo reale. I clienti non devono più perdere tempo a gestire un'infrastruttura separata, scrivere codice per connettersi a un altro servizio e duplicare i dati dal database principale.

Per ulteriori informazioni sull'intelligenza artificiale e su come AWS può supportare le tue esigenze di intelligenza artificiale, consulta questo articolo [«Cos'è»](#).

Argomenti

- [Apprendimento automatico senza codice con Amazon Canvas SageMaker](#)
- [Ricerca vettoriale per Amazon DocumentDB](#)

Apprendimento automatico senza codice con Amazon Canvas SageMaker

[Amazon SageMaker Canvas](#) ti consente di creare modelli AI/ML personalizzati senza dover scrivere una sola riga di codice. Puoi creare modelli di machine learning per casi d'uso comuni come regressione e previsione e accedere e valutare modelli di base (FM) da Amazon Bedrock. Puoi anche accedere alle FM pubbliche di Amazon SageMaker JumpStart per la generazione di contenuti, l'estrazione del testo e il riepilogo del testo per supportare soluzioni di intelligenza artificiale generativa.

Come creare modelli ML senza codice con Canvas SageMaker

Amazon DocumentDB ora si integra con Amazon SageMaker Canvas per abilitare l'apprendimento automatico (ML) senza codice con i dati archiviati in Amazon DocumentDB. Ora puoi creare modelli ML per esigenze di regressione e previsione e utilizzare modelli di base per il riepilogo e la generazione di contenuti utilizzando i dati archiviati in Amazon DocumentDB senza scrivere una sola riga di codice.

SageMaker Canvas fornisce un'interfaccia visiva che consente ai clienti di Amazon DocumentDB di generare previsioni senza richiedere alcuna esperienza di AI/ML o scrivere una sola riga di codice. I clienti possono ora avviare l' SageMaker area di lavoro Canvas dai dati di Amazon DocumentDB AWS Management Console, importarli e unirli per la preparazione dei dati e la formazione dei

modelli. I dati di Amazon DocumentDB possono ora essere utilizzati in SageMaker Canvas per creare e potenziare modelli per prevedere il tasso di abbandono dei clienti, rilevare frodi, prevedere gli errori di manutenzione, prevedere le metriche aziendali e generare contenuti. I clienti possono ora pubblicare e condividere informazioni basate sul machine learning tra i team utilizzando l'integrazione nativa di SageMaker Canvas con Amazon. QuickSight Le pipeline di inserimento dati in SageMaker Canvas vengono eseguite su istanze secondarie di Amazon DocumentDB per impostazione predefinita, garantendo che le prestazioni delle applicazioni e dei carichi di lavoro di importazione di SageMaker Canvas non siano ostacolate.

I clienti di Amazon DocumentDB possono iniziare a usare SageMaker Canvas accedendo alla nuova pagina della console ML senza codice di Amazon DocumentDB e connettendosi ad aree di lavoro Canvas nuove o disponibili. SageMaker

Configurazione del dominio e del profilo utente SageMaker

Puoi connetterti ai cluster Amazon DocumentDB da SageMaker domini in esecuzione in modalità Solo VPC. Avviando un SageMaker dominio nel tuo VPC, puoi controllare il flusso di dati dagli ambienti Studio e SageMaker Canvas. Ciò consente di limitare l'accesso a Internet, monitorare e ispezionare il traffico utilizzando funzionalità AWS di rete e sicurezza standard e connettersi ad altre AWS risorse tramite endpoint VPC. Consulta [Amazon SageMaker Canvas Getting started](#) and [Configure Amazon SageMaker Canvas in un VPC senza accesso a Internet disponibile](#) nella Amazon SageMaker Developer Guide per creare il tuo SageMaker dominio per la connessione al tuo cluster Amazon DocumentDB.

Configurazione delle autorizzazioni di accesso IAM per Amazon DocumentDB e Canvas SageMaker

Un utente di Amazon DocumentDB `AmazonDocDBConsoleFullAccess` collegato al ruolo e all'identità associati può accedere a. AWS Management Console Aggiungi le seguenti azioni al ruolo o all'identità di cui sopra per fornire l'accesso all'apprendimento automatico senza codice con Amazon Canvas. SageMaker

```
"sagemaker:CreatePresignedDomainUrl",  
"sagemaker:DescribeDomain",  
"sagemaker:ListDomains",  
"sagemaker:ListUserProfiles"
```

Creazione di utenti e ruoli del database per Canvas SageMaker

Puoi limitare l'accesso alle azioni che gli utenti possono eseguire sui database utilizzando il controllo degli accessi basato sui ruoli (RBAC) in Amazon DocumentDB. RBAC funziona concedendo uno o più ruoli a un utente. Questi ruoli determinano le operazioni che un utente può eseguire sulle risorse del database.

Come utente Canvas, ti connetti a un database Amazon DocumentDB con credenziali di nome utente e password. Puoi creare un utente/ruolo del database per un utente Canvas con accesso in lettura a database specifici utilizzando la funzionalità RBAC di Amazon DocumentDB.

Ad esempio, usa l'operazione: `createUser`

```
db.createUser({
  user: "canvas_user",
  pwd: "<insert-password>",
  roles: [{role: "read", db: "sample-database-1"}]
})
```

Questo crea un file `canvas_user` che ha i permessi di lettura per il `sample-database-1` database. I tuoi analisti Canvas possono utilizzare questa credenziale per accedere ai dati nel tuo cluster Amazon DocumentDB. Fai riferimento a [per saperne di più su Accesso al database tramite il controllo degli accessi basato sui ruoli](#).

Regioni disponibili

L'integrazione senza codice è disponibile nelle regioni in cui sono supportati sia Amazon DocumentDB che SageMaker Amazon Canvas. Le regioni includono:

- us-east-1 (Virginia settentrionale)
- us-east-2 (Ohio)
- us-west-2 (Oregon)
- ap-northeast-1 (Tokyo)
- ap-northeast-2 (Seoul)
- ap-south-1 (Mumbai)
- ap-southeast-1 (Singapore)
- ap-southeast-2 (Sydney)
- eu-central-1 (Francoforte)

- [eu-west-1 \(Irlanda\)](#)

Consulta [Amazon SageMaker Canvas nell'Amazon SageMaker Developer Guide](#) per conoscere la disponibilità più recente della regione.

Ricerca vettoriale per Amazon DocumentDB

La ricerca vettoriale è un metodo utilizzato nell'apprendimento automatico per trovare punti dati simili a un dato punto dati confrontando le relative rappresentazioni vettoriali utilizzando metriche di distanza o somiglianza. Più i due vettori sono vicini nello spazio vettoriale, più gli elementi sottostanti vengono considerati simili. Questa tecnica aiuta a catturare il significato semantico dei dati. Questo approccio è utile in varie applicazioni, come i sistemi di raccomandazione, l'elaborazione del linguaggio naturale e il riconoscimento delle immagini.

La ricerca vettoriale per Amazon DocumentDB combina la flessibilità e la ricca capacità di interrogazione di un database di documenti basato su JSON con la potenza della ricerca vettoriale. Se desideri utilizzare i dati esistenti di Amazon DocumentDB o una struttura di dati documentale flessibile per creare casi d'uso di machine learning e intelligenza artificiale generativa, come esperienza di ricerca semantica, consigli di prodotti, personalizzazione, chatbot, rilevamento di frodi e rilevamento di anomalie, la ricerca vettoriale per Amazon DocumentDB è la scelta ideale per te. La ricerca vettoriale è disponibile nei cluster basati su istanze di Amazon DocumentDB 5.0.

Argomenti

- [Inserimento di vettori](#)
- [Creazione di un indice vettoriale](#)
- [Ottenere una definizione dell'indice](#)
- [Interrogazione dei vettori](#)
- [Caratteristiche e limitazioni](#)
- [Best practice](#)

Inserimento di vettori

Per inserire vettori nel tuo database Amazon DocumentDB, puoi utilizzare i metodi di inserimento esistenti:

Esempio

Nell'esempio seguente, viene creata una raccolta di cinque documenti all'interno di un database di test. Ogni documento include due campi: il nome del prodotto e l'incorporamento vettoriale corrispondente.

```
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]}
]);
```

Creazione di un indice vettoriale

Amazon DocumentDB supporta sia i metodi di indicizzazione Hierarchical Navigable Small World (HNSW) che i metodi di indicizzazione Inverted File with Flat Compression (ivFFlat). Un indice IVFFlat separa i vettori in elenchi e successivamente cerca un sottoinsieme selezionato di quegli elenchi più vicini al vettore di query. D'altra parte, un indice HNSW organizza i dati vettoriali in un grafico a più livelli. Sebbene HNSW abbia tempi di compilazione più lenti rispetto a ivFFlat, offre prestazioni di query e richiamo migliori. A differenza di IVFFlat, HNSW non prevede alcuna fase di formazione, il che consente di generare l'indice senza alcun caricamento iniziale dei dati. Per la maggior parte dei casi d'uso, consigliamo di utilizzare il tipo di indice HNSW per la ricerca vettoriale.

Se non crei un indice vettoriale, Amazon DocumentDB esegue una ricerca esatta del vicino più vicino, assicurando un richiamo perfetto. Tuttavia, negli scenari di produzione, la velocità è fondamentale. Consigliamo di utilizzare indici vettoriali, che potrebbero sostituire alcuni richiami in cambio di una maggiore velocità. È importante notare che l'aggiunta di un indice vettoriale può portare a risultati di query diversi.

Modelli

È possibile utilizzare quanto segue `createIndex` o i `runCommand` modelli per creare un indice vettoriale su un campo vettoriale:

Using `createIndex`

In alcuni driver, come mongosh e Java, l'utilizzo dei `vectorOptions` parametri in `createIndex` può causare un errore. In questi casi, si consiglia di utilizzare: `runCommand`

```
db.collection.createIndex(
```

```

{ "<vectorField>": "vector" },
{ "name": "<indexName>",
  "vectorOptions": {
    "type": " <hns> | <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 alcuni driver, come mongosh e Java, l'utilizzo dei `vectorOptions` parametri in `createIndex` può causare un errore. In questi casi, si consiglia di utilizzare: `runCommand`

```

db.runCommand(
  { "createIndexes": "<collection>",
    "indexes": [{
      key: { "<vectorField>": "vector" },
      vectorOptions: {
        type: " <hns> | <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"
    }]
  }
);

```

Parametro	Requisito	Tipo di dati	Descrizione	Valore (i)
name	facoltativo	string	Specificate il nome dell'indice.	Carattere alfanumerico

Parametro	Requisito	Tipo di dati	Descrizione	Valore (i)
type	facoltativo		Specifica il tipo di indice.	Supportato: hnsw o ivfflat Impostazione predefinita: HNSW (patch del motore 3.0.4574 in poi)
dimensions	obbligatorio	integer	Specifica il numero di dimensioni nei dati vettoriali.	Massimo 2.000 dimensioni.
similarity	obbligatorio	string	Specifica la metrica della distanza utilizzata per il calcolo della somiglianza.	<ul style="list-style-type: none"> • euclidean • cosine • dotProduct

Parametro	Requisito	Tipo di dati	Descrizione	Valore (i)
lists	richiesto per IVFFlat	integer	Speciifica il numero di cluster utilizzati dall'indice IVFFlat per raggruppare i dati vettoriali. L'impostazione consigliata è il numero di documenti/1000 per un massimo di 1 milione di documenti e per oltre 1 milione di documenti $\sqrt{\text{\# of documents}}$	Minimo: 1 Massimo: fai riferimento alla tabella dei tipi di istanza degli elenchi per istanza riportata di seguito. Caratteristiche e limitazioni
m	facoltativo	integer	Speciifica il numero massimo di connessioni per un indice HNSW	Impostazione predefinita: 16 Intervallo [2, 100]

Parametro	Requisito	Tipo di dati	Descrizione	Valore (i)
efConstruction	facoltativo	integer	Specifica la dimensione dell'elenco dinamico dei candidati per la costruzione del grafico per l'indice HNSW. efConstruction deve essere maggiore o uguale a (2 * m)	Impostazione predefinita: 64 Intervallo [4, 1000]

È importante impostare il valore dei sottoparametri, ad esempio `lists` per `ivFFlat m` e `efConstruction` per HNSW, in modo appropriato, poiché ciò influirà sulla precisione/richiamo, sui tempi di compilazione e sulle prestazioni della ricerca. Un valore di elenco più elevato aumenta la velocità dell'interrogazione in quanto riduce il numero di vettori in ogni elenco, con conseguenti aree più piccole. Tuttavia, una dimensione dell'area più piccola può portare a più errori di richiamo, con conseguente minore precisione. Per HNSW, aumentare il valore `m` e la precisione dell'indice, ma anche `efConstruction` aumentare il tempo e le dimensioni di costruzione dell'indice. Fare riferimento agli esempi riportati di seguito:

Examples (Esempi)

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
    }
  }
)
```

Ottenere una definizione dell'indice

Puoi visualizzare i dettagli dei tuoi indici, inclusi gli indici vettoriali, usando il comando: `getIndexes`

Esempio

```
db.collection.getIndexes()
```

Output di esempio

```
[
  {
    "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"
}
]

```

Interrogazione dei vettori

Modello di interrogazione vettoriale

Utilizzate il seguente modello per interrogare un vettore:

```

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]
      }
    }
  }
]);

```

Parametro	Requisito	Type	Descrizione	Valore (i)
vectorSearch	obbligatorio	operatore	Utilizzato all'interno del comando \$search per interrogare i vettori.	

Parametro	Requisito	Type	Descrizione	Valore (i)
vector	obbligatorio	array	Indica il vettore di interrogazione che verrà utilizzato per trovare vettori simili.	
path	obbligatorio	string	Definisce il nome del campo vettoriale.	
k	obbligatorio	integer	Specifica il numero di risultati restituiti dalla ricerca.	
similarity	obbligatorio	string	Specifica la metrica della distanza utilizzata per il calcolo della somiglianza.	<ul style="list-style-type: none">• euclidean• cosine• dotProduct

Parametro	Requisito	Type	Descrizione	Valore (i)
probes	facoltativo	integer	Il numero di cluster che si desidera ispezionare tramite la ricerca vettoriale. Un valore più elevato offre una migliore capacità di richiamo a scapito della velocità. Può essere impostato sul numero di elenchi per la ricerca esatta del vicino più vicino (a quel punto il pianificatore non utilizzerà l'indice) . L'impostazione consigliata per avviare la regolazione fine è $\sqrt{\text{# of lists}}$	Impostazione predefinita: 1

Parametro	Requisito	Type	Descrizione	Valore (i)
efSearch	facoltativo	integer	Speciifica la dimensione dell'elenco dinamico di candidati utilizzati o dall'indice HNSW durante la ricerca. Un valore più elevato di efSearch fornisce un migliore richiamo a scapito della velocità.	Impostazione predefinita: 40 Intervallo [1, 1000]

È importante regolare con precisione il valore di efSearch (HNSW) o probes (IVFlat) per ottenere le prestazioni e la precisione desiderate. Vedi le seguenti operazioni di esempio:

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
      }
    }
  }
]);
```

Output di esempio

L'aspetto dell'output di questa operazione è simile al seguente.

```
{ "_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 ] }
```

Caratteristiche e limitazioni

Compatibilità delle versioni

- La ricerca vettoriale per Amazon DocumentDB è disponibile solo nei cluster basati su istanze Amazon DocumentDB 5.0.

Vettori

- Amazon DocumentDB può indicizzare vettori fino a 2.000 dimensioni. Tuttavia, è possibile archiviare fino a 16.000 dimensioni senza un indice.

Indici

- Per la creazione dell'indice IVFFlat, il parametro di impostazione consigliata per gli elenchi è il numero di documenti/1000 per un massimo di 1 milione di documenti e per oltre 1 milione di documenti. `sqrt(# of documents)` A causa di un limite di memoria di lavoro, Amazon DocumentDB supporta un determinato valore massimo del parametro `lists` a seconda del numero di dimensioni. A titolo di riferimento, la tabella seguente fornisce i valori massimi del parametro `lists` per vettori di 500, 1000 e 2.000 dimensioni:

Tipo di istanza	Elenchi con 500 dimensioni	Elenchi con 1000 dimensioni	Elenchi con 2000 dimensioni
t3.med	372	257	150
5r5.l	915	741	511
r5xl	1.393	1.196	901
r 5,2 xl	5.460	5.230	4.788
r 5,4 xl	7.842	7.599	7.138
r 5,8 xl	11.220	10.974	10.498
r 5,12 xl	13.774	13.526	13.044
r5,16 xl	15.943	15.694	15.208
r5.24 xl	19.585	19.335	18,845

- Nessun'altra opzione di indice come `compound sparse` o `partial` è supportata dagli indici vettoriali.
- La creazione di indici paralleli non è supportata per l'indice HNSW. È supportato solo per l'indice IVFFlat.

Interrogazione vettoriale

- Per le query di ricerca vettoriali, è importante ottimizzare i parametri come `probes` o `efSearch` per ottenere risultati ottimali. Più alto è il valore di `probes` o `efSearch` parametro, maggiore è il richiamo e minore è la velocità. L'impostazione consigliata per iniziare a regolare con precisione il parametro delle sonde è `sqrt(# of lists)`

Best practice

Scopri le best practice per lavorare con la ricerca vettoriale in Amazon DocumentDB. Questa sezione viene continuamente aggiornata man mano che vengono identificate nuove best practice.

- La creazione di indici Inverted File with Flat Compression (IVFFlat) prevede il raggruppamento e l'organizzazione dei punti dati in base alle somiglianze. Pertanto, affinché un indice sia più efficace, si consiglia di caricare almeno alcuni dati prima di creare l'indice.
- Per le query di ricerca vettoriali, è importante ottimizzare i parametri come `probes` o `efSearch` per ottenere risultati ottimali. Più alto è il valore del `efSearch` parametro `probes` or, maggiore è il richiamo e minore è la velocità. L'impostazione consigliata per iniziare a regolare con precisione il `probes` parametro è `sqrt(lists)`.

Risorse

- [Ricerca vettoriale: qual è il nuovo post del blog](#)
- [Esempio di codice di ricerca semantico](#)
- [Esempi di codice di ricerca vettoriale di Amazon DocumentDB](#)

Migrazione ad Amazon DocumentDB

Amazon DocumentDB (compatibile con MongoDB) è un servizio di database completamente gestito compatibile con l'API MongoDB. Puoi migrare i tuoi dati su Amazon DocumentDB dai database MongoDB in esecuzione in locale o su Amazon Elastic Compute Cloud (Amazon EC2) utilizzando la procedura descritta in questa sezione.

Argomenti

- [Aggiornamento del cluster Amazon DocumentDB tramite AWS Database Migration Service](#)
- [Strumenti di migrazione](#)
- [Individuazione](#)
- [Pianificazione: requisiti del cluster Amazon DocumentDB](#)
- [Approcci per la migrazione](#)
- [Origini della migrazione](#)
- [Connettività per la migrazione](#)
- [Test in corso](#)
- [Test delle performance](#)
- [Verifica del failover](#)
- [Risorse aggiuntive](#)
- [Guida alla migrazione: da MongoDB ad Amazon DocumentDB](#)

Aggiornamento del cluster Amazon DocumentDB tramite AWS Database Migration Service

Important

Amazon DocumentDB non segue gli stessi cicli di vita del supporto di MongoDB e la pianificazione di MongoDB non si applica ad Amazon DocumentDB. end-of-life Al momento non ci sono piani end-of-life per Amazon DocumentDB 3.6 e i driver, le applicazioni e gli strumenti di MongoDB 3.6 esistenti continueranno a funzionare con Amazon DocumentDB.

Puoi aggiornare il tuo cluster Amazon DocumentDB a una versione superiore con tempi di inattività minimi utilizzando AWS DMS. AWS DMS è un servizio completamente gestito che semplifica la migrazione da versioni precedenti di Amazon DocumentDB, database relazionali e database non relazionali al cluster Amazon DocumentDB di destinazione.

Argomenti

- [Fase 1: abilitare Change Streams](#)
- [Fase 2: modifica la durata di conservazione di Change Streams](#)
- [Fase 3: Migrazione degli indici](#)
- [Fase 4: Creare un'istanza di AWS DMS replica](#)
- [Fase 5: Creare un AWS DMS endpoint di origine](#)
- [Passaggio 6: creare un endpoint di AWS DMS destinazione](#)
- [Passaggio 7: Creare ed eseguire un'attività di migrazione](#)
- [Fase 8: Modifica dell'endpoint dell'applicazione nel cluster Amazon DocumentDB di destinazione](#)

Fase 1: abilitare Change Streams

Per eseguire una migrazione con tempi di inattività minimi, è AWS DMS necessario l'accesso ai flussi di modifica del cluster. I [flussi di modifica di Amazon DocumentDB](#) forniscono una sequenza temporale di eventi di aggiornamento che si verificano all'interno delle raccolte e dei database del cluster. La lettura dal flusso di modifiche consente di AWS DMS eseguire l'acquisizione dei dati di modifica (CDC) e applicare aggiornamenti incrementali al cluster Amazon DocumentDB di destinazione.

Per abilitare i flussi di modifica per tutte le raccolte su un database specifico, esegui l'autenticazione nel tuo cluster Amazon DocumentDB utilizzando la shell mongo ed esegui i seguenti comandi:

```
db.adminCommand({modifyChangeStreams: 1,
  database: "db_name",
  collection: "",
  enable: true});
```

Fase 2: modifica la durata di conservazione di Change Streams

Successivamente, modifica il periodo di conservazione del flusso di modifiche in base al periodo di conservazione degli eventi di modifica nel flusso di modifiche. Ad esempio, se prevedi che la

migrazione del cluster Amazon DocumentDB richiede 12 ore, devi impostare la conservazione del flusso di modifiche su un valore superiore a 12 ore. AWS DMS Il periodo di conservazione predefinito per il cluster Amazon DocumentDB è di tre ore. Puoi modificare la durata di conservazione dei log del flusso di modifiche per il tuo cluster Amazon DocumentDB in modo che sia compresa tra un'ora e sette giorni utilizzando il AWS Management Console . AWS CLI Per maggiori dettagli, consulta [Modifica della durata di conservazione dei log di Change Stream](#).

Fase 3: Migrazione degli indici

Crea gli stessi indici sul cluster Amazon DocumentDB di destinazione che hai sul cluster Amazon DocumentDB di origine. Sebbene AWS DMS gestisca la migrazione dei dati, non migra gli indici. Per migrare gli indici, utilizza Amazon DocumentDB Index Tool per esportare gli indici dal cluster Amazon DocumentDB di origine. Puoi ottenere lo strumento creando un clone del repository di GitHub strumenti Amazon DocumentDB e seguendo le istruzioni riportate in. [README.md](#) Puoi eseguire lo strumento da un'istanza Amazon EC2 o da un AWS Cloud9 ambiente in esecuzione nello stesso Amazon VPC del cluster Amazon DocumentDB.

Nell'esempio seguente, sostituisci ogni *segnaposto dell'input utente* con le tue informazioni.

Il codice seguente esegue il dump degli indici dal cluster Amazon DocumentDB di origine:

```
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-xxxxxxx.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/
```

Una volta che gli indici sono stati esportati con successo, ripristina tali indici nel cluster Amazon DocumentDB di destinazione. Per ripristinare gli indici esportati nel passaggio precedente, utilizza lo strumento di indicizzazione di Amazon DocumentDB. Il comando seguente ripristina gli indici nel cluster Amazon DocumentDB di destinazione dalla directory specificata.

```
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-xxxxxxx.us-  
east-1.docdb.amazonaws.com:27017  
2020-02-11 21:51:23,264: testdb.coll: added index: _id
```

Per confermare di aver ripristinato correttamente gli indici, connessi al cluster Amazon DocumentDB di destinazione con la shell mongo ed elenca gli indici per una determinata raccolta. Vedi il codice seguente:

```
mongo --ssl  
--host docdb-xx-xx.cluster-xxxxxxx.us-east-1.docdb.amazonaws.com:27017  
--sslCAFile rds-ca-2019-root.pem --username documentdb --password documentdb  
  
db.coll.getIndexes()
```

Fase 4: Creare un'istanza di AWS DMS replica

Un'istanza di AWS DMS replica collega e legge i dati dal cluster Amazon DocumentDB di origine e li scrive nel cluster Amazon DocumentDB di destinazione. L'istanza di AWS DMS replica può eseguire sia operazioni di carico di massa che operazioni CDC. La maggior parte di questa elaborazione avviene in memoria. Tuttavia, operazioni di grandi dimensioni potrebbero richiedere un certo buffering su disco. Anche le transazioni e i file di log memorizzati nella cache vengono scritti su disco. Dopo la migrazione dei dati, l'istanza di replica trasmette anche gli eventuali eventi di modifica per assicurarsi che l'origine e la destinazione siano sincronizzate.

Per creare un'istanza di replica AWS DMS :

1. Apri la AWS DMS [console](#).
2. Nel riquadro di navigazione, scegli Replication instances (Istanze di replica).
3. Scegliere Create replication instance (Crea istanza di replica) e immettere le seguenti informazioni:
 - In Nome, inserisci un nome a tua scelta. Ad esempio, docdb36todocdb40.

- In Descrizione, inserisci una descrizione a tua scelta. Per listitem, istanza di replica da Amazon DocumentDB 3.6 ad Amazon DocumentDB 4.0.
- Per la classe Instance, scegli la dimensione in base alle tue esigenze.
- Per la versione Engine, scegli 3.4.1.
- Per Amazon VPC, scegli Amazon VPC che ospita i cluster Amazon DocumentDB di origine e di destinazione.
- Per lo storage allocato (GiB), usa il valore predefinito di 50 GiB. Se hai un carico di lavoro con throughput di scrittura elevato, aumenta questo valore in modo che corrisponda al tuo carico di lavoro.
- Per Multi-AZ, scegli Sì se hai bisogno di supporto per alta disponibilità e failover.
- Per Publicly accessible (Accessibile pubblicamente), abilitare questa opzione.

Replication instance configuration

Name
The name must be unique among all of your replication instances in the current AWS region.

Replication instance name must not start with a numeric value

Description

The description must only have unicode letters, digits, whitespace, or one of these symbols: _:/=+-@. 1000 maximum character.

Instance class [Info](#)
Choose an appropriate instance class for your replication needs. Each instance class provides differing levels of compute, network and memory capacity. [DMS pricing](#)

16 vCPUs 30 GiB Memory

Include previous-generation instance classes

Engine version
Choose an AWS DMS version to run on your replication instance. [DMS versions](#)

Include Beta DMS versions

Allocated storage (GiB)
Choose the amount of storage space you want for your replication instance. AWS DMS uses this storage for log files and cached transactions while replication tasks are in progress.

VPC
Choose an Amazon Virtual Private Cloud (VPC) where your replication instance should run.

Multi AZ
If you choose this option, AWS DMS will perform a multi-AZ deployment, with a primary instance in one availability zone (AZ) and a standby instance in another AZ. This configuration provides a highly available, fault-tolerant replication environment. Billing is based on [DMS pricing](#)

Publicly accessible
If you choose this option, AWS DMS will assign a public IP address to your replication instance, and you'll be able to connect to databases outside of your Amazon VPC.

4. Scegli Create replication instance (Crea istanza di replica).

Fase 5: Creare un AWS DMS endpoint di origine

L'endpoint di origine viene utilizzato per il cluster Amazon DocumentDB di origine.

Per creare un endpoint di origine

1. Apri la AWS DMS [console](#).
2. Nel pannello di navigazione, seleziona Endpoint.
3. Scegli `Create endpoint` e inserisci le seguenti informazioni:
 - Per Endpoint type (Tipo di endpoint), scegliere Source (Origine).
 - >Per l'identificatore dell'endpoint, inserisci un nome facile da ricordare, ad esempio. `docdb-source`
 - Per Source engine, scegli. `docdb`
 - Per Nome server, inserisci il nome DNS del cluster Amazon DocumentDB di origine.
 - Per Porta, inserisci il numero di porta del cluster Amazon DocumentDB di origine.
 - Per la modalità SSL, scegli. `verify-full`
 - Per il certificato CA, scegli Aggiungi nuovo certificato CA. Scarica il [nuovo certificato CA, nuovo certificato](#) per creare un pacchetto di connessioni TLS. Per l'identificatore del certificato, inserisci. `rds-combined-ca-bundle` Per Import certificate file (Importa file certificato), scegliere Choose file (Seleziona file) e passare al file `.pem` scaricato in precedenza. Selezionare e aprire il file. Scegli Importa certificato, quindi scegli `rds-combined-ca-bundle` dal menu a discesa Scegli un certificato
 - Per Nome utente, inserisci il nome utente principale del cluster Amazon DocumentDB di origine.
 - Per Password, inserisci la password principale del cluster Amazon DocumentDB di origine.
 - Per Nome del database, inserisci il nome del database che desideri aggiornare.

Endpoint configuration

Endpoint identifier [Info](#)
A label for the endpoint to help you identify it.

Source engine
The type of database engine this endpoint is connected to.

Server name

Port
The port the database runs on for this endpoint.

Secure Socket Layer (SSL) mode
The type of Secure Socket Layer enforcement

CA certificate

 [Add new CA certificate](#)

User name [Info](#)

Password [Info](#)

Database name

4. Verifica la connessione per verificare che sia stata configurata correttamente.

▼ **Test endpoint connection (optional)**

VPC

vpc-2bf12540

Replication instance
A replication instance performs the database migration

docdb36todocdb40

Run test

Endpoint identifier	Replication instance	Status	Message
docdb36-source	docdb36todocdb40	successful	

5. Scegliere Create Endpoint (Crea endpoint).

Note

AWS DMS può migrare solo un database alla volta.

Passaggio 6: creare un endpoint di AWS DMS destinazione

L'endpoint di destinazione è per il cluster Amazon DocumentDB di destinazione.

Per creare un endpoint di destinazione:

1. Apri la [AWS DMS console](#).
2. Nel pannello di navigazione, seleziona Endpoint.
3. Scegliere Create endpoint (Crea endpoint) e immettere le informazioni seguenti:
 - Per Endpoint type (Tipo di endpoint), scegliere Target (Destinazione).
 - Per Endpoint identifier (Identificatore endpoint), immettere un nome facile da ricordare, ad esempio docdb-target.
 - Per Source engine, scegli docdb.
 - Per Nome server, inserisci il nome DNS del cluster Amazon DocumentDB di destinazione.

- Per Porta, inserisci il numero di porta del cluster Amazon DocumentDB di destinazione.
- Per la modalità SSL, scegli. `verify-full`
- Per il certificato CA, scegli il `rds-combined-ca-bundle` certificato esistente dal menu a discesa Scegli un certificato.
- Per Nome utente, inserisci il nome utente principale del cluster Amazon DocumentDB di destinazione.
- Per Password, inserisci la password principale del cluster Amazon DocumentDB di destinazione.
- Per Nome del database, inserisci lo stesso nome di database utilizzato per configurare l'endpoint di origine.

Endpoint configuration

Endpoint identifier [Info](#)
A label for the endpoint to help you identify it.

Target engine
The type of database engine this endpoint is connected to.

Server name

Port
The port the database runs on for this endpoint.

Secure Socket Layer (SSL) mode
The type of Secure Socket Layer enforcement

CA certificate

 [Add new CA certificate](#)

User name [Info](#)

Password [Info](#)

Database name

4. Verifica la connessione per verificare che sia stata configurata correttamente.

▼ **Test endpoint connection (optional)**

VPC
vpc-2bf12540 ▼

Replication instance
A replication instance performs the database migration
docdb36todocdb40 ▼

Run test

Endpoint identifier	Replication instance	Status	Message
docdb36-target	docdb36todocdb40	successful	

5. Scegliere Create Endpoint (Crea endpoint).

Passaggio 7: Creare ed eseguire un'attività di migrazione

Un' AWS DMS attività associa l'istanza di replica all'istanza di origine e di destinazione. Quando si crea un'attività di migrazione, si specifica l'endpoint di origine, l'endpoint di destinazione, l'istanza di replica e tutte le impostazioni di migrazione desiderate. È possibile creare un' AWS DMS attività con tre diversi tipi di migrazione: migrazione dei dati esistenti, migrazione dei dati esistenti e replica delle modifiche in corso o replica solo delle modifiche ai dati. Poiché lo scopo di questa procedura dettagliata è aggiornare un cluster Amazon DocumentDB con tempi di inattività minimi, i passaggi utilizzano l'opzione per migrare i dati esistenti e replicare le modifiche in corso. Con questa opzione, AWS DMS acquisisce le modifiche durante la migrazione dei dati esistenti. AWS DMS continua ad acquisire e applicare le modifiche anche dopo il caricamento di grandi quantità di dati. Alla fine i database di origine e di destinazione saranno sincronizzati, con tempi di inattività per la migrazione quasi nulli.

Di seguito sono riportati i passaggi per creare un'attività di migrazione per una migrazione con tempi di inattività minimi:

1. Apri la AWS DMS [console](#).
2. Nel riquadro di navigazione scegliere Tasks (Attività).
3. Scegliere Create task (Crea attività) e immettere le informazioni seguenti:

- Per Task name (Nome attività), immettere un nome facile da ricordare, ad esempio my-dms-upgrade-task.
- Per l'istanza di replica, scegli l'istanza di replica creata nel [passaggio 3: creazione](#) di un'istanza di replica AWS Database Migration Service
- Per l'endpoint di origine, scegli l'endpoint di origine creato nel [passaggio 4: Creazione di un endpoint di origine AWS Database Migration Service](#)
- Per Target endpoint, scegli l'endpoint di destinazione che hai creato nel [passaggio 5: Creare un endpoint di destinazione AWS Database Migration Service](#)
- Per il tipo di migrazione, scegli Migra i dati esistenti e replica le modifiche in corso.

Task configuration

Task identifier
my-dms-upgrade-task

Replication instance
docdb36todocdb40 - vpc-b06365ca

Source database endpoint
docdb36-source

Target database endpoint
docdb40-target

Migration type [Info](#)
Migrate existing data and replicate ongoing changes

4. Nella sezione Impostazioni attività, abilita i registri. CloudWatch
5. Per la sezione Mappature delle tabelle, scegli Non fare nulla. Ciò garantirà che gli indici creati nel passaggio 3 non vengano eliminati.
6. Per la configurazione di avvio dell'attività di migrazione, scegli Automaticamente al momento della creazione. Questo avvierà automaticamente l'attività di migrazione una volta creata.
7. Scegli Create task (Crea attività).

AWS DMS ora inizia la migrazione dei dati dal cluster Amazon DocumentDB di origine al cluster Amazon DocumentDB di destinazione. Lo stato dell'attività dovrebbe cambiare da Avvio a In esecuzione. Puoi monitorare l'avanzamento scegliendo Attività nella AWS DMS console. Dopo alcuni minuti/ore (a seconda delle dimensioni della migrazione), lo stato dovrebbe cambiare da Caricamento completo, replica in corso. Ciò significa che AWS DMS ha completato una migrazione a pieno carico del cluster Amazon DocumentDB di origine verso un cluster Amazon DocumentDB di destinazione e ora sta replicando gli eventi di modifica.

Summary			
Status	Type	Source	Target
🔄 Load complete, replication ongoing	Full load, ongoing replication	docdb36source	docdb40target

Alla fine l'origine e la destinazione saranno sincronizzate. Puoi verificare se sono sincronizzati eseguendo un'count () operazione sulle tue raccolte per verificare che tutti gli eventi di modifica siano stati migrati.

Fase 8: Modifica dell'endpoint dell'applicazione nel cluster Amazon DocumentDB di destinazione

Una volta completato il caricamento completo e dopo la replica continua del processo CDC, sei pronto a modificare l'endpoint di connessione al database dell'applicazione dal cluster Amazon DocumentDB di origine al cluster Amazon DocumentDB di destinazione.

Strumenti di migrazione

Per migrare ad Amazon DocumentDB, i due strumenti principali utilizzati dalla maggior parte dei clienti sono [AWS DMS\(\)](#) e [AWS Database Migration Service le](#) utilità da riga di comando come `and.mongodump mongorestore`. Come best practice, e per entrambe queste opzioni, consigliamo di creare indici in Amazon DocumentDB prima di iniziare la migrazione, in quanto ciò può ridurre il tempo complessivo e aumentare la velocità della migrazione. A tale scopo, puoi utilizzare [Amazon DocumentDB Index Tool](#).

AWS Database Migration Service

AWS Database Migration Service (AWS DMS) è un servizio cloud che semplifica la migrazione di database relazionali e non relazionali su Amazon DocumentDB. Puoi utilizzarli AWS DMS per migrare i dati su Amazon DocumentDB da database ospitati in locale o su EC2. Con AWS DMS, puoi eseguire migrazioni una tantum oppure replicare le modifiche in corso per mantenere sincronizzate fonti e destinazioni.

Per ulteriori informazioni sull'utilizzo per AWS DMS la migrazione ad Amazon DocumentDB, consulta:

- [Usare MongoDB come sorgente per AWS DMS](#)
- [Utilizzo di Amazon DocumentDB come destinazione per AWS Database Migration Service](#)
- [Procedura dettagliata: migrazione da MongoDB ad Amazon DocumentDB](#)

Utility della riga di comando

Le utilità comuni per la migrazione dei dati da e verso Amazon DocumentDB `mongodump` includono `mongorestore`, `mongoexport` e `mongoimport`. In genere, `mongodump` e `mongorestore` sono le utility più efficienti in quanto eseguono il dump e il ripristino dei dati dai database in formato binario. Questa è generalmente l'opzione più performante e produce una dimensione di dati più piccola rispetto alle esportazioni logiche. `mongoexport` e `mongoimport` sono utili se si desidera esportare e importare dati in un formato logico come JSON o CSV poiché i dati sono leggibili dalle persone, ma generalmente sono più lenti di `mongodump/mongorestore` e producono una maggiore dimensione dei dati.

La [Approcci per la migrazione](#) sezione seguente illustrerà quando è meglio utilizzare AWS DMS e le utilità da riga di comando in base al caso d'uso e ai requisiti.

Individuazione

Per ognuna delle distribuzioni MongoDB, è necessario identificare e registrare due set di dati: i dettagli dell'architettura e le caratteristiche operative. Queste informazioni ti aiuteranno a scegliere l'approccio di migrazione e il dimensionamento del cluster più appropriati.

Dettagli dell'architettura

- Nome

Scegliere un nome univoco per monitorare la distribuzione.

- Versione

Registrare la versione di MongoDB in esecuzione nella distribuzione. Per individuare la versione, connettersi a un membro del set di repliche con la shell mongo ed eseguire l'operazione `db.version()`.

- Type

Registrare se la distribuzione è un'istanza mongo autonoma, un set di repliche o un cluster con shard.

- Membri

Registrare i nomi host, gli indirizzi e le porte di ogni cluster, set di repliche o membro standalone.

Per una distribuzione in cluster, è possibile individuare i membri della shard connettendosi a un host mongo con la shell mongo ed eseguendo l'operazione `sh.status()`.

Per una set di repliche, è possibile recuperare i membri connettendosi a membro del set di repliche con la shell mongo ed eseguendo l'operazione `rs.status()`.

- Dimensioni oplog

Per i set di repliche o cluster con shard, registrare le dimensioni dell'oplog per ogni membro del set di repliche. Per trovare questa informazione, connettersi al membro del set di repliche con la shell mongo ed eseguire l'operazione `ps.printReplicationInfo()`.

- Priorità membri set di repliche

Per i set di repliche o cluster con shard, registrare la priorità per ogni membro del set di repliche. Per trovare questa informazione, connettersi a un membro del set di repliche con la shell mongo ed eseguire l'operazione `rs.conf()`. La priorità è indicata come valore della chiave `priority`.

- Utilizzo SSL/TLS

Registrare se per la crittografia dei dati in transito viene utilizzato il protocollo Transport Layer Security (TLS)/Secure Sockets Layer (SSL) in ogni nodo.

Caratteristiche operative

- Statistiche database

Per ogni raccolta, registrare le seguenti informazioni:

- Nome
- Dimensioni dei dati
- Conteggio delle raccolte

Per individuare le statistiche del database, connettersi al database con la shell Mongo ed eseguire il comando `db.runCommand({dbstats: 1})`.

- Statistiche raccolta

Per ogni raccolta, registrare le seguenti informazioni:

- Spazio dei nomi
- Dimensioni dei dati
- Conteggio degli indici
- Se la raccolta è limitata

- Statistiche indice

Per ogni raccolta, registrare le seguenti informazioni sull'indice:

- Spazio dei nomi
- ID
- Size
- Chiavi
- TTL

- Sparse
- Contesto

Per individuare le informazioni sull'indice, connettersi al database con la shell mongo ed eseguire il comando `db.collection.getIndexes()`.

- Opcounter

Oltre ad agevolare la comprensione degli attuali modelli dei carichi di lavoro (intensivi in lettura, intensivi in scrittura o bilanciati), Fornisce inoltre indicazioni sulla selezione iniziale delle istanze di Amazon DocumentDB.

Di seguito sono riportati le informazioni principali da raccogliere nel periodo di monitoraggio (in numero o in secondi):

- Query
- Inserimenti
- Aggiornamenti
- Eliminazioni

È possibile ottenere queste informazioni tramite una rappresentazione grafica dell'output del comando `db.serverStatus()` nel corso del tempo. Tramite lo strumento `mongostat` è inoltre possibile ottenere valori istantanei per queste statistiche, con i quali però si rischia di pianificare la migrazione considerando periodi di utilizzo che non comprendono carichi di picco.

- Statistiche di rete

Oltre ad agevolare la comprensione degli attuali modelli dei carichi di lavoro (intensivi in lettura, intensivi in scrittura o bilanciati), Fornisce inoltre indicazioni sulla selezione iniziale delle istanze di Amazon DocumentDB.

Di seguito sono riportati le informazioni principali da raccogliere nel periodo di monitoraggio (in numero o in secondi):

- Connessioni
- Byte di rete in ingresso
- Byte di rete in uscita

È possibile ottenere queste informazioni tramite una rappresentazione grafica dell'output del comando `db.serverStatus()` nel corso del tempo. Tramite lo strumento `mongostat` è inoltre possibile ottenere valori istantanei per queste statistiche, con i quali però si rischia di pianificare la migrazione considerando periodi di utilizzo che non comprendono carichi di picco.

Pianificazione: requisiti del cluster Amazon DocumentDB

Una migrazione di successo richiede un'attenta valutazione della configurazione del cluster Amazon DocumentDB e del modo in cui le applicazioni accederanno al cluster. Per determinare i requisiti del cluster, tieni conto di questi fattori:

- Disponibilità

Amazon DocumentDB offre un'elevata disponibilità attraverso la distribuzione di istanze di replica, che possono essere promosse a istanza principale in un processo noto come failover. Con la distribuzione di istanze di replica in diverse zone di disponibilità, puoi ottenere maggiori livelli di disponibilità.

La tabella seguente fornisce linee guida per le configurazioni di distribuzione di Amazon DocumentDB per soddisfare obiettivi di disponibilità specifici.

Disponibilità desiderata	Istanze totali	Repliche	Zone di disponibilità
99%	1	0	1

Disponibilità desiderata	Istanze totali	Repliche	Zone di disponibilità
99,9%	2	1	2
99,99%	3	2	3

L'affidabilità del sistema dipende da tutti i componenti, non solo dal database. Per le best practice e i consigli per soddisfare le esigenze complessive di affidabilità del sistema, consultate il white paper [AWS Well-Architected Reliability Pillar](#).

- Prestazioni

Le istanze Amazon DocumentDB consentono di leggere e scrivere sul volume di storage del cluster. Sono disponibili vari tipi di istanze cluster, con diverse quantità di memoria e vCPU, che influiscono sulle prestazioni di lettura e scrittura del cluster. Con le informazioni raccolte nella fase di individuazione, scegli un tipo di istanza che possa supportare i requisiti prestazionali del tuo carico di lavoro. Per una lista di tipi di istanze supportate, consulta [Gestione delle classi delle istanze](#).

Quando scegli un tipo di istanza per il tuo cluster Amazon DocumentDB, considera i seguenti aspetti dei requisiti prestazionali del tuo carico di lavoro:

- vCPU: le architetture che richiedono un numero maggiore di connessioni potrebbero trarre vantaggio dalle istanze con più vCPU.
- Memoria: quando possibile, mantenere il set di dati di lavoro in memoria offre le massime prestazioni. Una linea guida iniziale è quella di riservare un terzo della memoria dell'istanza per il motore Amazon DocumentDB, lasciando due terzi per il set di dati di lavoro.
- Connessioni: il numero minimo di connessioni ottimale è di otto connessioni per vCPU dell'istanza Amazon DocumentDB. Sebbene il limite di connessione delle istanze di Amazon

DocumentDB sia molto più elevato, i vantaggi prestazionali delle connessioni aggiuntive diminuiscono al di sopra delle otto connessioni per vCPU.

- **Rete:** i carichi di lavoro con un numero elevato di client o connessioni devono considerare le prestazioni di rete aggregate richieste per i dati inseriti e recuperati. L'esecuzione di operazioni in blocco può rendere più efficiente l'utilizzo delle risorse di rete.
- **Prestazioni di inserimento:** gli inserti di documenti singoli sono generalmente il modo più lento per inserire dati in Amazon DocumentDB. Le operazioni di inserimento in blocco possono essere nettamente più veloci.
- **Prestazioni di lettura:** le letture dalla memoria di lavoro sono sempre più veloci delle letture restituite dal volume di storage. Pertanto, l'ideale è ottimizzare le dimensioni della memoria dell'istanza per mantenere in memoria il set di lavoro.

Oltre a fornire letture dall'istanza principale, i cluster Amazon DocumentDB vengono configurati automaticamente come set di repliche. È quindi possibile instradare le query di sola lettura alle repliche di lettura impostando le relative preferenze nel driver MongoDB. È possibile dimensionare il traffico in lettura aggiungendo repliche e riducendo così il carico generale sull'istanza primaria.

È possibile distribuire repliche Amazon DocumentDB di diversi tipi di istanze nello stesso cluster. Un caso d'uso di esempio potrebbe essere quello di impostare una replica con un tipo di istanza più grande per gestire il traffico di analisi temporaneo. Se distribuisce un set di diversi tipi di istanza, assicurati di configurare la priorità di failover per ogni istanza. Questo garantisce che un evento di failover promuoverà sempre una replica di dimensioni sufficienti per gestire il tuo carico di scrittura.

- **Ripristino**

Amazon DocumentDB esegue continuamente il backup dei dati man mano che vengono scritti.

Fornisce funzionalità di point-in-time ripristino (PITR) entro un periodo configurabile di 1—35 giorni,

~~noto come periodo di conservazione del backup. Il periodo di conservazione dei backup predefinito~~

è di un giorno. Amazon DocumentDB crea inoltre automaticamente istantanee giornaliere del volume di storage, che vengono conservate anche per il periodo di conservazione dei backup configurato.

Se desideri conservare le istantanee oltre il periodo di conservazione del backup, puoi anche avviare istantanee manuali in qualsiasi momento utilizzando `awscli` o `aws`. AWS Management Console AWS Command Line Interface AWS CLI Per ulteriori informazioni, consulta [Backup e ripristino in Amazon DocumentDB](#).

Quando pianifichi la migrazione, tieni conto di quanto segue:

- Scegliete un periodo di conservazione dei backup di 1—35 giorni che soddisfi il vostro Recovery Point Objective (RPO).
- Decidi se hai bisogno di snapshot manuali e, in caso affermativo, con quale frequenza.

Approcci per la migrazione

Esistono tre approcci principali per la migrazione dei dati su Amazon DocumentDB.

Note

Sebbene sia possibile creare indici in qualsiasi momento in Amazon DocumentDB, nel complesso è più veloce creare gli indici prima di importare set di dati di grandi dimensioni. Come best practice, consigliamo di creare gli indici in Amazon DocumentDB per ciascuno degli approcci seguenti prima di eseguire la migrazione. A tale scopo, puoi utilizzare [Amazon DocumentDB Index Tool](#).

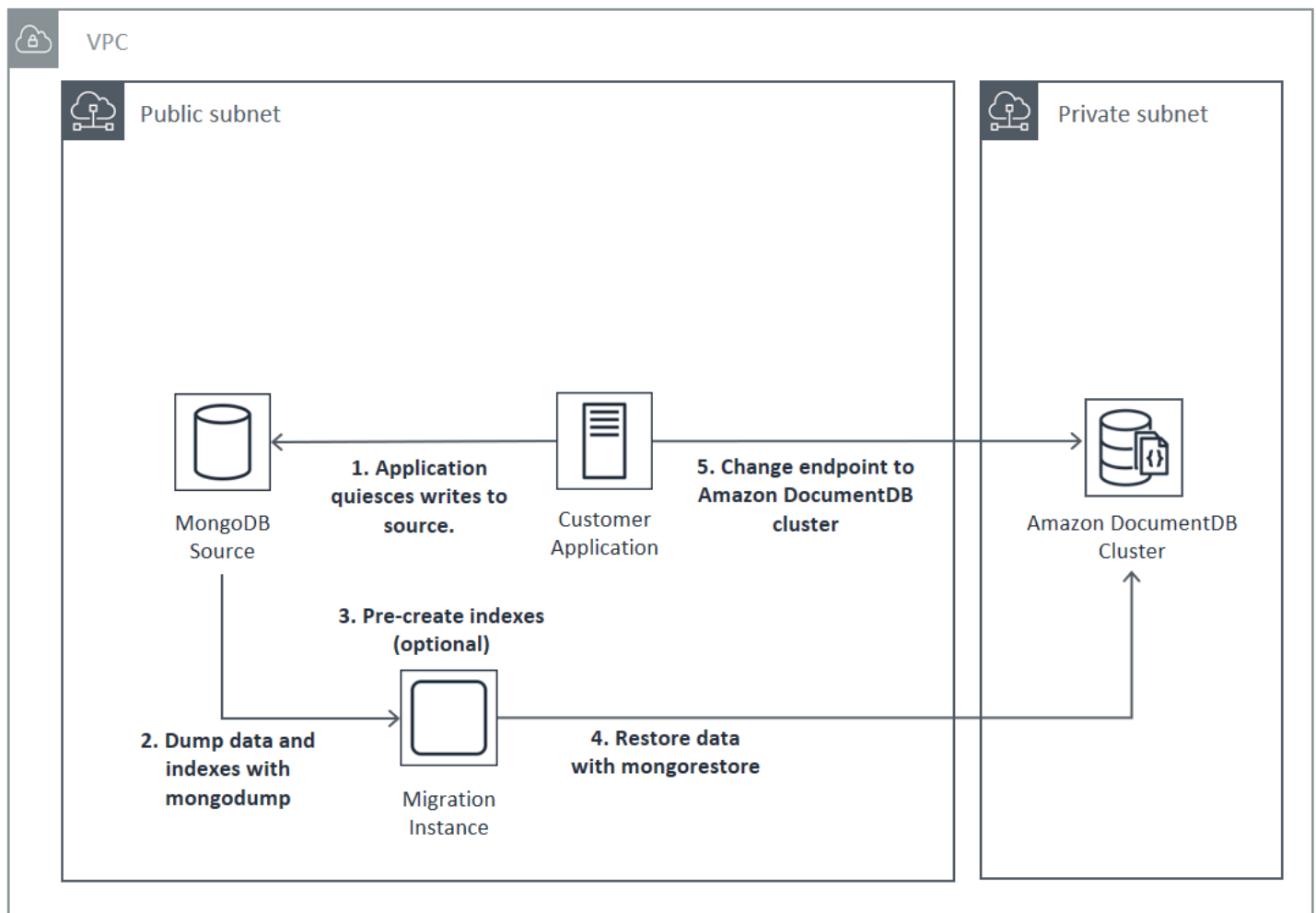
Offline

L'approccio offline utilizza gli strumenti `mongorestore` e `mongodump` per migrare i dati dalla distribuzione di MongoDB di origine al cluster Amazon DocumentDB. L'approccio offline è il più semplice per la migrazione, ma causa anche il tempo di inattività più lungo per il cluster.

Il processo di base per la migrazione offline è il seguente:

1. Sospendi le operazioni di scrittura sull'origine MongoDB.
2. Esegui il dump della raccolta di dati e indici dalla distribuzione MongoDB di origine.
3. Se stai migrando verso un cluster elastico, crea le tue raccolte suddivise utilizzando il comando `sh.shardCollection()`. Se stai migrando verso un cluster basato su istanze, vai al passaggio successivo.
4. Ripristina gli indici nel cluster Amazon DocumentDB.
5. Ripristina i dati di raccolta nel cluster Amazon DocumentDB.
6. Modifica l'endpoint dell'applicazione per scrivere nel cluster Amazon DocumentDB.

Offline Migration Approach



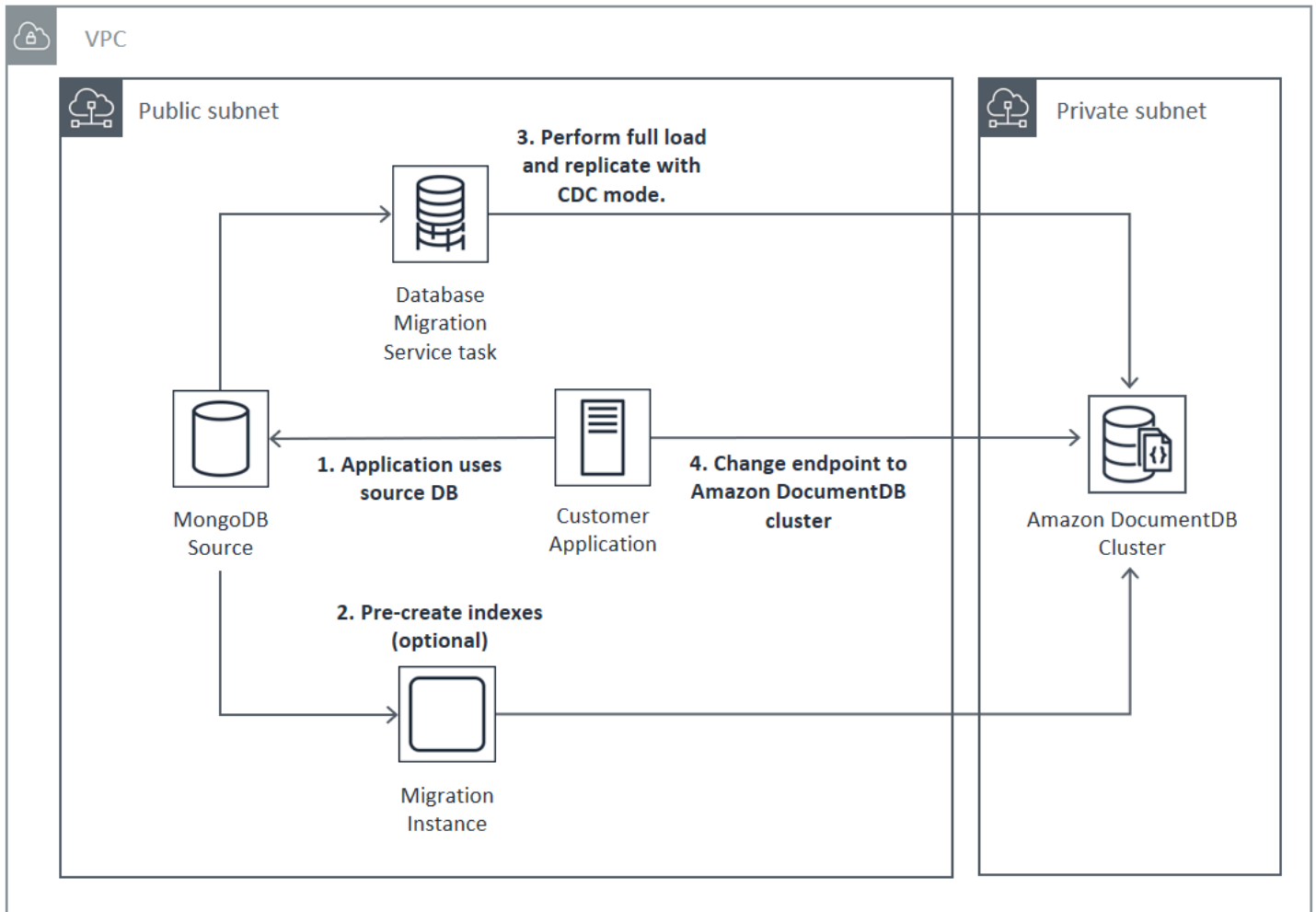
Online

L'approccio online utilizza AWS Database Migration Service (AWS DMS). Esegue un carico completo di dati dalla distribuzione di MongoDB di origine al cluster Amazon DocumentDB. Quindi passa in modalità Change Data Capture (CDC) per replicare le modifiche. L'approccio online riduce al minimo i tempi di inattività per il cluster, ma è il più lento dei tre metodi.

Il processo di base per la migrazione online è il seguente:

1. L'applicazione utilizza il database di origine normalmente.
2. Se stai migrando verso un cluster elastico, crea le tue raccolte frammentate utilizzando il comando `sh.shardCollection()`. Se stai migrando verso un cluster basato su istanze, vai al passaggio successivo.
3. Pre-crea indici nel cluster Amazon DocumentDB.
4. Crea un' AWS DMS attività per eseguire un carico completo, quindi abilita CDC dalla distribuzione MongoDB di origine al cluster Amazon DocumentDB.
5. Dopo aver completato AWS DMS un caricamento completo e aver replicato le modifiche in Amazon DocumentDB, passa l'endpoint dell'applicazione al cluster Amazon DocumentDB.

Online Migration Approach



Per ulteriori informazioni sull'utilizzo AWS DMS per la migrazione, consulta [Using Amazon DocumentDB as a Target AWS Database Migration Service](#) for e il [relativo](#) tutorial nella Guida per AWS Database Migration Service l'utente.

Ibrido

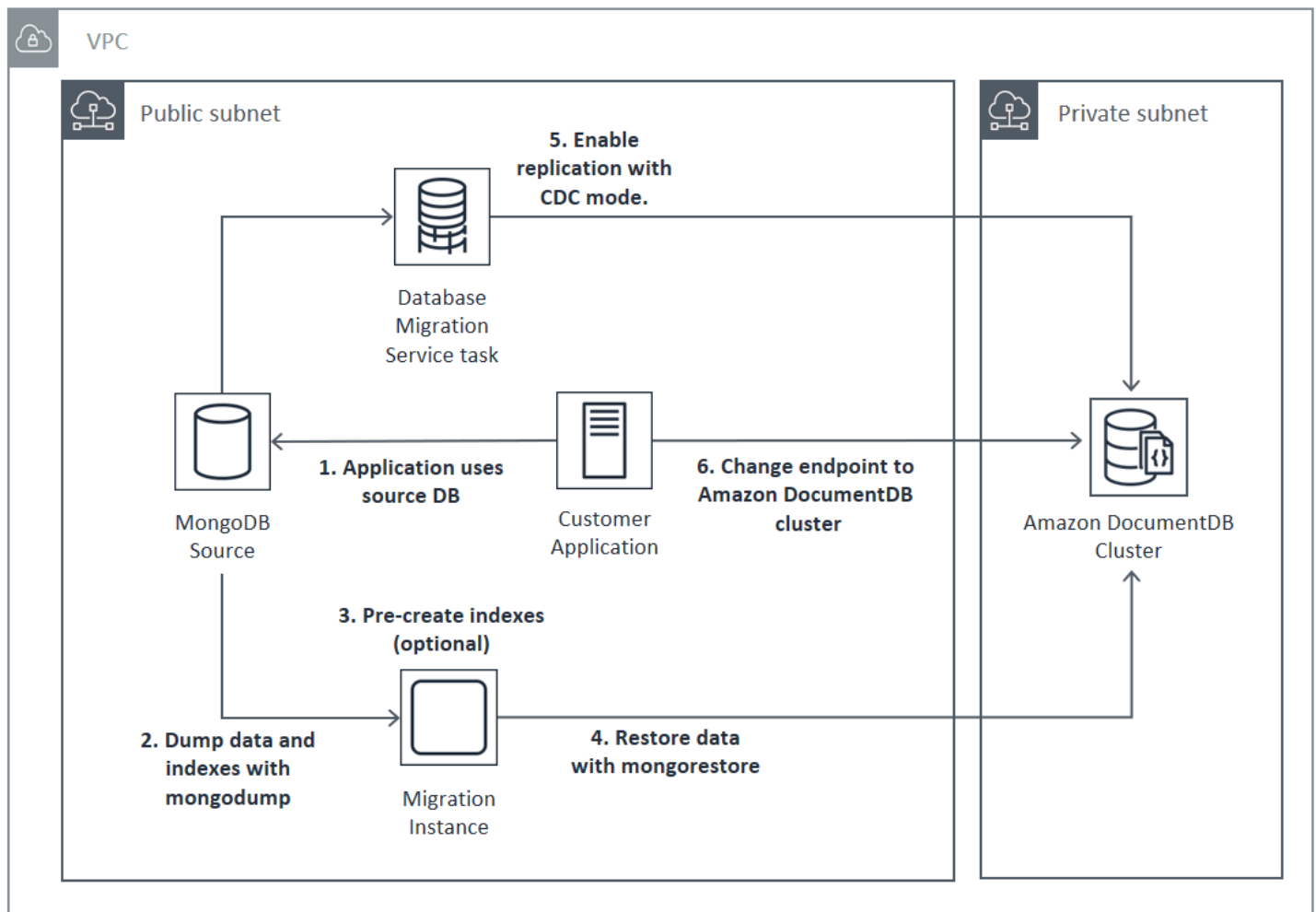
L'approccio ibrido utilizza gli `mongorestore` e strumenti `mongodump` e per migrare i dati dalla distribuzione di MongoDB di origine al cluster Amazon DocumentDB. Viene quindi utilizzato AWS DMS in modalità CDC per replicare le modifiche. L'approccio ibrido bilancia la velocità di migrazione con il tempo di inattività, ma è il più complesso dei tre approcci.

Il processo di base per la migrazione ibrida è il seguente:

1. L'applicazione utilizza la distribuzione MongoDB di origine normalmente.

2. Esegui il dump della raccolta di dati e indici dalla distribuzione MongoDB di origine.
3. Ripristina gli indici nel cluster Amazon DocumentDB.
4. Se stai migrando verso un cluster elastico, crea le tue raccolte frammentate usando il comando `sh.shardCollection()`. Se stai migrando verso un cluster basato su istanze, vai al passaggio successivo.
5. Ripristina i dati di raccolta nel cluster Amazon DocumentDB.
6. Crea un' AWS DMS attività per abilitare CDC dalla distribuzione MongoDB di origine al cluster Amazon DocumentDB.
7. Quando l' AWS DMS attività consiste nella replica delle modifiche all'interno di una finestra accettabile, modifica l'endpoint dell'applicazione per scrivere nel cluster Amazon DocumentDB.

Hybrid Migration Approach



⚠ Important

Attualmente un' AWS DMS attività può migrare solo un singolo database. Se l'origine MongoDB dispone di un numero elevato di database, potrebbe essere necessario automatizzare la creazione di attività di migrazione o considerare l'utilizzo del metodo offline.

Indipendentemente dall'approccio di migrazione scelto, è più efficiente precreare indici nel cluster Amazon DocumentDB prima di migrare i dati. Questo perché gli indici di Amazon DocumentDB sono dati inseriti in parallelo, ma la creazione di un indice su dati esistenti è un'operazione a thread singolo.

Poiché AWS DMS non migra gli indici (solo i tuoi dati), non è necessario alcun passaggio aggiuntivo per evitare di creare indici una seconda volta.

Origini della migrazione

Se l'origine MongoDB è un processo mongo standalone e vuoi utilizzare l'approccio di migrazione online o ibrido, prima converti il processo mongo standalone in un set di repliche, in modo che venga creato l'oplog da utilizzare come origine CDC.

Se la migrazione parte da un set di repliche o da un cluster MongoDB con shard, è consigliabile creare un secondario concatenato o nascosto per ogni set di repliche o shard da utilizzare come origine della migrazione. L'esecuzione di dump dei dati può forzare l'uscita dalla memoria del set di dati di lavoro e inficiare le prestazioni delle istanze di produzione. È possibile ridurre il rischio effettuando la migrazione da un nodo che non distribuisce dati di produzione.

Versioni delle origini della migrazione

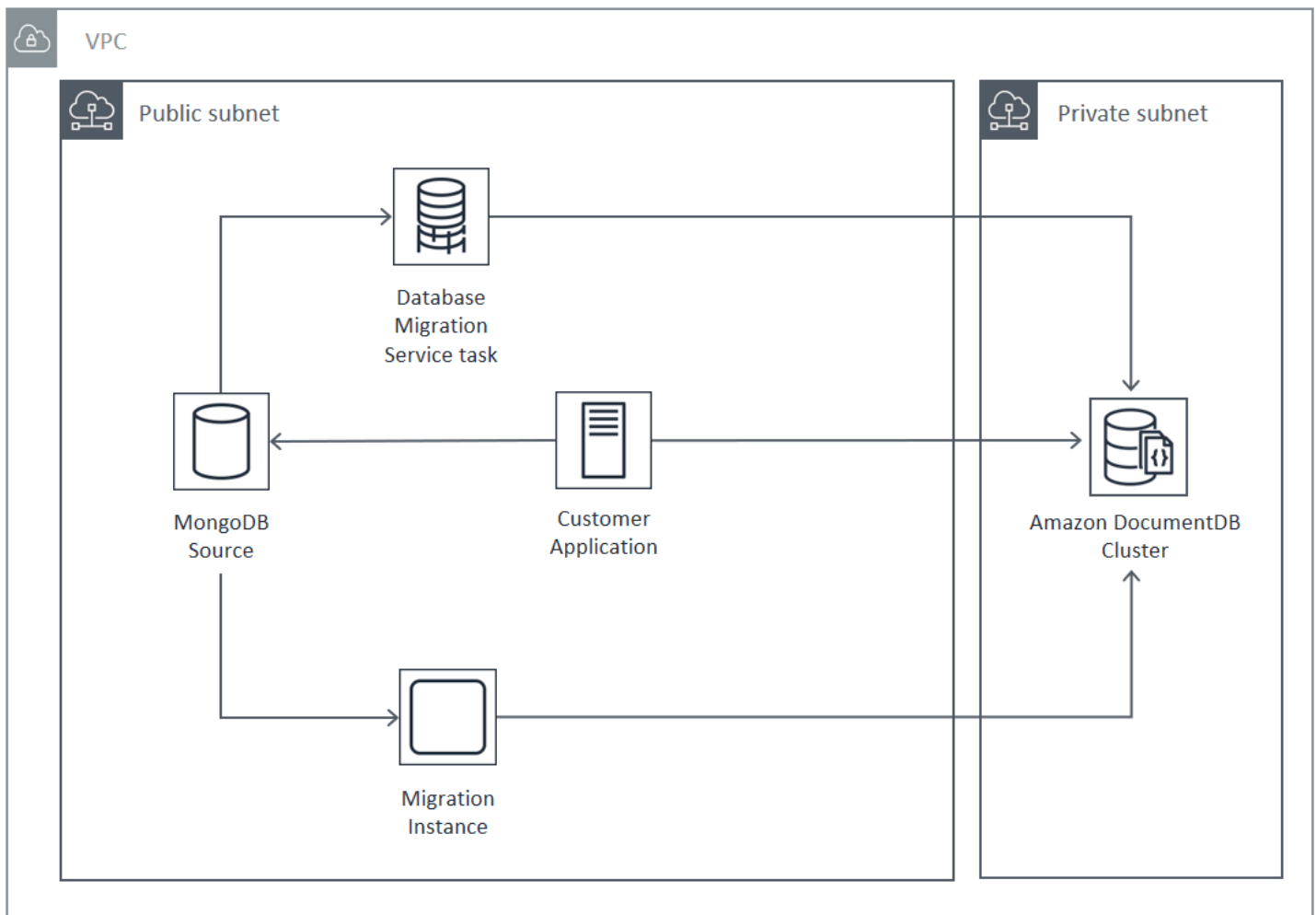
Se la versione del database MongoDB di origine è diversa dalla versione di compatibilità del cluster Amazon DocumentDB di destinazione, potrebbe essere necessario eseguire altre fasi di preparazione per garantire una migrazione di successo. I due requisiti più comuni riscontrati sono la necessità di aggiornare l'installazione di MongoDB di origine a una versione supportata per la migrazione (MongoDB versione 3.0 o successiva) e l'aggiornamento dei driver dell'applicazione per supportare la versione di destinazione di Amazon DocumentDB.

Se la migrazione prevede uno di questi requisiti, assicurati di includere queste fasi nel tuo piano di migrazione per aggiornare e testare qualsiasi modifica ai driver.

Connettività per la migrazione

Puoi migrare ad Amazon DocumentDB da una distribuzione MongoDB di origine in esecuzione nel tuo data center o da una distribuzione MongoDB in esecuzione su un'istanza Amazon EC2. quest'ultima opzione è semplice e richiede solo di configurare correttamente i gruppi di sicurezza e le sottoreti.

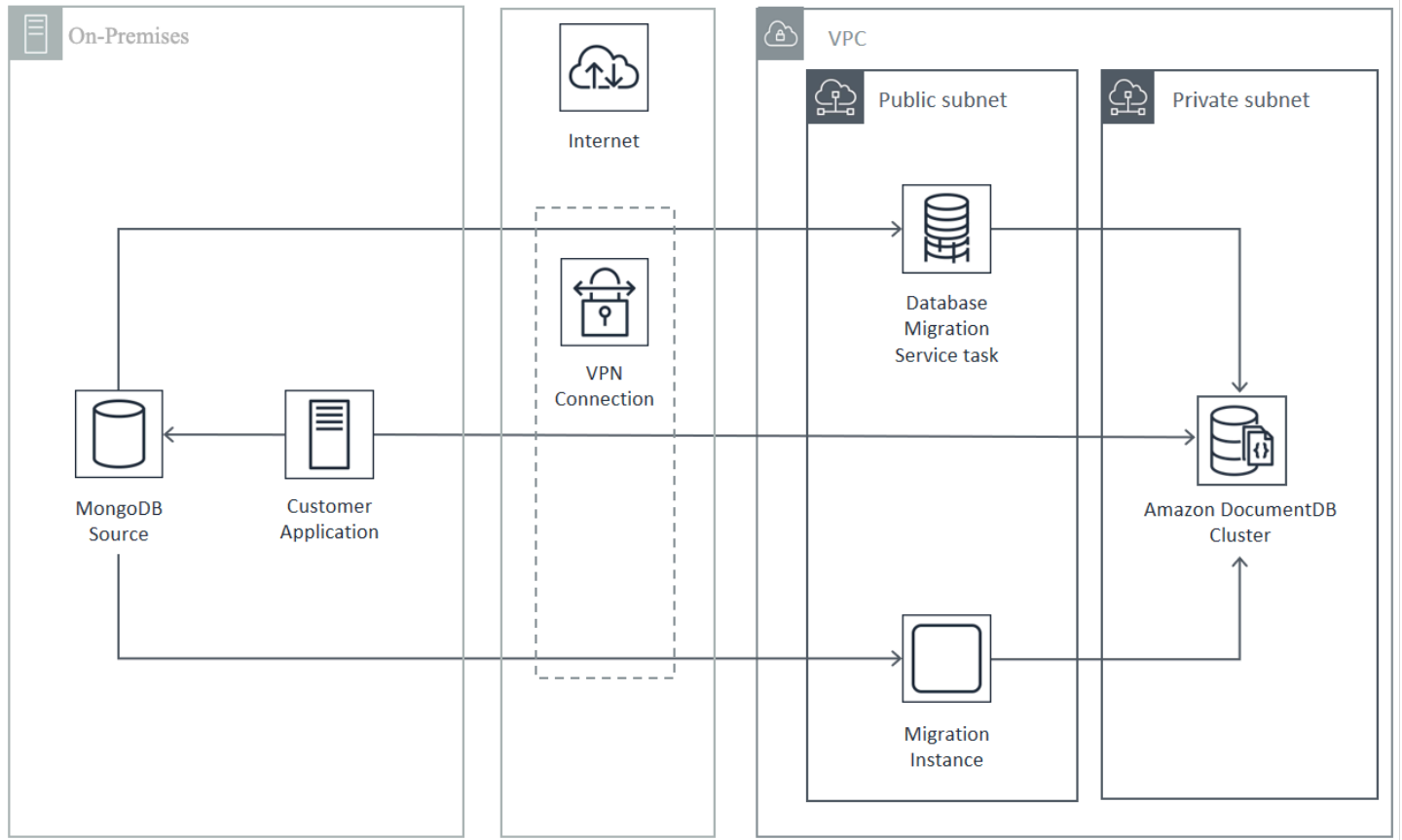
Migrating from EC2 Source



Per la migrazione da un database locale è necessaria una connessione tra la distribuzione MongoDB e il cloud privato virtuale (VPC). È possibile eseguire questa operazione tramite una connessione di rete privata virtuale (VPN) o utilizzando il servizio AWS Direct Connect. Anche se è possibile eseguire la migrazione al VPC tramite Internet, in termini di sicurezza questo metodo di connessione è il meno consigliato.

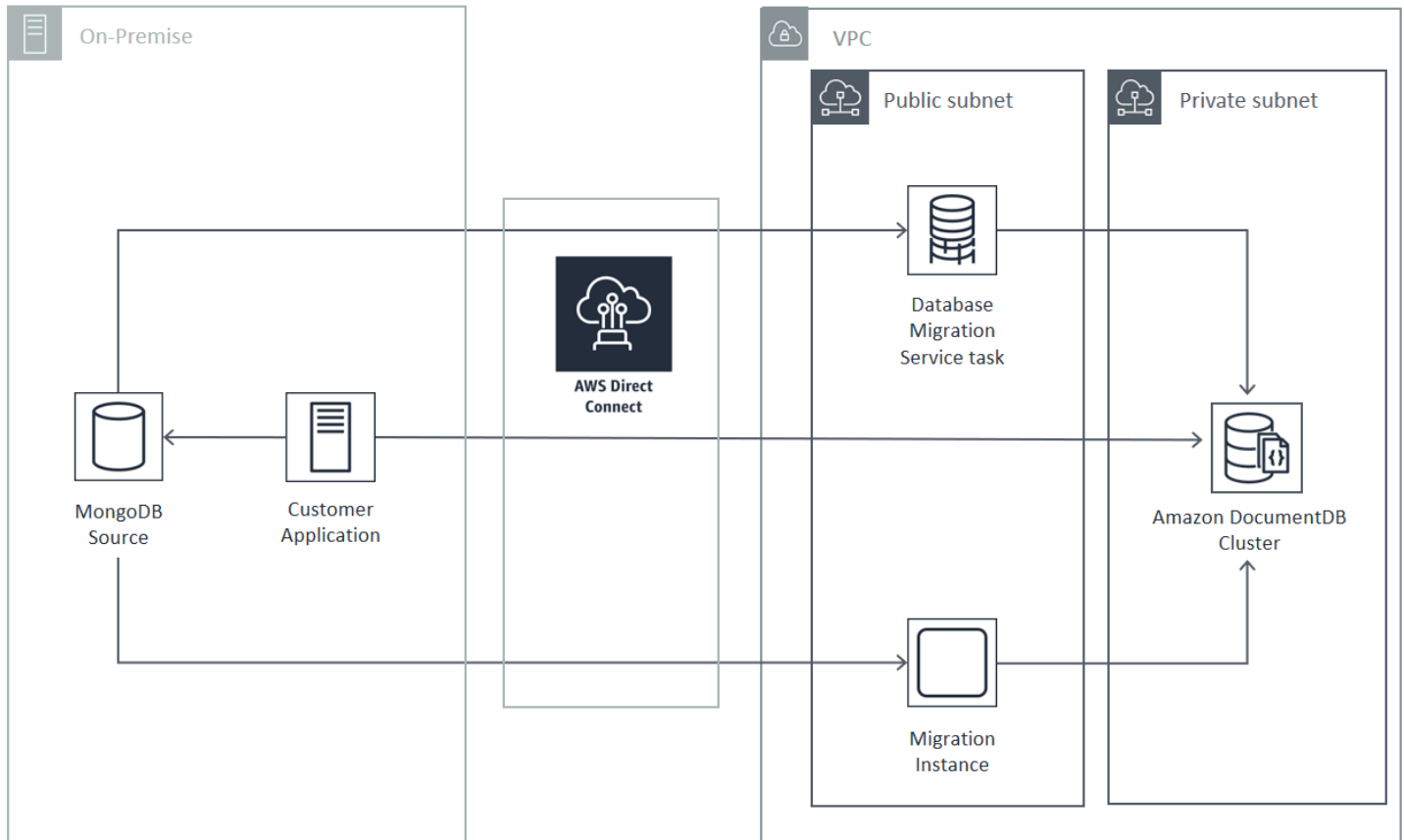
Il diagramma seguente illustra una migrazione ad Amazon DocumentDB da una fonte locale tramite una connessione VPN.

Migrating from On-Premise Source (VPN)



Quanto segue rappresenta una migrazione ad Amazon DocumentDB da una fonte locale utilizzando AWS Direct Connect

Migrating from On-Premise Source (Direct Connect)



Gli approcci di migrazione online e ibridi richiedono l'uso di un' AWS DMS istanza, che deve essere eseguita su Amazon EC2 in un Amazon VPC. Tutti gli approcci richiedono un server di migrazione per l'esecuzione di mongodump e mongorestore. In genere è più semplice eseguire il server di migrazione su un'istanza Amazon EC2 nel VPC in cui viene avviato il cluster Amazon DocumentDB perché semplifica notevolmente la connettività al cluster Amazon DocumentDB.

Test in corso

Di seguito sono elencati gli obiettivi dei test pre-migrazione:

- Verificare che l'approccio scelto raggiunga il risultato di migrazione desiderato.
- Verificare che il tipo di istanza e le preferenze di lettura scelte soddisfino i requisiti prestazionali dell'applicazione.
- Verificare il comportamento dell'applicazione durante il failover.

Considerazioni sul test del piano di migrazione

Per testare il piano di migrazione di Amazon DocumentDB, considera quanto segue.

Argomenti

- [Ripristino degli indici](#)
- [Dump dei dati](#)
- [Ripristino dei dati](#)
- [Dimensionamento oplog](#)
- [AWS Database Migration Service Configurazione](#)
- [Migrazione da un cluster con shard](#)

Ripristino degli indici

Per impostazione predefinita, `mongorestore` crea indici per raccolte del dump, ma solo dopo il ripristino dei dati. Nel complesso è più veloce creare indici in Amazon DocumentDB prima che i dati vengano ripristinati nel cluster. Questo perché le operazioni di indicizzazione sono parallelizzate durante il caricamento di dati.

Se scegli di creare preliminarmente gli indici, puoi saltare la fase di creazione degli indici nel ripristino dei dati con `mongorestore` fornendo l'opzione `--noIndexRestore`.

Dump dei dati

Lo strumento `mongodump` è il metodo preferito per eseguire il dump dei dati dalla distribuzione MongoDB di origine. A seconda delle risorse disponibili sulla tua istanza di migrazione, potresti velocizzare l'operazione `mongodump` utilizzando l'opzione `--numParallelCollections` per aumentare il numero di connessioni parallele del dump rispetto alle quattro predefinite.

Ripristino dei dati

Lo strumento `mongorestore` è il metodo preferito per ripristinare i dati scaricati nell'istanza di Amazon DocumentDB. Puoi utilizzare l'opzione `--numInsertionWorkersPerCollection` per migliorare le prestazioni di ripristino aumentando il numero di lavoratori per ogni raccolta durante il ripristino. Un worker per vCPU sull'istanza primaria del cluster Amazon DocumentDB è un buon punto di partenza.

Amazon DocumentDB attualmente non supporta l'opzione dello mongorestore `--oplogReplay` strumento.

Per impostazione predefinita, `mongorestore` salta gli errori di inserimento e continua il processo di ripristino. Ciò può verificarsi se stai ripristinando dati non supportati nella tua istanza Amazon DocumentDB. ad esempio in presenza di un documento che contiene chiavi o valori con stringhe nulle. Se preferisci che l'intera operazione `mongorestore` abbia esito negativo in caso di errori nel ripristino, utilizza l'opzione `--stopOnError`.

Dimensionamento oplog

Il log delle operazioni di MongoDB (`oplog`) è una raccolta limitata contenente tutte le modifiche ai dati per il database. Puoi visualizzare le dimensioni dell'`oplog` e l'intervallo di tempo che copre eseguendo l'operazione `db.printReplicationInfo()` su un set di repliche o su un membro della shard.

Se utilizzi un approccio online o ibrido, assicurati che l'`oplog` su ogni set o shard di repliche sia sufficientemente grande da contenere tutte le modifiche apportate durante l'intera durata del processo di migrazione dei dati (tramite `mongodump` o un' AWS DMS attività a pieno carico), oltre a un buffer ragionevole. Per ulteriori informazioni, consulta la sezione relativa al controllo della dimensione dell'`oplog` nella documentazione di MongoDB. Determina la dimensione minima necessaria dell'`oplog` registrando il tempo richiesto dalla prima esecuzione di test dei processi `mongodump` o `mongorestore` oppure dell'attività AWS DMS di caricamento completo.

AWS Database Migration Service Configurazione

La [Guida per AWS Database Migration Service l'utente](#) descrive i componenti e i passaggi necessari per migrare i dati di origine MongoDB al cluster Amazon DocumentDB. Di seguito è riportato il processo di base da utilizzare per AWS DMS eseguire una migrazione online o ibrida:

Per eseguire una migrazione utilizzando AWS DMS

1. Creare un endpoint di origine MongoDB. Per ulteriori informazioni, consulta [Utilizzo di MongoDB come origine per AWS DMS](#).
2. Crea un endpoint di destinazione Amazon DocumentDB. Per ulteriori informazioni, consulta [Utilizzo degli endpoint AWS DMS](#).

Se stai configurando l'endpoint di destinazione come cluster elastico, tieni presente che il certificato SSL Amazon DocumentDB esistente non funzionerà con i cluster elastici e dovrai allegare un nuovo certificato SSL all'endpoint utilizzando i seguenti passaggi:

- a. Visita <https://www.amazontrust.com/repository/SFSRootCAG2.pem> e salva il contenuto come file «SFSRootCag2.pem». Questo è il file di certificato che dovrai importare nei passaggi successivi.
- b. Quando crei l'endpoint del cluster elastico, in Configurazione dell'endpoint, scegli Aggiungi nuovo certificato CA.
 - Per Identificativo del certificato immetti SFSRootCAG2 . pem.
 - Per Import certificate file (Importa file certificato), scegliere Choose file (Seleziona file) e passare al file SFSRootCAG2 . pem scaricato in precedenza. Selezionare e aprire il file. Scegli Importa certificato, quindi scegli SFSRootCAG2 . pem dal menu a discesa Scegli un certificato.
3. Crea almeno un'istanza di AWS DMS replica. Per ulteriori informazioni, consulta [Lavorare con un'istanza di AWS DMS replica](#).
4. Crea almeno un'attività di AWS DMS replica. Per ulteriori informazioni, consulta [Utilizzo delle attività di AWS DMS](#).

Per una migrazione online, l'attività usa il tipo di migrazione Migrate existing data and replicate ongoing changes (Esegui la migrazione dei dati esistenti e replica le modifiche in corso).

Per una migrazione ibrida, l'attività usa il tipo di migrazione Replicate data changes only (Replica solo le modifiche ai dati). È possibile scegliere l'ora di inizio della funzionalità CDC per allinearla all'ora di dump dell'operazione mongodump. L'oplog MongoDB è idempotente. Per evitare di perdere modifiche, è consigliabile lasciare un valore di sovrapposizione di alcuni minuti per tra l'ora di fine di mongodump e l'ora di inizio della funzionalità CDC.

Migrazione da un cluster con shard

Il processo di migrazione dei dati da un cluster condiviso MongoDB alla tua istanza Amazon DocumentDB è essenzialmente quello di diverse migrazioni di set di repliche in parallelo. Nel testare la migrazione di un cluster con shard, è importante considerare che alcuni shard potrebbero essere molto più usati di altre. Questa situazione comporta tempi di migrazione differenti. Assicurati di valutare i requisiti di ogni shard durante la pianificazione e il test. `oplog`

Di seguito sono elencati alcuni fattori da tenere presenti in fase di migrazione di un cluster con shard:

- Prima di eseguire mongodump o di avviare un'operazione di migrazione AWS DMS , è necessario disabilitare il sistema di bilanciamento del cluster con shard e attendere il completamento di

eventuali migrazioni in elaborazione. Per ulteriori informazioni, consulta la pagina relativa alla disabilitazione del sistema di bilanciamento nella documentazione di MongoDB.

- Se utilizzi AWS DMS per replicare i dati, esegui il `cleanupOrphaned` comando su ogni shard prima di eseguire le attività di migrazione. In caso contrario, l'attività potrebbe non riuscire a causa di ID documento duplicati. Questo comando potrebbe influire sulle prestazioni. Per ulteriori informazioni, consulta la sezione `cleanupOrphaned` nella documentazione di MongoDB.
- Se utilizzi lo strumento `mongodump` per il dump dei dati, devi eseguire un processo `mongodump` per ogni shard. L'approccio più rapido potrebbe richiedere più server di migrazione per ottimizzare le prestazioni di dump.
- Se si utilizza AWS Database Migration Service per replicare i dati, è necessario creare un endpoint di origine per ogni shard. Inoltre devi eseguire almeno un'attività di migrazione per ogni shard da migrare. L'approccio più rapido potrebbe richiedere più istanze di replica per ottimizzare le prestazioni di migrazione.

Test delle performance

Dopo aver eseguito correttamente la migrazione dei dati nel cluster Amazon DocumentDB di prova, esegui il carico di lavoro di test sul cluster. Verifica tramite i CloudWatch parametri di Amazon che le tue prestazioni soddisfino o superino il throughput attuale della distribuzione sorgente MongoDB.

Verifica i seguenti parametri chiave di Amazon DocumentDB:

- Throughput di rete
- Throughput di scrittura
- Throughput di lettura
- Ritardo di replica

Per ulteriori informazioni, consulta [Monitoraggio Amazon DocumentDB](#).

Verifica del failover

Verifica che il comportamento dell'applicazione durante un evento di failover di Amazon DocumentDB soddisfi i requisiti di disponibilità. Per avviare un failover manuale di un cluster Amazon DocumentDB sulla console, nella pagina Cluster, scegli l'azione Failover nel menu Azioni.

Puoi avviare un failover anche eseguendo l'operazione `failover-db-cluster` dall' AWS CLI. Per ulteriori informazioni, [failover-db-cluster](#) consulta la sezione Amazon DocumentDB del AWS CLI riferimento.

Risorse aggiuntive

Consulta i seguenti argomenti nella Guida per l'utente di AWS Database Migration Service :

- [Utilizzo di Amazon DocumentDB come destinazione per AWS Database Migration Service](#)
- [Procedura dettagliata: Migrazione da MongoDB ad Amazon DocumentDB](#)

Guida alla migrazione: da MongoDB ad Amazon DocumentDB

Questo playbook sulla migrazione fornisce risorse e passaggi per aiutarti a migrare da un database MongoDB ad Amazon DocumentDB.

Processo di migrazione

Di seguito sono elencati i passaggi di alto livello generalmente necessari per la migrazione dei dati da un database MongoDB ad Amazon DocumentDB.

Argomenti

- [Fase 1: Compatibilità e differenze funzionali](#)
- [Fase 2: Prova del concetto](#)
- [Fase 3: Migrazione dei dati](#)
- [Fase 4: Convalida dei dati](#)
- [Fase 5: Cutover dell'applicazione](#)

Fase 1: Compatibilità e differenze funzionali

Amazon DocumentDB interagisce con le API open source Apache 2.0 MongoDB 3.6, 4.0 e 5.0. Di conseguenza, puoi utilizzare gli stessi driver, applicazioni e strumenti MongoDB con Amazon DocumentDB con modifiche minime o nulle.

Il primo passo consiste nel verificare la compatibilità tra gli operatori e gli indici utilizzati dall'applicazione nel database MongoDB e la loro disponibilità in Amazon DocumentDB, nonché comprendere le differenze funzionali tra di essi.

Compatibilità degli operatori

Utilizza lo [strumento di compatibilità Amazon DocumentDB*](#) per scoprire facilmente se la tua applicazione utilizza operatori non supportati nelle sue query. Questo strumento può scansionare i file di registro del server di database MongoDB o il codice sorgente dell'applicazione per fornire un rapporto sugli operatori non supportati. Se riscontri l'utilizzo di operatori non supportati, devi modificare l'applicazione per aggirare gli operatori non supportati.

Per verificare la compatibilità tra gli operatori MongoDB utilizzati nella configurazione e gli operatori Amazon DocumentDB supportati, esegui quanto segue:

```
git clone https://github.com/awslabs/amazon-documentdb-tools.git
cd amazon-documentdb-tools/compat-tool/
python3 compat.py --version <Amazon DocumentDB version> --directory <mongodb logfile/
source code>
```

Per ulteriori informazioni, consulta [API, operazioni e tipi di dati di MongoDB supportati](#).

* Non supportato ufficialmente da AWS

Compatibilità degli indici

Puoi utilizzare lo [strumento di indicizzazione Amazon DocumentDB*](#) per scoprire se stai utilizzando tipi di indice non supportati in Amazon DocumentDB. Questo strumento richiede una connessione al database di origine per leggere le definizioni degli indici.

Per questo, è necessario prima scaricare le definizioni degli indici in una directory utilizzando l'`--dump-indexes` opzione. Quindi esegui lo strumento con l'`--show-issues` opzione, fornendo la directory per individuare gli indici incompatibili.

Indici di esportazione:

```
git clone https://github.com/awslabs/amazon-documentdb-tools.git
sudo pip install -r amazon-documentdb-tools/index-tool/requirements.txt
mkdir <directory to dump index definitions>
python3 migrationtools/documentdb_index_tool.py --dump-indexes --dir <directory> --uri
<source-mongodb-uri>
```

Verifica la presenza di indici incompatibili:

```
python3 migrationtools/documentdb_index_tool.py --show-issues --dir <dumped-index-definitions-directory>
```

Se riscontri l'utilizzo di tipi di indice non supportati, devi modificare l'applicazione o il modello di dati per risolvere il problema o continuare senza gli indici incompatibili.

Per ulteriori informazioni sui tipi e sulle proprietà di indice supportati in Amazon DocumentDB, consulta [Indici e proprietà indice](#) e [Come indicizzare su Amazon DocumentDB](#).

* Non supportato ufficialmente da AWS

Differenze funzionali

Rivedi [Differenze funzionali con MongoDB](#) per familiarizzare con le differenze.

Fase 2: Prova del concetto

Esegui un proof of concept eseguendo la tua applicazione o la tua normale suite di test su Amazon DocumentDB per testare funzionalità e prestazioni. Potrebbe essere necessario popolare il cluster Amazon DocumentDB con dati per eseguire i test. Ad esempio, puoi utilizzare gli mongorestore strumenti mongodump e per copiare i dati dal tuo MongoDB di origine.

Test funzionali

Crea un cluster Amazon DocumentDB (vedi [Creazione di un cluster Amazon DocumentDB](#)) ed esegui la tua applicazione o la tua suite di test funzionali per verificare se tutti i flussi di lavoro dell'applicazione continuano a funzionare senza problemi su Amazon DocumentDB.

Test delle prestazioni

Esegui test delle prestazioni sulla tua applicazione o suite di test delle prestazioni in esecuzione su Amazon DocumentDB con un carico di lavoro simile a quello di produzione per verificare se la configurazione soddisfa i requisiti di latenza. Ottimizza il carico di lavoro in base alle prestazioni o ridimensiona il cluster Amazon DocumentDB a seconda dei casi. Per ulteriori informazioni, consultare [Prestazioni e utilizzo delle risorse](#) e [Scalabilità dei cluster Amazon DocumentDB](#).

È importante dimensionare il cluster Amazon DocumentDB con i tipi di istanza giusti per prestazioni ottimali. Per ulteriori informazioni, consulta le best practice per [Dimensione delle istanze](#).

Puoi utilizzare il [calcolatore di dimensionamento di Amazon DocumentDB*](#) per aiutarti a stimare le dimensioni del tuo cluster Amazon DocumentDB.

* Non supportato ufficialmente da AWS

Test di failover

Potresti voler osservare come la tua applicazione risponde al riavvio del nodo primario di Amazon DocumentDB, al failover del nodo primario o all'eliminazione di un nodo primario in un cluster a più nodi, nonché quando i nodi di replica vengono riavviati o rimossi. Questo ti aiuterà a confermare che l'applicazione è resiliente a questi eventi. Per ulteriori informazioni, consulta [Verifica del Failover](#).

Per comprendere le eccezioni che un'applicazione dovrebbe tollerare e come gestirle in modo efficiente, consulta [Creazione di applicazioni resilienti con Amazon DocumentDB](#).

Note

Non c'è nulla che possa sostituire il test del carico di lavoro su Amazon DocumentDB

Fase 3: Migrazione dei dati

Dopo una dimostrazione di fattibilità riuscita, esegui la migrazione dei dati su Amazon DocumentDB. La maggior parte dei nostri clienti utilizza approcci di migrazione online o offline per migrare i propri dati.

Migrazione online

Utilizzando il metodo di migrazione online, puoi migrare i dati dal tuo database di origine, da pochi gigabyte a più terabyte, verso Amazon DocumentDB con tempi di inattività quasi nulli. Per ulteriori informazioni, consulta [AWS Database Migration Service \(AWS DMS\)](#).

Se stai migrando da un database MongoDB, puoi AWS DMS utilizzarlo per eseguire un caricamento completo e replicare le modifiche in corso.

Per un step-by-step processo, consulta [Migrazione ad Amazon DocumentDB con il metodo online](#).

Ulteriori informazioni sono disponibili nella AWS Database Migration Service sezione [Using Amazon DocumentDB as a target for](#) della Guida per l'AWS Database Migration Service.

Punti da tenere in considerazione con AWS DMS:

- Segmentazione: la migrazione di database con più terabyte utilizzando le impostazioni predefinite può risultare lenta AWS DMS, poiché per impostazione predefinita il caricamento completo di DMS

è a thread singolo per raccolta, con conseguenti tempi di migrazione più lunghi. Per velocizzare il caricamento completo delle migrazioni di database di grandi dimensioni, puoi utilizzare la funzionalità di segmentazione in. AWS DMS

Per maggiori dettagli su come utilizzare la segmentazione con AWS DMS, consulta [Uso della segmentazione automatica](#) con. AWS DMS

- Tipo di istanza DMS: per accelerare la migrazione dei dati, devi [scegliere l'istanza DMS giusta](#).

Migrazione offline

La migrazione offline è l'approccio più semplice per spostare i database in Amazon DocumentDB. Questo approccio viene utilizzato principalmente per i POC e per i carichi di lavoro che possono richiedere tempi di inattività di scrittura durante la migrazione.

Per un step-by-step processo, consulta [Migrare da MongoDB ad Amazon DocumentDB](#) utilizzando il metodo offline.

Fase 4: Convalida dei dati

Una volta completata la migrazione dei dati, convalida la correttezza dei dati per acquisire sicurezza. Nella console delle attività di AWS DMS migrazione, puoi trovare le metriche dei dati migrati. Per ulteriori informazioni, consulta [Verificare i dati migrati](#).

Puoi anche utilizzare [Amazon DocumentDB DataDiffer Tool](#) * per convalidare la coerenza dei dati tra le raccolte di origine e di destinazione.

* Non supportato ufficialmente da. AWS

Fase 5: Cutover dell'applicazione

Ciò comporta la modifica della stringa di connessione al database dell'applicazione per utilizzare il cluster Amazon DocumentDB.

Per ulteriori informazioni sulla connessione ad Amazon DocumentDB, consulta. [Connessione ad Amazon DocumentDB come set di repliche](#)

Migrazione online

Al termine del caricamento completo dei dati, AWS DMS continua a replicare le modifiche in corso dall'origine ad Amazon DocumentDB. Una volta ripristinate le modifiche e completati i controlli di convalida dei dati, puoi eseguire un cutover su Amazon DocumentDB.

Migrazione offline

Una volta completati i controlli completi di caricamento e convalida dei dati, puoi eseguire il cutover su Amazon DocumentDB.

Risorse aggiuntive

Ecco alcune risorse aggiuntive che potrebbero aiutarti nella migrazione:

- Video: [Le migliori pratiche per la migrazione ad Amazon DocumentDB](#)
- Video: [Guida introduttiva all'osservabilità e al monitoraggio di Amazon DocumentDB](#)
- Utilità aggiuntive: [Amazon DocumentDB Tool*](#)
- Guida per gli sviluppatori di migrazione: [Migrazione ad Amazon DocumentDB](#)

* Non supportato ufficialmente daAWS.

Aggiornamento immediato della versione principale di Amazon DocumentDB

Amazon DocumentDB rende generalmente disponibili nuove versioni dei motori di database solo dopo test approfonditi. Puoi scegliere come e quando aggiornare i tuoi cluster Amazon DocumentDB alla nuova versione.

Attualmente, Amazon DocumentDB supporta tre versioni principali: Amazon DocumentDB 3.6, 4.0 e 5.0. È possibile eseguire un aggiornamento della versione principale (MVU) sul posto del database mantenendo gli stessi endpoint, storage e tag dei cluster e continuare a utilizzare le applicazioni senza alcuna modifica. Questa funzionalità è disponibile gratuitamente in tutte le regioni in cui è disponibile Amazon DocumentDB 5.0.

Important

I cluster Amazon DocumentDB non saranno disponibili durante l'aggiornamento della versione principale in loco e i cluster subiranno più riavvii. I tempi di inattività degli upgrade possono variare da cluster a cluster a seconda del numero di raccolte, indici, database e istanze. Si consiglia di eseguire l'aggiornamento durante la finestra di manutenzione o durante le ore di utilizzo limitate. Una volta aggiornato il cluster, non è possibile effettuare il downgrade del cluster alla versione precedente, ma è possibile scegliere di ripristinare l'istantanea precedente all'aggiornamento su un nuovo cluster.

Argomenti

- [Prerequisiti e limitazioni](#)
- [Procedure consigliate per gli aggiornamenti immediati delle versioni principali](#)
- [Esecuzione di un aggiornamento immediato della versione principale](#)
- [Risoluzione dei problemi relativi all'aggiornamento di una versione principale in corso](#)
- [Differenze tra i cluster aggiornati da Amazon DocumentDB da 3.6/4.0 a 5.0 e i nuovi cluster Amazon DocumentDB 5.0](#)

Prerequisiti e limitazioni

Di seguito sono riportati i prerequisiti e le limitazioni per l'aggiornamento in loco della versione principale che potrebbe essere necessario comprendere e di conseguenza agire prima di eseguire l'aggiornamento:

- Tipo di istanza: Amazon DocumentDB 4.0/5.0 non supporta le istanze r4.*. Per procedere con un aggiornamento immediato della versione principale, modifica le istanze r4.* in istanze r5.*. Per ulteriori informazioni, consulta [Modifica di un'istanza Amazon DocumentDB](#). Fai riferimento a [Classi di istanze supportate per regione](#) per le istanze supportate basate sulla versione del motore Amazon DocumentDB.
- Patch del sistema operativo dell'istanza: un aggiornamento immediato della versione principale richiede l'ultima patch del sistema operativo (OS) per procedere. Si prega di applicare eventuali azioni di manutenzione del sistema operativo in sospeso sulle istanze prima di procedere con l'aggiornamento in loco. Per ulteriori informazioni, consulta [Utilizzo degli aggiornamenti del sistema operativo](#).

Note

In alcune situazioni, se sono in sospeso le patch del motore a livello di cluster, le patch del sistema operativo delle istanze non sono visibili. Potrebbe essere necessario applicare le patch del motore a livello di cluster prima di procedere con l'applicazione delle patch del sistema operativo dell'istanza e, successivamente, con l'aggiornamento immediato della versione principale. Per informazioni, consulta [Esecuzione di un aggiornamento della patch alla versione del motore di un cluster](#).

- L'aggiornamento immediato della versione principale è disponibile in tutte le regioni in cui è disponibile Amazon DocumentDB 5.0.
- L'aggiornamento diretto della versione principale non è supportato con Amazon DocumentDB 4.0 come versione di destinazione.
- L'aggiornamento diretto della versione principale non è attualmente supportato sui cluster globali e sui cluster elastici di Amazon DocumentDB.

Note

Per aggiornare i cluster globali, elimina i cluster secondari dal cluster globale, converti il cluster primario in un cluster regionale, esegui un aggiornamento della versione principale

sul cluster regionale (primario), quindi ricrea il cluster globale aggiungendo cluster secondari con lo stesso nome per mantenere gli stessi endpoint di prima. Tieni presente che verranno addebitati costi di I/O mentre il cluster primario aggiornato replica i dati nei cluster secondari appena aggiunti. Per i passaggi dettagliati su come rimuovere i cluster secondari dal cluster globale prima dell'eliminazione, consulta [Rimozione di un cluster da un cluster globale Amazon DocumentDB](#)

- Se disponi di una grande quantità di indici (>10.000) e utilizzi un'istanza più piccola (ad esempio, t3.medium), devi scalare l'istanza principale su un'istanza più grande (ad esempio, almeno r5.xlarge) per riservare memoria sufficiente nell'istanza per eseguire l'aggiornamento immediato della versione principale. Puoi scegliere di ridurre le dimensioni dell'istanza una volta completato l'aggiornamento della versione principale sul posto. Consulta le tabelle seguenti per il numero massimo di indici supportati su ogni tipo di istanza per un aggiornamento immediato della versione principale:

Per le istanze ottimizzate per la memoria (db.r5.*):


Istanza	Numero massimo di indici supportati per la MVU locale
db.r5.large	100K
db.r5.xlarge	200 K
db.r5.2xlarge	300 K
db.r5.4xlarge	400 K
db.r5.8xlarge	500 K
db.r5.12xlarge	700 K
db.r5.16xlarge	800 K
db.r5.24xlarge	1 M

Per istanze con prestazioni stabili (db.t3, db.t4g)

Istanza	Numero massimo di indici supportati per la MVU locale
db.t4g.medium	3K
db.t3.medium	10K

Per istanze gravitroniche ottimizzate per la memoria (db.r6g.*):

Istanza	Numero massimo di indici supportati per la MVU locale
db.r6g.large	100K
db.r6g.xlarge	200 K
db.r6g.2xlarge	300 K
db.r6g.4xlarge	400 K
db.r6g.8xlarge	500 K
db.r6g.12xlarge	700 K
db.r6g.16xlarge	800 K

 Note

Se disponi di più di 1 milione di indici, contatta l' AWS assistenza e non procedere con un aggiornamento immediato della versione principale.

Procedure consigliate per gli aggiornamenti immediati delle versioni principali

Testa sul posto gli aggiornamenti delle versioni principali utilizzando cluster clonati

1. Per testare sul posto gli aggiornamenti delle versioni principali, consigliamo di utilizzare la funzionalità di clonazione rapida per creare un clone del cluster di destinazione. Non dovrai sostenere alcun costo di archiviazione per testare l'aggiornamento in loco della versione principale su un volume clonato, a meno che non modifichi i dati sul cluster. Per ulteriori informazioni sulla clonazione del volume, vedere. [Clonazione di un volume per un cluster Amazon DocumentDB](#)
2. Per ottenere una stima più realistica del tempo impiegato per completare l'aggiornamento immediato della versione principale, abbinare il numero di istanze del cluster clonato a quello del cluster di destinazione.
3. Consigliamo di testare completamente il cluster Amazon DocumentDB 5.0 appena aggiornato per eventuali differenze funzionali per garantire che tutto funzioni come previsto.

Prima di un aggiornamento immediato della versione principale

1. Tieni pronto un gruppo di parametri del cluster compatibile con la versione.

Utilizza il gruppo di parametri del cluster predefinito di Amazon DocumentDB per la nuova versione del motore o crea il tuo gruppo di parametri cluster personalizzato per la nuova versione del motore.

Se associ un gruppo di parametri del cluster Amazon DocumentDB come parte della richiesta di aggiornamento, l'aggiornamento della versione principale sul posto riavvierà automaticamente il cluster per applicare il nuovo gruppo di parametri.

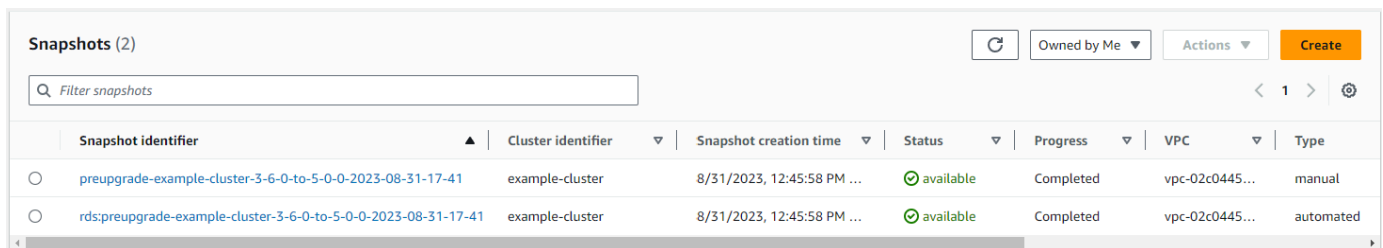
2. Assicurati di aver soddisfatto i prerequisiti per un aggiornamento immediato della versione principale, come indicato nella sezione Prerequisiti e limitazioni.
3. Crea un'istantanea manuale.

Il processo di aggiornamento crea un'istantanea del cluster di database durante l'aggiornamento. Si consiglia vivamente di creare un'istantanea manuale prima del processo di aggiornamento. Per informazioni, consulta [Creazione di una snapshot del cluster manuale](#).

Note

L'istantanea automatica creata dal processo di aggiornamento non verrà eliminata automaticamente dopo il completamento dell'aggiornamento della versione principale sul posto. Questa istantanea non comporterà alcun addebito purché rientri nel periodo di conservazione. È possibile scegliere di eliminare questa istantanea dopo aver verificato l'avvenuto aggiornamento del cluster.

L'istantanea è denominata come. `preupgrade-<name>-<version>-<timestamp>`



Snapshot identifier	Cluster identifier	Snapshot creation time	Status	Progress	VPC	Type
preupgrade-example-cluster-3-6-0-to-5-0-0-2023-08-31-17-41	example-cluster	8/31/2023, 12:45:58 PM ...	available	Completed	vpc-02c0445...	manual
rds:preupgrade-example-cluster-3-6-0-to-5-0-0-2023-08-31-17-41	example-cluster	8/31/2023, 12:45:58 PM ...	available	Completed	vpc-02c0445...	automated

4. Verifica se hai già pianificato un aggiornamento immediato della versione principale del cluster.

Se hai modificato il cluster e hai scelto di applicarlo nella finestra di manutenzione successiva, la pianificazione dell'aggiornamento della versione principale in atto non sarà visibile sulla console, ma puoi visualizzarla nella CLI. È possibile eseguire il comando seguente per verificare se un aggiornamento interno della versione principale è già pianificato:

```
aws docdb describe-db-cluster \
--region $REGION \
--db-cluster-identifier $CLUSTER_NAME

"PendingModifiedValues": {
  "EngineVersion": "5.0.0"
},
```

5. Esegui più dry-run utilizzando Volume Clone in ambienti inferiori per testare il cluster dopo l'aggiornamento della versione principale in base a qualsiasi piano di esecuzione e differenze funzionali. Consigliamo la clonazione con lo stesso numero e dimensione di istanze per ottenere

una stima migliore del tempo di esecuzione dell'aggiornamento delle versioni principali sul posto. Per ulteriori informazioni, consulta [Clonazione di un volume per un cluster Amazon DocumentDB](#).

6. Se il passaggio precedente ha esito positivo, procedi con l'aggiornamento immediato della versione principale nel cluster di produzione.

Durante un aggiornamento immediato della versione principale

È possibile monitorare lo stato di avanzamento dell'aggiornamento della versione principale in loco sottoscrivendo gli eventi di manutenzione del cluster. Al termine dell'aggiornamento, riceverai l'evento «La versione principale del cluster di database è stata aggiornata». Questo e altri eventi che si verificano durante l'aggiornamento vengono visualizzati nella sezione «Eventi e tag» della pagina dei dettagli del cluster nella console Amazon DocumentDB. Lo stato del cluster passa quindi da «in aggiornamento» a «disponibile».

Dalla CLI, puoi eseguire la creazione `aws docdb create-event-subscription` di eventi e il monitoraggio dei `aws docdb describe-events` progressi. Puoi anche impostare notifiche di eventi per gli eventi di cui sopra su Amazon SNS come destinazione da notificare tramite e-mail, messaggi push e altri metodi. Per ulteriori informazioni, consulta [Sottoscrizione alle sottoscrizioni agli eventi Amazon DocumentDB](#).

L'aggiornamento immediato della versione principale genera i seguenti eventi durante l'aggiornamento:

- `<cluster-name><timestamp>` Aggiornamento in corso: creazione di un'istantanea di pre-aggiornamento [`preupgrade-` -]
- Aggiornamento in corso: clonazione del volume.
- Aggiornamento in corso: aggiornamento di writer.
- Aggiornamento in corso: aggiornamento dei lettori.
- La versione principale del cluster di database è stata aggiornata.

Gli eventi sono visibili anche sulla console nella pagina Eventi:

Source	Type	Time	Message
example-cluster	db-instance	8/31/2023, 9:10:31 AM UTC-5	DB instance created
example-cluster	db-cluster	8/31/2023, 12:41:37 PM UTC-5	Database cluster engine version upgrade started.
example-cluster	db-cluster	8/31/2023, 12:44:44 PM UTC-5	Upgrade in progress: Performing online pre-upgrade checks.
example-cluster	db-cluster	8/31/2023, 12:45:35 PM UTC-5	Upgrade in progress: Performing offline pre-upgrade checks.
example-cluster	db-cluster	8/31/2023, 12:45:58 PM UTC-5	Upgrade in progress: Creating pre-upgrade snapshot [preupgrade-example-cluster-3-6-0-to-5-0-0-2023-08-31...

In AWS CLI, puoi utilizzare i seguenti comandi per tenere traccia dei progressi:

```
aws docdb describe-events --source-identifier $CLUSTER_NAME --source-type db-cluster
{
  "Events": [
    {
      "SourceIdentifier": "mycluster",
      "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"
    }
  ]
}
```

Dopo un aggiornamento immediato della versione principale

Per Amazon DocumentDB 3.6, aggiungi un tag al cluster per distinguere che il cluster è stato aggiornato ad Amazon DocumentDB 5.0 da Amazon DocumentDB 3.6 rispetto a un cluster Amazon DocumentDB 5.0 appena creato. Consulta la sezione sulle differenze tra un cluster Amazon DocumentDB 5.0 aggiornato e un nuovo cluster Amazon DocumentDB 5.0.

Scatta uno snapshot manuale al termine dell'aggiornamento della versione principale in atto, nel caso in cui sia necessario ripristinare lo stato successivo all'aggiornamento. Il processo di creazione automatica delle istantanee riprenderà non appena sarà completato l'aggiornamento della versione principale in atto. L'istantanea manuale non comporterà alcun addebito purché rientri nel periodo di conservazione.

Per utilizzare le nuove funzionalità associate ad Amazon DocumentDB 5.0, ad esempio la crittografia a livello di campo lato client, consigliamo di aggiornare la versione del driver alla versione API MongoDB 5.0. Per ulteriori informazioni, consulta [Novità di Amazon DocumentDB 5.0](#) un elenco delle funzionalità di Amazon DocumentDB 5.0.

Important

Immediatamente dopo aver eseguito l'aggiornamento della versione principale (MVU) sul posto, il cluster Amazon DocumentDB 5.0 ripopolerà i metadati dell'indice, in base ai quali il motore di database ottimizza i piani di esecuzione delle query. Le prestazioni di query previste sul cluster Amazon DocumentDB riprenderanno dopo il completamento del processo di ricalcolo dei metadati dell'indice. In genere, questo processo viene completato in pochi minuti, ma può durare fino a due ore a seconda del numero di indici presenti nel cluster. Inoltre, un riavvio, un failover o una scalabilità verso l'alto o verso il basso immediati dell'istanza di Writer dopo l'installazione della MVU possono interrompere il processo di calcolo dei metadati dell'indice sul cluster. Una volta completata l'MVU locale, consigliamo di apportare tali modifiche dopo aver osservato le prestazioni di query previste sul cluster Amazon DocumentDB 5.0.

Contatta l' AWS assistenza se noti che questo calo temporaneo delle prestazioni persiste per più di due ore dopo la MVU installata.

Testa completamente il cluster Amazon DocumentDB 5.0 aggiornato per assicurarti che tutto funzioni come previsto.

Note

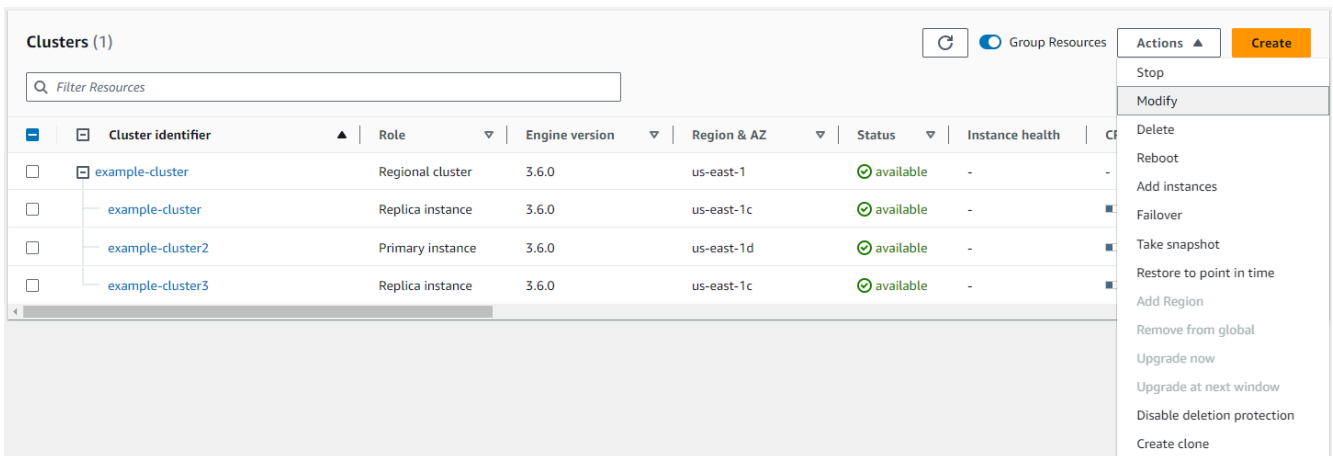
Dopo aver eseguito un MVU locale su un cluster Amazon DocumentDB con i flussi di modifica abilitati, gli eventi del flusso di modifiche precedenti vengono conservati e possono essere ripresi utilizzando `o.resumeToken.startAtOperationTime`. Come in ogni cluster Amazon DocumentDB appena creato, i log degli eventi di flusso di modifica più vecchi di `change_stream_log_retention_duration` vengono eliminati se la dimensione del registro è superiore a 51.200 MB.

Esecuzione di un aggiornamento immediato della versione principale

Using the AWS Management Console

Per eseguire un aggiornamento immediato della versione principale utilizzando: AWS Management Console

1. Accedi [AWS Management Console](#) e apri la console Amazon DocumentDB.
2. Nella tabella Cluster, seleziona il cluster di origine, fai clic su Azioni, quindi su Modifica.



3. Nella finestra di dialogo Modifica cluster nella sezione Specifiche del cluster, scegli la versione del database di destinazione (5.0) dal menu a discesa Versione del motore.

Cluster specifications

Cluster identifier [Info](#)
Specify a unique cluster identifier.

Engine version

VPC security groups
A security group acts as a virtual firewall for your instance to control inbound and outbound traffic.

New master password [Info](#)

Confirm password [Info](#)

Password must be at least eight characters long and cannot contain a / (slash), " (double quote) or @ (at symbol).

4. Nella sezione Opzioni del cluster, scegli il gruppo di parametri del cluster appropriato (default.docdb5.0) o un gruppo di parametri creato su misura.

Cluster options

Port
TCP/IP port that is used to connect to the cluster.

Cluster parameter group

[?](#) To create a new custom parameter group, please go to the Parameter group page, create your new custom parameter group and re-initiate the in-place Major Version Upgrade process.

5. Una volta completato, scorri verso il basso e scegli Continua.
6. Nella sezione Pianificazione delle modifiche, scegli il tuo piano di pianificazione preferito: applicalo immediatamente o applicalo nella finestra di manutenzione successiva.

Scegli **Modify cluster** (Modifica cluster).

Modify cluster: example-cluster

Summary of modifications
You are about to submit the following modifications. Only values that will change are displayed. Carefully verify your changes and click Modify cluster.

Attribute	Current value	New value
Cluster parameter group	default.docdb3.6	default.docdb5.0
Engine version	3.6.0	5.0.0

Scheduling of modifications

When to apply modifications

Apply during the next scheduled maintenance window
Current maintenance window: fri:09:03-fri:09:33

Apply immediately
The modifications in this request and any pending modifications will be asynchronously applied as soon as possible, regardless of the maintenance window setting for this database instance.

Modifications will not be applied immediately
Modifications will be applied during the next scheduled maintenance window (fri:09:03-fri:09:33). To apply these modifications immediately, choose "Apply immediately" above.

Cancel Back **Modify cluster**

7. Nella tabella dei cluster, annota lo stato del cluster durante l'aggiornamento:

Clusters (1) Group Resources Actions Create

Filter Resources

Cluster identifier	Role	Engine version	Region & AZ	Status	Instance health	CPU	Current activity
example-cluster	Regional cluster	3.6.0	us-east-1	⌚ upgrading...	-	-	-
example-cluster	Replica instance	3.6.0	us-east-1c	⌚ upgrading...	-	14.96%	0 Connections
example-cluster2	Primary instance	3.6.0	us-east-1d	⌚ upgrading...	-	13.54%	0 Connections
example-cluster3	Replica instance	3.6.0	us-east-1c	⌚ upgrading...	-	14.45%	0 Connections

Using the AWS CLI

Utilizza l'`modify-db-cluster` API con la versione del motore e il set di `allow-major-version-upgrade` flag desiderati:


```
aws docdb modify-db-cluster \
  --db-cluster-identifier $CLUSTER_NAME \
  --allow-major-version-upgrade \
  --engine-version 5.0 \
  --apply-immediately \
  --cluster-parameter-group $PARAMETER_GROUP \
  --region $REGION
```

Risoluzione dei problemi relativi all'aggiornamento di una versione principale in corso

In caso di errore, l'aggiornamento in loco della versione principale tenterà di ripristinare l'aggiornamento per presupporre l'ultimo stato operativo del cluster prima dell'inizio dell'aggiornamento. Un rollback riuscito genererà un evento: «Il cluster di database si trova in uno stato che non può essere aggiornato: il cluster DocumentDB si trova in uno stato in cui l'aggiornamento della versione principale non può essere completato con successo». A questo punto, è necessario contattare il team di AWS supporto per risolvere i problemi e tentare nuovamente l'aggiornamento della versione. Puoi continuare a utilizzare il tuo carico di lavoro come prima. In qualsiasi altro raro scenario in cui l'aggiornamento richieda più tempo del previsto, contatta il team di AWS supporto per ricevere assistenza.

Differenze tra i cluster aggiornati da Amazon DocumentDB da 3.6/4.0 a 5.0 e i nuovi cluster Amazon DocumentDB 5.0

- Confronti di documenti secondari per più tipi di dati numerici:
 - Se il cluster viene migrato da Amazon DocumentDB 3.6, erediterà il comportamento di confronto dei sottodocumenti di Amazon DocumentDB 3.6. La differenza funzionale è limitata ai tipi numerici (come Long, Double, Decimal128) in un documento secondario. Ad esempio, `{a: {b: {NumberLong(1)}}` non è uguale `{a: {b: 1}}` in Amazon DocumentDB 3.6, mentre vengono confrontati come uguali in Amazon DocumentDB 4.0 e versioni successive.
 - Questo comportamento di confronto dei documenti secondari esiste solo nei cluster Amazon DocumentDB 3.6 e Amazon DocumentDB 5.0 che sono stati aggiornati dalla versione 3.6 utilizzando un aggiornamento della versione principale in loco. Questo non si applica ai cluster Amazon DocumentDB 5.0 appena creati.
- Un aggiornamento immediato della versione principale mantiene gli indici originali sul cluster aggiornato. Ti consigliamo di ricreare gli indici per sfruttare appieno i miglioramenti delle prestazioni specifici di Amazon DocumentDB 5.0 (ad esempio la raccolta dei rifiuti). Tuttavia, la ricreazione di un indice può richiedere I/O e tempo aggiuntivi. Per ulteriori informazioni, consulta [Gestione degli indici Amazon DocumentDB](#).

 Note

Per un elenco delle differenze funzionali tra Amazon DocumentDB 3.6/4.0 e Amazon DocumentDB 5.0, consulta. [Compatibilità con MongoDB](#)

Sicurezza in Amazon DocumentDB

Per AWS, la sicurezza del cloud è la massima priorità. In quanto cliente AWS, puoi trarre vantaggio da un'architettura di data center e di rete progettata per soddisfare i requisiti delle aziende più esigenti a livello di sicurezza.

La sicurezza è una responsabilità condivisa tra AWS e l'utente. Questa documentazione aiuta a comprendere come applicare il modello di responsabilità condivisa quando si utilizza Amazon DocumentDB. Il [modello di responsabilità condivisa](#) descrive questo come sicurezza del cloud e sicurezza nel cloud:

- La sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che esegue servizi AWS nel cloud AWS. AWS fornisce anche servizi utilizzabili in maniera sicura. I revisori di terze parti testano e verificano regolarmente l'efficacia della sicurezza come parte dei [programmi di conformità AWS](#). Per ulteriori informazioni sui programmi di conformità che si applicano ad Amazon DocumentDB (compatibile con MongoDB), consultare [AWS Servizi coperti dal programma di conformità](#).
- Sicurezza nel cloud: la tua responsabilità è determinata dal servizio AWS che utilizzi. L'utente è anche responsabile per altri fattori, tra cui la riservatezza dei dati, i requisiti dell'azienda e leggi e normative applicabili.

Note

Questo capitolo si applica sia ai cluster basati su istanze che ai cluster elastici. Per ulteriori informazioni, consulta gli argomenti riportati di seguito.

È inoltre illustrato come utilizzare altri AWS servizi di per monitorare e proteggere le risorse Amazon DocumentDB. Gli argomenti seguenti descrivono come configurare Amazon DocumentDB per soddisfare gli obiettivi di sicurezza e conformità.

Argomenti

- [Protezione dei dati in Amazon DocumentDB](#)
- [Identity and Access Management per Amazon DocumentDB](#)
- [Gestione degli utenti Amazon DocumentDB](#)
- [Accesso al database tramite il controllo degli accessi basato sui ruoli](#)

- [Registrazione e monitoraggio in Amazon DocumentDB](#)
- [Aggiornamento dei certificati TLS di Amazon DocumentDB](#)
- [Aggiornamento dei certificati TLS Amazon DocumentDB — GovCloud \(Stati Uniti occidentali\)](#)
- [Convalida della conformità in Amazon DocumentDB](#)
- [Resilienza in Amazon DocumentDB](#)
- [Sicurezza dell'infrastruttura in Amazon DocumentDB](#)
- [Best practice di sicurezza per Amazon DocumentDB](#)
- [Controllo degli eventi di Amazon DocumentDB](#)

Protezione dei dati in Amazon DocumentDB

Il modello di [responsabilità AWS condivisa modello](#) si applica alla protezione dei dati in. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che esegue tutto l'Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. Inoltre, sei responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS che utilizzi. Per ulteriori informazioni sulla privacy dei dati, vedi le [Domande frequenti sulla privacy dei dati](#). Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al [Modello di responsabilità condivisa AWS e GDPR](#) nel Blog sulla sicurezza AWS.

Per garantire la protezione dei dati, ti suggeriamo di proteggere le credenziali Account AWS e di configurare singoli utenti con AWS IAM Identity Center o AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Utilizza SSL/TLS per comunicare con le risorse AWS. È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con AWS CloudTrail.
- Utilizza le soluzioni di crittografia AWS, insieme a tutti i controlli di sicurezza predefiniti in Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se necessiti di moduli crittografici convalidati FIPS 140-2 quando accedi ad AWS attraverso un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il [Federal Information Processing Standard \(FIPS\) 140-2](#).

Ti consigliamo vivamente di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori con Amazon DocumentDB o altro Servizi AWS utilizzando la console, l'API o AWS gli AWS CLI SDK. I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando fornisci un URL a un server esterno, ti suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

Argomenti

- [Crittografia lato client a livello di campo lato client a](#)
- [Crittografia dei dati Amazon DocumentDB inattiva](#)
- [Crittografia dei dati in transito](#)
- [Gestione delle chiavi](#)

Crittografia lato client a livello di campo lato client a

La crittografia a livello di campo (FLE) lato client di Amazon DocumentDB consente di crittografare i dati sensibili nelle applicazioni client prima che vengano trasferiti in un cluster Amazon DocumentDB. I dati sensibili rimangono crittografati quando vengono archiviati ed elaborati in un cluster e vengono decrittografati nell'applicazione client quando vengono recuperati.

Argomenti

- [Nozioni di base](#)
- [Esecuzione di tutte le in file lato client in file FLE lato client in](#)
- [Restrizioni](#)

Nozioni di base

La configurazione iniziale del FLE lato client in Amazon DocumentDB è un processo in quattro fasi che include la creazione di una chiave di crittografia, l'associazione di un ruolo all'applicazione, la configurazione dell'applicazione e la definizione del funzionamento CRUD con opzioni di crittografia.

Argomenti

- [Fase 1: Creazione delle chiavi di crittografia Creazione delle chiavi crittograf](#)
- [Fase 2: Associare un ruolo all'applicazione](#)

- [Fase 3: configurazione dell'applicazione](#)
- [Fase 4: Definire un'operazione CRUD](#)
- [Esempio: file di configurazione della crittografia a livello di campo lato client](#)

Fase 1: Creazione delle chiavi di crittografia

Utilizzando AWS Key Management Service, crea una chiave simmetrica che viene utilizzata per crittografare e decrittografare il campo di dati sensibili e fornirgli le autorizzazioni di utilizzo IAM necessarie. AWS KMS memorizza la chiave cliente (CK) utilizzata per crittografare le chiavi dati (DK). Ti consigliamo di archiviare la chiave cliente in KMS per rafforzare il tuo livello di sicurezza. La chiave dati è la chiave secondaria archiviata in una raccolta Amazon DocumentDB ed è necessaria per crittografare i campi sensibili prima di archiviare il documento in Amazon DocumentDB. La chiave cliente crittografa la chiave dati che a sua volta crittografa e decrittografa i dati. Se si utilizza un cluster globale, è possibile creare una chiave multiregionale che può essere utilizzata da diversi ruoli di servizio in diverse regioni.

Per ulteriori informazioni su AWS Key Management Service, incluso come creare una chiave, consulta la [AWS Key Management Service Developer Guide](#).

Fase 2: Associare un ruolo all'applicazione

Creare una policy IAM con autorizzazioni IAM con AWS KMS autorizzazioni IAM policy IAM con autorizz Questa policy consente alle identità IAM a cui è collegata di crittografare e decrittografare le identità IAM a cui è collegata di crittografare le identità IAM a cui è collegata di crittografare le chiavi KMS specificata nel campo delle risorse. L'applicazione assume questo ruolo IAM con cui autenticarsi AWS KMS.

La policy dovrebbe essere simile alla policy dovrebbe essere simile alla policy che segue:

```
{ "Effect": "Allow",
  "Action": ["kms:Decrypt", "kms:Encrypt"],
  "Resource": "Customer Key ARN"
}
```

Fase 3: configurazione dell'applicazione configurazione dell'applicazione: configurazione dell'applicazione

Ormai hai definito una chiave clienteAWS KMS e creato un ruolo IAM e gli hai fornito le autorizzazioni IAM giuste per accedere alla Customer Key. Importa i pacchetti richiesti.

```
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. Specifica 'aws' come tipo di provider KMS e inserisci le credenziali del tuo account che sono state recuperate nel passaggio precedente.

```
provider = "aws"
kms_providers = {
    provider: {
        "accessKeyId": current_credentials.access_key,
        "secretAccessKey": current_credentials.secret_key
    }
}
```

2. Specifica la chiave cliente utilizzato per crittografare la chiave cliente utilizzato per crittografare la chiave cliente utilizzato per crittografare la chiave

```
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. Configura l' MongoClient oggetto:

```
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. Genera la tua chiave dati:

```
data_key_id = client_encryption.create_data_key(provider,
    customer_key,
    key_alt_name = [key_alt_name])
```

5. Recupera la tua chiave dati esistente:

```
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})
```

Fase 4: Definire un'operazione CRUD

Definire l'operazione CRUD con opzioni di crittografia.

1. Definisci la raccolta per scrivere/leggere/eliminare un singolo documento:

```
coll = client.gameinfo.users
```

2. Crittografia esplicita: crittografa i campi e inserisci:

Note

Deve essere fornito esattamente uno tra «key_id» o «key_alt_name».

```
encrypted_first_name = client_encryption.encrypt(
    "Jane",
    Algorithm.AEAD_AES_256_CBC_HMAC_SHA_512_Deterministic,
    key_alt_name=data_key_id
)
encrypted_last_name = client_encryption.encrypt(
    "Doe",
    Algorithm.AEAD_AES_256_CBC_HMAC_SHA_512_Deterministic,
    key_alt_name=data_key_id
)
encrypted_dob = client_encryption.encrypt(
    "1990-01-01",
    Algorithm.AEAD_AES_256_CBC_HMAC_SHA_512_Random,
    key_alt_name=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"]}
    )
```

Esempio: file di configurazione della crittografia a livello di campo lato client

Nell'esempio seguente, sostituisci ogni *segnaposto dell'input utente* con le tue informazioni.

```
# 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["encryptedField"] = client_encryption.decrypt(doc["encryptedField"])
print('Decrypted document: %s' % (doc,))

# cleanup resources:
client_encryption.close()
client.close()

if __name__ == "__main__":
    main()
```


Esecuzione di tutte le in file lato client in file FLE lato client in

Amazon DocumentDB supporta le interrogazioni sull'uguaglianza dei punti con FLE lato client. Le interrogazioni sulla disuguaglianza e sul confronto possono restituire risultati imprecisi. Le operazioni di lettura e scrittura possono avere un comportamento imprevisto o errato rispetto all'esecuzione della stessa operazione sul valore decrittografato.

Ad esempio, per interrogare i filtri per i documenti in cui gamerscore è maggiore di 500:

```
db.users.find( {  
  "gamerscore" : { $gt : 500 }  
})
```

Il client utilizza un metodo di crittografia esplicito per crittografare il valore della query:

```
encrypted_gamerscore_filter = client_encryption.encrypt(  
  500,  
  Algorithm.AEAD_AES_256_CBC_HMAC_SHA_512_Deterministic,  
  key_alt_name=data_key_id  
)  
  
db.users.find( {  
  "gamerscore" : { $gt : encrypted_gamerscore_filter }  
} )
```

Nell'operazione di ricerca, Amazon DocumentDB confronta il valore crittografato di 500 con i valori dei campi crittografati archiviati in ciascun documento utilizzando il controllo superiore alla disuguaglianza. Il controllo della disuguaglianza nell'operazione di ricerca può restituire un risultato diverso se eseguito utilizzando dati e valori decrittografati, anche se l'operazione riesce a generare risultati.

Restrizioni

Le seguenti limitazioni si applicano alla crittografia a livello di campo lato client di Amazon DocumentDB:

- Amazon DocumentDB supporta solo interrogazioni con parità di punti. Le interrogazioni sulla disuguaglianza e sul confronto possono restituire risultati imprecisi. Le operazioni di lettura e scrittura possono avere un comportamento imprevisto o errato rispetto all'esecuzione della stessa

operazione sul valore decrittografato. Per interrogare i filtri per i documenti in cui gamerscore è maggiore di 500.

```
db.users.find( {  
  "gamerscore" : { $gt : 500 }  
})
```

Il client utilizza un metodo di crittografia esplicito per crittografare il valore della query.

```
encrypted_gamerscore_filter = client_encryption.encrypt(  
  500,  
  Algorithm.AEAD_AES_256_CBC_HMAC_SHA_512_Deterministic,  
  key_alt_name=data_key_id  
)  
  
db.users.find({  
  "gamerscore" : { $gt : encrypted_gamerscore_filter }  
})
```

Nell'operazione di ricerca, Amazon DocumentDB confronta il valore crittografato di 500 con i valori dei campi crittografati archiviati in ciascun documento utilizzando il controllo superiore alla disuguaglianza. Il controllo della disuguaglianza nell'operazione di ricerca può restituire un risultato diverso se eseguito utilizzando dati e valori decrittografati, anche se l'operazione riesce a generare risultati.

- Amazon DocumentDB non supporta FLE espliciti sul lato client provenienti da Mongo Shell. Tuttavia, la funzione funziona con tutti i driver supportati.

Crittografia dei dati Amazon DocumentDB inattiva

Note

AWS KMS sta sostituendo il termine chiave master del cliente (CMK) con AWS KMS key e chiave KMS. Il concetto non è cambiato. Per evitare cambiamenti sostanziali, AWS KMS sta mantenendo alcune varianti di questo termine.

Puoi crittografare i dati inattivi nel tuo cluster Amazon DocumentDB specificando l'opzione di crittografia dello storage al momento della creazione del cluster. La crittografia dello storage è

abilitata a livello del cluster e viene applicata a tutte le istanze, incluse l'istanza primaria e le repliche. Viene inoltre applicata al volume di archiviazione, ai dati, agli indici, ai registri, ai backup automatici e agli snapshot.

Amazon DocumentDB utilizza l'Advanced Encryption Standard a 256 bit (AES-256) per crittografare i dati utilizzando chiavi di crittografia archiviate in AWS Key Management Service (AWS KMS). Quando si utilizza un cluster Amazon DocumentDB con la crittografia a riposo abilitata, non è necessario modificare la logica dell'applicazione o la connessione client. Amazon DocumentDB gestisce la crittografia e la decrittografia dei dati in modo trasparente, con un impatto minimo sulle prestazioni.

Amazon DocumentDB si integra con AWS KMS e utilizza un metodo noto come crittografia delle buste per proteggere i tuoi dati. Quando un cluster Amazon DocumentDB è crittografato con un AWS KMS, Amazon DocumentDB chiede a AWS KMS di utilizzare la tua chiave KMS per [generare una chiave dati di testo cifrato](#) per crittografare il volume di archiviazione. La chiave dati cifrata viene crittografata utilizzando la chiave KMS definita e viene archiviata insieme ai dati crittografati e ai metadati di archiviazione. Quando Amazon DocumentDB deve accedere ai tuoi dati crittografati, richiede a AWS KMS di decrittografare la chiave di dati di testo cifrato utilizzando la tua chiave KMS e memorizza nella cache la chiave di dati in chiaro in memoria per crittografare e decrittografare in modo efficiente i dati nel volume di archiviazione.

La funzionalità di crittografia dello storage in Amazon DocumentDB è disponibile per tutte le dimensioni di istanze supportate e in tutti i Regioni AWS in cui è disponibile Amazon DocumentDB.


Abilitazione della crittografia inattiva per un cluster Amazon DocumentDB

È possibile abilitare o disabilitare la crittografia a riposo su un cluster Amazon DocumentDB quando il cluster viene fornito utilizzando AWS Management Console o l'AWS Command Line Interface (AWS CLI). I cluster creati utilizzando la console dispongono di crittografia inattiva per impostazione predefinita. I cluster creati utilizzando l'AWS CLI hanno la crittografia disattivata per impostazione predefinita. Pertanto, è necessario abilitare esplicitamente la crittografia inattiva utilizzando il parametro `--storage-encrypted`. In entrambi i casi, dopo la creazione del cluster, non è possibile modificare l'opzione di crittografia inattiva.

Amazon DocumentDB utilizza AWS KMS per recuperare e gestire le chiavi di crittografia e per definire le politiche che controllano il modo in cui queste chiavi possono essere utilizzate. Se non specifichi un identificatore AWS KMS chiave, Amazon DocumentDB utilizza la chiave KMS del servizio AWS gestito predefinito. Amazon DocumentDB crea una chiave KMS separata per ciascuna Regione AWS dei

tuo Account AWS. Per ulteriori informazioni, consulta l'[argomento relativo ai concetti di base di AWS Key Management Service](#).


Per iniziare a creare la tua chiave KMS, consulta Guida [introduttiva](#) nella Guida per gli AWS Key Management Service sviluppatori.

 Important

Per crittografare il cluster è necessario utilizzare una chiave KMS di crittografia simmetrica per crittografare il cluster, in quanto Amazon DocumentDB supporta solo chiavi KMS di crittografia simmetrica. Non utilizzare una chiave KMS asimmetrica per tentare di crittografare i dati nei cluster Amazon DocumentDB. Per ulteriori informazioni, consulta [Chiavi asimmetriche AWS KMS nella Guida per gli AWS Key Management Service sviluppatori](#).

Se Amazon DocumentDB non riesce più ad accedere alla chiave di crittografia per un cluster, ad esempio quando viene revocato l'accesso a una chiave, il cluster crittografato passa a uno stato terminale. In questo caso, puoi solo ripristinare il cluster da un backup. Per Amazon DocumentDB, i backup sono sempre abilitati per 1 giorno.

Inoltre, se disabiliti la chiave per un cluster Amazon DocumentDB crittografato, alla fine perderai l'accesso in lettura e scrittura a quel cluster. Quando Amazon DocumentDB trova un cluster crittografato da una chiave alla quale non ha accesso, passa a uno stato terminale. In questo stato, il cluster non è più disponibile e lo stato attuale del database non può essere ripristinato. Per ripristinare il cluster, devi riabilitare l'accesso alla chiave di crittografia per Amazon DocumentDB e ripristinare il cluster da un backup.

 Important


Non è possibile modificare la chiave KMS per un cluster crittografato dopo averlo già creato. Assicurati di determinare i requisiti della chiave crittografica prima di creare il tuo cluster crittografato.

Using the AWS Management Console

Puoi specificare l'opzione crittografia inattiva al momento della creazione di un cluster. La crittografia inattiva è abilitata per impostazione predefinita quando si crea un cluster utilizzando l'opzione AWS Management Console. Non può essere modificata dopo la creazione del cluster.

Per specificare l'opzione crittografia inattiva durante la creazione del cluster

1. Crea un cluster Amazon DocumentDB come descritto nella sezione [Guida introduttiva](#). Tuttavia, nel passaggio 6, non scegliere Create cluster (Crea cluster).
2. Nella sezione Authentication (Autenticazione), scegliere Show advanced settings (Mostra impostazioni avanzate).
3. Scorri verso il basso finonencryption-at-rest alla sezione E.
4. Scegliere l'opzione desiderata per la crittografia inattiva. Qualunque sia l'opzione scelta, non è possibile modificarla dopo la creazione del cluster.
 - Per crittografare i dati inattivi in questo cluster, scegliere Enable encryption (Abilita crittografia).
 - Se non si desidera crittografare i dati inattivi in questo cluster, scegliere Disable encryption (Disabilita crittografia).
5. Scegli la chiave master che desideri. Amazon DocumentDB utilizzaAWS Key Management Service (AWS KMS) per recuperare e gestire le chiavi di crittografia e per definire le politiche che controllano il modo in cui queste chiavi possono essere utilizzate. Se non specifichi un identificatoreAWS KMS chiave, Amazon DocumentDB utilizza la chiave KMS del servizioAWS gestito predefinito. Per ulteriori informazioni, consulta l'[argomento relativo ai concetti di base di AWS Key Management Service](#).

 Note

Dopo aver creato un cluster crittografato, non potrai utilizzare la chiave KMS per quel cluster. Assicurati di determinare i requisiti della chiave crittografica prima di creare il tuo cluster crittografato.

6. Completare le altre sezioni secondo necessità e creare il cluster.

Using the AWS CLI

Per crittografare un cluster Amazon DocumentDB utilizzando ilAWS CLI, è necessario specificare l'- -storage-encryptedopzione durante la creazione del cluster. I cluster Amazon DocumentDB creati utilizzandoAWS CLI non abilitano la crittografia dello storage per impostazione predefinita.

Nell'esempio seguente viene creato un cluster Amazon DocumentDB con la crittografia dello storage abilitata.

Example

Per Linux, macOS o Unix:

```
aws docdb create-db-cluster \  
  --db-cluster-identifier sample-cluster \  
  --port 27017 \  
  --engine docdb \  
  --master-username yourMasterUsername \  
  --master-user-password yourMasterPassword \  
  --storage-encrypted
```

Per Windows:

```
aws docdb create-db-cluster ^  
  --db-cluster-identifier sample-cluster ^  
  --port 27017 ^  
  --engine docdb ^  
  --master-username yourMasterUsername ^  
  --master-user-password yourMasterPassword ^  
  --storage-encrypted
```

Quando crei un cluster Amazon DocumentDB crittografato, puoi specificare un identificatore AWS KMS chiave, come nell'esempio seguente.

Example

Per Linux, macOS o Unix:

```
aws docdb create-db-cluster \  
  --db-cluster-identifier sample-cluster \  
  --port 27017 \  
  --engine docdb \  
  --master-username yourMasterUsername \  
  --master-user-password yourMasterPassword \  
  --storage-encrypted \  
  --kms-key-id key-arn-or-alias
```

Per Windows:

```
aws docdb create-db-cluster ^  
  --db-cluster-identifier sample-cluster ^
```

```
--port 27017 ^  
--engine docdb ^  
--master-username yourMasterUsername ^  
--master-user-password yourMasterPassword ^  
--storage-encrypted ^  
--kms-key-id key-arn-or-alias
```

Note

Dopo aver creato un cluster crittografato, non potrai utilizzare la chiave KMS per quel cluster. Assicurati di determinare i requisiti della chiave crittografica prima di creare il tuo cluster crittografato.

Limitazioni per i cluster crittografati di Amazon DocumentDB

Esistono le seguenti limitazioni per i cluster crittografati Amazon DocumentDB.

- È possibile abilitare o disabilitare la crittografia a riposo per un cluster Amazon DocumentDB solo al momento della creazione, non dopo la creazione del cluster. Tuttavia, è possibile creare una copia crittografata di un cluster non crittografato creando un'istantanea del cluster non crittografato e quindi ripristinando l'istantanea non crittografata come nuovo cluster specificando l'opzione di crittografia a riposo.

Per ulteriori informazioni, consulta i seguenti argomenti:

- [Creazione di una snapshot del cluster manuale](#)
- [Ripristino da una snapshot del cluster](#)
- [Copia degli snapshot del cluster Amazon DocumentDB](#)
- I cluster Amazon DocumentDB con crittografia dello storage abilitata non possono essere modificati per disabilitare la crittografia.
- Tutte le istanze, i backup automatici, le istantanee e gli indici in un cluster Amazon DocumentDB sono crittografati con la stessa chiave KMS.

Crittografia dei dati in transito

Puoi utilizzare Transport Layer Security (TLS) per crittografare la connessione tra l'applicazione e un cluster Amazon DocumentDB. Per impostazione predefinita, la crittografia in transito è abilitata per

i cluster Amazon DocumentDB appena creati. Può facoltativamente essere disabilitata al momento della creazione del cluster o in un secondo momento. Quando la crittografia in transito è abilitata, per connettersi al cluster sono necessarie connessioni protette tramite TLS. Per ulteriori informazioni sulla connessione ad Amazon DocumentDB utilizzando TLS, consulta [Connessione programmatica ad Amazon DocumentDB](#).

Gestione delle impostazioni TLS del cluster Amazon DocumentDB

La crittografia in transito per un cluster Amazon DocumentDB viene gestita tramite il parametro TLS in un [gruppo di parametri del cluster](#). Puoi gestire le impostazioni TLS del cluster Amazon DocumentDB utilizzando AWS Management Console o il AWS Command Line Interface (AWS CLI). Consulta le seguenti sezioni per ulteriori informazioni su come verificare e modificare le impostazioni TLS correnti.

Using the AWS Management Console

Segui questi passaggi per eseguire attività di gestione della crittografia TLS utilizzando la console, come identificare gruppi di parametri, verificare il valore TLS e apportare le modifiche necessarie.

Note

A meno che non si specifichi diversamente quando si crea un cluster, il cluster viene creato con il gruppo di parametri cluster predefinito. I parametri del gruppo di parametri del cluster default non possono essere modificati (ad esempio, `tls` abilitato/disabilitato). Pertanto, se il cluster utilizza un gruppo di parametri del cluster default, è necessario modificare il cluster per utilizzare un gruppo di parametri cluster non predefinito. Innanzitutto, potrebbe essere necessario creare un gruppo di parametri cluster personalizzato. Per ulteriori informazioni, consulta [Creazione di gruppi di parametri del cluster Amazon DocumentDB](#).

1. Determinare il gruppo di parametri cluster utilizzato dal cluster.
 - a. [Apri la console Amazon DocumentDB all'indirizzo https://console.aws.amazon.com/docdb](https://console.aws.amazon.com/docdb).
 - b. Nel pannello di navigazione scegliere Clusters (Cluster).

i Tip

Se il riquadro di navigazione non viene visualizzato sul lato sinistro della schermata, scegliere l'icona del menu (☰) nell'angolo in alto a sinistra della pagina.

- c. Tieni presente che nella casella di navigazione Cluster, la colonna Cluster Identifier mostra sia i cluster che le istanze. Le istanze sono elencate sotto i cluster. Guarda lo screenshot qui sotto come riferimento.

Cluster identifier	Role	Engine version	Region & AZ
docdb-cloud9-getstarted	Cluster	3.6.0	us-east-1
docdb-cloud9-getstarted	Primary	3.6.0	us-east-1f
robo3t	Cluster	3.6.0	us-east-1
robo3t	Primary	3.6.0	us-east-1d

- d. Scegli il cluster che ti interessa.
- e. Scegli la scheda Configurazione e scorri fino alla fine della pagina Dettagli del cluster e individua il gruppo di parametri del cluster. Annotare il nome del gruppo di parametri del cluster.

Se il nome del gruppo di parametri del cluster è default, ad esempio default.docdb3.6, è necessario disporre di un gruppo di parametri del cluster personalizzato e renderlo il gruppo di parametri del cluster prima di continuare. Per ulteriori informazioni, consulta gli argomenti seguenti:

1. [Creazione di gruppi di parametri del cluster Amazon DocumentDB](#)— Se non disponi di un gruppo di parametri del cluster personalizzato da utilizzare, creane uno.
2. [Modifica di un cluster Amazon DocumentDB](#)— Modifica il cluster per utilizzare il gruppo di parametri del cluster personalizzato.

2. Determinare l'attuale valore del parametro cluster **tls**.

- a. [Apri la console Amazon DocumentDB all'indirizzo `https://console.aws.amazon.com/docdb`.](https://console.aws.amazon.com/docdb)
 - b. Nel riquadro di navigazione scegliere Parameter groups (Gruppi di parametri).
 - c. Dall'elenco dei gruppi di parametri del cluster, scegliere il nome del gruppo che ti interessa.
 - d. Individuare la sezione Cluster parameters (Parametri cluster). Nell'elenco dei parametri del cluster individuare la riga dei parametri del cluster `tls`. A questo punto, sono importanti le seguenti quattro colonne:
 - Nome dei parametri del cluster: il nome dei parametri del cluster. Per gestire TLS, ti interessa il parametro `tls` del cluster.
 - Valori: il valore corrente di ogni parametro del cluster.
 - Valori consentiti: un elenco di valori che possono essere applicati a un parametro del cluster.
 - Tipo di applicazione: statico o dinamico. Le modifiche apportate ai parametri del cluster statico possono essere applicate solo quando le istanze vengono riavviate. Le modifiche apportate ai parametri del cluster dinamico possono essere applicate immediatamente oppure quando le istanze vengono riavviate.
3. Modificare il valore del parametro del cluster **tls**.

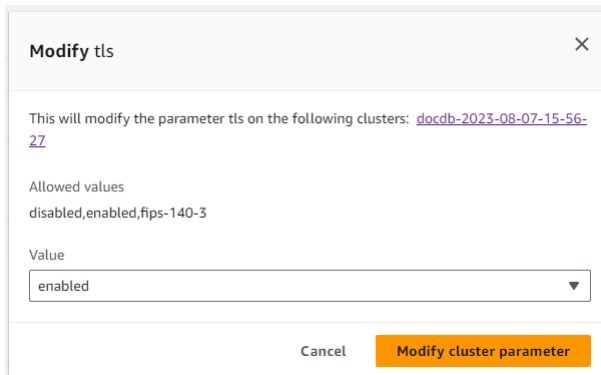
Se il valore di `tls` non corrisponde a quello richiesto, modificare il suo valore per questo gruppo di parametri del cluster. Per modificare il valore del parametro del cluster `tls`, continuare dalla sezione precedente seguendo questi passaggi.

- a. Scegliere il pulsante a sinistra del nome del parametro cluster (`tls`).
- b. Scegli Modifica.
- c. Per modificare il valore di `tls`, nella finestra di `tls` dialogo Modifica, scegliete il valore che desiderate per il parametro del cluster nell'elenco a discesa.

I valori validi sono:

- `disabilitato`: disabilita TLS
- `abilitato`: abilita TLS (versione 1.0, 1.1, 1.2 e 1.3)
- `fips-140-3` — Abilita TLS con FIPS. Il cluster accetta solo connessioni sicure in base ai requisiti della pubblicazione 140-3 degli standard federali di elaborazione delle

informazioni (FIPS). È supportato solo a partire dai cluster Amazon DocumentDB 5.0 (versione del motore 3.0.3727) in queste regioni: ca-central-1, us-west-2, us-east-1, us-east-2, -1. us-gov-east us-gov-west



The screenshot shows a dialog box titled "Modify tls" with a close button (X) in the top right corner. The main text reads: "This will modify the parameter tls on the following clusters: [docdb-2023-08-07-15-56-27](#)". Below this, it lists "Allowed values" as "disabled,enabled,fips-140-3". A "Value" dropdown menu is set to "enabled". At the bottom, there are two buttons: "Cancel" and "Modify cluster parameter".

- d. Scegliere Modify cluster parameter (Modifica parametro cluster). La modifica verrà applicata a ciascuna istanza di cluster quando viene riavviata.
4. Riavvia l'istanza Amazon DocumentDB.

Riavviare ogni istanza del cluster in modo che la modifica venga applicata a tutte le istanze nel cluster.

- a. [Apri la console Amazon DocumentDB all'indirizzo https://console.aws.amazon.com/docdb](https://console.aws.amazon.com/docdb).
- b. Nel riquadro di navigazione, seleziona Istanze.
- c. Per specificare un'istanza da riavviare, trova l'istanza nell'elenco e scegli il pulsante a sinistra del nome.
- d. Scegliere Actions (Azioni), quindi Reboot (Riavvia). Confermare che si desidera riavviare scegliendo Reboot (Riavvia).

Using the AWS CLI

Segui questi passaggi per eseguire attività di gestione della crittografia TLS utilizzando AWS CLI—come identificare gruppi di parametri, verificare il valore TLS e apportare le modifiche necessarie.

Note

A meno che non si specifichi diversamente quando si crea un cluster, il cluster viene creato con il gruppo di parametri cluster predefinito. I parametri del gruppo di parametri del cluster default non possono essere modificati (ad esempio, `tls` abilitato/disabilitato). Pertanto, se il cluster utilizza un gruppo di parametri del cluster default, è necessario modificare il cluster per utilizzare un gruppo di parametri cluster non predefinito. Potrebbe essere necessario creare prima un gruppo di parametri del cluster personalizzato. Per ulteriori informazioni, consulta [Creazione di gruppi di parametri del cluster Amazon DocumentDB](#).

1. Determinare il gruppo di parametri cluster utilizzato dal cluster.

Usa il comando `describe-db-clusters` con i parametri seguenti.

- **`--db-cluster-identifier`**: obbligatorio. Nome del cluster di interesse.
- **`--query`**— Facoltativo. Query che limita l'output ai soli campi di interesse, in questo caso il nome del cluster e del relativo gruppo di parametri.

```
aws docdb describe-db-clusters \
  --db-cluster-identifier docdb-2019-05-07-13-57-08 \
  --query 'DBClusters[*].[DBClusterIdentifier,DBClusterParameterGroup]'
```

L'aspetto dell'output di questa operazione è simile al seguente (formato JSON).

```
[
  [
    "docdb-2019-05-07-13-57-08",
    "custom3-6-param-grp"
  ]
]
```

Se il nome del gruppo di parametri del cluster è default, ad esempio `default.docdb3.6`, è necessario disporre di un gruppo di parametri del cluster personalizzato e renderlo il gruppo

di parametri del cluster prima di continuare. Per ulteriori informazioni, consulta i seguenti argomenti:

1. [Creazione di gruppi di parametri del cluster Amazon DocumentDB](#)— Se non disponi di un gruppo di parametri del cluster personalizzato da utilizzare, creane uno.
 2. [Modifica di un cluster Amazon DocumentDB](#)— Modifica il cluster per utilizzare il gruppo di parametri del cluster personalizzato.
2. Determinare l'attuale valore del parametro cluster **tls**.

Per ulteriori informazioni su questo gruppo di parametri del cluster, utilizzare l'operazione `describe-db-cluster-parameters` con i parametri elencati di seguito.

- **--db-cluster-parameter-group-name**: obbligatorio. Utilizzare il nome del gruppo di parametri del cluster dall'output del comando precedente.
- **--query**— Facoltativo. Una query che limita l'output solo ai campi di interesse, in questo caso, il `ParameterName`, `ParameterValue`, `AllowedValues` e `ApplyType`.

```
aws docdb describe-db-cluster-parameters \  
  --db-cluster-parameter-group-name custom3-6-param-grp \  
  --query 'Parameters[*].  
[ParameterName,ParameterValue,AllowedValues,ApplyType]'
```

L'aspetto dell'output di questa operazione è simile al seguente (formato JSON).

```
[  
  [  
    "audit_logs",  
    "disabled",  
    "enabled,disabled",  
    "dynamic"  
  ],  
  [  
    "tls",  
    "disabled",  
    "disabled,enabled,fips-140-3",  
    "static"  
  ],  
  [  
    "ttl_monitor",
```

```

        "enabled",
        "disabled,enabled",
        "dynamic"
    ]
]

```

3. Modificare il valore del parametro del cluster `tls`.

Se il valore di `tls` non corrisponde a quello richiesto, modificarlo per questo gruppo di parametri del cluster. Per modificare il valore del parametro del cluster `tls`, utilizza l'operazione `modify-db-cluster-parameter-group` con i parametri elencati di seguito.

- **--db-cluster-parameter-group-name**: obbligatorio. Il nome del gruppo di parametri del cluster da modificare. Questo non può essere un gruppo di parametri del default.*.
- **--parameters**: obbligatorio. Un elenco di parametri del gruppo di parametri del cluster.
 - **ParameterName**: obbligatorio. Il nome del parametro del cluster da modificare.
 - **ParameterValue**: obbligatorio. Il nuovo valore per questo parametro del cluster. Deve essere uno dei valori `AllowedValues` del parametro del cluster.
 - **enabled**— Il cluster accetta solo connessioni sicure utilizzando la versione TLS 1.0, 1.1, 1.2 o 1.3.
 - **disabled**— Il cluster non accetta connessioni sicure tramite TLS.
 - **fips-140-3**— Il cluster accetta solo connessioni sicure in base ai requisiti della pubblicazione 140-3 degli standard federali di elaborazione delle informazioni (FIPS). È supportato solo a partire dai cluster Amazon DocumentDB 5.0 (versione del motore 3.0.3727) in queste regioni: `ca-central-1`, `us-west-2`, `us-east-1`, `us-east-2`, `-1.us-gov-east` `us-gov-west`
 - **ApplyMethod**— Quando deve essere applicata questa modifica. Per i parametri del cluster statici, ad esempio `tle`, questo valore deve essere `pending-reboot`.
 - **pending-reboot**— La modifica viene applicata a un'istanza solo dopo il riavvio. È necessario riavviare ogni istanza del cluster individualmente per consentire l'applicazione di questo cambiamento tra tutte le istanze del cluster.

Il codice seguente disabilita `tls`, applicando la modifica a ogni istanza database al riavvio.

```

aws docdb modify-db-cluster-parameter-group \
  --db-cluster-parameter-group-name custom3-6-param-grp \

```

```
--parameters "ParameterName=tls,ParameterValue=disabled,ApplyMethod=pending-reboot"
```

Il codice seguente consente `tls` (versioni 1.0, 1.1, 1.2 e 1.3) di applicare la modifica a ciascuna istanza DB al riavvio.

```
aws docdb modify-db-cluster-parameter-group \
  --db-cluster-parameter-group-name custom3-6-param-grp \
  --parameters "ParameterName=tls,ParameterValue=enabled,ApplyMethod=pending-reboot"
```

Il codice seguente abilita TLS `confips-140-3`, applicando la modifica a ciascuna istanza DB al riavvio.

```
aws docdb modify-db-cluster-parameter-group \
  --db-cluster-parameter-group-name custom5-0-param-grp \
  --parameters
  "ParameterName=tls,ParameterValue=fips-140-3,ApplyMethod=pending-reboot"
```

L'aspetto dell'output di questa operazione è simile al seguente (formato JSON).

```
{
  "DBClusterParameterGroupName": "custom3-6-param-grp"
}
```

4. Riavvia l'istanza Amazon DocumentDB.

Riavviare ogni istanza del cluster in modo che la modifica venga applicata a tutte le istanze nel cluster. Per riavviare un'istanza Amazon DocumentDB, utilizza l'operazione con `reboot-db-instance` il seguente parametro:

- **--db-instance-identifier**: obbligatorio. L'identificatore dell'istanza da riavviare.

Il codice seguente riavvia l'istanza `sample-db-instance`.

Example

Per Linux, macOS o Unix:

```
aws docdb reboot-db-instance \
```

```
--db-instance-identifier sample-db-instance
```

Per Windows:

```
aws docdb reboot-db-instance ^  
  --db-instance-identifier sample-db-instance
```

L'aspetto dell'output di questa operazione è simile al seguente (formato JSON).

```
{  
  "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": "sample-cluster-instance-00",
"Engine": "docdb",
"AvailabilityZone": "us-east-1a",
"DBInstanceArn": "arn:aws:rds:us-east-1:012345678901:db:sample-cluster-
instance-00",

```

```
    "BackupRetentionPeriod": 1,
    "Endpoint": {
      "Address": "sample-cluster-instance-00.corcjozrlsfc.us-
east-1.docdb.amazonaws.com",
      "Port": 27017,
      "HostedZoneId": "Z2R2ITUGPM61AM"
    },
    "DBClusterIdentifier": "sample-cluster"
  }
}
```

Per il riavvio dell'istanza sono necessari alcuni minuti. Puoi utilizzare l'istanza solo quando ha lo stato disponibile. Puoi monitorare lo stato dell'istanza con la console o l' AWS CLI. Per ulteriori informazioni, consulta [Monitoraggio dello stato di un'istanza Amazon DocumentDB](#).

Gestione delle chiavi

Amazon DocumentDB utilizza AWS Key Management Service (AWS KMS) per recuperare e gestire le chiavi di crittografia. AWS KMS combina hardware e software sicuri e ad alta disponibilità per fornire un sistema di gestione delle chiavi scalabile per il cloud. AWS KMS consente di creare chiavi di crittografia e definire le policy che controllano il modo in cui queste chiavi possono essere utilizzate. AWS KMS supporta AWS CloudTrail, pertanto è possibile verificare che le chiavi vengano utilizzate in modo appropriato.

AWS KMS Le tue chiavi possono essere utilizzate in combinazione con Amazon DocumentDB e AWS servizi supportati come Amazon Simple Storage Service (Amazon S3), Amazon Relational Database Service (Amazon RDS), Amazon Elastic Block Store (Amazon EBS) Elastic Block Store (Amazon EBS) e Amazon Redshift. Per un elenco dei servizi che supportano AWS KMS, consulta [How AWS Services](#) use nella Developer Guide. AWS KMS AWS Key Management Service Per informazioni su AWS KMS, consultare [Che cos'è AWS Key Management Service?](#).

Identity and Access Management per Amazon DocumentDB

AWS Identity and Access Management (IAM) è uno strumento Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle risorse. AWS Gli amministratori IAM controllano chi può essere autenticato (effettuare l'accesso) e autorizzato (disporre delle

autorizzazioni) a utilizzare le risorse Amazon DocumentDB. IAM è uno strumento Servizio AWS che puoi utilizzare senza costi aggiuntivi.

Argomenti

- [Destinatari](#)
- [Autenticazione con identità](#)
- [Gestione dell'accesso con policy](#)
- [Come funziona Amazon DocumentDB con IAM](#)
- [Esempi di policy basate sull'identità per Amazon DocumentDB](#)
- [Risoluzione dei problemi relativi all'identità e all'accesso ad Amazon DocumentDB](#)
- [Gestione delle autorizzazioni di accesso alle risorse Amazon DocumentDB](#)
- [Utilizzo di politiche basate sull'identità \(politiche IAM\) per Amazon DocumentDB](#)
- [AWS politiche gestite per Amazon DocumentDB](#)
- [Autorizzazioni API Amazon DocumentDB: riferimento ad azioni, risorse e condizioni](#)

Destinatari

Il modo in cui usi AWS Identity and Access Management (IAM) varia a seconda del lavoro svolto in Amazon DocumentDB.

Utente del servizio: se utilizzi il servizio Amazon DocumentDB per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più funzionalità di Amazon DocumentDB per svolgere il tuo lavoro, potresti aver bisogno di autorizzazioni aggiuntive. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità in Amazon DocumentDB, consulta [Risoluzione dei problemi relativi all'identità e all'accesso ad Amazon DocumentDB](#)

Amministratore del servizio: se sei responsabile delle risorse di Amazon DocumentDB presso la tua azienda, probabilmente hai pieno accesso ad Amazon DocumentDB. È tuo compito determinare a quali funzionalità e risorse di Amazon DocumentDB devono accedere gli utenti del servizio. Devi inviare le richieste all'amministratore IAM per cambiare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa pagina per comprendere i concetti di base relativi a IAM. Per ulteriori informazioni su come la tua azienda può utilizzare IAM con Amazon DocumentDB, consulta [Come funziona Amazon DocumentDB con IAM](#)

Amministratore IAM: se sei un amministratore IAM, potresti voler saperne di più su come scrivere policy per gestire l'accesso ad Amazon DocumentDB. Per visualizzare esempi di policy basate sull'identità di Amazon DocumentDB che puoi utilizzare in IAM, consulta [Esempi di policy basate sull'identità per Amazon DocumentDB](#)

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi essere autenticato (aver effettuato l'accesso AWS) come utente IAM o assumendo un ruolo IAM.

Puoi accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center (precedentemente AWS Single Sign-On), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Quando accedi AWS utilizzando la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al AWS Management Console o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi [Come accedere al tuo Account AWS nella Guida per l'Accedi ad AWS utente](#).

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le tue richieste utilizzando le tue credenziali. Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sull'utilizzo del metodo consigliato per firmare autonomamente le richieste, consulta [Signing AWS API request](#) nella IAM User Guide.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo account. Per ulteriori informazioni, consulta [Autenticazione a più fattori](#) nella Guida per l'utente di AWS IAM Identity Center e [Utilizzo dell'autenticazione a più fattori \(MFA\) in AWS](#) nella Guida per l'utente di IAM.

Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane.

Conserva le credenziali dell'utente root e utilizzarle per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione [Attività che richiedono le credenziali dell'utente root](#) nella Guida per l'utente di IAM.

Identità federata

Come procedura consigliata, richiedi agli utenti umani, compresi gli utenti che richiedono l'accesso come amministratore, di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente dell'elenco utenti aziendale, di un provider di identità Web AWS Directory Service, della directory Identity Center o di qualsiasi utente che accede utilizzando le Servizi AWS credenziali fornite tramite un'origine di identità. Quando le identità federate accedono Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. Puoi creare utenti e gruppi in IAM Identity Center oppure puoi connetterti e sincronizzarti con un set di utenti e gruppi nella tua fonte di identità per utilizzarli su tutte le tue applicazioni. Account AWS Per ulteriori informazioni sul Centro identità IAM, consulta [Cos'è Centro identità IAM?](#) nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

Un [utente IAM](#) è un'identità interna Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Tuttavia, per casi d'uso specifici che richiedono credenziali a lungo termine con utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina [Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine](#) nella Guida per l'utente di IAM.

Un [gruppo IAM](#) è un'identità che specifica un insieme di utenti IAM. Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, è possibile avere un gruppo denominato Amministratori IAM e concedere a tale gruppo le autorizzazioni per amministrare le risorse IAM.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli

utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta [Quando creare un utente IAM \(invece di un ruolo\)](#) nella Guida per l'utente di IAM.

Ruoli IAM

Un [ruolo IAM](#) è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. Puoi assumere temporaneamente un ruolo IAM in AWS Management Console [cambiando ruolo](#). Puoi assumere un ruolo chiamando un'operazione AWS CLI o AWS API o utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta [Utilizzo di ruoli IAM](#) nella Guida per l'utente di IAM.

I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:

- **Accesso utente federato:** per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta [Creazione di un ruolo per un provider di identità di terza parte](#) nella Guida per l'utente di IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per ulteriori informazioni sui set di autorizzazioni, consulta [Set di autorizzazioni](#) nella Guida per l'utente di AWS IAM Identity Center .
- **Autorizzazioni utente IAM temporanee:** un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- **Accesso multi-account:** è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per informazioni sulle differenze tra ruoli e policy basate su risorse per l'accesso multi-account, consulta [Differenza tra i ruoli IAM e le policy basate su risorse](#) nella Guida per l'utente di IAM.
- **Accesso a più servizi:** alcuni Servizi AWS utilizzano le funzionalità di altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è comune che tale servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.

- **Sessioni di accesso diretto (FAS):** quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra azione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama un Servizio AWS, combinate con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le operazioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina [Forward access sessions](#).
- **Ruolo di servizio:** un ruolo di servizio è un [ruolo IAM](#) assunto da un servizio per eseguire operazioni per conto dell'utente. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione [Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS](#) nella Guida per l'utente di IAM.
- **Ruolo collegato al servizio:** un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un Servizio AWS. Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.
- **Applicazioni in esecuzione su Amazon EC2:** puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 e che AWS CLI effettuano richieste API. AWS Cloud è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un ruolo AWS a un'istanza EC2 e renderlo disponibile per tutte le sue applicazioni, crei un profilo di istanza collegato all'istanza. Un profilo dell'istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le credenziali temporanee. Per ulteriori informazioni, consulta [Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2](#) nella Guida per l'utente di IAM.

Per informazioni sull'utilizzo dei ruoli IAM, consulta [Quando creare un ruolo IAM \(invece di un utente\)](#) nella Guida per l'utente di IAM.

Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e collegandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La

maggior parte delle politiche viene archiviata AWS come documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta [Panoramica delle policy JSON](#) nella Guida per l'utente di IAM.

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. Successivamente l'amministratore può aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Le policy IAM definiscono le autorizzazioni relative a un'operazione, a prescindere dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'azione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dall' AWS Management Console AWS CLI, dall' o dall' AWS API.

Policy basate su identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta [Creazione di policy IAM](#) nella Guida per l'utente di IAM.

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono incorporate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli nel tuo Account AWS. Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta [Scelta fra policy gestite e policy inline](#) nella Guida per l'utente di IAM.

Policy basate su risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile allegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarle per controllare l'accesso a una risorsa specifica. Quando è allegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario [specificare un principale](#) in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non puoi utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Liste di controllo degli accessi (ACL)

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni per accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3 e Amazon VPC sono esempi di servizi che supportano gli ACL. AWS WAF Per maggiori informazioni sulle ACL, consulta [Panoramica delle liste di controllo degli accessi \(ACL\)](#) nella Guida per gli sviluppatori di Amazon Simple Storage Service.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi e meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- **Limiti delle autorizzazioni:** un limite delle autorizzazioni è una funzione avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM (utente o ruolo IAM). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal` sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta [Limiti delle autorizzazioni per le entità IAM](#) nella Guida per l'utente di IAM.
- **Politiche di controllo dei servizi (SCP):** le SCP sono politiche JSON che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in AWS Organizations. AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più Account AWS di proprietà dell'azienda. Se abiliti tutte le funzionalità in un'organizzazione, puoi applicare le policy di controllo dei servizi (SCP) a uno o tutti i tuoi account. L'SCP limita le autorizzazioni per le entità negli account dei membri, inclusa ciascuna. Utente root dell'account AWS Per ulteriori informazioni su organizzazioni e policy SCP, consulta la pagina sulle [Policy di controllo dei servizi](#) nella Guida per l'utente di AWS Organizations .
- **Policy di sessione:** le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire

da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta [Policy di sessione](#) nella Guida per l'utente di IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire una richiesta quando sono coinvolti più tipi di policy, consulta [Logica di valutazione delle policy](#) nella IAM User Guide.

Come funziona Amazon DocumentDB con IAM

Prima di utilizzare IAM per gestire l'accesso ad Amazon DocumentDB, scopri quali funzionalità IAM sono disponibili per l'uso con Amazon DocumentDB.

Funzionalità IAM che puoi usare con Amazon DocumentDB

Funzionalità IAM	Cluster basati su istanze	Cluster elastici
Policy basate su identità	Sì	Sì
Policy basate su risorse	No	No
Azioni di policy	Sì	Sì
Risorse relative alle policy	Sì	Sì
Chiavi di condizione della policy (specifica del servizio)	Sì	Sì
Liste di controllo degli accessi (ACL)	No	No
ABAC (tag nelle policy)	Parziale	Sì
Credenziali temporanee	Sì	Sì
Autorizzazioni del principale	Sì	Sì
Ruoli di servizio	Sì	Sì

Funzionalità IAM	Cluster basati su istanze	Cluster elastici
Ruoli collegati al servizio	No	Sì

Per avere una visione di alto livello di come Amazon DocumentDB e AWS altri servizi funzionano con la maggior parte delle funzionalità IAM, [AWS consulta i servizi che funzionano con IAM](#) nella IAM User Guide.

Politiche basate sull'identità per Amazon DocumentDB

Supporta le policy basate su identità	Sì
---------------------------------------	----

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta [Creazione di policy IAM](#) nella Guida per l'utente di IAM.

Con le policy basate su identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Non è possibile specificare l'entità principale in una policy basata sull'identità perché si applica all'utente o al ruolo a cui è associato. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta [Guida di riferimento agli elementi delle policy JSON IAM](#) nella Guida per l'utente di IAM.

Esempi di policy basate sull'identità per Amazon DocumentDB

Per visualizzare esempi di policy basate sull'identità di Amazon DocumentDB, consulta [Esempi di policy basate sull'identità per Amazon DocumentDB](#)

Policy basate sulle risorse all'interno di Amazon DocumentDB

Supporta le policy basate su risorse	No
--------------------------------------	----

Le policy basate su risorse sono documenti di policy JSON che è possibile allegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy

dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarle per controllare l'accesso a una risorsa specifica. Quando è allegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario [specificare un principale](#) in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Per consentire l'accesso multi-account, puoi specificare un intero account o entità IAM in un altro account come principale in una policy basata sulle risorse. L'aggiunta di un principale multi-account a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando il principale e la risorsa sono diversi Account AWS, un amministratore IAM dell'account affidabile deve inoltre concedere all'entità principale (utente o ruolo) l'autorizzazione ad accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un principale nello stesso account, non sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta [Differenza tra i ruoli IAM e le policy basate su risorse](#) nella Guida per l'utente di IAM.

Azioni politiche per Amazon DocumentDB

Supporta le azioni di policy

Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Action` di una policy JSON descrive le azioni che è possibile utilizzare per consentire o negare l'accesso a una policy. Le azioni politiche in genere hanno lo stesso nome dell'operazione AWS API associata. Ci sono alcune eccezioni, ad esempio le azioni di sola autorizzazione che non hanno un'operazione API corrispondente. Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Note

Per alcune funzionalità di gestione, Amazon DocumentDB utilizza la tecnologia operativa condivisa con Amazon Relational Database Service (Amazon RDS).

Per visualizzare un elenco di azioni RDS, consulta [Actions defined by Amazon Relational Database Service nel Service Authorization Reference](#).

Per visualizzare le azioni politiche per i cluster elastici di Amazon DocumentDB, consulta [Azioni definite dai cluster elastici di Amazon DocumentDB nel Service Authorization Reference](#).

Le azioni politiche in Amazon DocumentDB utilizzano il seguente prefisso prima dell'azione:

```
aws
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

```
"Action": [  
    "aws:action1",  
    "aws:action2"  
]
```

Per visualizzare esempi di policy basate sull'identità di Amazon DocumentDB, consulta [Esempi di policy basate sull'identità per Amazon DocumentDB](#)

Risorse relative alle policy per Amazon DocumentDB

Supporta le risorse di policy

Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento JSON `Resource` della policy specifica l'oggetto o gli oggetti ai quali si applica l'azione. Le istruzioni devono includere un elemento `Resource` o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il suo [nome della risorsa Amazon \(ARN\)](#). Puoi eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

```
"Resource": "*"
```

Note

Per alcune funzionalità di gestione, Amazon DocumentDB utilizza la tecnologia operativa condivisa con Amazon Relational Database Service (Amazon RDS).

Per visualizzare un elenco dei tipi di risorse RDS e dei relativi ARN, consulta [Resources defined by Amazon Relational Database Service nel Service Authorization Reference](#). Per sapere con quali azioni puoi specificare l'ARN di ogni risorsa, consulta [Azioni definite da Amazon Relational Database Service](#).

Per visualizzare i tipi di risorse per i cluster elastici di Amazon DocumentDB, consulta [Tipi di risorse definiti dai cluster elastici di Amazon DocumentDB nel Service Authorization Reference](#).

Per visualizzare esempi di policy basate sull'identità di Amazon DocumentDB, consulta [Esempi di policy basate sull'identità per Amazon DocumentDB](#)

Chiavi delle condizioni delle policy per Amazon DocumentDB

Supporta le chiavi di condizione delle policy specifiche del servizio	Sì
---	----

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Condition` (o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition` è facoltativo. Puoi compilare espressioni condizionali che utilizzano [operatori di condizione](#), ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi `Condition` in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione AND logica. Se si specificano più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione logica. OR Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, puoi autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo nome utente IAM. Per ulteriori informazioni, consulta [Elementi delle policy IAM: variabili e tag](#) nella Guida per l'utente di IAM.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche del servizio. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di [contesto delle condizioni AWS globali nella Guida](#) per l'utente IAM.

Note

Per alcune funzionalità di gestione, Amazon DocumentDB utilizza la tecnologia operativa condivisa con Amazon Relational Database Service (Amazon RDS).

Per visualizzare un elenco di chiavi di condizione RDS, consulta [Condition keys for Amazon Relational Database Service nel Service Authorization Reference](#). Per sapere con quali azioni e risorse puoi utilizzare una chiave di condizione, consulta [Azioni definite da Amazon Relational Database Service](#).

Per visualizzare le chiavi di condizione per i cluster elastici di Amazon DocumentDB, consulta Chiavi di [condizione per i cluster elastici di Amazon DocumentDB nel Service Authorization Reference](#).

Per visualizzare esempi di policy basate sull'identità di Amazon DocumentDB, consulta [Esempi di policy basate sull'identità per Amazon DocumentDB](#)

ACL in Amazon DocumentDB

Supporta le ACL

No

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni ad accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

ABAC con Amazon DocumentDB

Note

ABAC è supportato solo parzialmente per i cluster basati su istanze, ma è supportato per i cluster elastici.

Il controllo dell'accesso basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, questi attributi sono chiamati tag. Puoi allegare tag a entità IAM (utenti o ruoli) e a molte AWS risorse. L'assegnazione di tag alle entità e alle risorse è il primo passaggio di ABAC. In seguito, vengono progettate policy ABAC per consentire operazioni quando il tag dell'entità principale corrisponde al tag sulla risorsa a cui si sta provando ad accedere.

La strategia ABAC è utile in ambienti soggetti a una rapida crescita e aiuta in situazioni in cui la gestione delle policy diventa impegnativa.

Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'[elemento condizione](#) di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Yes (Sì). Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per ulteriori informazioni su ABAC, consulta [Che cos'è ABAC?](#) nella Guida per l'utente di IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta [Utilizzo del controllo degli accessi basato su attributi \(ABAC\)](#) nella Guida per l'utente di IAM.

Utilizzo di credenziali temporanee con Amazon DocumentDB

Supporta le credenziali temporanee Sì

Alcune Servizi AWS non funzionano quando accedi utilizzando credenziali temporanee. Per ulteriori informazioni, incluse quelle che Servizi AWS funzionano con credenziali temporanee, consulta la sezione relativa alla [Servizi AWS compatibilità con IAM nella IAM User Guide](#).

Stai utilizzando credenziali temporanee se accedi AWS Management Console utilizzando qualsiasi metodo tranne nome utente e password. Ad esempio, quando accedete AWS utilizzando il link Single

Sign-On (SSO) della vostra azienda, tale processo crea automaticamente credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sullo scambio dei ruoli, consulta [Cambio di un ruolo \(console\)](#) nella Guida per l'utente di IAM.

È possibile creare manualmente credenziali temporanee utilizzando l'API o AWS CLI. AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta [Credenziali di sicurezza provvisorie in IAM](#).

Autorizzazioni principali multiservizio per Amazon DocumentDB

Supporta sessioni di accesso diretto (FAS)	Sì
--	----

Quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra azione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama un Servizio AWS, in combinazione con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le operazioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina [Forward access sessions](#).

Ruoli di servizio per Amazon DocumentDB

Supporta i ruoli di servizio	Sì
------------------------------	----

Un ruolo di servizio è un [ruolo IAM](#) che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione [Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS](#) nella Guida per l'utente di IAM.

⚠ Warning

La modifica delle autorizzazioni per un ruolo di servizio potrebbe interrompere la funzionalità di Amazon DocumentDB. Modifica i ruoli di servizio solo quando Amazon DocumentDB fornisce indicazioni in tal senso.

Ruoli collegati ai servizi per Amazon DocumentDB

ℹ Note

I ruoli collegati ai servizi non sono supportati per i cluster basati su istanze, ma sono supportati per i cluster elastici.

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un servizio AWS. Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

Per ulteriori informazioni su come creare e gestire i ruoli collegati ai servizi, consulta [Servizi AWS supportati da IAM](#). Trova un servizio nella tabella che include un Yes nella colonna Service-linked role (Ruolo collegato ai servizi). Scegli il collegamento Sì per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Esempi di policy basate sull'identità per Amazon DocumentDB

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare risorse Amazon DocumentDB. Inoltre, non possono eseguire attività utilizzando AWS Management Console, AWS Command Line Interface (AWS CLI) o AWS API. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta [Creazione di policy IAM](#) nella Guida per l'utente di IAM.

Per informazioni dettagliate sulle azioni e sui tipi di risorse definiti da Amazon DocumentDB, incluso il formato degli ARN per ciascun tipo di risorsa, consulta [Azioni, risorse e chiavi di condizione per Amazon Relational Database Service](#) nel Service Authorization Reference.

Argomenti

- [Best practice per le policy](#)
- [Utilizzo della console Amazon DocumentDB](#)
- [Consentire agli utenti di visualizzare le loro autorizzazioni](#)

Best practice per le policy

Le policy basate sull'identità determinano se qualcuno può creare, accedere o eliminare risorse Amazon DocumentDB nel tuo account. Queste operazioni possono comportare costi aggiuntivi per l'Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le policy gestite che concedono le autorizzazioni per molti casi d'uso comuni. AWS Sono disponibili nel tuo Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta [Policy gestite da AWS](#) o [Policy gestite da AWS per le funzioni dei processi](#) nella Guida per l'utente IAM.
- Applica le autorizzazioni con privilegi minimi: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta [Policy e autorizzazioni in IAM](#) nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso a operazioni e risorse puoi aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione [Elementi delle policy JSON di IAM: condizione](#) nella Guida per l'utente di IAM.
- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano alla

sintassi della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta [Convalida delle policy per IAM Access Analyzer](#) nella Guida per l'utente di IAM.

- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta [Configurazione dell'accesso alle API protetto con MFA](#) nella Guida per l'utente di IAM.

Per maggiori informazioni sulle best practice in IAM, consulta [Best practice di sicurezza in IAM](#) nella Guida per l'utente di IAM.

Utilizzo della console Amazon DocumentDB

Per accedere alla console Amazon DocumentDB (con compatibilità con MongoDB), devi disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle risorse Amazon DocumentDB presenti nel tuo Account AWS. Se crei una policy basata sull'identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti o ruoli) associate a tale policy.

Non è necessario concedere autorizzazioni minime per la console agli utenti che effettuano chiamate solo verso AWS CLI o l'API. Al contrario, concedi l'accesso solo alle operazioni che corrispondono all'operazione API che stanno cercando di eseguire.

Per garantire che utenti e ruoli possano ancora utilizzare la console Amazon DocumentDB, collega anche Amazon *ConsoleAccess* DocumentDB *ReadOnly* AWS o la policy gestita alle entità. Per ulteriori informazioni, consulta [Aggiunta di autorizzazioni a un utente](#) nella Guida per l'utente IAM.

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono allegate alla relativa identità utente. Questa policy include le autorizzazioni per completare questa azione sulla console o utilizzando l'API o in modo programmatico. 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": "*"
}
]
```

Risoluzione dei problemi relativi all'identità e all'accesso ad Amazon DocumentDB

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con Amazon DocumentDB e IAM.

Argomenti

- [Non sono autorizzato a eseguire un'azione in Amazon DocumentDB](#)
- [Non sono autorizzato a eseguire iam: PassRole](#)

- [Voglio consentire a persone esterne a me di accedere Account AWS alle mie risorse Amazon DocumentDB](#)

Non sono autorizzato a eseguire un'azione in Amazon DocumentDB

Se ricevi un errore che indica che non sei autorizzato a eseguire un'operazione, le tue policy devono essere aggiornate per poter eseguire l'operazione.

L'errore di esempio seguente si verifica quando l'utente IAM `mateojackson` prova a utilizzare la console per visualizzare i dettagli relativi a una risorsa `my-example-widget` fittizia ma non dispone di autorizzazioni `aws:GetWidget` fittizie.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
aws:GetWidget on resource: my-example-widget
```

In questo caso, la policy per l'utente `mateojackson` deve essere aggiornata per consentire l'accesso alla risorsa `my-example-widget` utilizzando l'azione `aws:GetWidget`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Non sono autorizzato a eseguire iam: PassRole

Se ricevi un messaggio di errore indicante che non sei autorizzato a eseguire l'`iam:PassRole` azione, le tue policy devono essere aggiornate per consentirti di passare un ruolo ad Amazon DocumentDB.

Alcuni Servizi AWS consentono di passare un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

Il seguente errore di esempio si verifica quando un utente IAM denominato `marymajor` tenta di utilizzare la console per eseguire un'azione in Amazon DocumentDB. Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per passare il ruolo al servizio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire a persone esterne a me di accedere Account AWS alle mie risorse Amazon DocumentDB

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per servizi che supportano policy basate su risorse o liste di controllo accessi (ACL), utilizza tali policy per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se Amazon DocumentDB supporta queste funzionalità, consulta [Come funziona Amazon DocumentDB con IAM](#)
- Per sapere come fornire l'accesso alle tue risorse attraverso Account AWS le risorse di tua proprietà, consulta [Fornire l'accesso a un utente IAM in un altro Account AWS di tua proprietà](#) nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta [Fornire l'accesso a soggetti Account AWS di proprietà di terze parti](#) nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta [Fornire l'accesso a utenti autenticati esternamente \(Federazione delle identità\)](#) nella Guida per l'utente di IAM.
- Per informazioni sulle differenze tra l'utilizzo di ruoli e policy basate su risorse per l'accesso multi-account, consulta [Differenza tra i ruoli IAM e le policy basate su risorse](#) nella Guida per l'utente IAM.

Gestione delle autorizzazioni di accesso alle risorse Amazon DocumentDB

Ogni AWS risorsa è di proprietà di un utente e Account AWS le autorizzazioni per creare o accedere alle risorse sono regolate da politiche di autorizzazione. Un amministratore di account può associare politiche di autorizzazione alle identità IAM (ovvero utenti, gruppi e ruoli) e alcuni servizi (come AWS Lambda) supportano anche l'associazione di politiche di autorizzazione alle risorse.

Note

Un amministratore account (o un utente amministratore) è un utente con autorizzazioni di amministratore. Per ulteriori informazioni, consulta [Best practice IAM](#) nella Guida per l'utente di IAM.

Argomenti

- [Risorse e operazioni di Amazon DocumentDB](#)
- [Informazioni sulla proprietà delle risorse](#)
- [Gestione dell'accesso alle risorse](#)
- [Specifica degli elementi delle policy: operazioni, effetti, risorse ed entità](#)
- [Specifica delle condizioni in una policy](#)

Risorse e operazioni di Amazon DocumentDB

In Amazon DocumentDB, la risorsa principale è un cluster. Amazon DocumentDB supporta altre risorse che possono essere utilizzate con la risorsa principale, come istanze, gruppi di parametri e sottoscrizioni a eventi. Queste risorse vengono chiamate risorse secondarie.

A risorse e risorse secondarie sono associati nomi Amazon Resource Name (ARN) univoci, come illustrato nella tabella seguente.

Tipo di risorsa	Formato ARN
Cluster	<code>arn:aws:rds: <i>region</i>:<i>account-id</i> :cluster: <i>db-cluster-name</i></code>
Cluster parameter group (Gruppo di parametri del cluster)	<code>arn:aws:rds: <i>region</i>:<i>account-id</i> :cluster-pg: <i>cluster-parameter-group-name</i></code>
Snapshot del cluster	<code>arn:aws:rds: <i>region</i>:<i>account-id</i> :cluster-snapshot: <i>cluster-snapshot-name</i></code>
Istanza	<code>arn:aws:rds: <i>region</i>:<i>account-id</i> :db:<i>db-instance-name</i></code>

Tipo di risorsa	Formato ARN
Gruppo di sicurezza	<code>arn:aws:rds: <i>region</i>:<i>account-id</i> :secgrp:<i>security-group-name</i></code>
Subnet group (Gruppo di sottoreti)	<code>arn:aws:rds: <i>region</i>:<i>account-id</i> :subgrp:<i>subnet-group-name</i></code>

Amazon DocumentDB fornisce una serie di operazioni per lavorare con le risorse di Amazon DocumentDB. Per un elenco di operazioni disponibili, consulta [Operazioni](#).

Informazioni sulla proprietà delle risorse

Il proprietario di una risorsa è colui Account AWS che ha creato una risorsa. Cioè, il proprietario Account AWS della risorsa è l'entità principale (l'account root, un utente IAM o un ruolo IAM) che autentica la richiesta che crea la risorsa. Negli esempi seguenti viene illustrato il funzionamento:

- Se utilizzi le credenziali dell'account root del tuo account Account AWS per creare una risorsa Amazon DocumentDB, ad esempio un'istanza, sei Account AWS il proprietario della risorsa Amazon DocumentDB.
- Se crei un utente IAM nel tuo Account AWS e concedi le autorizzazioni per creare risorse Amazon DocumentDB a quell'utente, l'utente può creare risorse Amazon DocumentDB. Tuttavia, l'utente Account AWS a cui appartiene l'utente possiede le risorse di Amazon DocumentDB.
- Se crei un ruolo IAM in azienda Account AWS con le autorizzazioni necessarie per creare risorse Amazon DocumentDB, chiunque possa assumere il ruolo può creare risorse Amazon DocumentDB. Il tuo Account AWS, a cui appartiene il ruolo, possiede le risorse di Amazon DocumentDB.

Gestione dell'accesso alle risorse

La policy delle autorizzazioni descrive chi ha accesso a cosa. Nella sezione seguente vengono descritte le opzioni disponibili per la creazione di policy relative alle autorizzazioni.

Note

Questa sezione descrive l'uso di IAM nel contesto di Amazon DocumentDB. Non vengono fornite informazioni dettagliate sul servizio IAM. Per la documentazione di IAM completa,

consulta [Che cos'è IAM?](#) nella Guida per l'utente di IAM. Per informazioni sulla sintassi e le descrizioni delle policy IAM, consulta [AWSIAM Policy Reference](#) nella IAM User Guide.

Le policy collegate a un'identità IAM sono denominate policy basate su identità (policy IAM). Le policy collegate a una risorsa sono denominate policy basate sulle risorse. Amazon DocumentDB supporta solo policy basate sull'identità (policy IAM).

Argomenti

- [Policy basate su identità \(policy IAM\)](#)
- [Policy basate su risorse](#)

Policy basate su identità (policy IAM)

Puoi collegare le policy alle identità IAM. Ad esempio, puoi eseguire le operazioni seguenti:

- Allega una politica di autorizzazioni a un utente o a un gruppo nel tuo account: un amministratore dell'account può utilizzare una politica di autorizzazioni associata a un particolare utente per concedere a quell'utente le autorizzazioni per creare una risorsa Amazon DocumentDB, ad esempio un'istanza.
- Collega una policy di autorizzazione a un ruolo (assegnazione di autorizzazioni tra account): per concedere autorizzazioni tra più account, è possibile collegare una policy di autorizzazione basata su identità a un ruolo IAM. Ad esempio, un amministratore può creare un ruolo per concedere autorizzazioni su più account a un altro o a un Account AWS servizio nel modo seguente: AWS
 1. L'amministratore dell'account A crea un ruolo IAM e attribuisce una policy di autorizzazione al ruolo che concede le autorizzazioni sulle risorse per l'account A.
 2. L'amministratore dell'account A attribuisce una policy di attendibilità al ruolo, identificando l'account B come il principale per tale ruolo.
 3. L'amministratore dell'account B può quindi delegare le autorizzazioni per assumere il ruolo a qualsiasi utente dell'account B. In questo modo gli utenti dell'account B possono creare o accedere alle risorse nell'account A. Il responsabile della politica di fiducia può anche essere un responsabile del AWS servizio se si desidera concedere le autorizzazioni a un AWS servizio per assumere il ruolo.

Per ulteriori informazioni sull'uso di IAM per delegare le autorizzazioni, consulta [Access Management](#) nella IAM User Guide (Guida per l'utente di IAM).

Di seguito è riportato un esempio di politica che consente all'utente con l'ID di creare istanze 123456789012 per il tuo Account AWS. La nuova istanza database deve utilizzare un gruppo di opzioni e un gruppo di parametri che inizia con default e deve utilizzare il gruppo di sottoreti default.

```
{
  "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"
      ]
    }
  ]
}
```

Per ulteriori informazioni sull'utilizzo di politiche basate sull'identità con Amazon DocumentDB, consulta [Utilizzo di politiche basate sull'identità \(politiche IAM\) per Amazon DocumentDB](#). Per ulteriori informazioni su utenti, gruppi, ruoli e autorizzazioni, consulta [Identità \(utenti, gruppi e ruoli\)](#) nella Guida per l'utente di IAM.

Policy basate su risorse

Anche altri servizi, come Amazon Simple Storage Service (Amazon S3), supportano politiche di autorizzazione basate sulle risorse. Ad esempio, è possibile associare una policy a un bucket Amazon S3 per gestire le autorizzazioni di accesso a quel bucket. Amazon DocumentDB non supporta policy basate sulle risorse.

Specifiche degli elementi delle policy: operazioni, effetti, risorse ed entità

Per ogni risorsa Amazon DocumentDB (vedi [Risorse e operazioni di Amazon DocumentDB](#)), il servizio definisce un set di operazioni API. Per ulteriori informazioni, consulta [Operazioni](#). Per concedere le autorizzazioni per queste operazioni API, Amazon DocumentDB definisce una serie di azioni che è

possibile specificare in una policy. L'esecuzione di un'operazione API può richiedere le autorizzazioni per più di un'operazione.

Di seguito sono elencati gli elementi di base di una policy:

- **Risorsa:** in una policy si utilizza il nome della risorsa Amazon (ARN) per identificare la risorsa a cui si applica la policy stessa.
- **Operazione:** utilizzi le parole chiave per identificare le operazioni sulla risorsa da permettere o rifiutare. Ad esempio, l'autorizzazione `rds:DescribeDBInstances` concede all'utente le autorizzazioni per eseguire l'operazione `DescribeDBInstances`.
- **Effetto:** l'effetto prodotto quando l'utente richiede l'operazione specifica, ovvero un'autorizzazione o un rifiuto. USe non concedi esplicitamente (consenti) l'accesso a una risorsa, l'accesso viene implicitamente rifiutato. Puoi anche rifiutare esplicitamente l'accesso a una risorsa per garantire che un utente non possa accedervi, anche se l'accesso viene concesso da un'altra policy.
- **Principale -** Nelle policy basate su identità (policy IAM), l'utente a cui la policy è collegata è il principale implicito. Per policy basate su risorse, specifichi l'utente, l'account, il servizio o un'altra entità che desideri riceva le autorizzazioni (si applica solo alle policy basate su risorse). Amazon DocumentDB non supporta policy basate sulle risorse.

Per ulteriori informazioni sulla sintassi e le descrizioni delle policy IAM, consulta [AWS Riferimento alle policy IAM](#) nella Guida per l'utente di IAM.

Per una tabella che mostra tutte le azioni API di Amazon DocumentDB e le risorse a cui si applicano, consulta [Autorizzazioni API Amazon DocumentDB: riferimento ad azioni, risorse e condizioni](#)

Specifiche delle condizioni in una policy

Quando si concedono le autorizzazioni, è possibile utilizzare il linguaggio della policy IAM per specificare le condizioni in base a cui la policy deve essere applicata. Ad esempio, potresti decidere che una policy venga applicata solo dopo una data specifica. Per ulteriori informazioni su come specificare le condizioni in un linguaggio di policy, consulta la sezione [Condizione](#) nella Guida per l'utente di IAM.

Per esprimere le condizioni è necessario utilizzare chiavi di condizione predefinite. Amazon DocumentDB non dispone di chiavi di contesto specifiche del servizio che possano essere utilizzate in una policy IAM. Per un elenco delle chiavi di contesto per le condizioni globali disponibili per tutti i servizi, consulta [Chiavi disponibili per le condizioni](#) nella Guida per l'utente di IAM.

Utilizzo di politiche basate sull'identità (politiche IAM) per Amazon DocumentDB

Important

Per alcune funzionalità di gestione, Amazon DocumentDB utilizza una tecnologia operativa condivisa con Amazon RDS. Le chiamate alla console e alle API di Amazon DocumentDB vengono registrate come chiamate effettuate all'API Amazon RDS. AWS CLI

Ti consigliamo di consultare prima gli argomenti introduttivi che spiegano i concetti e le opzioni di base disponibili per gestire l'accesso alle tue risorse di Amazon DocumentDB. Per ulteriori informazioni, consulta [Gestione delle autorizzazioni di accesso alle risorse Amazon DocumentDB](#).

In questo argomento vengono forniti esempi di policy basate su identità in cui un amministratore account può collegare policy di autorizzazione a identità IAM, ovvero utenti, gruppi e ruoli.

Di seguito è riportato un esempio di policy IAM.

```
{
  "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"
      ]
    }
  ]
}
```

La policy include una singola istruzione che specifica le autorizzazioni seguenti per l'utente IAM:

- La policy consente all'utente IAM di creare un'istanza utilizzando l'azione [CreateDBInstance](#) (ciò vale anche per [create-db-instance](#) AWS CLI l'operazione e la). AWS Management Console
- L'elemento `Resource` specifica che l'utente può eseguire azioni in o con altre risorse. Specifica le risorse utilizzando un Amazon Resource Name (ARN). Questo ARN include il nome del servizio a cui appartiene la risorsa (`rds`), il Regione AWS (*indica qualsiasi regione in questo esempio), il numero di account utente (123456789012 è l'ID utente in questo esempio) e il tipo di risorsa.

L'elemento `Resource` nell'esempio specifica i seguenti vincoli della policy sulle risorse per l'utente:

- L'identificatore dell'istanza per la nuova istanza deve iniziare con `test` (per esempio, `testCustomerData1`, `test-region2-data`).
- Il gruppo di parametri cluster per la nuova istanza database deve iniziare con `default`.
- Il gruppo di sottoreti per la nuova istanza deve essere il gruppo di sottoreti `default`.

La policy non specifica l'elemento `Principal` poiché in una policy basata su identità l'entità che ottiene l'autorizzazione non viene specificata. Quando si collega una policy a un utente, quest'ultimo è l'entità implicita. Quando colleghi una policy di autorizzazioni a un ruolo IAM, il principale identificato nella policy di attendibilità del ruolo ottiene le autorizzazioni.

Per una tabella che mostra tutte le operazioni API di Amazon DocumentDB e le risorse a cui si applicano, consulta. [Autorizzazioni API Amazon DocumentDB: riferimento ad azioni, risorse e condizioni](#)

Autorizzazioni necessarie per utilizzare la console Amazon DocumentDB

Affinché un utente possa lavorare con la console Amazon DocumentDB, deve disporre di un set minimo di autorizzazioni. Queste autorizzazioni consentono all'utente di descrivere le Account AWS proprie risorse Amazon DocumentDB e di fornire altre informazioni correlate, tra cui la sicurezza e le informazioni di rete di Amazon EC2.

Se decidi di creare una policy IAM più restrittiva delle autorizzazioni minime richieste, la console non funzionerà come previsto per gli utenti con tale policy IAM. Per garantire che tali utenti possano continuare a utilizzare la console Amazon DocumentDB, collega anche la policy `AmazonDocDBConsoleFullAccess` gestita all'utente, come descritto in. [AWS politiche gestite per Amazon DocumentDB](#)

Non è necessario consentire autorizzazioni minime per la console per gli utenti che effettuano chiamate solo verso l' AWS CLI API di Amazon DocumentDB.

Esempi di policy gestite dal cliente

In questa sezione, puoi trovare esempi di politiche utente che concedono autorizzazioni per varie azioni di Amazon DocumentDB. Queste policy funzionano quando utilizzi azioni API di Amazon DocumentDB, AWS SDK o AWS CLI. Se utilizzi la console, sarà necessario concedere autorizzazioni aggiuntive specifiche per quest'ultima, come illustrato in [Autorizzazioni necessarie per utilizzare la console Amazon DocumentDB](#).

Per alcune funzionalità di gestione, Amazon DocumentDB utilizza una tecnologia operativa condivisa con Amazon Relational Database Service (Amazon RDS) e Amazon Neptune.

Note

Tutti gli esempi utilizzano la regione Stati Uniti orientali (Virginia settentrionale) () e contengono ID di account us-east-1 fittizi.

Esempi

- [Esempio 1: consentire a un utente di eseguire qualsiasi azione di descrizione su qualsiasi risorsa Amazon DocumentDB](#)
- [Esempio 2: impedire a un utente di eliminare un'istanza](#)
- [Esempio 3: impedire a un utente di creare un cluster a meno che non sia abilitata la crittografia dello storage](#)

Esempio 1: consentire a un utente di eseguire qualsiasi azione di descrizione su qualsiasi risorsa Amazon DocumentDB

La seguente policy di autorizzazione concede a un utente le autorizzazioni per eseguire tutte le operazioni che iniziano con `Describe`. Queste azioni mostrano informazioni su una risorsa Amazon DocumentDB, ad esempio un'istanza. Il carattere jolly (*) nell'`Resource` elemento indica che le azioni sono consentite per tutte le risorse Amazon DocumentDB di proprietà dell'account.

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

```
        "Action": "rds:Describe*",
        "Resource": "*"
    }
]
}
```

Esempio 2: impedire a un utente di eliminare un'istanza

La seguente policy di autorizzazione assegna le autorizzazioni per impedire a un utente di eliminare un'istanza specifica. Ad esempio, potresti voler negare la possibilità di eliminare le istanze di produzione a qualsiasi utente che non sia un amministratore.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyDelete1",
      "Effect": "Deny",
      "Action": "rds>DeleteDBInstance",
      "Resource": "arn:aws:rds:us-east-1:123456789012:db:my-db-instance"
    }
  ]
}
```

Esempio 3: impedire a un utente di creare un cluster a meno che non sia abilitata la crittografia dello storage

La seguente politica di autorizzazione nega l'autorizzazione a un utente per la creazione di un cluster Amazon DocumentDB a meno che non sia abilitata la crittografia dello storage.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PreventUnencryptedDocumentDB",
      "Effect": "Deny",
      "Action": "RDS:CreateDBCluster",
      "Condition": {
        "Bool": {
          "rds:StorageEncrypted": "false"
        }
      },
      "StringEquals": {
```



```
        "rds:DatabaseEngine": "docdb"
      }
    },
    "Resource": "*"
  }
]
```

AWS politiche gestite per Amazon DocumentDB

Per aggiungere autorizzazioni a utenti, gruppi e ruoli, è più facile utilizzare politiche AWS gestite che scriverle autonomamente. Creare [policy gestite dal cliente IAM](#) per fornire al tuo team solo le autorizzazioni di cui ha bisogno richiede tempo e competenza. Per iniziare rapidamente, puoi utilizzare le nostre politiche AWS gestite. Queste politiche coprono casi d'uso comuni e sono disponibili nel tuo AWS account. Per ulteriori informazioni sulle policy AWS gestite, consulta [le policy AWS gestite](#) nella AWS Identity and Access Management User Guide.

AWS i servizi mantengono e aggiornano le politiche AWS gestite. Non è possibile modificare le autorizzazioni nelle politiche AWS gestite. I servizi aggiungono occasionalmente autorizzazioni aggiuntive a una policy AWS gestita per supportare nuove funzionalità. Questo tipo di aggiornamento interessa tutte le identità (utenti, gruppi e ruoli) a cui è collegata la policy. È più probabile che i servizi aggiornino una politica AWS gestita quando viene lanciata una nuova funzionalità o quando diventano disponibili nuove operazioni. I servizi non rimuovono le autorizzazioni da una policy AWS gestita, quindi gli aggiornamenti delle policy non comprometteranno le autorizzazioni esistenti.

Inoltre, AWS supporta politiche gestite per le funzioni lavorative che si estendono su più servizi. Ad esempio, la policy `ViewOnlyAccess` AWS gestita fornisce l'accesso in sola lettura a molti AWS servizi e risorse. Quando un servizio lancia una nuova funzionalità, AWS aggiunge autorizzazioni di sola lettura per nuove operazioni e risorse. Per un elenco e una descrizione delle politiche relative alle funzioni lavorative, consulta [le politiche AWS gestite per le funzioni lavorative](#) nella AWS Identity and Access Management User Guide.

Le seguenti policy AWS gestite, che puoi allegare agli utenti del tuo account, sono specifiche di Amazon DocumentDB:

- [AmazonDocDB FullAccess](#)— Garantisce l'accesso completo a tutte le risorse Amazon DocumentDB per l' AWS account root.
- [AmazonDocDB ReadOnlyAccess](#)— Garantisce l'accesso in sola lettura a tutte le risorse Amazon DocumentDB per l'account root. AWS

- [AmazonDocDB ConsoleFullAccess](#)— Garantisce l'accesso completo alla gestione delle risorse del cluster elastico Amazon DocumentDB e Amazon DocumentDB utilizzando il. AWS Management Console
- [AmazonDocDB ElasticReadOnlyAccess](#)— Concede l'accesso in sola lettura a tutte le risorse del cluster elastico di Amazon DocumentDB per l'account root. AWS
- [AmazonDocDB ElasticFullAccess](#)— Garantisce l'accesso completo a tutte le risorse del cluster elastico di Amazon DocumentDB per l' AWS account root.

AmazonDocDB FullAccess

Questa policy concede autorizzazioni amministrative che consentono l'accesso completo principale a tutte le azioni di Amazon DocumentDB. Le autorizzazioni in questa policy sono raggruppate come segue:

- Le autorizzazioni di Amazon DocumentDB consentono tutte le azioni di Amazon DocumentDB.
- Alcune delle autorizzazioni di Amazon EC2 incluse in questa policy sono necessarie per convalidare le risorse trasmesse in una richiesta API. Questo serve a garantire che Amazon DocumentDB sia in grado di utilizzare correttamente le risorse con un cluster. Le altre autorizzazioni di Amazon EC2 incluse in questa policy consentono ad Amazon DocumentDB di creare AWS le risorse necessarie per consentirti di connetterti ai tuoi cluster.
- Le autorizzazioni di Amazon DocumentDB vengono utilizzate durante le chiamate API per convalidare le risorse passate in una richiesta. Sono necessari per consentire ad Amazon DocumentDB di utilizzare la chiave passata con il cluster Amazon DocumentDB.
- CloudWatch I log sono necessari per Amazon DocumentDB per garantire che le destinazioni di consegna dei log siano raggiungibili e che siano validi per l'utilizzo dei log da parte dei broker.

```
{
  "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:AWSServiceName": "rds.amazonaws.com"
        }
      }
    }
  ]
}

```

AmazonDocDB ReadOnlyAccess

Questa policy concede autorizzazioni di sola lettura che consentono agli utenti di visualizzare le informazioni in Amazon DocumentDB. I responsabili a cui è associata questa policy non possono effettuare aggiornamenti o eliminare risorse esistenti, né possono creare nuove risorse Amazon DocumentDB. Ad esempio, i principali con queste autorizzazioni possono visualizzare l'elenco dei cluster e delle configurazioni associati al proprio account, ma non possono modificare la configurazione o le impostazioni di alcun cluster. Le autorizzazioni in questa policy sono raggruppate come segue:

- Le autorizzazioni di Amazon DocumentDB consentono di elencare le risorse di Amazon DocumentDB, descriverle e ottenere informazioni su di esse.
- Le autorizzazioni Amazon EC2 vengono utilizzate per descrivere Amazon VPC, sottoreti, gruppi di sicurezza ed ENI associati a un cluster.
- Un'autorizzazione Amazon DocumentDB viene utilizzata per descrivere la chiave associata al cluster.

```

{
  "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:*"
    ]
}
]
}

```

AmazonDocDB ConsoleFullAccess

Garantisce l'accesso completo alla gestione delle risorse di Amazon DocumentDB utilizzando quanto AWS Management Console segue:

- Le autorizzazioni di Amazon DocumentDB per consentire tutte le azioni dei cluster Amazon DocumentDB e Amazon DocumentDB.
- Alcune delle autorizzazioni di Amazon EC2 incluse in questa policy sono necessarie per convalidare le risorse trasmesse in una richiesta API. Questo serve a garantire che Amazon DocumentDB sia in grado di utilizzare correttamente le risorse per il provisioning e la manutenzione del cluster. Le altre autorizzazioni di Amazon EC2 incluse in questa policy consentono ad Amazon DocumentDB di creare AWS le risorse necessarie per consentirti di connetterti ai tuoi cluster come VPCEndpoint.
- AWS KMS le autorizzazioni vengono utilizzate durante le chiamate API per convalidare le risorse passate in una AWS KMS richiesta. Sono necessari per consentire ad Amazon DocumentDB di utilizzare la chiave passata per crittografare e decrittografare i dati inattivi con il cluster elastico Amazon DocumentDB.

- CloudWatch I log sono necessari per Amazon DocumentDB per garantire che le destinazioni di consegna dei log siano raggiungibili e che siano validi per il controllo e la profilazione dell'utilizzo dei log.
- Le autorizzazioni di Secrets Manager sono necessarie per convalidare un determinato segreto e utilizzarlo, configurare l'utente amministratore per i cluster elastici di Amazon DocumentDB.
- Le autorizzazioni Amazon RDS sono necessarie per le azioni di gestione dei cluster Amazon DocumentDB. Per alcune funzionalità di gestione, Amazon DocumentDB utilizza una tecnologia operativa condivisa con Amazon RDS.
- Le autorizzazioni SNS consentono ai responsabili di abbonamenti e argomenti Amazon Simple Notification Service (Amazon SNS) e di pubblicare messaggi Amazon SNS.
- Le autorizzazioni IAM sono necessarie per creare i ruoli collegati al servizio necessari per la pubblicazione di metriche e log.

```
{
  "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",
        "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:RemoveTagsForResource",
        "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"
        }
      }
    }
  ]
}

```

AmazonDocDB ElasticReadOnlyAccess

Questa policy concede autorizzazioni di sola lettura che consentono agli utenti di visualizzare le informazioni sui cluster elastici in Amazon DocumentDB. I responsabili a cui è associata questa policy non possono effettuare aggiornamenti o eliminare risorse esistenti, né possono creare nuove risorse Amazon DocumentDB. Ad esempio, i principali con queste autorizzazioni possono visualizzare l'elenco dei cluster e delle configurazioni associati al proprio account, ma non possono modificare la configurazione o le impostazioni di alcun cluster. Le autorizzazioni in questa policy sono raggruppate come segue:

- Le autorizzazioni del cluster elastico di Amazon DocumentDB consentono di elencare le risorse del cluster elastico di Amazon DocumentDB, descriverle e ottenere informazioni su di esse.
- CloudWatch le autorizzazioni vengono utilizzate per verificare le metriche del servizio.

```
{
  "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": "*"
    }
  ]
}
```

AmazonDocDB ElasticFullAccess

Questa policy concede autorizzazioni amministrative che consentono l'accesso completo principale a tutte le azioni di Amazon DocumentDB per il cluster elastico Amazon DocumentDB.

Questa policy utilizza i AWS tag (<https://docs.aws.amazon.com/tag-editor/latest/userguide/tagging.html>) entro condizioni atte a definire l'accesso alle risorse. Se stai usando un segreto, deve essere etichettato con la chiave del tag `DocDBElasticFullAccess` e un valore del tag. Se si utilizza una chiave gestita dal cliente, questa deve essere contrassegnata con una chiave tag `DocDBElasticFullAccess` e un valore di tag.

Le autorizzazioni in questa policy sono raggruppate come segue:

- Le autorizzazioni del cluster elastico di Amazon DocumentDB consentono tutte le azioni di Amazon DocumentDB.

- Alcune delle autorizzazioni di Amazon EC2 incluse in questa policy sono necessarie per convalidare le risorse trasmesse in una richiesta API. Questo serve a garantire che Amazon DocumentDB sia in grado di utilizzare correttamente le risorse per il provisioning e la manutenzione del cluster. Le altre autorizzazioni Amazon EC2 incluse in questa policy consentono ad Amazon DocumentDB di creare AWS le risorse necessarie per consentirti di connetterti ai tuoi cluster come un endpoint VPC.
- AWS KMS sono necessarie autorizzazioni per consentire ad Amazon DocumentDB di utilizzare la chiave passata per crittografare e decrittografare i dati inattivi all'interno del cluster elastico Amazon DocumentDB.

Note

La chiave gestita dal cliente deve avere un tag con chiave e un valore del tag.
DocDBElasticFullAccess

- SecretsManager sono necessarie autorizzazioni per convalidare un determinato segreto e utilizzarlo, configurare l'utente amministratore per i cluster elastici di Amazon DocumentDB.

Note

Il segreto utilizzato deve avere un tag con chiave DocDBElasticFullAccess e un valore di tag.

- Le autorizzazioni IAM sono necessarie per creare i ruoli collegati al servizio necessari per la pubblicazione di metriche e log.

```
{
  "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"
    ],
    "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

Non puoi collegarti AmazonDocDBElasticServiceRolePolicy alle tue AWS Identity and Access Management entità. Questa policy è associata a un ruolo collegato al servizio che consente ad Amazon DocumentDB di eseguire azioni per tuo conto. Per ulteriori informazioni, consulta [Ruoli collegati ai servizi nei cluster elastici](#).

```

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

```

```

"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "cloudwatch:PutMetricData"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "cloudwatch:namespace": [
          "AWS/DocDB-Elastic"
        ]
      }
    }
  }
]
}

```

Amazon DocumentDB aggiorna le policy gestite AWS

Modifica	Descrizione	Data
AmazonDocDB ElasticFullAccess , AmazonDocDB ConsoleFullAccess - Modifica	Politiche aggiornate per aggiungere azioni di avvio/arresto del cluster e copiare le azioni di snapshot del cluster.	21/02/2024
AmazonDocDB ElasticReadOnlyAccess , - Modifica AmazonDocDB ElasticFullAccess	Politiche aggiornate per aggiungere cloudwatch:GetMetricData azioni.	21/06/2023
AmazonDocDB ElasticReadOnlyAccess : nuova policy	Nuova policy gestita per i cluster elastici di Amazon DocumentDB	08/06/2023
AmazonDocDB ElasticFullAccess : nuova policy	Nuova policy gestita per i cluster elastici di Amazon DocumentDB	5/06/2023

Modifica	Descrizione	Data
AmazonDocDB- ElasticServiceRolePolicy : nuova policy	Amazon DocumentDB crea un nuovo ruolo collegato al servizio AWS ServiceRoleForDoc DB-Elastic per i cluster elastici di Amazon DocumentDB	30/11/2022
AmazonDocDB ConsoleFullAccess - Cambia	Policy aggiornata per aggiungere autorizzazioni per cluster globali ed elastici di Amazon DocumentDB	30/11/2022
AmazonDocDB ConsoleFullAccess , AmazonDocDB FullAccess , AmazonDocDB ReadOnlyAccess - Nuova politica	Avvio del servizio	19/1/2017

Autorizzazioni API Amazon DocumentDB: riferimento ad azioni, risorse e condizioni

Utilizza le seguenti sezioni come riferimento quando configuri [Utilizzo di politiche basate sull'identità \(politiche IAM\) per Amazon DocumentDB](#) e scrivi politiche di autorizzazione da allegare a un'identità IAM (politiche basate sull'identità).

Di seguito sono elencate tutte le operazioni API di Amazon DocumentDB. Nell'elenco sono incluse le azioni corrispondenti per le quali è possibile concedere le autorizzazioni per eseguire l'azione, la AWS risorsa per la quale è possibile concedere le autorizzazioni e le chiavi di condizione che è possibile includere per un controllo granulare degli accessi. Le operazioni, il valore della risorsa e le condizioni vengono specificati rispettivamente nei campi Action, Resource e Condition della policy. Per ulteriori informazioni sulle condizioni, consulta [Specifiche delle condizioni in una policy](#).

Puoi utilizzare chiavi di condizione AWS -wide nelle policy di Amazon DocumentDB per esprimere condizioni. Per un elenco completo delle chiavi AWS -wide, consulta Available [Keys](#) nella IAM User Guide.

Puoi testare le policy IAM con il simulatore di policy IAM. Fornisce automaticamente un elenco di risorse e parametri necessari per ogni AWS azione, incluse le azioni di Amazon DocumentDB. Il simulatore di policy IAM determina le autorizzazioni necessarie per ciascuna delle azioni specificate. Per informazioni sul simulatore di policy IAM, consulta [Testing IAM Policies with the IAM Policy Simulator nella IAM User Guide](#).

Note

Per specificare un'operazione, utilizza il prefisso `rds:` seguito dal nome dell'operazione API (ad esempio, `rds:CreateDBInstance`).

Di seguito sono elencate le operazioni dell'API Amazon RDS e le relative azioni, risorse e chiavi di condizione.

Argomenti

- [Azioni di Amazon DocumentDB che supportano le autorizzazioni a livello di risorsa](#)
- [Azioni di Amazon DocumentDB che non supportano le autorizzazioni a livello di risorsa](#)

Azioni di Amazon DocumentDB che supportano le autorizzazioni a livello di risorsa

Le autorizzazioni a livello di risorsa offrono la possibilità di specificare le risorse su cui gli utenti possono eseguire azioni. Amazon DocumentDB supporta parzialmente le autorizzazioni a livello di risorsa. Ciò significa che per determinate azioni di Amazon DocumentDB, puoi controllare quando gli utenti sono autorizzati a utilizzare tali azioni in base a condizioni che devono essere soddisfatte o a risorse specifiche che gli utenti sono autorizzati a utilizzare. Ad esempio, puoi concedere agli utenti l'autorizzazione a modificare solo specifiche istanze.

Di seguito sono elencate le operazioni dell'API di Amazon DocumentDB e le relative azioni, risorse e chiavi di condizione.

Note

Per alcune funzionalità di gestione, Amazon DocumentDB utilizza una tecnologia operativa condivisa con Amazon RDS.

Operazioni e azioni dell'API Amazon DocumentDB	Risorse	Chiavi di condizione
AddTagsToResource rds:AddTagsToResource	Istanza arn:aws:rds: <i>region</i> : <i>account-id</i> :db: <i>db-instance-name</i>	rds:db-tag
	Subnet group (Gruppo di sottoreti) arn:aws:rds: <i>region</i> : <i>account-id</i> :subgrp: <i>subnet-group-name</i>	rds:subgrp-tag
ApplyPendingMaintenanceAction rds:ApplyPendingMaintenanceAction	Istanza arn:aws:rds: <i>region</i> : <i>account-id</i> :db: <i>db-instance-name</i>	rds:db-tag
CopyDBClusterSnapshot rds:CopyDBClusterSnapshot	Snapshot del cluster arn:aws:rds: <i>region</i> : <i>account-id</i> :cluster-snapshot: <i>cluster-snapshot-name</i>	rds:cluster-snapshot-tag
CreateDBCluster rds>CreateDBCluster	Cluster arn:aws:rds: <i>region</i> : <i>account-id</i> :cluster: <i>db-cluster-name</i>	rds:cluster-tag
	Cluster parameter group (Gruppo di parametri del cluster)	rds:cluster-pg-tag

Operazioni e azioni dell'API Amazon DocumentDB	Risorse	Chiavi di condizione
	arn:aws:rds: <i>region</i> : <i>account-id</i> :cluster-pg: <i>cluster-parameter-group-name</i>	
	Subnet group (Gruppo di sottoreti) arn:aws:rds: <i>region</i> : <i>account-id</i> :subgrp: <i>subnet-group-name</i>	rds:subgrp-tag
Crea DB ClusterParameterGroup rds:CreateDBClusterParameterGroup	Cluster parameter group (Gruppo di parametri del cluster) arn:aws:rds: <i>region</i> : <i>account-id</i> :cluster-pg: <i>cluster-parameter-group-name</i>	rds:cluster-pg-tag
Crea DB ClusterSnapshot rds:CreateDBClusterSnapshot	Cluster arn:aws:rds: <i>region</i> : <i>account-id</i> :cluster: <i>db-cluster-name</i> Snapshot del cluster arn:aws:rds: <i>region</i> : <i>account-id</i> :cluster-snapshot: <i>cluster-snapshot-name</i>	rds:cluster-tag rds:cluster-snapshot-tag
CreateDBInstance rds:CreateDBInstance	Istanza arn:aws:rds: <i>region</i> : <i>account-id</i> :db: <i>db-instance-name</i>	rds:DatabaseClass rds:db-tag

Operazioni e azioni dell'API Amazon DocumentDB	Risorse	Chiavi di condizione
	Cluster arn:aws:rds: <i>region</i> : <i>account-id</i> :cluster: <i>db-cluster-name</i>	rds:cluster-tag
Crea DB SubnetGroup rds:CreateDBSubnetGroup	Subnet group (Gruppo di sottoreti) arn:aws:rds: <i>region</i> : <i>account-id</i> :subgrp: <i>subnet-group-name</i>	rds:subgrp-tag
Elimina DB Instance rds:DeleteDBInstance	Istanza arn:aws:rds: <i>region</i> : <i>account-id</i> :db: <i>db-instance-name</i>	rds:db-tag
Elimina DB SubnetGroup rds:DeleteDBSubnetGroup	Subnet group (Gruppo di sottoreti) arn:aws:rds: <i>region</i> : <i>account-id</i> :subgrp: <i>subnet-group-name</i>	rds:subgrp-tag
Descrivi ClusterParameterGroups rds:DescribeDBClusterParameterGroups	Cluster parameter group (Gruppo di parametri del cluster) arn:aws:rds: <i>region</i> : <i>account-id</i> :cluster-pg: <i>cluster-parameter-group-name</i>	rds:cluster-pg-tag

Operazioni e azioni dell'API Amazon DocumentDB	Risorse	Chiavi di condizione
Descritto B ClusterParameters rds:DescribeDBClusterParameters	Cluster parameter group (Gruppo di parametri del cluster) arn:aws:rds: <i>region</i> : <i>account-id</i> :cluster-pg: <i>cluster-parameter-group-name</i>	rds:cluster-pg-tag
DescribeDBClusters rds:DescribeDBClusters	Cluster arn:aws:rds: <i>region</i> : <i>account-id</i> :cluster: <i>db-cluster-instance-name</i>	rds:cluster-tag
Descritto B ClusterSnapshotAttributes rds:DescribeDBClusterSnapshotAttributes	Snapshot del cluster arn:aws:rds: <i>region</i> : <i>account-id</i> :cluster-snapshot: <i>cluster-snapshot-name</i>	rds:cluster-snapshot-tag
Descritto B SubnetGroups rds:DescribeDBSubnetGroups	Subnet group (Gruppo di sottoreti) arn:aws:rds: <i>region</i> : <i>account-id</i> :subgrp: <i>subnet-group-name</i>	rds:subgrp-tag
DescribePendingMaintenanceActions rds:DescribePendingMaintenanceActions	Istanza arn:aws:rds: <i>region</i> : <i>account-id</i> :db: <i>db-instance-name</i>	rds:DatabaseClass rds:db-tag

Operazioni e azioni dell'API Amazon DocumentDB	Risorse	Chiavi di condizione
FailoverDBCluster rds:FailoverDBCluster	Cluster arn:aws:rds: <i>region</i> : <i>account-id</i> :cluster: <i>db-cluster-instance-name</i>	rds:cluster-tag
ListTagsForResource rds:ListTagsForResource	Istanza arn:aws:rds: <i>region</i> : <i>account-id</i> :db: <i>db-instance-name</i>	rds:db-tag
	Subnet group (Gruppo di sottoreti) arn:aws:rds: <i>region</i> : <i>account-id</i> :subgrp: <i>subnet-group-name</i>	rds:subgrp-tag
ModifyDBCluster rds:ModifyDBCluster	Cluster arn:aws:rds: <i>region</i> : <i>account-id</i> :cluster: <i>db-cluster-name</i>	rds:cluster-tag
	Cluster parameter group (Gruppo di parametri del cluster) arn:aws:rds: <i>region</i> : <i>account-id</i> :cluster-pg: <i>cluster-parameter-group-name</i>	rds:cluster-pg-tag

Operazioni e azioni dell'API Amazon DocumentDB	Risorse	Chiavi di condizione
Modifica DB ClusterParameterGroup rds:ModifyDBClusterParameterGroup	Cluster parameter group (Gruppo di parametri del cluster) arn:aws:rds: <i>region</i> : <i>account-id</i> :cluster-pg: <i>cluster-parameter-group-name</i>	rds:cluster-pg-tag
Modifica DB ClusterSnapshotAttribute rds:ModifyDBClusterSnapshotAttribute	Snapshot del cluster arn:aws:rds: <i>region</i> : <i>account-id</i> :cluster-snapshot: <i>cluster-snapshot-name</i>	rds:cluster-snapshot-tag
ModifyDBInstance rds:ModifyDBInstance	Istanza arn:aws:rds: <i>region</i> : <i>account-id</i> :db: <i>db-instance-name</i>	rds:DatabaseClass rds:db-tag
RebootDBInstance rds:RebootDBInstance	Istanza arn:aws:rds: <i>region</i> : <i>account-id</i> :db: <i>db-instance-name</i>	rds:db-tag
RemoveTagsFromResource rds:RemoveTagsFromResource	Istanza arn:aws:rds: <i>region</i> : <i>account-id</i> :db: <i>db-instance-name</i> Subnet group (Gruppo di sottoreti) arn:aws:rds: <i>region</i> : <i>account-id</i> :subgrp: <i>subnet-group-name</i>	rds:db-tag rds:subgrp-tag

Operazioni e azioni dell'API Amazon DocumentDB	Risorse	Chiavi di condizione
Reimposta DB ClusterParameterGroup rds:ResetDBClusterParameterGroup	Cluster parameter group (Gruppo di parametri del cluster) arn:aws:rds: <i>region</i> : <i>account-id</i> :cluster-pg: <i>cluster-parameter-group-name</i>	rds:cluster-pg-tag
Ripristina DB ClusterFromSnapshot rds:RestoreDBClusterFromSnapshot	Cluster arn:aws:rds: <i>region</i> : <i>account-id</i> :cluster: <i>db-cluster-instance-name</i>	rds:cluster-tag
	Snapshot del cluster arn:aws:rds: <i>region</i> : <i>account-id</i> :cluster-snapshot: <i>cluster-snapshot-name</i>	rds:cluster-snapshot-tag
RestoreDB ClusterToPointInTime rds:RestoreDBClusterToPointInTime	Cluster arn:aws:rds: <i>region</i> : <i>account-id</i> :cluster: <i>db-cluster-instance-name</i>	rds:cluster-tag
	Subnet group (Gruppo di sottoreti) arn:aws:rds: <i>region</i> : <i>account-id</i> :subgrp: <i>subnet-group-name</i>	rds:subgrp-tag

Azioni di Amazon DocumentDB che non supportano le autorizzazioni a livello di risorsa

Puoi utilizzare tutte le azioni di Amazon DocumentDB in una policy IAM per concedere o negare agli utenti l'autorizzazione a utilizzare tale azione. Tuttavia, non tutte le azioni di Amazon DocumentDB supportano le autorizzazioni a livello di risorsa, che consentono di specificare le risorse su cui eseguire un'azione. Le seguenti azioni API di Amazon DocumentDB attualmente non supportano le autorizzazioni a livello di risorsa. Pertanto, per utilizzare queste azioni in una policy IAM, devi concedere agli utenti l'autorizzazione a utilizzare tutte le risorse per l'azione utilizzando un carattere * jolly per l'elemento nella tua dichiarazione. Resource

- `rds:DescribeDBClusterSnapshots`
- `rds:DescribeDBInstances`

Gestione degli utenti Amazon DocumentDB

In Amazon DocumentDB, gli utenti si autenticano in un cluster con una password. Ogni cluster dispone di credenziali di accesso primarie che vengono stabilite durante la creazione del cluster.

Note

Tutti i nuovi utenti creati prima del 26 marzo 2020 hanno ottenuto i ruoli `dbAdminAnyDatabase`, `readWriteAnyDatabase` e `clusterAdmin`. Ti consigliamo di rivalutare tutti gli utenti e modificare i ruoli in base alle necessità per applicare i privilegi minimi per tutti gli utenti nel cluster.

Per ulteriori informazioni, consulta [Accesso al database tramite il controllo degli accessi basato sui ruoli](#).

Principale `serviceadmin` utente

Un cluster Amazon DocumentDB appena creato ha due utenti: l'utente principale e l'`serviceadmin`utente.

L'utente principale è un singolo utente privilegiato in grado di eseguire attività amministrative e creare utenti aggiuntivi con ruoli. Quando ti connetti a un cluster Amazon DocumentDB per la prima volta, devi autenticarti utilizzando le credenziali di accesso primarie. L'utente principale riceve queste autorizzazioni amministrative per un cluster Amazon DocumentDB al momento della creazione del cluster e gli viene concesso il ruolo `dirroot`.

L'utente `serviceadmin` viene creato implicitamente quando viene creato il cluster. Ogni cluster Amazon DocumentDB ha un `serviceadmin` utente che offre AWS la possibilità di gestire il cluster. Non puoi eseguire l'accesso come `serviceadmin`, né eliminarlo, rinominarlo, modificarne la password o le autorizzazioni. Qualsiasi tentativo comporta la generazione di un errore.

Note

Il primario `serviceadmin` gli utenti di un cluster Amazon DocumentDB non possono essere eliminati e `root` il ruolo dell'utente principale non può essere revocato. Se dimentichi la password dell'utente principale, puoi reimpostarla utilizzando AWS Management Console o AWS CLI.

Creazione di utenti aggiuntivi

Dopo esserti connesso come utente principale (o qualsiasi utente con il ruolo `createUser`), puoi creare un nuovo utente, come illustrato di seguito.

```
db.createUser(  
  {  
    user: "sample-user-1",  
    pwd: "password123",  
    roles:  
      [{"db":"admin", "role":"dbAdminAnyDatabase" }]  
  }  
)
```

Per visualizzare i dettagli dell'utente, puoi utilizzare il comando `show users` come segue. Puoi inoltre rimuovere gli utenti con il comando `dropUser`. Per ulteriori informazioni, consulta [Comandi comuni](#).

```
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"
      }
    ]
  }
}
```

Nel precedente esempio, il nuovo utente `sample-user-1` viene attribuito al database `admin`. Questo è sempre il caso di un nuovo utente. Amazon DocumentDB non ha il concetto di `unauthenticationDatabase` e quindi tutte le autenticazioni vengono eseguite nel contesto del `admin` database.

Quando si creano utenti, se si omette il `db` campo quando si specifica il ruolo, Amazon DocumentDB attribuirà implicitamente il ruolo al database in cui viene emessa la connessione. Ad esempio, se la connessione viene emessa in relazione al database `sample-database` ed esegui il comando seguente, l'utente `sample-user-2` verrà creato nel database `admin` e avrà le autorizzazioni `readWrite` per il database `sample-database`.

```
db.createUser(
```

```
{
  user: "sample-user-2",
  pwd: "password123",
  roles:
    ["readWrite"]
}
```

La creazione di utenti con ruoli con ambito in tutti i database (ad esempio, `readInAnyDatabase`) richiede che tu sia nell'ambito del database `admin` durante la creazione dell'utente oppure devi specificare esplicitamente il database per il ruolo durante la creazione dell'utente.

Per cambiare il contesto del database, puoi utilizzare il seguente comando.

```
use admin
```

Per ulteriori informazioni sul controllo degli accessi basato sui ruoli e sull'applicazione dei privilegi minimi tra gli utenti del cluster, consulta [Accesso al database tramite il controllo degli accessi basato sui ruoli](#).

Password a rotazione automatica per Amazon DocumentDB

Con AWS Secrets Manager, puoi sostituire le credenziali nel codice (incluse le password) con una chiamata API a Secrets Manager in modo da recuperare il segreto a livello di codice. Questo approccio aiuta a garantire che il segreto non venga compromesso da qualcuno che esamina il codice, perché semplicemente il segreto non è presente. Inoltre, puoi configurare Secrets Manager affinché ruoti automaticamente il segreto in base a una pianificazione specificata. In questo modo puoi sostituire i segreti a lungo termine con altri a breve termine, contribuendo a ridurre notevolmente il rischio di compromissione.

Utilizzando Secrets Manager, è possibile ruotare automaticamente le password Amazon DocumentDB (ovvero, segreti) utilizzando una AWS Lambda funzione fornita da Secrets Manager.

Per ulteriori informazioni sull'AWS Secrets Manager integrazione nativa con Amazon DocumentDB, consultare:

- [Blog: Come ruotare le credenziali Amazon DocumentDB e Amazon Redshift in AWS Secrets Manager](#)

- [Cos'è AWS Secrets Manager?](#)
- [Rotazione dei segreti per Amazon DocumentDB](#)

Accesso al database tramite il controllo degli accessi basato sui ruoli

Puoi limitare l'accesso alle azioni che gli utenti possono eseguire sui database utilizzando il controllo degli accessi basato sui ruoli (RBAC) in Amazon DocumentDB (con compatibilità con MongoDB). RBAC funziona concedendo uno o più ruoli a un utente. Questi ruoli determinano le operazioni che un utente può eseguire sulle risorse del database. Amazon DocumentDB attualmente supporta sia ruoli integrati con ambito a livello di database, come `read`, `readWrite`, `readAnyDatabase`, `clusterAdmin`, sia ruoli definiti dall'utente che possono essere limitati ad azioni specifiche e risorse granulari come raccolte basate sui requisiti dell'utente.

I casi d'uso più comuni di RBAC includono l'applicazione dei privilegi minimi mediante la creazione di utenti con accesso in sola lettura ai database o alle raccolte in un cluster e la progettazione di applicazioni multi-tenant che consentono a un singolo utente di accedere a un determinato database o raccolta in un cluster.

Note

Tutti i nuovi utenti creati prima del 26 marzo 2020 hanno ottenuto i ruoli `dbAdminAnyDatabase`, `readWriteAnyDatabase` e `clusterAdmin`. Ti consigliamo di rivalutare tutti gli utenti esistenti e modificare i ruoli in base alle necessità per applicare i privilegi minimi per i cluster.

Argomenti

- [Concetti RBAC](#)
- [Guida introduttiva ai ruoli integrati RBAC](#)
- [Guida introduttiva ai ruoli RBAC definiti dall'utente](#)
- [Connessione ad Amazon DocumentDB come utente](#)
- [Comandi comuni](#)
- [Differenze funzionali](#)

- [Limiti](#)
- [Accesso al database mediante il controllo degli accessi basato sui ruoli](#)

Concetti RBAC

Di seguito sono riportati termini e concetti importanti relativi al controllo accessi basato sui ruoli. Per ulteriori informazioni sugli utenti di Amazon DocumentDB, consulta [Gestione degli utenti Amazon DocumentDB](#)

- **Utente:** una singola entità che può autenticarsi nel database ed eseguire operazioni.
- **Password:** un segreto utilizzato per autenticare l'utente.
- **Ruolo:** autorizza un utente a eseguire azioni su uno o più database.
- **Database di amministrazione:** il database in cui gli utenti sono archiviati e su cui sono autorizzati.
- **Database (**db**):** lo spazio dei nomi all'interno dei cluster che contiene le raccolte per l'archiviazione dei documenti.

Il comando seguente crea un utente denominato `sample-user`.

```
db.createUser({user: "sample-user", pwd: "abc123", roles: [{role: "read", db: "sample-database"}]})
```

In questo esempio:

- `user: "sample-user"`— Indica il nome utente.
- `pwd: "abc123"`— Indica la password dell'utente.
- `role: "read", "db: "sample-database"`— Indica che l'utente `sample-user` avrà i permessi di lettura in `sample-database`.

```
db.createUser({user: "sample-user", pwd: "abc123", roles: [{role: "read", db: "sample-database"}]})
```

L'esempio seguente mostra l'output dopo aver ottenuto l'utente `sample-user` con `db.getUser(sample-user)`. In questo esempio, l'utente `sample-user` risiede nel database `admin` ma ha il ruolo di lettura per il database `sample-database`.

```

{
  "_id" : "sample-user",
  "user" : "sample-user",
  "db" : "admin",
  "roles" : [
    {
      "db" : "sample-database",
      "role" : "read"
    }
  ]
}

```

← User ID

← Username

← All users created in the *admin* database

← User *sample-user* has read permissions in database *sample-database*

Durante la creazione di utenti, se si omette il `db` campo quando si specifica il ruolo, Amazon DocumentDB attribuirà implicitamente il ruolo al database in cui viene emessa la connessione. Ad esempio, se la connessione viene emessa in relazione al database `sample-database` ed esegui il comando seguente, l'utente `sample-user` verrà creato nel database `admin` e avrà le autorizzazioni `readWrite` per il database `sample-database`.

```
db.createUser({user: "sample-user", pwd: "abc123", roles: ["readWrite"]})
```

L'aspetto dell'output di questa operazione è simile al seguente.

```

{
  "user":"sample-user",
  "roles":[
    {
      "db":"sample-database",
      "role":"readWrite"
    }
  ]
}

```

La creazione di utenti con ruoli con ambito in tutti i database (ad esempio, `readAnyDatabase`) richiede che tu sia nell'ambito del database `admin` durante la creazione dell'utente oppure devi specificare esplicitamente il database per il ruolo durante la creazione dell'utente. Per emettere comandi sul database `admin`, puoi utilizzare il comando `use admin`. Per ulteriori informazioni, consulta [Comandi comuni](#).

Guida introduttiva ai ruoli integrati RBAC

Per aiutarti a iniziare a utilizzare il controllo accessi basato sui ruoli, questa sezione illustra uno scenario di esempio per l'applicazione dei privilegi minimi creando ruoli per tre utenti con funzioni di lavoro diverse.

- `user1` è un nuovo manager che deve essere in grado di visualizzare e accedere a tutti i database in un cluster.
- `user2` è un nuovo dipendente che ha bisogno di accedere a un solo database `sample-database-1`, nello stesso cluster.
- `user3` è un dipendente esistente che deve visualizzare e accedere a un database diverso, `sample-database-2` a cui non aveva accesso prima, nello stesso cluster.

Successivamente, sia `user1` che `user2` lasciano la società e quindi il loro accesso deve essere revocato.

Per creare utenti e concedere ruoli, l'utente per il quale esegui l'autenticazione nel cluster deve disporre di un ruolo associato in grado di eseguire operazioni per `createUser` e `grantRole`. Ad esempio, i ruoli `admin` e `userAdminAnyDatabase` possono entrambi concedere tali capacità, per esempio. Per le operazioni per ruolo, consulta [Accesso al database mediante il controllo degli accessi basato sui ruoli](#).

Note

In Amazon DocumentDB, tutte le operazioni relative agli utenti e ai ruoli (ad esempio `create`, `get`, `drop`, `grant`, `revoke`, ecc.) vengono eseguite implicitamente nel `admin` database indipendentemente dal fatto che tu stia emettendo comandi sul database o meno. `admin`

Innanzitutto, per capire quali sono gli utenti e i ruoli correnti nel cluster, puoi eseguire il comando `show users`, come nell'esempio seguente. Vedrai due utenti, `serviceadmin` e l'utente `master` per il cluster. Questi due utenti sono sempre presenti e non possono essere eliminati. Per ulteriori informazioni, consulta [Gestione degli utenti Amazon DocumentDB](#).

```
show users
```

Per `user1`, crea un ruolo con accesso in lettura e scrittura a tutti i database dell'intero cluster con il comando seguente.

```
db.createUser({user: "user1", pwd: "abc123", roles: [{role: "readWriteAnyDatabase", db: "admin"}]})
```

L'aspetto dell'output di questa operazione è simile al seguente.

```
{
  "user": "user1",
  "roles": [
    {
      "role": "readWriteAnyDatabase",
      "db": "admin"
    }
  ]
}
```

Per `user2`, crea un ruolo con accesso di sola lettura al database `sample-database-1` con il comando seguente.

```
db.createUser({user: "user2", pwd: "abc123", roles: [{role: "read", db: "sample-database-1"}]})
```

L'aspetto dell'output di questa operazione è simile al seguente.

```
{
  "user": "user2",
  "roles": [
    {
      "role": "read",
      "db": "sample-database-1"
    }
  ]
}
```

Per simulare lo scenario nel quale `user3` è un utente esistente, crea innanzitutto l'utente `user3` e quindi assegna un nuovo ruolo a `user3`.

```
db.createUser({user: "user3", pwd: "abc123", roles: [{role: "readWrite", db: "sample-database-1"}]})
```

L'aspetto dell'output di questa operazione è simile al seguente.

```
{
  "user": "user3",
  "roles": [
    {
      "role": "readWrite",
      "db": "sample-database-1"
    }
  ]
}
```

Ora che l'utente `user3` è stato creato, assegna a `user3` il ruolo `read` su `sample-database-2`.

```
db.grantRolesToUser("user3", [{role: "read", db: "sample-database-2"}])
```

Infine, `user1` e `user2` lasciano l'azienda ed è necessario che il loro accesso al cluster venga revocato. Puoi farlo rilasciando gli utenti, come segue.

```
db.dropUser("user1")
db.dropUser("user2")
```

Per garantire che tutti gli utenti dispongano dei ruoli appropriati, puoi elencare tutti gli utenti con il comando seguente.

```
show users
```

L'aspetto dell'output di questa operazione è simile al seguente.

```
{
  "_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"
    }
  ]
}
}
```

Guida introduttiva ai ruoli RBAC definiti dall'utente

Per aiutarti a iniziare a usare i ruoli definiti dall'utente, questa sezione illustra uno scenario di esempio di applicazione del privilegio minimo mediante la creazione di ruoli per tre utenti con diverse funzioni lavorative.

In questo esempio, vale quanto segue:

- `user1` è un nuovo manager che deve essere in grado di visualizzare e accedere a tutti i database in un cluster.
- `user2` è un nuovo dipendente che necessita solo dell'azione 'find' per un solo database `sample-database-1`, nello stesso cluster.

- `user3` è un dipendente esistente che deve visualizzare e accedere a una raccolta specifica, `col2` in un database diverso, a `sample-database-2` cui non aveva accesso prima, nello stesso cluster.
- Per `user1`, crea un ruolo con accesso in lettura e scrittura a tutti i database dell'intero cluster con il comando seguente.

```
db.createUser(  
  {  
    user: "user1", pwd: "abc123",  
    roles: [{role: "readWriteAnyDatabase", db: "admin"}]  
  }  
)
```

L'aspetto dell'output di questa operazione è simile al seguente.

```
{  
  "user": "user1",  
  "roles": [  
    {  
      "role": "readWriteAnyDatabase",  
      "db": "admin"  
    }  
  ]  
}
```

Per `user2`, crea un ruolo con privilegi di 'find' per tutte le raccolte nel database `sample-database-1` con il seguente comando. Tieni presente che questo ruolo garantirebbe che tutti gli utenti associati possano eseguire solo query di ricerca.

```
db.createRole(  
  {  
    role: "findRole",  
    privileges: [  
      {  
        resource: {db: "sample-database-1", collection: ""}, actions: ["find"]  
      }  
    ],  
    roles: []  
  }  
)
```

L'aspetto dell'output di questa operazione è simile al seguente.

```
{
  "role": "findRole",
  "privileges": [
    {
      "resource": {
        "db": "sample-database-1",
        "collection": ""
      },
      "actions": [
        "find"
      ]
    }
  ],
  "roles": [
  ]
}
```

Quindi, crea l'utente (`user2`) e associa all'utente il ruolo creato `findRole` di recente.

```
db.createUser(
{
  user: "user2",
  pwd: "abc123",
  roles: []
})

db.grantRolesToUser("user2", ["findRole"])
```

Per simulare lo scenario in cui `user3` si tratta di un utente esistente, prima crea l'utente `user3`, quindi crea un nuovo ruolo chiamato `collectionRole` che verrà assegnato nel passaggio successivo. `user3`

Ora puoi assegnare un nuovo ruolo a `user3`. Questo nuovo ruolo permetterà di `user3` poter inserire, aggiornare, eliminare e trovare l'accesso a una specifica raccolta `col2` in `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: []  
}]  
)
```

L'aspetto dell'output di questa operazione è simile al seguente.

```
{  
  "role":"collectionRole",  
  "privileges":[  
    {  
      "resource":{  
        "db":"sample-database-2",  
        "collection":"col2"  
      },  
      "actions":[  
        "find",  
        "update",  
        "insert",  
        "remove"  
      ]  
    }  
  ],  
  "roles":[  
  ]  
}
```

Ora che l'utente `user3` è stato creato, puoi concedere `user3` il ruolo `collectionFind`.

```
db.grantRolesToUser("user3",["collectionRole"])
```

Infine, `user1` e `user2` lasciano l'azienda ed è necessario che il loro accesso al cluster venga revocato. Puoi farlo rilasciando gli utenti, come segue.

```
db.dropUser("user1")
db.dropUser("user2")
```

Per garantire che tutti gli utenti dispongano dei ruoli appropriati, puoi elencare tutti gli utenti con il comando seguente.

```
show users
```

L'aspetto dell'output di questa operazione è simile al seguente.

```
{
  "_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"
    }
  ]
}
```

```
}
```

Connessione ad Amazon DocumentDB come utente

Quando ti connetti a un cluster Amazon DocumentDB, ti connetti nel contesto di un particolare database. Per impostazione predefinita, se non specifichi un database nella stringa di connessione, ti connetti automaticamente al cluster nell'ambito del database `test`. Tutti i comandi a livello di raccolta come `insert` e `find` sono emessi in relazione alle raccolte nel database `test`.

Per visualizzare il database in cui ti trovi o, in altre parole, per impartire comandi, usa il `db` comando nella shell mongo, come segue.

Query:

```
db
```

Output:

```
test
```

Sebbene la connessione predefinita possa trovarsi nell'ambito del database `test`, ciò non significa necessariamente che l'utente associato alla connessione sia autorizzato a eseguire operazioni sul database `test`. Nello scenario di esempio precedente, se esegui l'autenticazione come utente `user3`, che ha il ruolo `readWrite` per il database `sample-database-1`, l'ambito predefinito della connessione è il database `test`. Tuttavia, se tenti di inserire un documento in una raccolta nel database `test`, visualizzerai un messaggio di errore di autorizzazione. Questo perché tale utente non è autorizzato a eseguire tale comando su tale database, come illustrato di seguito.

Query:

```
db
```

Output:

```
test
```

Query:

```
db.col.insert({x:1})
```

Output:

```
WriteCommandError({ "ok" : 0, "code" : 13, "errmsg" : "Authorization failure" })
```

Se modifichi l'ambito della connessione al database `sample-database-1`, puoi scrivere nella raccolta per la quale l'utente dispone della relativa autorizzazione.

Query:

```
use sample-database-1
```

Output:

```
switched to db sample-database-1
```

Query:

```
db.col.insert({x:1})
```

Output:

```
WriteResult({ "nInserted" : 1})
```

Quando esegui l'autenticazione in un cluster con un determinato utente, puoi anche specificare il database nella stringa di connessione. In questo modo viene rimossa la necessità di eseguire il comando `use` dopo che l'utente è stato autenticato nel database `admin`.

La seguente stringa di connessione autentica l'utente in relazione al database `admin`, ma l'ambito della connessione sarà relativo al database `sample-database-1`.

```
mongo "mongodb://user3:abc123@sample-cluster.node.us-east-1.docdb.amazonaws.com:27017/sample-database-2"
```

Comandi comuni

Questa sezione fornisce esempi di comandi comuni che utilizzano il controllo degli accessi basato sui ruoli in Amazon DocumentDB. Devi trovarti nell'ambito del database `admin` per creare e modificare utenti e ruoli. Puoi utilizzare il comando `use admin` per passare al database `admin`.

Note

Modifiche a utenti e ruoli si verificheranno implicitamente nel database `admin`. La creazione di utenti con ruoli con ambito in tutti i database (ad esempio, `readAnyDatabase`) richiede che tu sia nell'ambito del database `admin` (ovvero, `use admin`) durante la creazione dell'utente, oppure devi specificare esplicitamente il database per il ruolo durante la creazione dell'utente (come illustrato nell'esempio 2 in questa sezione).

Esempio 1: creare un utente con `read` ruolo per il database. `foo`

```
db.createUser({user: "readInFooBar", pwd: "abc123", roles: [{role: "read", db: "foo"}]})
```

L'aspetto dell'output di questa operazione è simile al seguente.

```
{
  "user": "readInFooBar",
  "roles": [
    {
      "role": "read",
      "db": "foo"
    }
  ]
}
```

Esempio 2: creare un utente con accesso in lettura su tutti i database.

```
db.createUser({user: "readAllDBs", pwd: "abc123", roles: [{role: "readAnyDatabase", db: "admin"}]})
```

L'aspetto dell'output di questa operazione è simile al seguente.

```
{
  "user": "readAllDBs",
  "roles": [
    {
      "role": "readAnyDatabase",
      "db": "admin"
    }
  ]
}
```

```
]
}
```

Esempio 3: concedere read il ruolo a un utente esistente su un nuovo database.

```
db.grantRolesToUser("readInFooBar", [{role: "read", db: "bar"}])
```

Esempio 4: Aggiornare il ruolo di un utente.

```
db.updateUser("readInFooBar", {roles: [{role: "read", db: "foo"}, {role: "read", db: "baz"}]})
```

Esempio 5: revoca dell'accesso a un database per un utente.

```
db.revokeRolesFromUser("readInFooBar", [{role: "read", db: "baz"}])
```

Esempio 6: descrivi un ruolo integrato.

```
db.getRole("read", {showPrivileges:true})
```

L'aspetto dell'output di questa operazione è simile al seguente.

```
{
  "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"
    ]
  }
]
}
```

Esempio 7: Eliminare un utente dal cluster.

```
db.dropUser("readInFooBar")
```

L'aspetto dell'output di questa operazione è simile al seguente.

```
true
```

Esempio 8: creazione di un ruolo con accesso in lettura e scrittura a una raccolta specifica

```
db.createRole(
{
  role: "collectionRole",
  privileges: [
    {
```

```

        resource: {db: "sample-database-2", collection: "col2"}, actions: ["find",
"update", "insert", "remove"]
    }],
    roles: []
}
)

```

L'aspetto dell'output di questa operazione è simile al seguente.

```

{
  "role":"collectionRole",
  "privileges":[
    {
      "resource":{
        "db":"sample-database-2",
        "collection":"col2"
      },
      "actions":[
        "find",
        "update",
        "insert",
        "remove"
      ]
    }
  ],
  "roles":[]
}

```

Esempio 9: creazione di un utente e assegnazione di un ruolo definito dall'utente

```

db.createUser(
{
  user: "user3",
  pwd: "abc123",
  roles: []
})

db.grantRolesToUser("user3",["collectionRole"])

```

Esempio 10: concedere privilegi aggiuntivi a un ruolo definito dall'utente


```
db.grantPrivilegesToRole(
  "collectionRole",
  [
    {
      resource: { db: "sample-database-1", collection: "col1" },
      actions: ["find", "update", "insert", "remove"]
    }
  ]
)
```

Esempio 11: rimuovere i privilegi da un ruolo definito dall'utente

```
db.revokePrivilegesFromRole(
  "collectionRole",
  [
    {
      resource: { db: "sample-database-1", collection: "col2" },
      actions: ["find", "update", "insert", "remove"]
    }
  ]
)
```

Esempio 12: aggiornamento di un ruolo definito dall'utente esistente

```
db.updateRole(
  "collectionRole",
  {
    privileges: [
      {
        resource: {db: "sample-database-3", collection: "sample-collection-3"},
        actions: ["find", "update", "insert", "remove"]
      }
    ],
    roles: []
  }
)
```

Differenze funzionali

In Amazon DocumentDB, le definizioni degli utenti e dei ruoli vengono archiviate nel `admin` database e gli utenti vengono autenticati tramite il database. `admin` Questa funzionalità differisce da MongoDB Community Edition, ma è coerente con MongoDB Atlas.

Amazon DocumentDB supporta anche i flussi di modifica, che forniscono una sequenza ordinata nel tempo di eventi di modifica che si verificano all'interno delle raccolte del cluster. L'`listChangeStreams` viene applicata a livello di cluster (ovvero su tutti i database) e può essere applicata a livello di database e cluster. `modifyChangeStreams`

Limiti

La tabella seguente contiene i limiti per il controllo degli accessi basato sui ruoli in Amazon DocumentDB.

Descrizione	Limite
Numero di utenti per cluster	1000
Numero di ruoli associati a un utente	1000
Numero di ruoli definiti dall'utente	100
Numero di risorse associate a un privilegio	100

Accesso al database mediante il controllo degli accessi basato sui ruoli

Con il controllo accessi basato sui ruoli, puoi creare un utente e concedere uno o più ruoli per determinare le operazioni che l'utente può eseguire in un database o in un cluster.

Di seguito è riportato un elenco di ruoli integrati attualmente supportati in Amazon DocumentDB.

Note

In Amazon DocumentDB 4.0 e 5.0, i `ListDatabase` comandi `ListCollection` and possono utilizzare facoltativamente i `authorizedDatabases` parametri `authorizedCollections` e per elencare le raccolte e i database a cui l'utente è autorizzato ad accedere richiedendo rispettivamente i `listDatabase` ruoli `listCollections` and. Inoltre, gli utenti ora hanno la possibilità di eliminare i propri cursori senza richiedere il ruolo. `KillCursor`

Database user

Nome ruolo	Descrizione	Azioni
read	Concede a un utente l'accesso in lettura al database specificato.	changeStreams collStats dbStats find killCursors listIndexes listCollections
readWrite	Concede all'utente l'accesso in lettura e scrittura al database specificato.	Tutte le operazioni dalle autorizzazioni read. createCollection dropCollection createIndex dropIndex insert killCursors listIndexes listCollections remove

Nome ruolo	Descrizione	Azioni
		update

Cluster user

Nome ruolo	Descrizione	Azioni
readAnyDatabase	Concede a un utente l'accesso in lettura a tutti i database nel cluster.	Tutte le operazioni dalle autorizzazioni read. listChangeStreams listDatabases
readWriteAnyDatabase	Concede a un utente l'accesso in lettura e scrittura a tutti i database nel cluster.	Tutte le operazioni dalle autorizzazioni readWrite . listChangeStreams listDatabases
userAdminAnyDatabase	Concede a un utente la possibilità di assegnare e modificare i ruoli o i privilegi di un utente al database specificato.	changeCustomData changePassword createUser dropRole dropUser grantRole listDatabases

Nome ruolo	Descrizione	Azioni
		revokeRole viewRole viewUser
dbAdminAnyDatabase	Concede a un utente la possibilità di eseguire ruoli di amministrazione del database su qualsiasi database specificato.	Tutte le operazioni dalle autorizzazioni dbAdmin. dropCollection listDatabases listChangeStreams modifyChangeStreams

Superuser

Nome ruolo	Descrizione	Azioni
root	Concede a un utente l'accesso alle risorse e alle operazioni di tutti i ruoli seguenti combinati: readWriteAnyDatabase , dbAdminAnyDatabase , userAdminAnyDatabase , clusterAdmin , restore e backup.	Tutte le operazioni da readWriteAnyDatabase , dbAdminAnyDatabase , userAdminAnyDatabase , clusterAdmin , restore e backup.

Database administrator

Nome ruolo	Descrizione	Azioni
dbAdmin	Concede a un utente la possibilità di eseguire attività amministrative nel database specifico.	collMod collStats createCollection createIndex dropCollection dropDatabase dropIndex dbStats find killCursors listIndexes listCollections modifyChangeStreams
dbOwner	Concede a un utente la possibilità di eseguire qualsiasi attività amministrativa nel database specificato combinando i ruoli dbAdmin e readWrite .	Tutte le operazioni da dbAdmin e readWrite .

Registrazione e monitoraggio in Amazon DocumentDB

Amazon DocumentDatabase (con compatibilità MongoDB) fornisce una varietà di CloudWatch parametri Amazon che puoi monitorare per determinare lo stato e le prestazioni dei cluster e delle istanze Amazon DocumentDB. Puoi visualizzare le metriche di Amazon DocumentDB utilizzando vari strumenti, tra cui la console Amazon DocumentDBAWS CLI, la CloudWatch console Amazon e l' CloudWatch API. Per ulteriori informazioni sul monitoraggio, consulta [Monitoraggio Amazon DocumentDB](#).

Oltre alle CloudWatch metriche di Amazon, puoi utilizzare il profiler per registrare i tempi di esecuzione e i dettagli delle operazioni eseguite sul tuo cluster. Il profiler è utile per monitorare le operazioni più lente sul cluster per aiutare a migliorare le prestazioni delle singole query e le prestazioni complessive del cluster. Se abilitato, le operazioni vengono registrate su Amazon CloudWatch Logs e puoi utilizzare CloudWatch Insight per analizzare, monitorare e archiviare i dati di profilazione Amazon DocumentDB. Per ulteriori informazioni, consulta [Profilazione delle operazioni di Amazon DocumentDB](#).

Amazon DocumentDB si integra anche conAWS CloudTrail, un servizio che offre un record delle operazioni eseguite da utenti, un ruolo o unAWS servizio in Amazon DocumentDatabase (con compatibilità con MongoDB). CloudTrail acquisisce tutte le chiamateAWS CLI API per Amazon DocumentDB come eventi, incluse le chiamate da Amazon DocumentDBAWS Management Console e dal codice all'SDK di Amazon DocumentDB. Per ulteriori informazioni, consulta [Registrazione delle chiamate API di AmazonAWS CloudTrail](#).

Con Amazon DocumentDB, puoi controllare gli eventi che sono stati eseguiti nel tuo cluster. Sono esempi di eventi registrati i tentativi di autenticazione riusciti e non riusciti, l'eliminazione di una raccolta in un database o la creazione di un indice. Per impostazione predefinita, il controllo è disabilitato su Amazon DocumentDB e richiede l'attivazione di questa funzionalità. Per ulteriori informazioni, consulta [Controllo degli eventi di Amazon DocumentDB](#).

Aggiornamento dei certificati TLS di Amazon DocumentDB

Argomenti

- [Aggiornamento dell'applicazione e del cluster Amazon DocumentDB](#)
- [Risoluzione dei problemi](#)
- [Domande frequenti](#)

Il certificato di autorità di certificazione (CA) per i cluster Amazon DocumentDB verrà aggiornato a partire da agosto 2024. Se utilizzi cluster Amazon DocumentDB con Transport Layer Security (TLS) abilitato (impostazione predefinita) e non hai ruotato i certificati dell'applicazione client e del server, sono necessari i seguenti passaggi per mitigare i problemi di connettività tra l'applicazione e i cluster Amazon DocumentDB.

- [Fase 1: Scaricare il nuovo certificato CA e aggiornare l'applicazione](#)
- [Fase 2: Aggiornare il certificato del server](#)

I certificati CA e server sono stati aggiornati come parte delle best practice standard di manutenzione e sicurezza per Amazon DocumentDB. Le applicazioni client devono aggiungere i nuovi certificati CA ai propri trust store e le istanze Amazon DocumentDB esistenti devono essere aggiornate per utilizzare i nuovi certificati CA prima di questa data di scadenza.

Aggiornamento dell'applicazione e del cluster Amazon DocumentDB

Attenersi alla procedura descritta in questa sezione per aggiornare il bundle di certificati CA dell'applicazione ([Fase 1](#)) e i certificati server del cluster ([Fase 2](#)). Prima di applicare le modifiche agli ambienti di produzione, si consiglia di testare questi passaggi in un ambiente di sviluppo o di gestione temporanea.

Note

È necessario completare i passaggi 1 e 2 Regione AWS in ognuno dei quali sono presenti cluster Amazon DocumentDB.

Fase 1: Scaricare il nuovo certificato CA e aggiornare l'applicazione

Scarica il nuovo certificato CA e aggiorna la tua applicazione per utilizzare il nuovo certificato CA per creare connessioni TLS ad Amazon DocumentDB. Scaricare il nuovo bundle di certificati CA da <https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem>. Questa operazione scarica un file denominato `global-bundle.pem`.

Note

Se accedi al keystore che contiene sia il vecchio certificato CA (`rds-ca-2019-root.pem`) che i nuovi certificati CA (`rds-ca-rsa2048-g1`, `rds-ca-rsa4096-g1`), verifica che il keystore selezioni `global-bundle`

```
wget https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem
```

Successivamente, aggiornare le applicazioni per utilizzare il nuovo bundle di certificati. Il nuovo pacchetto CA contiene sia il vecchio certificato CA (`rds-ca-2019`) che i nuovi certificati CA (`2048-g1`, `4096-g1`). `rds-ca-rsa` `rds-ca-rsa` La presenza di entrambi i certificati CA nel nuovo bundle CA consente di aggiornare l'applicazione e il cluster in due fasi.

Per verificare che l'applicazione utilizzi il bundle di certificati CA più recente, consulta [Come posso essere sicuro di utilizzare il bundle CA più recente?](#). Se già utilizzi il bundle di certificati CA più recente nell'applicazione, puoi passare alla fase 2.

Per esempi di utilizzo di un bundle CA con l'applicazione, consulta [Crittografia dei dati in transito e Connessione con TLS abilitato](#).

Note

Attualmente, MongoDB Go Driver 1.2.1 accetta solo un certificato del server emesso da una CA in `sslcertificateauthorityfile`. Consulta [Connessione con TLS abilitato](#) per la connessione ad Amazon DocumentDB utilizzando Go quando TLS è abilitato.

Fase 2: Aggiornare il certificato del server

Dopo che l'applicazione è stata aggiornata per utilizzare il nuovo pacchetto CA, il passaggio successivo consiste nell'aggiornare il certificato del server modificando ogni istanza in un cluster Amazon DocumentDB. Per modificare le istanze per utilizzare il nuovo certificato server, vedere le istruzioni riportate di seguito.

Amazon DocumentDB fornisce le seguenti CA per firmare il certificato del server DB per un'istanza DB:

- `rds-ca-rsa2048-g1`: utilizza un'autorità di certificazione con algoritmo a chiave privata RSA 2048 e algoritmo di firma SHA256 nella maggior parte delle regioni. AWS supporta la rotazione automatica dei certificati del server.
- `rds-ca-rsa4096-g1`: utilizza un'autorità di certificazione con algoritmo a chiave privata RSA 4096 e algoritmo di firma SHA384. supporta la rotazione automatica dei certificati del server.

Note

Se si utilizza la AWS CLI, è possibile visualizzare le validità delle autorità di certificazione elencate in precedenza utilizzando [describe-certificates](#).

Questi certificati CA sono inclusi nel bundle di certificati regionali e globali. Quando utilizzi la CA `rds-ca-rsa 2048-g1` o `rds-ca-rsa 4096-g1` con un database, Amazon DocumentDB gestisce il certificato del server DB sul database. Amazon DocumentDB ruota automaticamente il certificato del server DB prima della scadenza (potrebbe essere necessario il riavvio).

Note

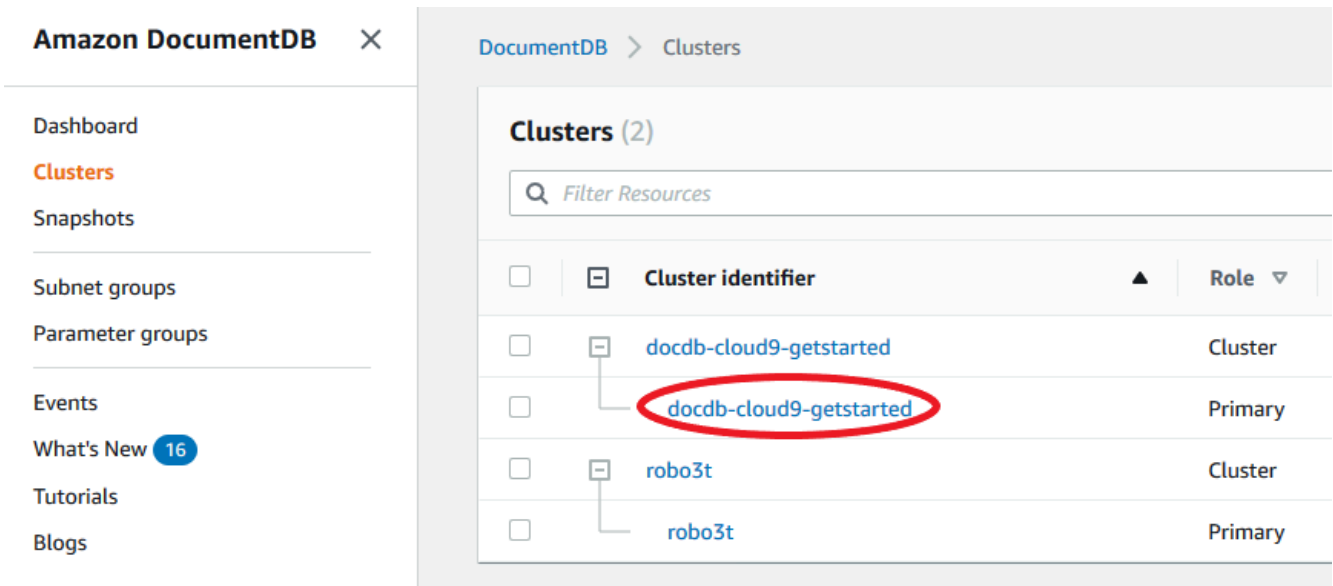
L'aggiornamento delle istanze richiede un riavvio, che potrebbe causare interruzioni del servizio. Prima di aggiornare il certificato del server, assicurati di aver completato la [fase 1](#).

Using the AWS Management Console

Completa i seguenti passaggi per identificare e ruotare il vecchio certificato del server per le tue istanze Amazon DocumentDB esistenti utilizzando il. AWS Management Console

1. [Accedi a e apri AWS Management Console la console Amazon DocumentDB all'indirizzo `https://console.aws.amazon.com/docdb`.](https://console.aws.amazon.com/docdb)
2. Nell'elenco delle regioni nell'angolo in alto a destra dello schermo, scegli quella Regione AWS in cui risiedono i tuoi cluster.
3. Nel riquadro di navigazione sul lato sinistro della console, scegli Cluster.
4. Potrebbe essere necessario identificare quali istanze sono ancora presenti nel vecchio certificato del server (`rds-ca-2019`). Puoi farlo nella colonna Autorità di certificazione che si trova all'estrema destra della tabella Cluster.

- Nella tabella Cluster, vedrai la colonna Cluster identifier all'estrema sinistra. Le tue istanze sono elencate in cluster, in modo simile alla schermata seguente.



- Seleziona la casella a sinistra dell'istanza che ti interessa.
- Scegliere Actions (Operazioni), quindi Modify (Modifica).
- In Certificate authority (Autorità di certificazione), selezionare il nuovo certificato del server (ad esempio `rds-ca-rsa2048-g1`) per questa istanza.
- È possibile visualizzare un riepilogo delle modifiche nella pagina successiva. Considera che è presente un avviso aggiuntivo per ricordare di assicurarsi che l'applicazione stia utilizzando il bundle CA più recente del certificato prima di modificare l'istanza per evitare di causare un'interruzione della connettività.
- Puoi scegliere di applicare la modifica durante la prossima finestra di manutenzione o applicarla immediatamente. Se si intende modificare immediatamente il certificato del server, utilizzare l'opzione Apply Immediately (Applica immediatamente).
- Scegliere Modify instance (Modifica istanza) per completare l'aggiornamento.

Using the AWS CLI

Completa i seguenti passaggi per identificare e ruotare il vecchio certificato del server per le tue istanze Amazon DocumentDB esistenti utilizzando il. AWS CLI

- Per modificare immediatamente le istanze, eseguire il comando seguente per ogni istanza del cluster.

```
aws docdb modify-db-instance --db-instance-identifier <yourInstanceIdentifier>
--ca-certificate-identifier rds-ca-rsa2048-g1 --apply-immediately
```

2. Per modificare le istanze del cluster in modo da utilizzare il nuovo certificato CA durante la successiva finestra di manutenzione del cluster, eseguire il comando seguente per ogni istanza del cluster.

```
aws docdb modify-db-instance --db-instance-identifier <yourInstanceIdentifier>
--ca-certificate-identifier rds-ca-rsa2048-g1 --no-apply-immediately
```

Risoluzione dei problemi

Se si verificano problemi di connessione al cluster durante la rotazione dei certificati, si consiglia di eseguire quanto segue:

- Riavviare le istanze. La rotazione del nuovo certificato richiede il riavvio di ciascuna delle istanze. Se il nuovo certificato è stato applicato a una o più istanze ma le stesse non sono state riavviate, riavviare le istanze per applicare il nuovo certificato. Per ulteriori informazioni, consulta [Riavvio di un'istanza Amazon DocumentDB](#).
- Verificare che i client stiano utilizzando il pacchetto di certificati più recente. Per informazioni, consulta [Come posso essere sicuro di utilizzare il bundle CA più recente?](#).
- Verificare che le istanze stiano utilizzando il certificato più recente. Per informazioni, consulta [Come faccio a sapere quali delle mie istanze Amazon DocumentDB utilizzano il vecchio/nuovo certificato del server?](#).
- Verificare che l'applicazione utilizzi il certificato CA più recente. Alcuni driver, come Java e Go, richiedono un codice aggiuntivo per importare più certificati da un bundle di certificati nell'archivio attendibile. Per ulteriori informazioni sulla connessione ad Amazon DocumentDB con TLS, consulta [Connessione programmatica ad Amazon DocumentDB](#).
- Contatta l'assistenza. Se avete domande o problemi, contattateci [AWS Support](#).

Domande frequenti

Di seguito sono riportate le risposte ad alcune domande comuni sui certificati TLS.

Cosa succede se ho domande o problemi?

Se avete domande o problemi, contattateci [AWS Support](#).

Come faccio a sapere se sto usando TLS per connettermi al mio cluster Amazon DocumentDB?

È possibile stabilire se il cluster utilizza TLS esaminando il parametro `tls` per il gruppo di parametri cluster del cluster. Se il parametro `tls` è impostato su `enabled`, si utilizza il certificato TLS per connettersi al cluster. Per ulteriori informazioni, consulta [Gestione dei gruppi di parametri del cluster Amazon DocumentDB](#).

Perché si aggiornano i certificati CA e server?

I certificati CA e server di Amazon DocumentDB vengono aggiornati come parte delle best practice standard di manutenzione e sicurezza per Amazon DocumentDB. Gli attuali certificati CA e server scadono a partire da agosto 2024.

Cosa succede se non intraprendo alcuna azione entro la data di scadenza?

Se utilizzi TLS per connetterti al tuo cluster Amazon DocumentDB e non apporti la modifica del certificato le applicazioni che si connettono tramite TLS non saranno più in grado di comunicare con il cluster Amazon DocumentDB.

Amazon DocumentDB non ruoterà automaticamente i certificati del database prima della scadenza. È necessario aggiornare le applicazioni e i cluster per utilizzare i nuovi certificati CA prima o dopo la data di scadenza.

Come faccio a sapere quali delle mie istanze Amazon DocumentDB utilizzano il vecchio/nuovo certificato del server?

Per identificare le istanze di Amazon DocumentDB che utilizzano ancora il vecchio certificato del server, puoi utilizzare Amazon DocumentDB o il. AWS Management Console AWS CLI

Utilizzo di AWS Management Console

Per identificare le istanze nei cluster che utilizzano il certificato precedente

1. [Accedi a e apri AWS Management Console la console Amazon DocumentDB all'indirizzo `https://console.aws.amazon.com/docdb`](https://console.aws.amazon.com/docdb).

2. Nell'elenco delle regioni nell'angolo in alto a destra dello schermo, scegli quella Regione AWS in cui risiedono le tue istanze.
3. Nel riquadro di navigazione sul lato sinistro della console, scegli Cluster.
4. La colonna Autorità di certificazione (all'estrema destra della tabella) mostra quali istanze sono ancora presenti nel vecchio certificato del server (`rds-ca-2019`) e nel nuovo certificato del server (`rds-ca-rsa2048-g1`).

Utilizzo di AWS CLI

Per identificare le istanze nei cluster che utilizzano il certificato del server precedente, utilizzare il comando `describe-db-clusters` con quanto riportato di seguito.

```
aws docdb describe-db-instances \  
  --filters Name=engine,Values=docdb \  
  --query 'DBInstances[*].  
{CertificateVersion:CACertificateIdentifier,InstanceID:DBInstanceIdentifier}'
```

Come posso modificare singole istanze nel mio cluster Amazon DocumentDB per aggiornare il certificato del server?

Consigliamo di aggiornare contemporaneamente i certificati server per tutte le istanze di un determinato cluster. Per modificare le istanze nel cluster, è possibile utilizzare la console o l'AWS CLI.

Note

L'aggiornamento delle istanze richiede un riavvio, che potrebbe causare interruzioni del servizio. Prima di aggiornare il certificato del server, assicurati di aver completato la [fase 1](#).

Utilizzo di AWS Management Console

1. [Accedi a e apri AWS Management Console la console Amazon DocumentDB all'indirizzo https://console.aws.amazon.com/docdb.](https://console.aws.amazon.com/docdb)
2. Nell'elenco delle regioni nell'angolo in alto a destra dello schermo, scegli quella Regione AWS in cui risiedono i tuoi cluster.

3. Nel riquadro di navigazione sul lato sinistro della console, scegli Cluster.
4. La colonna Autorità di certificazione (all'estrema destra della tabella) mostra quali istanze si trovano ancora nel vecchio certificato del server (`rds-ca-2019`).
5. Nella tabella Cluster, in Cluster identifier, selezionate un'istanza da modificare.
6. Scegliere Actions (Operazioni), quindi Modify (Modifica).
7. In Certificate authority (Autorità di certificazione), selezionare il nuovo certificato del server (ad esempio `rds-ca-rsa2048-g1`) per questa istanza.
8. È possibile visualizzare un riepilogo delle modifiche nella pagina successiva. Considera che è presente un avviso aggiuntivo per ricordare di assicurarsi che l'applicazione stia utilizzando il bundle CA più recente del certificato prima di modificare l'istanza per evitare di causare un'interruzione della connettività.
9. Puoi scegliere di applicare la modifica durante la prossima finestra di manutenzione o applicarla immediatamente.
10. Scegliere Modify instance (Modifica istanza) per completare l'aggiornamento.

Utilizzo di AWS CLI

Completa i seguenti passaggi per identificare e ruotare il vecchio certificato del server per le tue istanze Amazon DocumentDB esistenti utilizzando il AWS CLI

1. Per modificare immediatamente le istanze, eseguire il comando seguente per ogni istanza del cluster.

```
aws docdb modify-db-instance --db-instance-identifier <yourInstanceIdentifier> --ca-certificate-identifier rds-ca-rsa2048-g1 --apply-immediately
```

2. Per modificare le istanze del cluster in modo da utilizzare il nuovo certificato CA durante la successiva finestra di manutenzione del cluster, eseguire il comando seguente per ogni istanza del cluster.

```
aws docdb modify-db-instance --db-instance-identifier <yourInstanceIdentifier> --ca-certificate-identifier rds-ca-rsa2048-g1 --no-apply-immediately
```

Cosa succede se si aggiunge una nuova istanza a un cluster esistente?

Tutte le nuove istanze create utilizzano il vecchio certificato server e richiedono connessioni TLS utilizzando il vecchio certificato CA. Tutte le nuove istanze di Amazon DocumentDB create dopo il 25 gennaio 2024 utilizzeranno per impostazione predefinita il nuovo certificato 2048-g1. rds-ca-rsa

Cosa succede se nel cluster è presente una sostituzione o un failover di istanza?

Se nel cluster è presente una sostituzione di istanza, la nuova istanza creata continua a utilizzare lo stesso certificato server utilizzato in precedenza dall'istanza. Si consiglia di aggiornare contemporaneamente i certificati server per tutte le istanze. Se si verifica un failover nel cluster, viene utilizzato il certificato server sul nuovo primario.

Se non si utilizza TLS per connettersi al cluster, è comunque necessario aggiornare ciascuna delle istanze?

Se non utilizzi TLS per connetterti ai cluster Amazon DocumentDB, non è necessaria alcuna azione.

Se attualmente non uso TLS per connettermi al cluster ma ho intenzione di farlo in futuro, cosa devo fare?

Se hai creato un cluster prima di gennaio 2024, segui i [passaggi 1](#) e [2](#) nella sezione precedente per assicurarti che l'applicazione utilizzi il pacchetto CA aggiornato e che ogni istanza di Amazon DocumentDB utilizzi il certificato server più recente. Se crei un cluster dopo il 25 gennaio 2024, il cluster disporrà già del certificato server più recente (2048-g1). rds-ca-rsa Per verificare che l'applicazione utilizzi il bundle di certificati CA più recente, consulta [Se non si utilizza TLS per connettersi al cluster, è comunque necessario aggiornare ciascuna delle istanze?](#).

La scadenza può essere prorogata oltre agosto 2024?

Se le candidature si connettono tramite TLS, la scadenza non può essere prorogata.

Come posso essere sicuro di utilizzare il bundle CA più recente?

Per verificare di disporre del pacchetto più recente, utilizzate il seguente comando. Per eseguire questo comando, dovete avere installato java e gli strumenti java devono essere nella variabile PATH della shell. Per ulteriori informazioni, consultate [Uso di Java](#)

macOS e Amazon Linux

```
keytool -printcert -v -file global-bundle.pem
```


Windows

```
keytool -printcert -v -file global-bundle.p7b
```

Perché viene visualizzato «RDS» nel nome del bundle CA?

Per alcune funzionalità di gestione, come la gestione dei certificati, Amazon DocumentDB utilizza una tecnologia operativa condivisa con Amazon Relational Database Service (Amazon RDS).

Quando scadrà il nuovo certificato?

Il nuovo certificato del server scadrà (in genere) come segue:

- rds-ca-rsa2048-g1: scade nel 2061
- rds-ca-rsa4096-g1 — Scade il 2121

Se è stato applicato il nuovo certificato server, è possibile ripristinare il vecchio certificato?

Se è necessario ripristinare un'istanza al certificato server precedente, consigliamo di farlo per tutte le istanze del cluster. È possibile ripristinare il certificato del server per ogni istanza in un cluster utilizzando la AWS Management Console o l'AWS CLI.

Utilizzo di AWS Management Console

1. [Accedi a e apri AWS Management Console la console Amazon DocumentDB all'indirizzo https://console.aws.amazon.com/docdb.](https://console.aws.amazon.com/docdb)
2. Nell'elenco delle regioni nell'angolo in alto a destra dello schermo, scegli quella Regione AWS in cui risiedono i tuoi cluster.
3. Nel riquadro di navigazione sul lato sinistro della console, scegli Cluster.
4. Nella tabella Cluster, in Identificatore cluster, seleziona un'istanza da modificare. Scegli Actions (Operazioni), quindi Modify (Modifica).
5. In Certificate authority (Autorità di certificazione), è possibile selezionare il vecchio certificato del server (rds-ca-2019).
6. Scegliere Continue (Continua) per visualizzare un riepilogo delle modifiche.

7. In questa pagina, è possibile scegliere di pianificare le modifiche da applicare nella finestra di manutenzione successiva o di applicare le modifiche immediatamente. Effettuare la selezione e scegliere Modify instance (Modifica istanza).

Note

Se si sceglie di applicare le modifiche immediatamente, anche tutte le modifiche incluse nella coda delle modifiche in sospeso saranno applicate. Se nessuna delle modifiche in sospeso richiede tempi di inattività, la scelta di applicarle può provocare tempi di inattività imprevisti.

Utilizzo di AWS CLI

```
aws docdb modify-db-instance --db-instance-identifier <db_instance_name> ca-  
certificate-identifier rds-ca-2019 <--apply-immediately | --no-apply-immediately>
```

Se si sceglie `--no-apply-immediately`, la modifica verrà applicata durante la prossima finestra di manutenzione del cluster.

Se ripristino da uno snapshot o un da un momento specifico, sarà disponibile il nuovo certificato del server?

Se ripristini un'istantanea o esegui un point-in-time ripristino dopo agosto 2024, il nuovo cluster creato utilizzerà il nuovo certificato CA.

Cosa succede se ho problemi a connettermi direttamente al mio cluster Amazon DocumentDB da qualsiasi sistema operativo Mac?

Mac OS ha aggiornato i requisiti per i certificati affidabili. I certificati affidabili devono ora essere validi per 397 giorni o meno (vedi <https://support.apple.com/en-us/HT211025>).

Note

Questa restrizione viene rispettata nelle versioni più recenti di Mac OS.

I certificati di istanza Amazon DocumentDB sono validi per oltre quattro anni, più a lungo del limite massimo consentito per Mac OS. Per connetterti direttamente a un cluster Amazon DocumentDB da

un computer con sistema operativo Mac OS, devi consentire certificati non validi durante la creazione della connessione TLS. In questo caso, i certificati non validi indicano che il periodo di validità è superiore a 397 giorni. È necessario comprendere i rischi prima di consentire certificati non validi durante la connessione al cluster Amazon DocumentDB.

Per connetterti a un cluster Amazon DocumentDB da Mac OS utilizzando ilAWS CLI, usa il `tlsAllowInvalidCertificates` parametro.

```
mongo --tls --host <hostname> --username <username> --password <password> --port 27017  
--tlsAllowInvalidCertificates
```

Aggiornamento dei certificati TLS Amazon DocumentDB — GovCloud (Stati Uniti occidentali)

Note

Queste informazioni si applicano solo agli utenti nella regione GovCloud (Stati Uniti occidentali).

Il certificato dell'autorità di certificazione (CA) per i cluster Amazon DocumentDB (con compatibilità MongoDB) verrà aggiornato il 18 maggio 2022. Se utilizzi cluster Amazon DocumentDB con Transport Layer Security (TLS) abilitato (impostazione predefinita) e non hai ruotato i certificati dell'applicazione client e del server, sono necessari i seguenti passaggi per mitigare i problemi di connettività tra l'applicazione e i cluster Amazon DocumentDB.

- [Fase 1: Scaricare il nuovo certificato CA e aggiornare l'applicazione](#)
- [Fase 2: Aggiornare il certificato del server](#)

I certificati CA e server sono stati aggiornati come parte delle best practice standard di manutenzione e sicurezza per Amazon DocumentDB. Il precedente certificato CA scadrà il 18 maggio 2022. Le applicazioni client devono aggiungere i nuovi certificati CA ai propri trust store e le istanze Amazon DocumentDB esistenti devono essere aggiornate per utilizzare i nuovi certificati CA prima di questa data di scadenza.

Aggiornamento dell'applicazione e del cluster Amazon DocumentDB

Attenersi alla procedura descritta in questa sezione per aggiornare il bundle di certificati CA dell'applicazione ([Fase 1](#)) e i certificati server del cluster ([Fase 2](#)). Prima di applicare le modifiche agli ambienti di produzione, si consiglia di testare questi passaggi in un ambiente di sviluppo o di gestione temporanea.

Note

È necessario completare i passaggi 1 e 2 Regione AWS in ognuno dei quali sono presenti cluster Amazon DocumentDB.

Fase 1: Scaricare il nuovo certificato CA e aggiornare l'applicazione

Scarica il nuovo certificato CA e aggiorna l'applicazione per utilizzare il nuovo certificato CA per creare connessioni TLS ad Amazon DocumentDB. Scaricare il nuovo bundle di certificati CA da <https://truststore.pki.us-gov-west-1.rds.amazonaws.com/us-gov-west-1/us-gov-west-1-bundle.pem>. Questa operazione scarica un file denominato `us-gov-west-1-bundle.pem`.

Note

Se si accede al keystore che contiene sia il vecchio certificato CA (`rds-ca-2017-root.pem`) che il nuovo certificato CA (`rds-ca-rsa4096-g1.pem`), verificare che il keystore selezioni `CA-RSA4096-G1`.

```
wget https://truststore.pki.us-gov-west-1.rds.amazonaws.com/us-gov-west-1/us-gov-west-1-bundle.pem
```

Successivamente, aggiornare le applicazioni per utilizzare il nuovo bundle di certificati. Il nuovo pacchetto CA contiene sia il vecchio certificato CA che il nuovo certificato CA (`rds-ca-rsa4096-g1.pem`). La presenza di entrambi i certificati CA nel nuovo bundle CA consente di aggiornare l'applicazione e il cluster in due fasi.

Qualsiasi download del pacchetto di certificati CA dopo il 21 dicembre 2021 deve utilizzare il nuovo pacchetto di certificati CA. Per verificare che l'applicazione utilizzi il bundle di certificati CA più

recente, consulta [Come posso essere sicuro di utilizzare il bundle CA più recente?](#). Se già utilizzi il bundle di certificati CA più recente nell'applicazione, puoi passare alla fase 2.

Per esempi di utilizzo di un bundle CA con l'applicazione, consulta [Crittografia dei dati in transito](#) e [Connessione con TLS abilitato](#).

Note

Attualmente, MongoDB Go Driver 1.2.1 accetta solo un certificato del server emesso da una CA in `sslcertificateauthorityfile`. Consulta [Connessione con TLS abilitato](#) per la connessione ad Amazon DocumentDB utilizzando Go quando TLS è abilitato.

Fase 2: Aggiornare il certificato del server

Dopo l'aggiornamento dell'applicazione per utilizzare il nuovo pacchetto CA, il passaggio successivo consiste nell'aggiornare il certificato del server modificando ogni istanza in un cluster Amazon DocumentDB. Per modificare le istanze per utilizzare il nuovo certificato server, vedere le istruzioni riportate di seguito.

Note

L'aggiornamento delle istanze richiede un riavvio, che potrebbe causare interruzioni del servizio. Prima di aggiornare il certificato del server, assicurati di aver completato la [fase 1](#).

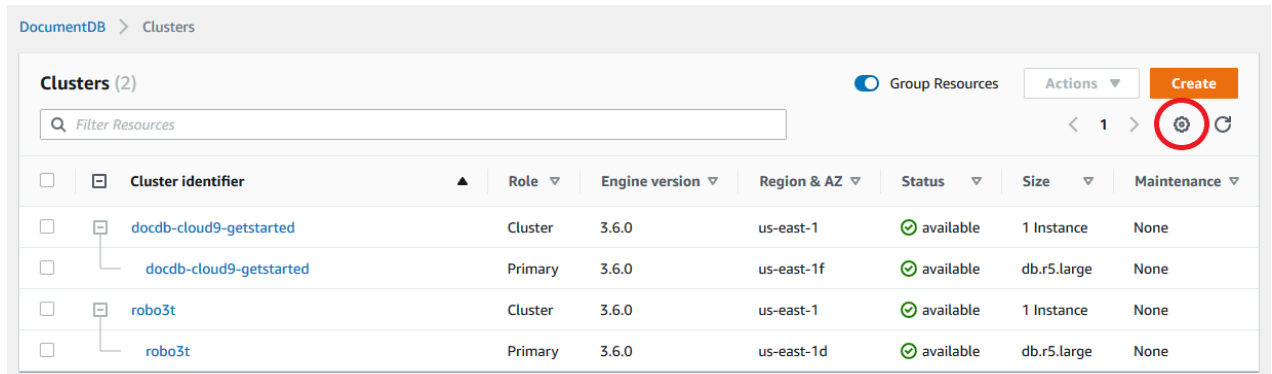
Using the AWS Management Console

Completa i seguenti passaggi per identificare e ruotare il vecchio certificato del server per le istanze Amazon DocumentDB esistenti utilizzando ilAWS Management Console.

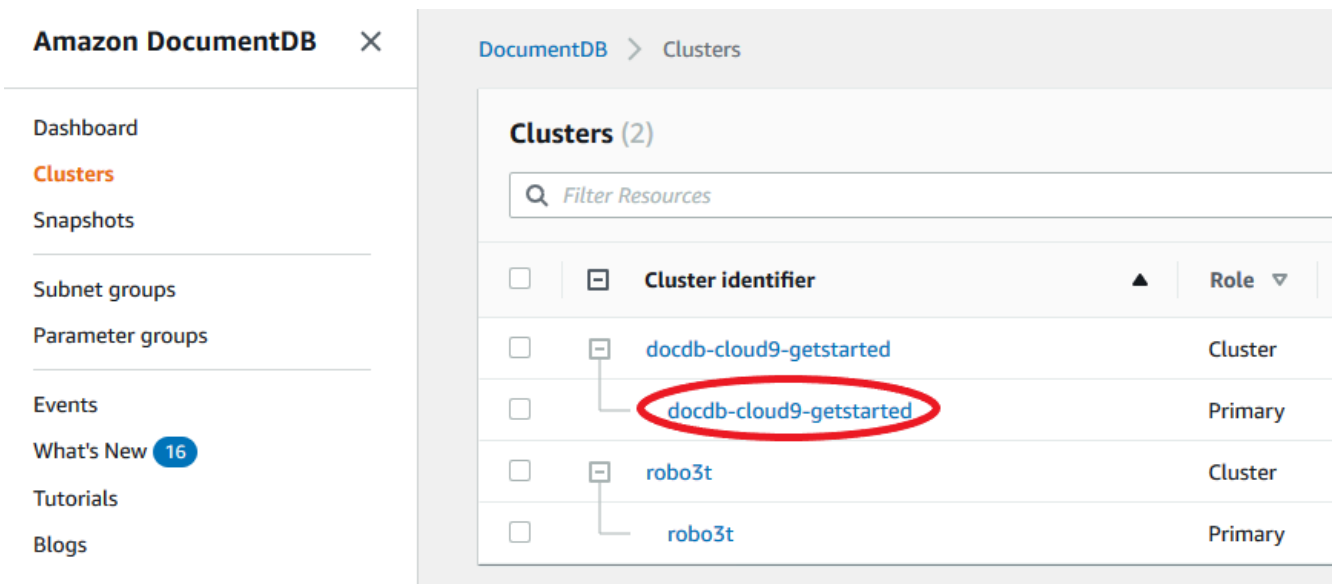
1. Accedi alla e apri laAWS Management Console la ri ri Amazon DocumentDB all'[indirizzo https://console.aws.amazon.com/docdb](https://console.aws.amazon.com/docdb).
2. Nell'elenco delle regioni nell'angolo in alto a destra dello schermo, seleziona laRegione AWS in cui si trovano i cluster.
3. chi

Nel riquadro di navigazione sul lato sinistro della console, seleziona Cluster.

4. Potrebbe essere necessario identificare quali istanze sono ancora presenti nel vecchio certificato del server (`rds-ca-2017`). Puoi farlo nella colonna Autorità di certificazione, nascosta per impostazione predefinita. Per visualizzare la colonna Certificate authority column (Autorità di certificazione) effettuare le operazioni seguenti:
 - a. Selezionare l'icona Settings (Impostazioni).



- b. Nell'elenco delle colonne visibili, scegliere la colonna Certificate authority (Autorità di certificazione).
 - c. Quindi scegliere Confirm (Conferma) per salvare le modifiche.
5. Ora, di nuovo nella casella di navigazione Cluster, vedrai la colonna Cluster Identifier. Le tue istanze sono elencate in cluster, in modo simile alla schermata seguente.



6. Seleziona la casella a sinistra dell'istanza che ti interessa.
7. Scegliere Actions (Operazioni), quindi Modify (Modifica).
8. In Certificate authority (Autorità di certificazione), selezionare il nuovo certificato del server (ad esempio `rds-ca-rsa4096-g1`) per questa istanza.

9. È possibile visualizzare un riepilogo delle modifiche nella pagina successiva. Considera che è presente un avviso aggiuntivo per ricordare di assicurarsi che l'applicazione stia utilizzando il bundle CA più recente del certificato prima di modificare l'istanza per evitare di causare un'interruzione della connettività.
10. Puoi scegliere di applicare la modifica durante la prossima finestra di manutenzione o applicarla immediatamente. Se si intende modificare immediatamente il certificato del server, utilizzare l'opzione Apply Immediately (Applica immediatamente) .
11. Scegliere Modify instance (Modifica istanza) per completare l'aggiornamento.

Using the AWS CLI

Completa i seguenti passaggi per identificare e ruotare il vecchio certificato del server per le istanze Amazon DocumentDB esistenti utilizzando ilAWS CLI.

1. Per modificare immediatamente le istanze, eseguire il comando seguente per ogni istanza del cluster.

```
aws docdb modify-db-instance --db-instance-identifier <yourInstanceIdentifier>
--ca-certificate-identifier rds-ca-rsa4096-g1 --apply-immediately
```

2. Per modificare le istanze del cluster in modo da utilizzare il nuovo certificato CA durante la successiva finestra di manutenzione del cluster, eseguire il comando seguente per ogni istanza del cluster.

```
aws docdb modify-db-instance --db-instance-identifier <yourInstanceIdentifier>
--ca-certificate-identifier rds-ca-rsa4096-g1 --no-apply-immediately
```

Risoluzione dei problemi

Se si verificano problemi di connessione al cluster durante la rotazione dei certificati, si consiglia di eseguire quanto segue:

- Riavviare le istanze. La rotazione del nuovo certificato richiede il riavvio di ciascuna delle istanze. Se il nuovo certificato è stato applicato a una o più istanze ma le stesse non sono state riavviate, riavviare le istanze per applicare il nuovo certificato. Per ulteriori informazioni, consulta [Riavvio di un'istanza Amazon DocumentDB](#).

- Verificare che i client stiano utilizzando il pacchetto di certificati più recente. Consultare [Come posso essere sicuro di utilizzare il bundle CA più recente?](#).
- Verificare che le istanze stiano utilizzando il certificato più recente. Consultare [Come faccio a sapere quali delle mie istanze Amazon DocumentDB utilizzano il vecchio o il nuovo certificato del server?](#).
- Verificare che l'applicazione utilizzi il certificato CA più recente. Alcuni driver, come Java e Go, richiedono un codice aggiuntivo per importare più certificati da un bundle di certificati nell'archivio attendibile. Per ulteriori informazioni sulla connessione ad Amazon DocumentDB con il protocollo TLS, consulta [Connessione programmatica ad Amazon DocumentDB](#).
- Contatta l'assistenza. In caso di domande o problemi, contattaci [AWS Support](#).

Domande frequenti

Di seguito sono riportate le risposte ad alcune domande comuni sui certificati TLS.

Cosa succede se ho domande o problemi?

In caso di domande o problemi, contattaci [AWS Support](#).

Come faccio a sapere se sto usando TLS per connettermi al mio cluster Amazon DocumentDB?

È possibile stabilire se il cluster utilizza TLS esaminando il parametro `tls` per il gruppo di parametri cluster del cluster. Se il parametro `tls` è impostato su `enabled`, si utilizza il certificato TLS per connettersi al cluster. Per ulteriori informazioni, consulta [Gestione dei gruppi di parametri del cluster Amazon DocumentDB](#).

Perché si aggiornano i certificati CA e server?

I certificati CA e server di Amazon DocumentDB sono stati aggiornati come parte delle best practice standard di manutenzione e sicurezza per Amazon DocumentDB. Gli attuali certificati CA e server scadranno mercoledì 18 maggio 2022.

Cosa succede se non eseguo alcuna azione entro la data di scadenza?

Se utilizzi TLS per connetterti al tuo cluster Amazon DocumentDB e non apporti la modifica entro il 18 maggio 2022, le tue applicazioni che si connettono tramite TLS non saranno più in grado di comunicare con il cluster Amazon DocumentDB.

Amazon DocumentDB non ruoterà automaticamente i certificati del database prima della scadenza. È necessario aggiornare le applicazioni e i cluster per utilizzare i nuovi certificati CA prima o dopo la data di scadenza.

Come faccio a sapere quali delle mie istanze Amazon DocumentDB utilizzano il vecchio o il nuovo certificato del server?

Per identificare le istanze di Amazon DocumentDB che utilizzano ancora il vecchio certificato del server, puoi utilizzare Amazon DocumentDBAWS Management Console o ilAWS CLI.

Utilizzo di AWS Management Console

Per identificare le istanze nei cluster che utilizzano il certificato precedente

1. Accedi alla e apri laAWS Management Console la ri ri Amazon DocumentDB all'[indirizzo https://console.aws.amazon.com/docdb](https://console.aws.amazon.com/docdb).
2. Nell'elenco delle regioni nell'angolo in alto a destra dello schermo, seleziona la regioneRegione AWS in cui si trovano le istanze.
3. Nel riquadro di navigazione sul lato sinistro della console scegliere Instances (Istanze).
4. La colonna Certificate authority (Autorità di certificazione) (nascosta per impostazione predefinita) mostra quali istanze sono ancora sul vecchio certificato del server (ad esempio rds-ca-2017) e sul nuovo certificato del server (rds-ca-rsa4096-g1). Per visualizzare la colonna Certificate authority column (Autorità di certificazione) effettuare le operazioni seguenti:
 - a. Selezionare l'icona Settings (Impostazioni).
 - b. Nell'elenco delle colonne visibili, scegliere la colonna Certificate authority (Autorità di certificazione).
 - c. Quindi scegliere Confirm (Conferma) per salvare le modifiche.

Utilizzo di AWS CLI

Per identificare le istanze nei cluster che utilizzano il certificato del server precedente, utilizzare il comando `describe-db-clusters` con quanto riportato di seguito.

```
aws docdb describe-db-instances \
  --filters Name=engine,Values=docdb \
  --query 'DBInstances[*].
{CertificateVersion:CACertificateIdentifier,InstanceID:DBInstanceIdentifier}'
```

Come posso modificare le singole istanze nel mio cluster Amazon DocumentDB per aggiornare il certificato del server?

Consigliamo di aggiornare contemporaneamente i certificati server per tutte le istanze di un determinato cluster. Per modificare le istanze nel cluster, è possibile utilizzare la console o l'AWS CLI.

Note

L'aggiornamento delle istanze richiede un riavvio, che potrebbe causare interruzioni del servizio. Prima di aggiornare il certificato del server, assicurati di aver completato la [fase 1](#).

Utilizzo di AWS Management Console

1. Accedi alla e apri laAWS Management Console la ri ri Amazon DocumentDB all'[indirizzo https://console.aws.amazon.com/docdb](https://console.aws.amazon.com/docdb).
2. Nell'elenco delle regioni nell'angolo in alto a destra dello schermo, seleziona laRegione AWS in cui si trovano i cluster.
3. Nel riquadro di navigazione sul lato sinistro della console scegliere Instances (Istanze).
4. La colonna Certificate authority (Autorità di certificazione) (nascosta per impostazione predefinita) mostra quali istanze sono ancora sul vecchio certificato server (rds-ca-2017). Per visualizzare la colonna Certificate authority column (Autorità di certificazione) effettuare le operazioni seguenti:
 - a. Selezionare l'icona Settings (Impostazioni).
 - b. Nell'elenco delle colonne visibili, scegliere la colonna Certificate authority (Autorità di certificazione).
 - c. Quindi scegliere Confirm (Conferma) per salvare le modifiche.
5. Selezionare un'istanza da modificare.
6. Scegliere Actions (Operazioni), quindi Modify (Modifica).
7. In Autorità di certificazione, seleziona il nuovo certificato del server (rds-ca-rsa4096-g1) per questa istanza.

- È possibile visualizzare un riepilogo delle modifiche nella pagina successiva. Considera che è presente un avviso aggiuntivo per ricordare di assicurarsi che l'applicazione stia utilizzando il bundle CA più recente del certificato prima di modificare l'istanza per evitare di causare un'interruzione della connettività.
- Puoi scegliere di applicare la modifica durante la prossima finestra di manutenzione o applicarla immediatamente.
- Scegliere Modify instance (Modifica istanza) per completare l'aggiornamento.

Utilizzo di AWS CLI

Completa i seguenti passaggi per identificare e ruotare il vecchio certificato del server per le istanze Amazon DocumentDB esistenti utilizzando ilAWS CLI.

- Per modificare immediatamente le istanze, eseguire il comando seguente per ogni istanza del cluster.

```
aws docdb modify-db-instance --db-instance-identifier <yourInstanceIdentifier> --ca-certificate-identifier rds-ca-rsa4096-g1 --apply-immediately
```

- Per modificare le istanze del cluster in modo da utilizzare il nuovo certificato CA durante la successiva finestra di manutenzione del cluster, eseguire il comando seguente per ogni istanza del cluster.

```
aws docdb modify-db-instance --db-instance-identifier <yourInstanceIdentifier> --ca-certificate-identifier rds-ca-rsa4096-g1 --no-apply-immediately
```

Cosa succede se si aggiunge una nuova istanza a un cluster esistente?

Tutte le nuove istanze create utilizzano il vecchio certificato server e richiedono connessioni TLS utilizzando il vecchio certificato CA. Qualsiasi nuova istanza Amazon DocumentDB creata dopo il 21 marzo 2022 utilizzerà per impostazione predefinita i nuovi certificati.

Cosa succede se nel cluster è presente una sostituzione o un failover di istanza?

Se nel cluster è presente una sostituzione di istanza, la nuova istanza creata continua a utilizzare lo stesso certificato server utilizzato in precedenza dall'istanza. Si consiglia di aggiornare contemporaneamente i certificati server per tutte le istanze. Se si verifica un failover nel cluster, viene utilizzato il certificato server sul nuovo primario.

Se non si utilizza TLS per connettersi al cluster, è comunque necessario aggiornare ciascuna delle istanze?

Se non utilizzi TLS per connetterti ai cluster Amazon DocumentDB, non è necessaria alcuna azione.

Se attualmente non uso TLS per connettermi al cluster ma ho intenzione di farlo in futuro, cosa devo fare?

Se hai creato un cluster prima del 21 marzo 2022, segui i [passaggi 1](#) e [2](#) della sezione precedente per assicurarti che l'applicazione utilizzi il pacchetto CA aggiornato e che ogni istanza di Amazon DocumentDB utilizzi il certificato server più recente. Se crei un cluster dopo il 21 marzo 2022, il cluster disporrà già del certificato server più recente. Per verificare che l'applicazione utilizzi il bundle di certificati CA più recente, consulta [Se non si utilizza TLS per connettersi al cluster, è comunque necessario aggiornare ciascuna delle istanze?](#).

La scadenza può essere prorogata oltre il 18 maggio 2022?

Se le tue candidature si connettono tramite TLS, la scadenza non può essere prorogata oltre il 18 maggio 2022.

Come posso essere sicuro di utilizzare il bundle CA più recente?

Per motivi di compatibilità, vengono denominati sia i file bundle CA vecchi sia quelli nuovi, denominati `us-gov-west-1-bundle.pem`. È anche possibile utilizzare strumenti come `openssl` o `keytool` per ispezionare il bundle CA.

Perché viene visualizzato «RDS» nel nome del bundle CA?

Per alcune funzionalità di gestione, come la gestione dei certificati, Amazon DocumentDB utilizza una tecnologia operativa condivisa con Amazon Relational Database Service (Amazon RDS).

Se è stato applicato il nuovo certificato server, è possibile ripristinare il vecchio certificato?

Se è necessario ripristinare un'istanza al certificato server precedente, consigliamo di farlo per tutte le istanze del cluster. È possibile ripristinare il certificato del server per ogni istanza in un cluster utilizzando la AWS Management Console o l'AWS CLI.

Utilizzo di AWS Management Console

1. Accedi alla e apri laAWS Management Console la ri ri Amazon DocumentDB all'[indirizzo https://console.aws.amazon.com/docdb](https://console.aws.amazon.com/docdb).
2. Nell'elenco delle regioni nell'angolo in alto a destra dello schermo, seleziona laRegione AWS in cui si trovano i cluster.
3. Nel riquadro di navigazione sul lato sinistro della console scegliere Instances (Istanze).
4. Selezionare un'istanza da modificare. Scegli Actions (Operazioni), quindi Modify (Modifica).
5. In Autorità di certificazione, puoi selezionare il vecchio certificato del server (rds-ca-2017).
6. Scegliere Continue (Continua) per visualizzare un riepilogo delle modifiche.
7. In questa pagina, è possibile scegliere di pianificare le modifiche da applicare nella finestra di manutenzione successiva o di applicare le modifiche immediatamente. Effettuare la selezione e scegliere Modify instance (Modifica istanza).

Note

Se si sceglie di applicare le modifiche immediatamente, anche tutte le modifiche incluse nella coda delle modifiche in sospeso saranno applicate. Se nessuna delle modifiche in sospeso richiede tempi di inattività, la scelta di applicarle può provocare tempi di inattività imprevisti.

Utilizzo di AWS CLI

```
aws docdb modify-db-instance --db-instance-identifier <db_instance_name> ca-  
certificate-identifier rds-ca-2017 <--apply-immediately | --no-apply-immediately>
```

Se si sceglie `--no-apply-immediately`, la modifica verrà applicata durante la prossima finestra di manutenzione del cluster.

Se ripristino da uno snapshot o un da un momento specifico, sarà disponibile il nuovo certificato del server?

Se ripristini uno snapshot o esegui un point-in-time ripristino dopo il 21 marzo 2022, il nuovo cluster creato utilizzerà il nuovo certificato CA.

Cosa succede se ho problemi a connettermi direttamente al mio cluster Amazon DocumentDB da Mac OS X Catalina?

Mac OS X Catalina ha aggiornato i requisiti per i certificati attendibili. I certificati attendibili ora devono essere validi per 825 giorni o meno (vedi <https://support.apple.com/en-us/HT210176>). I certificati di istanza Amazon DocumentDB sono validi per oltre quattro anni, più a lungo del massimo di Mac OS X. Per connetterti direttamente a un cluster Amazon DocumentDB da un computer con Mac OS X Catalina, devi consentire certificati non validi durante la creazione della connessione TLS. In questo caso, i certificati non validi indicano che il periodo di validità è superiore a 825 giorni. È necessario comprendere i rischi prima di consentire certificati non validi durante la connessione al cluster Amazon DocumentDB.

Per connetterti a un cluster Amazon DocumentDB da OS X Catalina utilizzando il AWS CLI, usa il `tlsAllowInvalidCertificates` parametro.

```
mongo --tls --host <hostname> --username <username> --password <password> --port 27017  
--tlsAllowInvalidCertificates
```

Convalida della conformità in Amazon DocumentDB

Revisori di terze parti valutano la sicurezza e la conformità di Amazon DocumentDB di più programmi di conformità delle MongoDB con più programmi di conformità delle risorse con più programmi di conformità delle risorse con più programmi di conformità delle risorse con più programmi di conformità delle risorse con più programmi di AWS conformità delle risorse con più programmi di conformità delle risorse con

- System and Organization Controls (SOC) 1, 2 e 3. Per ulteriori informazioni, consulta [SOC](#).
- Payment Card Industry Data Security Standard (PCI DSS). Per ulteriori informazioni, consulta [PCI DSS](#).
- ISO 9001, 27001, 27017 e 27018 Per ulteriori informazioni, vedere la [certificazione ISO](#).
- Health Insurance Portability and Accountability Act Business Associate Agreement (HIPAA BAA). Per ulteriori informazioni, consulta [Compliance HIPAA](#).

AWS fornisce un elenco aggiornato di frequente dei servizi AWS nell'ambito di specifici programmi di conformità all'indirizzo [Servizi AWS coperti dal programma di conformità](#).

si estende sempre su tre zone di disponibilità per fornire storage durevole con minori possibilità di perdita di dati.

Per ulteriori informazioni sulle Regioni AWS e le zone di disponibilità, consulta [Infrastruttura globale di AWS](#).

Oltre all'AWS infrastruttura globale, Amazon DocumentDB offre numerose funzionalità per supportare la resilienza dei dati e le esigenze di backup.

Storage con tolleranza ai guasti e riparazione automatica

Ogni parte di 10 GB del volume di storage viene replicata in sei modi, su tre zone di disponibilità. Amazon DocumentDB utilizza storage con tolleranza di errore che gestisce in modo trasparente la perdita di un massimo di due copie di dati senza influire sulla disponibilità di scrittura del database e fino a tre copie senza influire sulla disponibilità di lettura. Anche lo storage Amazon DocumentDB è auto-curativo; i blocchi di dati e i dischi vengono sottoposti a scansione continua alla ricerca di errori e sostituiti automaticamente.

Backup e ripristino manuali

Amazon DocumentDB offre la possibilità di creare backup completi del cluster per la conservazione e il ripristino a lungo termine. Per ulteriori informazioni, consultare [Backup e ripristino in Amazon DocumentDB](#).

Ripristino point-in-time

Il ripristino point-in-time ti permette di proteggere i cluster Amazon DocumentDB da operazioni di scrittura o eliminazione accidentali. Grazie al ripristino point-in-time, non devi preoccuparti di creare, gestire o programmare i backup on-demand. Per ulteriori informazioni, consultare [Ripristino a un punto temporale specifico](#).

Sicurezza dell'infrastruttura in Amazon DocumentDB

In quanto servizio gestito, Amazon DocumentDB è protetto dalla sicurezza globale della rete di AWS. Per informazioni sui servizi di sicurezza AWS e su come AWS protegge l'infrastruttura, consulta la pagina [Sicurezza del cloud AWS](#). Per progettare l'ambiente AWS utilizzando le best practice per la sicurezza dell'infrastruttura, consulta la pagina [Protezione dell'infrastruttura](#) nel Pilastro della sicurezza di AWS Well-Architected Framework.

Tu usi le API pubblicate per accedere ad Amazon DocumentDB tramite la rete. I clienti devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. In alternativa, è possibile utilizzare [AWS Security Token Service](#) (AWS STS) per generare le credenziali di sicurezza temporanee per sottoscrivere le richieste.

Puoi chiamare queste operazioni API da una qualsiasi posizione di rete. Puoi utilizzare le policy di Amazon DocumentDB per controllare l'accesso da specifici endpoint Amazon Virtual Private Cloud (Amazon VPC) o VPC specifici. In effetti, questo isola l'accesso di rete a una determinata risorsa Amazon DocumentDB solo dallo specifico VPC all'interno delAWSrete.

Note

Amazon DocumentDB non supporta politiche di accesso basate sulle risorse.

Best practice di sicurezza per Amazon DocumentDB

Per le best practice di sicurezza, è necessario utilizzareAWS Identity and Access Management(IAM) per controllare l'accesso alle operazioni API Amazon DocumentDB, specialmente operazioni che creano, modificano o eliminano risorse Amazon DocumentDB. Tali risorse includono i cluster, i gruppi di sicurezza e i gruppi di parametri. Devi utilizzare anche IAM per controllare le operazioni che eseguono operazioni amministrative comuni come il backup del ripristino dei cluster. Quando si creano ruoli IAM, utilizzare il principio del privilegio minimo.

- Applica privilegi minimi con il [controllo accessi basato sui ruoli](#).
- Assegna un account IAM individuale a ogni persona che gestisce risorse Amazon DocumentDB. Non utilizzare ilAccount AWSutente root per gestire le risorse Amazon DocumentDB. Crea un utente IAM per tutti, incluso te stesso.
- Assegna a ciascun utente il set minimo di autorizzazioni richieste per eseguire le proprie mansioni.

- Utilizza gruppi IAM per gestire in modo efficace le autorizzazioni per più utenti. Per ulteriori informazioni su IAM, consulta la [Guida per l'utente di IAM](#). Per informazioni sulle best practice IAM consulta [Best Practice di IAM](#).
- Ruota periodicamente le credenziali IAM.
- Configura AWS Secrets Manager per ruotare automaticamente i segreti per Amazon DocumentDB. Per ulteriori informazioni, consulta [Rotazione delle AWS Segreti di Secrets Manager](#) e [Rotazione dei segreti per Amazon DocumentDB](#) nella AWS Guida utente di Secrets Manager.
- Utilizza Transport Layer Security (TLS) e la crittografia dei dati inattivi per crittografare i dati.

Controllo degli eventi di Amazon DocumentDB

Con Amazon DocumentDB (con compatibilità con MongoDB), puoi controllare gli eventi che sono stati eseguiti nel tuo cluster. Sono esempi di eventi registrati i tentativi di autenticazione riusciti e non riusciti, l'eliminazione di una raccolta in un database o la creazione di un indice. Per impostazione predefinita, il controllo è disabilitato su Amazon DocumentDB e richiede che tu scelga di utilizzare questa funzionalità.

Quando il controllo è abilitato, Amazon DocumentDB registra gli eventi di Data Definition Language (DDL), Data Manipulation Language (DML), autenticazione, autorizzazione e gestione degli utenti su Amazon Logs. CloudWatch Quando il controllo è abilitato, Amazon DocumentDB esporta i record di controllo del cluster (documenti JSON) in Amazon Logs. CloudWatch Puoi utilizzare Amazon CloudWatch Logs per analizzare, monitorare e archiviare gli eventi di audit di Amazon DocumentDB.

Sebbene Amazon DocumentDB non addebiti costi aggiuntivi per abilitare l'auditing, ti vengono addebitate tariffe standard per l'utilizzo dei log. CloudWatch [Per informazioni sui prezzi di CloudWatch Logs, consulta i prezzi di Amazon. CloudWatch](#)

La funzionalità di controllo di Amazon DocumentDB è nettamente diversa dall'utilizzo delle risorse di servizio con cui viene monitorato. AWS CloudTrail CloudTrail registra le operazioni eseguite con AWS Command Line Interface (AWS CLI) o AWS Management Console su risorse come cluster, istanze, gruppi di parametri e istantanee. Il controllo delle AWS risorse con CloudTrail è attivo per impostazione predefinita e non può essere disabilitato. La funzionalità di auditing di Amazon DocumentDB è una funzionalità opzionale. Registra le operazioni eseguite all'interno del cluster sugli oggetti, ad esempio database, raccolte, indici e utenti.

Argomenti

- [Eventi supportati](#)

- [Abilitazione dell'audit](#)
- [Disabilitazione dell'audit](#)
- [Accesso agli eventi di audit](#)

Eventi supportati

L'auditing di Amazon DocumentDB supporta le seguenti categorie di eventi:

- Data Definition Language (DDL): include operazioni di gestione del database, connessioni, gestione degli utenti e autorizzazione.
- Data Manipulation Language read events (letture DML): include i vari operatori di aggregazione, operatori aritmetici, operatori booleani `find()` e altri operatori di query di lettura.
- Eventi di scrittura del Data Manipulation Language (scritture DML): include e operatori `insert()`, `update()`, `delete()`, `bulkWrite()`

I tipi di evento sono i seguenti:

Tipo di evento	Categoria	Descrizione
authCheck	Autorizzazione	Codice risultato 0: successo Codice risultato 13: tentativi non autorizzati di eseguire un'operazione.
authenticate	Connessione	Tentativi di autenticazione riusciti o non riusciti in una nuova connessione.
createDatabase	DDL	Creazione di un nuovo database.

Tipo di evento	Categoria	Descrizione
<code>createCollection</code>	DDL	Creazione di una nuova raccolta all'interno di un database.
<code>createIndex</code>	DDL	Creazione di un nuovo indice all'interno di una raccolta.
<code>dropCollection</code>	DDL	Eliminazione di una raccolta all'interno di un database.
<code>dropDatabase</code>	DDL	Eliminazione di un database.
<code>dropIndex</code>	DDL	Eliminazione di un indice all'interno di una raccolta.
<code>modifyChangeStreams</code>	DDL	È stato creato il flusso di modifiche.
<code>renameCollection</code>	DDL	Ridenominazione di una raccolta all'interno di un database.
<code>createRole</code>	Gestione dei ruoli	Creazione di un ruolo.
<code>dropAllRolesFromDatabase</code>	Gestione dei ruoli	Eliminazione di tutti i ruoli all'interno di un database.
<code>dropRole</code>	Gestione dei ruoli	Abbandono di un ruolo.
<code>grantPrivilegesToRole</code>	Gestione dei ruoli	Concessione di privilegi a un ruolo.

Tipo di evento	Categoria	Descrizione
<code>grantRolesToRole</code>	Gestione dei ruoli	Concessione di ruoli a un ruolo definito dall'utente.
<code>revokePrivilegesFromRole</code>	Gestione dei ruoli	Revoca dei privilegi da un ruolo.
<code>revokeRolesFromRole</code>	Gestione dei ruoli	Revoca di ruoli da un ruolo definito dall'utente.
<code>updateRole</code>	Gestione dei ruoli	Aggiornamento di un ruolo.
<code>createUser</code>	Gestione degli utenti	Creazione di un nuovo utente.
<code>dropAllUsersFromDatabase</code>	Gestione degli utenti	Eliminazione di tutti gli utenti all'interno di un database.
<code>dropUser</code>	Gestione degli utenti	Eliminazione di un utente esistente.
<code>grantRolesToUser</code>	Gestione degli utenti	Concessione di ruoli a un utente.
<code>revokeRolesFromUser</code>	Gestione degli utenti	Revoca di ruoli a un utente.
<code>updateUser</code>	UserManagement	Aggiornamento di un utente esistente.
<code>insert</code>	Scrittura DML	Inserisce uno o più documenti in una raccolta.

Tipo di evento	Categoria	Descrizione
<code>delete</code>	Scrittura DML	Elimina uno o più documenti da una raccolta.
<code>update</code>	Scrittura DML	Modifica uno o più documenti esistenti in una raccolta.
<code>bulkWrite</code>	Scrittura DML	Esegue più operazioni di scrittura con controlli per l'ordine di esecuzione.
<code>count</code>	Lettura DML	Restituisce il numero di documenti che corrisponderebbero a una query <code>find()</code> per la raccolta o la visualizzazione.
<code>countDocuments</code>	Lettura in formato DML	Restituisce il numero di documenti che corrispondono alla query per una raccolta o una visualizzazione.
<code>find</code>	Lettura in formato DML	Seleziona i documenti in una raccolta o in una vista e riporta il cursore sui documenti selezionati.
<code>findAndModify</code>	Lettura DML e scrittura DML	Modifica e restituisce un singolo documento.

Tipo di evento	Categoria	Descrizione
<code>findOneAndDelete</code>	Lettura DML e scrittura DML	Elimina un singolo documento in base ai criteri di filtro e ordinamento, restituendo il documento eliminato.
<code>findOneAndReplace</code>	Lettura DML e scrittura DML	Sostituisce un singolo documento in base al filtro specificato.
<code>findOneAndUpdate</code>	Lettura DML e scrittura DML	Aggiorna un singolo documento in base ai criteri di filtro e ordinamento.
<code>aggregate</code>	Lettura DML e scrittura DML	Supporta le API nella pipeline di aggregazione.
<code>distinct</code>	Lettura DML	Trova i valori distinti per un campo specificato in una singola raccolta o visualizzazione e restituisce i risultati in un array.

Note

I valori nel campo dei parametri del documento di evento DML hanno un limite di dimensione di 1 KB. Amazon DocumentDB tronca il valore se supera 1 KB.

Note

Gli eventi di eliminazione TTL non vengono controllati in questo momento.

Abilitazione dell'audit

La procedura per abilitare l'audit in un cluster prevede due fasi: Assicurati che entrambi i passaggi siano stati completati, altrimenti i log di controllo non verranno inviati a Logs. CloudWatch

Fase 1. Abilita il parametro del cluster `audit_logs`

Per abilitare il controllo, è necessario modificare il `audit_logs` parametro nel gruppo di parametri. `audit_logs` è un elenco di eventi delimitato da virgole da registrare. Gli eventi devono essere specificati in lettere minuscole e non devono esserci spazi bianchi tra gli elementi dell'elenco.


È possibile impostare i seguenti valori per il gruppo di parametri:

Value (Valore)	Descrizione
<code>ddl</code>	Questa impostazione abiliterà il controllo per eventi DDL come <code>CreateDatabase</code> , <code>DropDatabase</code> , <code>CreateCollection</code> , <code>DropCollection</code> , <code>CreateIndex</code> , <code>DropIndex</code> , <code>AuthCheck</code> , <code>authenticate</code> , <code>createUser</code> , <code>DropUser</code> , <code>User</code> , <code>User</code> , <code>User</code> , <code>updateUser</code> e <code>grantRolesTo</code> , <code>revokeRolesFrom</code> , <code>dropAllUsersFromDatabase</code>

Value (Valore)	Descrizione	
<code>dml_read</code>	L'impostazione di questa impostazione abiliterà il controllo per gli eventi di lettura DML come <code>find</code> , <code>sort</code> , <code>count</code> , <code>distinct</code> , <code>group</code> , <code>project</code> , <code>unwind</code> , <code>GeoNear</code> , <code>GeoIntersects</code> , <code>GeoWithin</code> e altri operatori di query di lettura MongoDB.	
<code>dml_write</code>	L'impostazione di questa impostazione abiliterà il controllo per gli eventi di scrittura DML come <code>insert ()</code> , <code>update ()</code> , <code>delete ()</code> e <code>bulkWrite ()</code>	
<code>all</code>	Questa impostazione consentirà il controllo degli eventi del database, come le query di lettura, le query di scrittura, le azioni del database e le azioni dell'amministratore.	
<code>none</code>	L'impostazione di questa impostazione disabiliterà il controllo	

Value (Valore)	Descrizione	
enabled(legacy)	<p>Questa è un'impostazione dei parametri legacy equivalente a 'ddl'. L'impostazione di questa impostazione abiliterà il controllo per eventi DDL come CreateDatabase, DropDatabase, CreateCollection, DropCollection, CreateIndex, DropIndex, AuthCheck, authenticate, createUser, DropUser, User, User, UpdateUser e grantRolesTo revokeRolesFrom dropAllUsersFromDatabase. Non è consigliabile utilizzare questa impostazione perché si tratta di un'impostazione precedente.</p>	

Value (Valore)	Descrizione
disabled (eredità)	Questa è un'impostazione dei parametri legacy equivalente a «nessuna». Non è consigliabile utilizzare e questa impostazione perché si tratta di un'impostazione precedente.

 Note

Il valore predefinito per il parametro del cluster `audit_logs` è `none` (legacy "«disabled»).

È inoltre possibile utilizzare i valori sopra menzionati in combinazioni.

Value (Valore)	Descrizione
ddl, dml_read	L'impostazione di questa impostazione abiliterà l'auditing per gli eventi DDL e gli eventi di lettura DML.
ddl, dml_write	L'impostazione di questa impostazione abiliterà l'auditing per gli eventi DDL e la scrittura DML.
dml_read, dml_write	L'impostazione di questa impostazione

Value (Valore)	Descrizione
	abiliterà il controllo per tutti gli eventi DML

Note

Non è consentito modificare un gruppo di parametri predefinito.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- [Creazione di gruppi di parametri del cluster Amazon DocumentDB](#)

Dopo la creazione di un gruppo personalizzato di parametri, modificarlo impostando il valore del parametro `audit_logs` su `enabled`.

- [Modifica dei gruppi di parametri del cluster Amazon DocumentDB](#)

Fase 2. Abilita Amazon Logs Export CloudWatch

Quando il valore del parametro `audit_logs cluster` è `enabled`, o `ddl dml_readdml_write`, devi anche abilitare Amazon DocumentDB per esportare i log in Amazon. CloudWatch Se ometti uno di questi passaggi, i log di controllo non verranno inviati a. CloudWatch

Quando si crea un cluster, si esegue o si ripristina un'istantanea, è possibile abilitare CloudWatch i log seguendo questi passaggi. `point-in-time-restore`

Using the AWS Management Console

Per abilitare l'esportazione dei log da parte di Amazon DocumentDB per l' CloudWatch utilizzo della console, consulta i seguenti argomenti:

- Quando si crea un cluster [Creazione di un cluster e di un'istanza primaria utilizzando il AWS Management Console](#), in, consulta Creare un cluster: configurazioni aggiuntive (fase 5, esportazioni di log)
- Quando si modifica un cluster esistente: [Modifica di un cluster Amazon DocumentDB](#)
- Quando si esegue il ripristino di un'istantanea del cluster: [Ripristino da una snapshot del cluster](#)

- Quando si esegue un point-in-time ripristino: [Ripristino a un punto temporale specifico](#)

Using the AWS CLI

Per abilitare i log di audit durante la creazione di un nuovo cluster

Il codice seguente crea il cluster `sample-cluster` e abilita i log di CloudWatch controllo.

Example

Per Linux, macOS o 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
```

Per 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
```

Per abilitare i log di audit durante la modifica di un cluster esistente

Il codice seguente modifica il cluster `sample-cluster` e abilita i log di CloudWatch controllo.

Example

Per Linux, macOS o Unix:

```
aws docdb modify-db-cluster \  
  --db-cluster-identifier sample-cluster \  
  --enable-cloudwatch-logs-exports audit
```

```
--db-cluster-identifier sample-cluster \  
--cloudwatch-logs-export-configuration '{"EnableLogTypes":["audit"]}'
```

Per Windows:

```
aws docdb modify-db-cluster ^  
--db-cluster-identifier sample-cluster ^  
--cloudwatch-logs-export-configuration '{"EnableLogTypes":["audit"]}'
```

L'aspetto dell'output di queste operazioni è simile al seguente (formato JSON).

```
{  
  "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-Y0S52CUXGDTNKDQ7DH72I4LED4",
    "Endpoint": "sample-cluster.cluster-corcjozrlsfc.us-
east-1.docdb.amazonaws.com",
    "PreferredBackupWindow": "07:16-07:46",
    "DBClusterIdentifier": "sample-cluster"
  }
}
```

Disabilitazione dell'audit

È possibile disabilitare il controllo disabilitando l'esportazione dei CloudWatch registri e disabilitando il parametro. `audit_logs`

Disabilitazione dell'esportazione dei log CloudWatch

È possibile disabilitare l'esportazione di log di audit tramite la AWS Management Console o l'AWS CLI.

Using the AWS Management Console

La procedura seguente utilizza AWS Management Console per disabilitare l'esportazione dei log in Amazon DocumentDB in. CloudWatch

Per disabilitare i log di audit

1. [Accedi a e apri AWS Management Console la console Amazon DocumentDB all'indirizzo `https://console.aws.amazon.com/docdb`.](https://console.aws.amazon.com/docdb)
2. Nel pannello di navigazione scegliere Clusters (Cluster). Quindi, scegliere il pulsante a sinistra del nome del cluster per il quale si desidera disabilitare l'esportazione dei log.
3. Scegli Actions (Operazioni), quindi Modify (Modifica).
4. Scorrere verso il basso fino alla sezione Log exports (Esportazioni log) e scegliere Disabled (Disabilitato).
5. Scegli Continue (Continua).
6. Esaminare le modifiche, quindi scegliere quando applicare la modifica al cluster.
 - Apply during the next scheduled maintenance window (Applica durante la prossima finestra di manutenzione pianificata)

- Apply immediately (Applica immediatamente)
7. Scegliere Modify cluster (Modifica cluster).

Using the AWS CLI

Il codice seguente modifica il cluster `sample-cluster` e disabilita CloudWatch i log di controllo.

Example

Per Linux, macOS o Unix:

```
aws docdb modify-db-cluster \  
  --db-cluster-identifier sample-cluster \  
  --cloudwatch-logs-export-configuration '{"DisableLogTypes":["audit"]}'
```

Per Windows:

```
aws docdb modify-db-cluster ^  
  --db-cluster-identifier sample-cluster ^  
  --cloudwatch-logs-export-configuration '{"DisableLogTypes":["audit"]}'
```

L'aspetto dell'output di questa operazione è simile al seguente (formato JSON).

```
{  
  "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"
      }
    ]
  }
}

```

Disabilitazione del parametro `audit_logs`

Per disabilitare il parametro `audit_logs` per il cluster, puoi modificarlo in modo che venga utilizzato un gruppo di parametri in cui il parametro `audit_logs` ha il valore `disabled`. In alternativa, puoi modificare il valore del parametro `audit_logs` nel gruppo di parametri del cluster in modo che sia `disabled`.

Per ulteriori informazioni, consulta i seguenti argomenti:

- [Modifica di un cluster Amazon DocumentDB](#)
- [Modifica dei gruppi di parametri del cluster Amazon DocumentDB](#)

Accesso agli eventi di audit

Utilizza i seguenti passaggi per accedere ai tuoi eventi di controllo su Amazon. CloudWatch

1. Apri la CloudWatch console all'[indirizzo https://console.aws.amazon.com/cloudwatch/](https://console.aws.amazon.com/cloudwatch/).

2. Assicurati di trovarti nella stessa regione del cluster Amazon DocumentDB.
3. Nel riquadro di navigazione scegli Logs (Log).
4. Per trovare i log di audit del cluster, dall'elenco individuare e scegliere **/aws/docdb/*yourClusterName*/audit**.

Gli eventi di audit per ogni istanza sono disponibili nei rispettivi nomi di istanza.

Backup e ripristino in Amazon DocumentDB

Amazon DocumentDB (compatibile con MongoDB) esegue il backup continuo dei dati su Amazon Simple Storage Service (Amazon S3) per 1-35 giorni, in modo da consentirti di ripristinarli rapidamente in qualsiasi momento entro il periodo di conservazione del backup. Amazon DocumentDB acquisisce anche istantanee automatiche dei dati come parte di questo processo di backup continuo.

Note

Si tratta di bucket Amazon S3 gestiti dal servizio e non avrai accesso ai file di backup. Se desideri controllare i tuoi backup, segui le istruzioni su [Dumping, Ripristino, Importazione ed Esportazione dei dati](#).

Puoi anche conservare i dati di backup oltre il periodo di retention dei backup creando una snapshot dei dati del cluster. Il processo di backup non ha impatto sulle prestazioni del cluster.

Questa sezione illustra i casi d'uso delle funzionalità di backup in Amazon DocumentDB e mostra come gestire i backup per i cluster Amazon DocumentDB.

Argomenti

- [Backup e ripristino: concetti](#)
- [Informazioni sull'utilizzo dello storage di backup](#)
- [Dump, ripristino, importazione ed esportazione di dati](#)
- [Considerazioni sulle snapshot del cluster](#)
- [Confronto tra snapshot automatiche e manuali](#)
- [Creazione di una snapshot del cluster manuale](#)
- [Copia degli snapshot del cluster Amazon DocumentDB](#)
- [Condivisione di istantanee del cluster Amazon DocumentDB](#)
- [Ripristino da una snapshot del cluster](#)
- [Ripristino a un punto temporale specifico](#)
- [Eliminazione di una snapshot del cluster](#)

Backup e ripristino: concetti

Sostantivo	Descrizione	API (verbi)
Backup retention period (Periodo di retention dei backup)	Un periodo di tempo compreso tra 1 e 35 giorni per il quale è possibile eseguire un ripristino o. point-in-time	<pre>create-db-cluster</pre> <pre>modify-db-cluster</pre> <pre>restore-db-cluster-to-point-in-time</pre>
Volume di storage Amazon DocumentDB	Volume di storage a disponibilità elevata ed estremamente durevole che replica i dati in sei modi su tre zone di disponibilità. Un cluster Amazon DocumentDB è altamente	<pre>create-db-cluster</pre> <pre>delete-db-cluster</pre>

Sostantivo	Descrizione	API (verbi)
	durevole indipendentemente dal numero di istanze nel cluster.	
Finestra di backup	Periodo di tempo durante il giorno in cui vengono acquisite le snapshot automatiche.	<code>create-db-cluster</code> <code>describe-db-cluster</code> <code>modify-db-cluster</code>
Snapshot automatica	Snapshot giornalieri che sono backup completi del cluster e vengono creati automaticamente dal processo di backup continuo in Amazon DocumentDB.	<code>restore-db-cluster-from-snapshot</code> <code>describe-db-cluster-snapshot-attributes</code> <code>describe-db-cluster-snapshots</code>

Sostantivo	Descrizione	API (verbi)
Snapshot manuale	Snapshot create manualmente per conservare i backup completi di un cluster oltre il periodo di backup.	<pre>create-db-cluster-snapshot</pre> <pre>copy-db-cluster-snapshot</pre> <pre>delete-db-cluster-snapshot</pre> <pre>describe-db-cluster-snapshot-attributes</pre> <pre>describe-db-cluster-snapshots</pre> <pre>modify-db-cluster-snapshot-attribute</pre>

Informazioni sull'utilizzo dello storage di backup

Lo storage di backup di Amazon DocumentDB è costituito da backup continui entro il periodo di conservazione dei backup e istantanee manuali al di fuori del periodo di conservazione. Per controllare l'utilizzo dello storage di backup, è possibile ridurre l'intervallo di retention dei backup e/o rimuovere gli snapshot manuali obsoleti e non più necessari. Per informazioni generali sui backup di Amazon DocumentDB, consulta [Backup e ripristino in Amazon DocumentDB](#). Per informazioni sui prezzi dello storage di backup di Amazon DocumentDB, consulta i prezzi di [Amazon DocumentDB](#).

Per controllare i costi, è sufficiente monitorare la quantità di storage occupata da backup continui e snapshot manuali che permangono oltre il periodo di retention e, all'occorrenza, ridurre l'intervallo di retention dei backup nonché rimuovere gli snapshot manuali non più necessari.

Puoi utilizzare i CloudWatch parametri `TotalBackupStorageBilled` di Amazon e rivedere e `BackupRetentionPeriodStorageUsed` monitorare la quantità di storage utilizzata dai tuoi backup di Amazon DocumentDB, come segue: `SnapshotStorageUsed`

- `BackupRetentionPeriodStorageUsed` rappresenta la quantità di storage di backup al momento utilizzata per l'archiviazione di backup continui. Il valore di questo parametro dipende dalle dimensioni del volume del cluster e dalla quantità di modifiche apportate durante il periodo di retention. Tuttavia, ai fini della fatturazione, il parametro non supera mai il volume di cluster cumulativo nel periodo di retention. Con un cluster di 100 GiB e un periodo di retention di due

giorni, ad esempio, il valore massimo previsto per `BackRetentionPeriodStorageUsed` è di 200 GiB (100 GiB + 100 GiB).

- `SnapshotStorageUsed` rappresenta la quantità di storage di backup utilizzata per l'archiviazione di snapshot manuali oltre il periodo di retention dei backup. Gli snapshot manuali acquisiti nel periodo di retention non rientrano nel calcolo dello storage di backup. Analogamente, anche gli snapshot automatici non vengono inclusi nel novero dello storage di backup. Ogni snapshot corrisponde, per dimensioni, al volume del cluster al momento della sua acquisizione. Il valore di `SnapshotStorageUsed` dipende dal numero e dalle dimensioni degli snapshot conservati. Supponiamo, ad esempio, di disporre di uno snapshot al di fuori del periodo di retention, con il volume del cluster, al momento dell'acquisizione di tale snapshot, di 100 GiB. In questo caso, lo `SnapshotStorageUsed` corrisponde a 100 GiB.
- `TotalBackupStorageBilled` corrisponde alla somma di `BackupRetentionPeriodStorageUsed` e `SnapshotStorageUsed`, meno una quantità di storage di backup gratuito pari alla dimensione del volume del cluster per un giorno. Ad esempio, se la dimensione del cluster è 100 GiB, si dispone di un giorno di conservazione e si dispone di una snapshot al di fuori del periodo di conservazione, è 100 GiB (`TotalBackupStorageBilled` 100 GiB + 100 GiB - 100 GiB).
- Questi parametri vengono calcolati indipendentemente per ogni cluster Amazon DocumentDB.

[Puoi monitorare i tuoi cluster Amazon DocumentDB e creare report utilizzando i CloudWatch parametri tramite la console. CloudWatch](#) Per ulteriori informazioni su come utilizzare i CloudWatch parametri, consulta [Monitoraggio Amazon DocumentDB](#)

Dump, ripristino, importazione ed esportazione di dati

Puoi utilizzare le `mongoimport` utilità `mongodump`, `mongorestore` `mongoexport`, e per spostare i dati all'interno e all'esterno del cluster Amazon DocumentDB. In questa sezione viene descritto lo scopo di ognuno di questi strumenti e configurazioni per migliorare le prestazioni.

Argomenti

- [mongodump](#)

- [mongorestore](#)
- [mongoexport](#)
- [mongoimport](#)
- [Tutorial](#)

mongodump

L'utilità mongodump crea un backup binario (BSON) di un database MongoDB. Lo mongodump strumento è il metodo preferito per scaricare i dati dalla distribuzione di MongoDB di origine quando si desidera ripristinarli nel cluster Amazon DocumentDB, grazie all'efficienza delle dimensioni ottenuta archiviando i dati in formato binario.

A seconda delle risorse disponibili sull'istanza o sulla macchina che si sta utilizzando per eseguire il comando, è possibile velocizzare l'operazione mongodump aumentando il numero di connessioni parallele eliminate dal valore predefinito 1 utilizzando l'`--numParallelCollections` opzione. Una buona regola empirica è iniziare con un worker per vCPU sull'istanza principale del cluster Amazon DocumentDB.

Note

Consigliamo MongoDB Database Tools fino alla versione 100.6.1 inclusa per Amazon DocumentDB. [Puoi accedere ai download di MongoDB Database Tools qui.](#)

Esempio di utilizzo

Di seguito è riportato un esempio di utilizzo dell'`mongodump` utilità nel cluster Amazon DocumentDB, `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

L'utilità `mongorestore` consente di ripristinare un backup binario (BSON) di un database creato con l'utilità `mongodump`. Puoi utilizzare l'opzione `--numInsertionWorkersPerCollection` per migliorare le prestazioni di ripristino aumentando il numero di worker per ogni raccolta durante il ripristino (il valore predefinito è 1). Una buona regola empirica è iniziare con un worker per vCPU sull'istanza principale del cluster Amazon DocumentDB.

Esempio di utilizzo

Di seguito è riportato un esempio di utilizzo dell'utilità `mongorestore` nel cluster Amazon DocumentDB, `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

Lo strumento `mongoexport` esporta i dati in Amazon DocumentDB nei formati di file JSON, CSV o TSV. Lo strumento `mongoexport` è il metodo preferito per esportare i dati che devono essere leggibili dall'uomo o dal computer.

Note

`mongoexport` non supporta direttamente le esportazioni parallele. Tuttavia, è possibile aumentare le prestazioni eseguendo più attività `mongoexport` contemporaneamente per raccolte diverse.

Esempio di utilizzo

Di seguito è riportato un esempio di utilizzo dello strumento `mongoexport` nel cluster Amazon DocumentDB, `sample-cluster`

```
mongoexport --ssl \  
  --host="sample-cluster.node.us-east-1.docdb.amazonaws.com:27017" \  
  --collection=sample-collection \  
  --out=sample-collection.json
```

```
--db=sample-database \  
--out=sample-output-file \  
--username=sample-user \  
--password=abc0123 \  
--sslCAFile global-bundle.pem
```

mongoimport

Lo `mongoimport` strumento importa il contenuto di file JSON, CSV o TSV in un cluster Amazon DocumentDB. È possibile utilizzare il parametro `--numInsertionWorkers` per parallelizzare e velocizzare l'importazione (il valore predefinito è 1).

Esempio di utilizzo

Di seguito è riportato un esempio di utilizzo dello `mongoimport` strumento nel cluster Amazon DocumentDB, `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

Il seguente tutorial descrive come utilizzare le `mongoimport` utilità `mongodump`, `mongorestore` `mongoexport`, e per spostare dati da e verso un cluster Amazon DocumentDB.

1. **Prerequisiti:** prima di iniziare, assicurati che il cluster Amazon DocumentDB sia predisposto e che tu abbia accesso a un'istanza Amazon EC2 nello stesso VPC del cluster. Per ulteriori informazioni, consulta [Connect tramite Amazon EC2](#).

Per poter utilizzare gli strumenti di utilità mongo, devi avere il `mongodb-org-tools` pacchetto installato nella tua istanza EC2, come segue.

```
sudo yum install mongodb-org-tools-4.0.18
```

Poiché Amazon DocumentDB utilizza la crittografia Transport Layer Security (TLS) per impostazione predefinita, devi anche scaricare il file Amazon RDS certificate authority (CA) per utilizzare la shell mongo per connetterti, come segue.

```
wget https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem
```

2. Scarica dati di esempio: per questo tutorial, scaricherai alcuni dati di esempio che contengono informazioni sui ristoranti.

```
wget https://raw.githubusercontent.com/ozlerhakan/mongodb-json-files/master/datasets/restaurant.json
```

3. Importa i dati di esempio in Amazon DocumentDB: poiché i dati sono in un formato JSON logico, utilizzerai l'utilità `mongoimport` per importare i dati nel tuo cluster Amazon DocumentDB.

```
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. Scarica i dati con **mongodump**: ora che hai dati nel tuo cluster Amazon DocumentDB, puoi eseguire un dump binario di tali dati utilizzando l'utilità `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. Elimina la **restaurants** raccolta: prima di ripristinare la `restaurants` raccolta nel `business` database, devi prima eliminare la raccolta già esistente in quel database, come segue.

```
use business
```

```
db.restaurants.drop()
```

6. Ripristina i dati con **mongorestore**: con il dump binario dei dati della fase 3, ora puoi utilizzare l'utility **mongorestore** per ripristinare i dati nel tuo cluster Amazon DocumentDB.

```
mongorestore --ssl \  
  --host="tutorialCluster.us-east-1.docdb.amazonaws.com:27017" \  
  --numParallelCollections 4 \  
  --username=<yourUsername> \  
  --password=<yourPassword> \  
  --sslCAFile global-bundle.pem restaurantDump.bson
```

7. Esporta i dati utilizzando **mongoexport**: per completare il tutorial, esporta i dati dal cluster nel formato di un file JSON, non diverso dal file importato nella fase 1.

```
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. Convalida: è possibile verificare che l'output del passaggio 5 produca lo stesso risultato del passaggio 1 con i seguenti comandi.

```
wc -l restaurant.json
```

Output da questo comando:

```
2548 restaurant.json
```

```
wc -l restaurant2.json
```

Output da questo comando:

```
2548 restaurant2.json
```

Considerazioni sulle snapshot del cluster

Amazon DocumentDB crea istantanee automatiche giornaliere del cluster durante la finestra di backup del cluster. Amazon DocumentDB salva le istantanee automatiche del cluster in base al periodo di conservazione dei backup specificato. Se necessario, puoi ripristinare il tuo cluster a uno specifico momento durante il periodo di retention dei backup. Le snapshot automatiche non vengono eseguite quando un'operazione di copia è in corso nella stessa regione dello stesso cluster.

Argomenti

- [Storage di backup](#)
- [Finestra di backup](#)
- [Periodo di retention dei backup](#)
- [Copiare Cluster Snapshot Encryption](#)

Oltre alle snapshot del cluster automatiche, puoi creare manualmente anche una snapshot del cluster. È possibile copiare gli snapshot automatici e manuali. Per ulteriori informazioni, consulta [Creazione di una snapshot del cluster manuale](#) e [Copia degli snapshot del cluster Amazon DocumentDB](#).

Note

Il cluster deve essere in stato disponibile per poter acquisire una snapshot automatica. Non puoi condividere uno snapshot del cluster automatizzato di Amazon DocumentDB. Come soluzione alternativa, è possibile creare uno snapshot manuale copiando lo snapshot automatico e quindi condividere la copia. Per ulteriori informazioni sulla copia di uno snapshot, consulta [Copia degli snapshot del cluster Amazon DocumentDB](#). Per ulteriori informazioni sul ripristino di un cluster da uno snapshot, consulta [Ripristino da una snapshot del cluster](#).

Storage di backup

Lo storage di backup di Amazon DocumentDB per ciascuno di essi Regione AWS è composto dallo storage di backup necessario per il periodo di conservazione dei backup, che include istantanee automatiche e manuali del cluster in quella regione. Il periodo di retention dei backup predefinito è 1 giorno. Per ulteriori informazioni sui prezzi dello storage di backup, consulta i prezzi di [Amazon DocumentDB](#).

Quando elimini un cluster, tutte le relative snapshot automatiche vengono eliminate e non possono essere recuperate. Tuttavia, le istantanee manuali non vengono eliminate quando si elimina un cluster. Se scegli di fare in modo che Amazon DocumentDB crei uno snapshot finale (snapshot manuale) prima dell'eliminazione del cluster, puoi utilizzare lo snapshot finale per ripristinare il cluster.

Per ulteriori informazioni su snapshot e storage, consulta [Informazioni sull'utilizzo dello storage di backup](#).

Finestra di backup

Le snapshot automatiche vengono eseguite quotidianamente durante la finestra di backup scelta. Se la snapshot richiede più tempo rispetto a quello previsto per la finestra di backup, il processo di backup continua fino al completamento, anche se la finestra di backup è terminata. La finestra di backup non può sovrapporsi con la finestra di manutenzione settimanale per il cluster.

Se non specifichi una finestra di backup preferita quando crei il cluster, Amazon DocumentDB assegna una finestra di backup predefinita di 30 minuti. Questa finestra viene scelta a caso da un blocco di 8 ore associato alla regione del cluster. Puoi modificare la finestra di backup preferita modificando il cluster. Per ulteriori informazioni, consulta [Modifica di un cluster Amazon DocumentDB](#).

Nome della regione	Regione	Blocco di tempo UTC
Stati Uniti orientali (Ohio)	us-east-2	03:00-11:00
US East (N. Virginia)	us-east-1	03:00-11:00
US West (Oregon)	us-west-2	06:00-14:00
Asia Pacifico (Hong Kong)	ap-east-1	06:00-14:00
Asia Pacific (Hyderabad)	ap-south-2	06:30 — 14:30

Nome della regione	Regione	Blocco di tempo UTC
Asia Pacific (Mumbai)	ap-south-1	06:00-14:00
Asia Pacifico (Seoul)	ap-northeast-2	13:00-21:00
Asia Pacific (Singapore)	ap-southeast-1	14:00-22:00
Asia Pacific (Sydney)	ap-southeast-2	12:00-20:00
Asia Pacifico (Tokyo)	ap-northeast-1	13:00-21:00
Canada (Central)	ca-central-1	03:00-11:00
China (Beijing)	cn-north-1	06:00-14:00
Cina (Ningxia)	cn-northwest-1	06:00-14:00
Europe (Frankfurt)	eu-central-1	21:00-05:00
Europa (Irlanda)	eu-west-1	22:00-06:00
Europe (London)	eu-west-2	22:00-06:00
Europa (Milano)	eu-south-1	02:00-10:00
Europe (Paris)	eu-west-3	23:59-07:29
Medio Oriente (Emirati Arabi Uniti)	me-central-1	05:00 — 13:00
Sud America (São Paulo)	sa-east-1	00:00-08:00
AWS GovCloud (Stati Uniti orientali)	us-gov-east-1	17:00-01:00
AWS GovCloud (Stati Uniti occidentali)	us-gov-west-1	06:00-14:00

Periodo di retention dei backup

Il periodo di conservazione dei backup è il numero di giorni in cui un backup automatico viene conservato prima di essere eliminato automaticamente. Amazon DocumentDB supporta un periodo di conservazione dei backup di 1—35 giorni.

Puoi impostare il periodo di retention dei backup al momento della creazione di un cluster. Se non imposti esplicitamente il periodo di retention dei backup, verrà assegnato un periodo predefinito di un giorno al cluster. Dopo aver creato un cluster, puoi modificare il periodo di conservazione dei backup modificando il cluster utilizzando il o il. [AWS Management Console](#) [AWS CLI](#) Per ulteriori informazioni, consulta [Modifica di un cluster Amazon DocumentDB](#).

Copiare Cluster Snapshot Encryption

La crittografia di cluster e snapshot si basa su una chiave di crittografia KMS. L'ID della chiave KMS è l'Amazon Resource Name (ARN), l'identificatore della chiave KMS o l'alias della chiave KMS per la chiave di crittografia KMS.

Si applicano le seguenti linee guida e limitazioni:

- La crittografia viene dedotta dal cluster durante la creazione di un'istantanea. Se il cluster è crittografato, l'istantanea di quel cluster viene crittografata con la stessa chiave KMS. Se il cluster non è crittografato, lo snapshot non è crittografato.
- Se copi uno snapshot del cluster crittografato dal tuo account Amazon Web Services, puoi specificare un valore per `KmsKeyId` crittografare la copia con una nuova chiave di crittografia KMS. Se non specifichi un valore per `KmsKeyId`, la copia dello snapshot del cluster viene crittografata con la stessa chiave KMS dello snapshot del cluster di origine.
- Se copi un'istantanea del cluster crittografata condivisa da un altro account Amazon Web Services, devi specificare un valore per `KmsKeyId`.
- Per copiare uno snapshot del cluster crittografato in un'altra regione Amazon Web Services, imposta `KmsKeyId` l'ID della chiave KMS che desideri utilizzare per crittografare la copia dello snapshot del cluster nella regione di destinazione. Le chiavi di crittografia KMS sono specifiche della regione Amazon Web Services in cui vengono create e non è possibile utilizzare le chiavi di crittografia di una regione Amazon Web Services in un'altra regione Amazon Web Services.
- Se si copia uno snapshot del cluster non crittografato e si specifica un valore per il `KmsKeyId` parametro, viene restituito un errore.

Confronto tra snapshot automatiche e manuali

Di seguito sono elencate le caratteristiche principali degli snapshot automatici e manuali di Amazon DocumentDB (con compatibilità MongoDB).

Le istantanee automatiche di Amazon DocumentDB hanno le seguenti caratteristiche chiave:

- Denominazione automatica degli snapshot: i nomi automatici degli snapshot seguono lo schema `rds:<cluster-name>-yyyy-mm-dd-hh-mm` e `yyyy-mm-dd-hh-mm` rappresentano la data e l'ora di creazione dello snapshot.
- Creato automaticamente in base a una pianificazione: quando si crea o si modifica un cluster, è possibile impostare il periodo di conservazione del backup su un valore intero compreso tra 1 e 35 giorni. Per impostazione predefinita, i nuovi cluster hanno un periodo di retention dei backup di un giorno. Il periodo di retention dei backup definisce il numero di giorni di conservazione delle snapshot automatiche prima di essere eliminate automaticamente. Non puoi disabilitare i backup automatici sui cluster Amazon DocumentDB.

Oltre a impostare il periodo di retention dei backup, puoi anche impostare la finestra di backup, l'ora del giorno in cui vengono create le snapshot automatiche.

- Eliminazione degli snapshot automatici: gli snapshot automatici vengono eliminati quando si elimina il cluster dello snapshot automatico. Non puoi eliminare manualmente una snapshot automatica.
- Incrementale: durante il periodo di conservazione dei backup, gli aggiornamenti del database vengono registrati in modo da creare un record incrementale delle modifiche.
- Ripristino da un'istantanea automatica: è possibile eseguire il ripristino da un'istantanea automatica utilizzando o il `AWS Management Console` o `AWS CLI`. Quando si esegue il ripristino da un'istantanea utilizzando il `AWS CLI`, è necessario aggiungere istanze separatamente dopo che il cluster è disponibile.
- Condivisione: non è possibile condividere uno snapshot del cluster automatizzato di Amazon DocumentDB. Come soluzione alternativa, è possibile creare uno snapshot manuale copiando lo snapshot automatico e quindi condividere la copia. Per ulteriori informazioni sulla copia di uno snapshot, consulta [Copia degli snapshot del cluster Amazon DocumentDB](#). Per ulteriori informazioni sul ripristino di un cluster da uno snapshot, consulta [Ripristino da una snapshot del cluster](#).

- È possibile eseguire il ripristino da qualsiasi momento all'interno del periodo di conservazione del backup: poiché gli aggiornamenti del database vengono registrati in modo incrementale, è possibile ripristinare il cluster in qualsiasi momento entro il periodo di conservazione del backup.

Quando si esegue il ripristino da un'istantanea automatica o da un point-in-time ripristino utilizzando il AWS CLI, è necessario aggiungere istanze separatamente dopo che il cluster è disponibile.

Le istantanee manuali di Amazon DocumentDB hanno le seguenti caratteristiche chiave:

- Creati su richiesta: gli snapshot manuali di Amazon DocumentDB vengono creati su richiesta utilizzando la console di gestione Amazon DocumentDB o. AWS CLI
- Eliminazione di uno snapshot manuale: uno snapshot manuale viene eliminato solo quando lo elimini esplicitamente utilizzando la console Amazon DocumentDB o. AWS CLI Una snapshot manuale non viene eliminata quando elimini il cluster.
- Backup completi: quando viene scattata una istantanea manuale, viene creato e archiviato un backup completo dei dati del cluster.
- Denominazione manuale delle istantanee: si specifica il nome dell'istantanea manuale. Amazon DocumentDB non aggiunge un `date:time` timbro al nome, quindi è necessario aggiungere tali informazioni se si desidera che siano incluse nel nome.
- Ripristino da un'istantanea manuale: è possibile ripristinare da un'istantanea manuale utilizzando la console o il. AWS CLI Quando si esegue il ripristino da un'istantanea utilizzando il AWS CLI, è necessario aggiungere le istanze separatamente dopo che il cluster è disponibile.
- Service Quotas: è consentito un massimo di 100 istantanee manuali per persona. Regione AWS
- Condivisione: è possibile condividere istantanee manuali del cluster, che possono essere copiate da persone autorizzate. Account AWS È possibile condividere snapshot manuali crittografati o non crittografati. Per ulteriori informazioni sulla copia di uno snapshot, consulta [Copia degli snapshot del cluster Amazon DocumentDB](#).
- Si esegue il ripristino a quando è stata scattata l'istantanea manuale: quando si ripristina da un'istantanea manuale, si ripristina a quando è stata scattata l'istantanea manuale.

Quando si esegue il ripristino da un'istantanea utilizzando il AWS CLI, è necessario aggiungere le istanze separatamente dopo che il cluster è disponibile.

Creazione di una snapshot del cluster manuale

Puoi creare uno snapshot manuale utilizzando o. AWS Management Console AWS CLI La quantità di tempo necessaria per creare uno snapshot varia a seconda della dimensione dei database. Quando crei una snapshot, devi:

1. Identificare il cluster di cui eseguire il backup.
2. Dare un nome alla tua snapshot. In questo modo potrai eseguire il ripristino da qui in un secondo momento.

Using the AWS Management Console

Per creare un'istantanea manuale utilizzando AWS Management Console, puoi seguire uno dei metodi seguenti.

1. Metodo 1:
 1. [Accedi a e apri AWS Management Console la console Amazon DocumentDB all'indirizzo https://console.aws.amazon.com/docdb.](https://console.aws.amazon.com/docdb)
 2. Nel pannello di navigazione, selezionare Snapshots (Snapshot).

Tip

Se il riquadro di navigazione non viene visualizzato sul lato sinistro della schermata, scegliere l'icona del menu (☰) nell'angolo in alto a sinistra della pagina.

3. Nella pagina Snapshots (Snapshot) scegli Create (Crea).
4. Nella pagina Create cluster snapshot (Crea snapshot cluster):
 - a. Identificatore del cluster: dall'elenco a discesa dei cluster, scegli il cluster di cui desideri creare uno snapshot.
 - b. Identificatore dell'istantanea: inserisci un nome per la tua istantanea.

Vincoli per la denominazione di snapshot:

- La lunghezza è di [1-255] lettere, numeri o trattini.
- Il primo carattere deve essere una lettera.

- Non può terminare con un trattino o contenere due trattini consecutivi.
- Deve essere unico per tutti i cluster (tra Amazon RDS, Amazon Neptune e Amazon DocumentDB) per account e per regione. AWS

c. Scegli Crea.

2. Metodo 2:

1. [Accedi a e apri AWS Management Console la console Amazon DocumentDB all'indirizzo https://console.aws.amazon.com/docdb.](https://console.aws.amazon.com/docdb)
2. Nel pannello di navigazione scegliere Clusters (Cluster).

 Tip

Se il riquadro di navigazione non viene visualizzato sul lato sinistro della schermata, scegliere l'icona del menu (☰) nell'angolo in alto a sinistra della pagina.

3. Nella pagina Clusters (Cluster) scegli il pulsante a sinistra del cluster di cui eseguire lo snapshot.
4. Dal menu Actions (Operazioni) scegli Take snapshot (Acquisisci snapshot).
5. Nella pagina Create cluster snapshot (Crea snapshot cluster):
 - a. Identificatore dello snapshot: inserisci un nome per lo snapshot.

Vincoli per la denominazione di snapshot:

- La lunghezza è di [1—63] lettere, numeri o trattini.
- Il primo carattere deve essere una lettera.
- Non può terminare con un trattino o contenere due trattini consecutivi.
- Deve essere unico per tutti i cluster (tra Amazon RDS, Amazon Neptune e Amazon DocumentDB) per account e per regione. AWS

b. Scegli Crea.

Using the AWS CLI

Per creare uno snapshot del cluster utilizzando, utilizza l'operazione con AWS CLI `create-db-cluster-snapshot` seguenti parametri.

Parametri

- **--db-cluster-identifier**: obbligatorio. Il nome del cluster di cui si sta eseguendo la snapshot. Questo cluster deve esistere ed essere disponibile.
- **--db-cluster-snapshot-identifier**: obbligatorio. Il nome della snapshot manuale che stai creando.

Nell'esempio seguente viene creato uno snapshot denominato `sample-cluster-snapshot` per un cluster denominato `sample-cluster`.

Per Linux, macOS o Unix:

```
aws docdb create-db-cluster-snapshot \  
  --db-cluster-identifier sample-cluster \  
  --db-cluster-snapshot-identifier sample-cluster-snapshot
```

Per Windows:

```
aws docdb create-db-cluster-snapshot ^  
  --db-cluster-identifier sample-cluster ^  
  --db-cluster-snapshot-identifier sample-cluster-snapshot
```

L'aspetto dell'output di questa operazione è simile al seguente.

```
{  
  "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"
  }
}
```

Copia degli snapshot del cluster Amazon DocumentDB

In Amazon DocumentDB, puoi copiare istantanee manuali e automatiche all'interno dello stesso account Regione AWS o su un altro Regione AWS all'interno dello stesso account. Puoi anche condividere istantanee di proprietà di altri Account AWS nello stesso. Regione AWS Tuttavia, non è possibile copiare un'istananea del cluster Account AWS in un unico passaggio. Regioni AWS Queste azioni devono essere eseguite singolarmente.

In alternativa alla copia, puoi anche condividere istantanee manuali con altri. Account AWS Per ulteriori informazioni, consulta [Condivisione di istantanee del cluster Amazon DocumentDB](#).

Note

Amazon DocumentDB fattura le fatture in base alla quantità di dati di backup e snapshot conservati e al periodo di tempo in cui vengono conservati. Per ulteriori informazioni sullo storage associato ai backup e agli snapshot di Amazon DocumentDB, consulta [Informazioni sull'utilizzo dello storage di backup](#) Per informazioni sui prezzi dello storage Amazon DocumentDB, consulta i prezzi di [Amazon DocumentDB](#).

Argomenti

- [Copia di snapshot condivise](#)
- [Copiare istantanee da una parte all'altra Regioni AWS](#)
- [Limitazioni](#)
- [Gestione della crittografia](#)
- [Considerazioni sui gruppi di parametri](#)

- [Copia di una snapshot del cluster](#)

Copia di snapshot condivise

Puoi copiare istantanee condivise con te da altri. Account AWS Se stai copiando un'istananea crittografata che è stata condivisa da un'altra persona Account AWS, devi avere accesso alla chiave di AWS KMS crittografia utilizzata per crittografare l'istananea.

È possibile copiare solo un'istananea condivisa nella stessa Regione AWS, indipendentemente dal fatto che l'istananea sia crittografata o meno. Per ulteriori informazioni, consulta [Gestione della crittografia](#).

Copiare istantanee da una parte all'altra Regioni AWS

Quando si copia un'istananea su un'istananea diversa da Regione AWS quella di origine Regione AWS, ogni copia è un'istananea completa. Una copia istantanea completa contiene tutti i dati e i metadati necessari per ripristinare il cluster Amazon DocumentDB.

A seconda del soggetto Regioni AWS coinvolto e della quantità di dati da copiare, il completamento di una copia istantanea tra diverse regioni può richiedere ore. In alcuni casi, potrebbe esserci un gran numero di richieste di copia di istantanee tra regioni diverse da una determinata fonte. Regione AWS In questi casi, Amazon DocumentDB potrebbe mettere in coda nuove richieste di copia interregionali provenienti da tale fonte fino al completamento di alcune copie Regione AWS in corso. Nessuna informazione di progresso viene visualizzata sulle richieste di copia mentre sono in coda. Le informazioni sul progresso vengono visualizzate quando inizia la copia.

Limitazioni

Di seguito sono riportate alcune limitazioni che si applicano quando si copiano le snapshot:

- Se elimini una snapshot origine prima che la snapshot target diventi disponibile, la copia della snapshot può non riuscire. Verifica che la snapshot target abbia lo stato di AVAILABLE prima di eliminare una snapshot origine.
- Puoi avere un massimo di cinque richieste di copia di snapshot in corso in una singola regione di destinazione per account
- A seconda delle regioni coinvolte e la quantità di dati da copiare, la copia di una snapshot tra regioni potrebbe richiedere diverse ore. Per ulteriori informazioni, consulta [Copiare istantanee da una parte all'altra Regioni AWS](#).

Gestione della crittografia

Puoi copiare una snapshot che è stata crittografata utilizzando una chiave di crittografia AWS KMS . Se la copia di una snapshot crittografata, la copia della snapshot deve anche essere crittografata. Se copi uno snapshot crittografato all'interno della stessa Regione AWS, puoi crittografare la copia con la stessa chiave di crittografia dello snapshot originale oppure puoi specificare una chiave di AWS KMS crittografia diversa. AWS KMS Se si copia un'istantanea crittografata in più regioni, non è possibile utilizzare per la copia la stessa chiave di AWS KMS crittografia utilizzata per lo snapshot di origine, poiché le chiavi sono specifiche della regione. AWS KMS È invece necessario specificare una AWS KMS chiave valida nella destinazione n. Regione AWS

La snapshot di origine resta crittografata nel processo di copia. Per ulteriori informazioni, consulta [Protezione dei dati in Amazon DocumentDB](#).

Note

Per le istantanee del cluster Amazon DocumentDB, non è possibile crittografare un'istantanea del cluster non crittografata quando la si copia.

Considerazioni sui gruppi di parametri

Quando copi uno snapshot tra regioni, la copia non include il gruppo di parametri utilizzato dal cluster Amazon DocumentDB originale. Quando ripristini uno snapshot per creare un nuovo cluster, a quel cluster viene assegnato il gruppo di parametri predefinito in cui Regione AWS è stato creato. Per assegnare al nuovo cluster gli stessi parametri dell'originale, devi fare quanto segue:

1. Nella destinazione Regione AWS, [crea un gruppo di parametri del cluster Amazon DocumentDB](#) con le stesse impostazioni del cluster originale. Se ne esiste già uno nel nuovo Regione AWS, puoi utilizzarlo.
2. Dopo aver ripristinato lo snapshot nella destinazione Regione AWS, modifica il nuovo cluster Amazon DocumentDB e aggiungi il gruppo di parametri nuovo o esistente del passaggio precedente. Per ulteriori informazioni, consulta [Modifica di un cluster Amazon DocumentDB](#).

Copia di una snapshot del cluster

Puoi copiare un cluster Amazon DocumentDB utilizzando AWS Management Console o AWS CLI, come segue.

Using the AWS Management Console

Per creare una copia di uno snapshot del cluster utilizzando il AWS Management Console, completa i seguenti passaggi. Questa procedura consente di copiare istantanee di cluster crittografate o non crittografate, nella stessa Regione AWS regione o in più regioni.

1. [Accedi a e apri AWS Management Console la console Amazon DocumentDB all'indirizzo https://console.aws.amazon.com/docdb.](https://console.aws.amazon.com/docdb)
2. Nel pannello di navigazione, scegli Istantanee, quindi scegli il pulsante a sinistra dell'istananea che desideri copiare.

Tip

Se il riquadro di navigazione non viene visualizzato sul lato sinistro della schermata, scegliere l'icona del menu (☰) nell'angolo in alto a sinistra della pagina.

3. Nel menu Actions (Operazioni) scegliere Copy (Copia).
4. Nella pagina Crea copia dell'istananea del cluster risultante, completa la sezione Impostazioni.
 - a. Regione di destinazione: facoltativa. Per copiare l'istananea del cluster in un'altra Regione AWS, selezionala in Regione Regione AWS di destinazione.
 - b. Nuovo identificatore di istantanea: immetti un nome per la nuova istantanea.

Vincoli per la denominazione di snapshot di destinazione:

- Non può essere il nome di uno snapshot esistente.
 - La lunghezza è di [1—63] lettere, numeri o trattini.
 - Il primo carattere deve essere una lettera.
 - Non può terminare con un trattino o contenere due trattini consecutivi.
 - Deve essere unico per tutti i cluster di Amazon RDS, Neptune e Amazon DocumentDB per regione. Account AWS
- c. Copia tag: per copiare tutti i tag presenti sullo snapshot di origine nella copia dello snapshot, scegli Copia tag.
5. Completa la sezione E. nryption-at-rest

- a. Crittografia a riposo: se l'istantanea non è crittografata, queste opzioni non sono disponibili perché non è possibile creare una copia crittografata da un'istantanea non crittografata. Se l'istantanea è crittografata, è possibile modificare quella AWS KMS key utilizzata durante la crittografia a riposo.

Per ulteriori informazioni sulla crittografia delle copie degli snapshot, consulta [Copiare Cluster Snapshot Encryption](#)

Per ulteriori informazioni sulla crittografia dei dati inattivi, consultare [Crittografia dei dati Amazon DocumentDB inattiva](#).

- b. Chiave principale: dall'elenco a discesa, scegli una delle seguenti opzioni:
 - (impostazione predefinita) `aws/rds`: il numero di account e l'ID della AWS KMS chiave vengono elencati dopo questa opzione.
 - `< some-key-name >` - Se hai creato una chiave, questa viene elencata e puoi sceglierla.
 - Inserisci una chiave ARN: nella casella ARN, inserisci l'Amazon Resource Name (ARN) per la tua chiave. AWS KMS Il formato dell'ARN è `arn:aws:kms:<region>:<accountID>:key/<key-id>` .
6. Per eseguire una copia della snapshot selezionata, scegliere Copy snapshot (Copia snapshot). In alternativa, puoi scegliere Annulla per non creare una copia dello snapshot.

Using the AWS CLI

Per creare una copia di un'istantanea del cluster non crittografata utilizzando il AWS CLI, utilizzate l'`copy-db-cluster-snapshot` operazione con i seguenti parametri. Se state copiando l'istantanea su un'altra Regione AWS, eseguite il comando in cui verrà copiata Regione AWS l'istantanea.

- **`--source-db-cluster-snapshot-identifier`**: obbligatorio. L'identificatore della snapshot del cluster di cui eseguire una copia. Una snapshot del cluster con questo nome deve esistere ed essere disponibile. Se si copia l'istantanea su un'altra Regione AWS, questo identificatore deve essere nel formato ARN dell'origine. Regione AWS Questo parametro non distingue tra maiuscole e minuscole.

- **--target-db-cluster-snapshot-identifier**: obbligatorio. L'identificatore della nuova snapshot del cluster da creare dalla snapshot del cluster di origine. Questo parametro non distingue tra maiuscole e minuscole.

Vincoli per la denominazione di snapshot di destinazione:

- Non può essere il nome di uno snapshot esistente.
 - La lunghezza è di [1—63] lettere, numeri o trattini.
 - Il primo carattere deve essere una lettera.
 - Non può terminare con un trattino o contenere due trattini consecutivi.
 - Deve essere unico per tutti i cluster di Amazon RDS, Neptune e Amazon DocumentDB per regione. Account AWS
- **--source-region**— Se stai copiando lo snapshot su un altro Regione AWS, specifica da dove verrà copiato lo snapshot del Regione AWS cluster crittografato.

Se stai copiando lo snapshot su un altro Regione AWS e non lo specifichi `--source-region`, devi invece specificare l'opzione `pre-signed-url`. Il `pre-signed-url` valore deve essere un URL che contiene una richiesta firmata Signature Version 4 per `CopyDBClusterSnapshot` richiamare l'azione nell'origine da Regione AWS cui viene copiata lo snapshot del cluster. [Per ulteriori informazioni su `pre-signed-url`, consulta `CopyDBClusterSnapshot`](#)

- **--kms-key-id**— L'identificatore della chiave KMS per la chiave da utilizzare per crittografare la copia dello snapshot del cluster.

Se si copia un'istantanea del cluster crittografata su un'altra Regione AWS, questo parametro è obbligatorio. È necessario specificare una chiave KMS per la destinazione. Regione AWS

Se si copia un'istantanea del cluster crittografata nello stesso Regione AWS, il parametro AWS KMS chiave è facoltativo. La copia dell'istantanea del cluster viene crittografata con la stessa AWS KMS chiave dell'istantanea del cluster di origine. Se si desidera specificare una nuova chiave di AWS KMS crittografia da utilizzare per crittografare la copia, è possibile farlo utilizzando questo parametro.

- **--copy-tags**— Facoltativo. I tag e i valori da copiare.

Per annullare un'operazione di copia una volta che è in corso, è possibile eliminare lo snapshot del cluster di destinazione identificato da **--target-db-cluster-snapshot-identifier** o **TargetDBClusterSnapshotIdentifier** mentre lo snapshot del cluster è in stato di copia.

Example

Esempio 1: copiare un'istantanea non crittografata nella stessa regione

L' AWS CLI esempio seguente crea una copia di `sample-cluster-snapshot` named `sample-cluster-snapshot-copy` nella stessa dello snapshot Regione AWS di origine. Quando viene creata la copia, tutti i tag della snapshot originale vengono copiati nella copia della snapshot.

Per Linux, macOS o 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
```

Per 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
```

L'aspetto dell'output di questa operazione è simile al seguente.

```
{  
  "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

Esempio 2: Copiare un'istantanea non crittografata su Regioni AWS

L' AWS CLI esempio seguente crea una copia di `sample-cluster-snapshot`, che ha l'ARN `arn:aws:rds:us-east-1:123456789012:cluster-snapshot:sample-cluster-snapshot`. Questa copia è denominata `sample-cluster-snapshot-copy` e si trova nella cartella Regione AWS in cui viene eseguito il comando.

Per Linux, macOS o 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

```

Per 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

```

L'aspetto dell'output di questa operazione è simile al seguente.

```

{
  "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-1:111122223333:cluster-
snapshot:sample-cluster-snapshot-copy",
    "SourceDBClusterSnapshotArn": "arn:aws:rds:us-east-1:111122223333:cluster-
snapshot:sample-cluster-snapshot",
  }
}

```

Example

Esempio 3: Copiare un'istantanea crittografata Regioni AWS

L' AWS CLI esempio seguente crea una copia di `sample-cluster-snapshot` dalla regione `us-west-2` alla regione `us-east-1`. Questo comando viene chiamato nella regione `us-east-1`.

Per Linux, macOS o 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

```

Per 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

```

L'aspetto dell'output di questa operazione è simile al seguente.

```

{
  "DBClusterSnapshot": {
    "AvailabilityZones": [],
    "DBClusterSnapshotIdentifier": "sample-cluster-snapshot-copy",
    "DBClusterIdentifier": "ayhu-xrsc-test-ap-southeast-1-small-cluster-kms",
    "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-1:111122223333:key/sample-key-id",
    "DBClusterSnapshotArn": "arn:aws:rds:us-east-1:111122223333:cluster-
snapshot:sample-cluster-snapshot-copy",
    "SourceDBClusterSnapshotArn": "arn:aws:rds:us-west-2:111122223333:cluster-
snapshot:sample-cluster-snapshot",
  }
}

```

Note

Per ulteriori informazioni sulla crittografia delle copie di istantanee, vedere [Copiare Cluster Snapshot Encryption](#)

Per ulteriori informazioni sulla crittografia dei dati inattivi, consultare [Crittografia dei dati Amazon DocumentDB inattiva](#).

Condivisione di istantanee del cluster Amazon DocumentDB

In Amazon DocumentDB, puoi condividere istantanee manuali del cluster, che possono essere copiate da persone autorizzate. Account AWS È possibile condividere snapshot manuali crittografati o non crittografati. Quando si condivide un'istananea non crittografata, gli utenti autorizzati Account AWS possono ripristinare il cluster direttamente dalla snapshot invece di crearne una copia ed eseguire il ripristino da quella. Tuttavia, non è possibile ripristinare un cluster da uno snapshot sia condiviso che crittografato. In alternativa, è possibile effettuare una copia dalla quale ripristinare il cluster. Per ulteriori informazioni sulla copia di uno snapshot, consulta [Copia degli snapshot del cluster Amazon DocumentDB](#).

Note

Non puoi condividere uno snapshot del cluster automatizzato di Amazon DocumentDB. Come soluzione alternativa, è possibile creare uno snapshot manuale copiando lo snapshot automatico e quindi condividere la copia. Per ulteriori informazioni sulla copia di uno snapshot, consulta [Copia degli snapshot del cluster Amazon DocumentDB](#). Per ulteriori informazioni sul ripristino di un cluster da uno snapshot, consulta [Ripristino da una snapshot del cluster](#).

Puoi condividere uno snapshot manuale con un massimo di 20 altri. Account AWS Puoi anche condividere uno snapshot manuale non crittografato come pubblico, per renderlo disponibile a tutti gli account . Quando si condivide uno snapshot come pubblico, assicurarsi che non siano incluse informazioni personali.

Quando condividi snapshot manuali con altri Account AWS e ripristini un cluster da uno snapshot condiviso utilizzando l'API Amazon DocumentDB, devi specificare l'Amazon Resource Name (ARN) dello snapshot condiviso come AWS CLI identificatore dello snapshot.

Condivisione di uno snapshot crittografato

Per la condivisione di snapshot crittografati vigono le seguenti restrizioni:

- Non puoi condividere le snapshot crittografate come pubbliche.
- Non puoi condividere uno snapshot che è stato crittografato utilizzando la chiave di AWS KMS crittografia predefinita dell'account che ha condiviso lo snapshot.

Per condividere snapshot crittografati, attieniti alla seguente procedura.

1. Condividi la chiave di crittografia AWS Key Management Service (AWS KMS) utilizzata per crittografare l'istantanea con tutti gli account a cui desideri consentire l'accesso all'istantanea.

Puoi condividere le chiavi di AWS KMS crittografia con altri AWS account aggiungendo gli altri account alla politica delle AWS KMS chiavi. Per i dettagli sull'aggiornamento di una politica chiave, consulta [Uso delle politiche chiave in AWS KMS](#) nella Guida per gli AWS Key Management Service sviluppatori. Per un esempio di creazione di una policy delle chiavi, consulta [Creazione di una policy IAM per abilitare la copia di una snapshot crittografata](#) più avanti in questo argomento.

2. Utilizza AWS CLI, [come illustrato di seguito](#), per condividere l'istantanea crittografata con gli altri account.

Consentire l'accesso a una chiave di AWS KMS crittografia

Affinché un altro Account AWS utente possa copiare un'istantanea crittografata condivisa dal tuo account, l'account con cui condividi l'istantanea deve avere accesso alla AWS KMS chiave che ha crittografato l'istantanea. Per consentire a un altro account di accedere a una AWS KMS chiave, aggiorna la politica della AWS KMS chiave con l'ARN dell'account con cui stai condividendo come principale nella politica AWS KMS chiave. Successivamente, autorizza l'operazione `kms:CreateGrant`.

Dopo aver concesso a un account l'accesso alla tua chiave di AWS KMS crittografia, per copiare lo snapshot crittografato, tale account deve creare un utente AWS Identity and Access Management (IAM) se non ne ha già uno. Inoltre, quell'account deve anche allegare una policy IAM a quell'utente IAM che consenta all'utente di copiare uno snapshot crittografato utilizzando la tua AWS KMS chiave. L'account deve essere un utente IAM e non può essere un' Account AWS identità root a causa di restrizioni AWS KMS di sicurezza.

Nel seguente esempio di policy chiave, l'utente 123451234512 è il proprietario della chiave di crittografia. AWS KMS L'utente 123456789012 corrisponde all'account con cui è stata condivisa la chiave. Questa politica delle chiavi aggiornata consente all'account di accedere alla chiave. AWS KMS A tale scopo include l'ARN per l' Account AWS identità root dell'utente 123456789012 come principale della policy e consente l'azione. `kms:CreateGrant`

```
{
  "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}}
  }
]
}

```

Creazione di una policy IAM per abilitare la copia di una snapshot crittografata

Quando l'esterno Account AWS ha accesso alla tua AWS KMS chiave, il proprietario di quell'account può creare una policy per consentire a un utente IAM creato per l'account di copiare un'istantanea crittografata con quella chiave. AWS KMS

L'esempio seguente mostra una policy che può essere associata a un utente IAM per Account AWS 123456789012. La policy consente all'utente IAM di copiare un'istantanea condivisa dall'account 123451234512 che è stata crittografata con la chiave AWS KMS nella c989c1dd-a3f2-4a5d-8d96-e793d082ab26 regione us-west-2.

```
{
  "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
        }
      }
    }
  ]
}
```

Per i dettagli sull'aggiornamento di una policy chiave, consulta [Using Key Policies](#) nella [Developer Guide](#). AWS KMSAWS Key Management Service

Condivisione di una snapshot

Per condividere uno snapshot, utilizza l'operazione Amazon `modify-db-snapshot-attribute` DocumentDB. Utilizza il `--values-to-add` parametro per aggiungere un elenco degli ID autorizzati a ripristinare Account AWS lo snapshot manuale.

L'esempio seguente consente a due Account AWS identificatori, `123451234512` e `123456789012`, di ripristinare l'istantanea denominata. `manual-snapshot1` Inoltre, rimuove il valore dell'attributo `all` per contrassegnare lo snapshot come privato.

Per Linux, macOS o Unix:

```
aws docdb modify-db-cluster-snapshot-attribute \  
  --db-cluster-snapshot-identifier sample-cluster-snapshot \  
  --attribute-name restore \  
  --values-to-add '["123451234512","123456789012"]'
```

Per Windows:

```
aws docdb modify-db-cluster-snapshot-attribute ^  
  --db-cluster-snapshot-identifier sample-cluster-snapshot ^  
  --attribute-name restore ^  
  --values-to-add '["123451234512","123456789012"]'
```

L'aspetto dell'output di questa operazione è simile al seguente.

```
{  
  "DBClusterSnapshotAttributesResult": {  
    "DBClusterSnapshotIdentifier": "sample-cluster-snapshot",  
    "DBClusterSnapshotAttributes": [  
      {  
        "AttributeName": "restore",  
        "AttributeValues": [  
          "123451234512",  
          "123456789012"  
        ]  
      }  
    ]  
  }  
}
```

```
}
```

Per rimuovere un identificatore dall'elenco, utilizzare il parametro. Account AWS --values-to-remove L'esempio seguente impedisce all' Account AWS ID 123456789012 di ripristinare l'istantanea.

Per Linux, macOS o Unix:

```
aws docdb modify-db-cluster-snapshot-attribute \  
  --db-cluster-snapshot-identifier sample-cluster-snapshot \  
  --attribute-name restore \  
  --values-to-remove '["123456789012"]'
```

Per Windows:

```
aws docdb modify-db-cluster-snapshot-attribute ^  
  --db-cluster-snapshot-identifier sample-cluster-snapshot ^  
  --attribute-name restore ^  
  --values-to-remove '["123456789012"]'
```

L'aspetto dell'output di questa operazione è simile al seguente.

```
{  
  "DBClusterSnapshotAttributesResult": {  
    "DBClusterSnapshotIdentifier": "sample-cluster-snapshot",  
    "DBClusterSnapshotAttributes": [  
      {  
        "AttributeName": "restore",  
        "AttributeValues": [  
          "123451234512"  
        ]  
      }  
    ]  
  }  
}
```

Ripristino da una snapshot del cluster

Amazon DocumentDB (con compatibilità con MongoDB) crea uno snapshot del cluster del volume di storage. Puoi creare un nuovo cluster ripristinandolo da una snapshot del cluster. Quando ripristini il

cluster, devi fornire il nome della snapshot del cluster da cui effettuare il ripristino e il nome del nuovo cluster creato dal ripristino. Non puoi eseguire il ripristino da una snapshot in un cluster esistente poiché al momento del ripristino viene creato un nuovo cluster.

Quando ripristini un cluster da una snapshot del cluster:

- Questa operazione ripristina solo il cluster, non le istanze del cluster. Devi utilizzare l'operazione `create-db-instance` per creare le istanze per il cluster ripristinato, specificandone l'identificatore in `--db-cluster-identifier`. Puoi creare le istanze solo dopo che il cluster è disponibile.
- Non puoi ripristinare una snapshot crittografata in un cluster non crittografato. Tuttavia, puoi ripristinare un'istantanea non crittografata in un cluster crittografato specificando la chiave. AWS KMS
- Per ripristinare un cluster da un'istantanea crittografata, è necessario avere accesso alla chiave. AWS KMS

Note

Non è possibile ripristinare un cluster 3.6 su un cluster 4.0 ma è possibile migrare da una versione del cluster a un'altra. Per ulteriori informazioni, consulta [Migrazione ad Amazon DocumentDB](#).

Using the AWS Management Console

La procedura seguente mostra come ripristinare un cluster Amazon DocumentDB da uno snapshot del cluster utilizzando la console di gestione Amazon DocumentDB.

1. [Accedi a e apri AWS Management Console la console Amazon DocumentDB all'indirizzo `https://console.aws.amazon.com/docdb`.](https://console.aws.amazon.com/docdb)
2. Nel riquadro di navigazione scegli Snapshots (Snapshot) e seleziona il pulsante a sinistra della snapshot che desideri usare per ripristinare un cluster.

Tip

Se il riquadro di navigazione non viene visualizzato sul lato sinistro della schermata, scegliere l'icona del menu



nell'angolo in alto a sinistra della pagina.



3. Dal menu Actions (Operazioni) scegli Restore (Ripristina).
4. Nella pagina Restore snapshot (Ripristina snapshot) completa la sezione Configuration (Configurazione).
 - a. Identificatore del cluster: il nome del nuovo cluster. Puoi accettare il nome fornito da Amazon DocumentDB o digitare un nome che preferisci. Il nome fornito da Amazon DocumentDB è nel formato docdb- più un timestamp UTC; ad esempio, `docdb-yyyy-mm-dd-hh-mm-ss`
 - b. Classe di istanza: la classe di istanza per il nuovo cluster. Puoi accettare la classe di istanza predefinita o scegliere una classe di istanza dall'elenco a discesa.
 - c. Numero di istanze: il numero di istanze che si desidera creare con questo cluster. È possibile accettare l'impostazione predefinita di 3 istanze (1 primaria di lettura/scrittura e 2 repliche di sola lettura) o scegliere il numero di istanze dall'elenco a discesa.
5. Per la configurazione dello storage del cluster, scegli un'opzione di archiviazione.



Note

La configurazione di storage ottimizzata per l'I/O di Amazon DocumentDB è disponibile solo nella versione del motore Amazon DocumentDB 5.0.

6. Se si è soddisfatti della configurazione del cluster, scegliere Restore cluster (Ripristina cluster) e attendere il ripristino del cluster.
7. Se preferisci modificare alcune configurazioni, ad esempio specificare un Amazon VPC o un gruppo di sicurezza non predefinito, scegli Mostra impostazioni avanzate nella parte inferiore sinistra della pagina, quindi continua con i passaggi seguenti.
 - a. Completa la sezione Network settings (Impostazioni di rete).
 - Virtual Private Cloud (VPC): accetta il VPC corrente o scegli un VPC dall'elenco a discesa.
 - Gruppo di sottoreti: accetta il gruppo di default sottoreti o scegline uno dall'elenco a discesa.
 - Gruppi di sicurezza VPC: accetta il gruppo default (VPC) di sicurezza o scegline uno dall'elenco.

- b. Completa la sezione Cluster options (Opzioni cluster).
 - Porta del database: accetta la porta predefinita o utilizza la freccia su o giù per impostare la porta che desideri utilizzare per le connessioni alle applicazioni. 27017
- c. Completa la sezione Encryption (Crittografia).
 - Crittografia a riposo: se l'istantanea è crittografata, queste opzioni non sono disponibili. Se non è crittografata, puoi scegliere una delle seguenti opzioni:
 - Per crittografare tutti i dati del cluster, scegli Abilita. encryption-at-rest Se scegli questa opzione, è necessario specificare una Master key (Chiave master).
 - Per non crittografare i dati del cluster, scegli Disabilita. encryption-at-rest Se scegli questa opzione, hai terminato con la sezione relativa alla crittografia.
 - Chiave principale: scegli una delle seguenti opzioni dall'elenco a discesa:
 - (impostazione predefinita) aws/rds: il numero di account e l'ID della AWS KMS chiave vengono elencati dopo questa opzione.
 - Chiave gestita dal cliente: questa opzione è disponibile solo se hai creato una chiave di crittografia IAM nella console (IAM). AWS Identity and Access Management Puoi scegliere la chiave per eseguire la crittografia del cluster.
 - Inserisci una chiave ARN: nella casella ARN, inserisci l'Amazon Resource Name (ARN) per la tua chiave. AWS KMS Il formato dell'ARN è `arn:aws:kms:<region>:<accountID>:key/<key-id>`.
- d. Compila la sezione Log exports (Esportazioni di log).
 - Seleziona i tipi di log su cui pubblicare CloudWatch: scegli una delle seguenti opzioni:
 - Abilitato: consente al cluster di esportare i log DDL in Amazon CloudWatch Logs.
 - Disabilitato: impedisce al cluster di esportare i log DDL in Amazon Logs. CloudWatch L'opzione predefinita è Disabled (Disabilitato).
 - Ruolo IAM: dall'elenco, scegli RDS Service Linked Role.
- e. Completa la sezione Tag .
 - Aggiungi tag: nella casella Chiave, inserisci il nome del tag per il tuo cluster. Nella casella Value (Valore) immetti facoltativamente il valore del tag. I tag vengono utilizzati con le policy AWS Identity and Access Management (IAM) per gestire l'accesso alle risorse di Amazon DocumentDB e per controllare quali azioni possono essere applicate alle risorse.

- f. Completa la sezione Deletion protection (Protezione da eliminazione) .
 - Abilita la protezione da eliminazione: protegge il cluster dall'eliminazione accidentale. Quando questa opzione è abilitata, non puoi eliminare il cluster.
8. Scegli Restore cluster (Ripristina cluster).

Using the AWS CLI

Per ripristinare un cluster da un'istantanea utilizzando il AWS CLI, utilizzare l'`restore-db-cluster-from-snapshot` operazione con i seguenti parametri. Per ulteriori informazioni, consulta [RestoreDBClusterFromSnapshot](#).

- **--db-cluster-identifier**: obbligatorio. Il nome del cluster che viene creato dall'operazione. Prima di questa operazione non devono esistere cluster con questo nome.

Vincoli per la denominazione del cluster:

- La lunghezza è di [1-63] lettere, numeri o trattini.
- Il primo carattere deve essere una lettera.
- Non può terminare con un trattino o contenere due trattini consecutivi.
- Deve essere unico per tutti i cluster di Amazon RDS, Neptune e Amazon DocumentDB per regione. Account AWS
- **--snapshot-identifier**: obbligatorio. Il nome della snapshot utilizzata per eseguire il ripristino. Una snapshot con questo nome deve esistere ed essere disponibile.
- **--engine**: obbligatorio. Deve essere `docdb`.
- **--storage-type standard | iopt1**— Facoltativo. Default: `standard`.
- **--kms-key-id**— Facoltativo. L'ARN dell'identificatore di AWS KMS chiave da utilizzare per il ripristino di un'istantanea crittografata o per la crittografia di un cluster durante il ripristino da un'istantanea non crittografata. Fornendo l'ID della AWS KMS chiave, il cluster ripristinato viene crittografato con la chiave, indipendentemente dal fatto che l'istantanea sia stata crittografata o AWS KMS meno.

Il formato di `--kms-key-id` è `arn:aws:kms:<region>:<accountID>:key/<key-id>`.

Se non specifichi un valore per il parametro `--kms-key-id`, avviene quanto segue:

- Se l'istantanea in ingresso `--snapshot-identifier` è crittografata, il cluster ripristinato viene crittografato utilizzando la stessa AWS KMS chiave utilizzata per crittografare l'istantanea.

- Se la snapshot in `--snapshot-identifier` non è crittografata, il cluster ripristinato non è crittografato.

Per Linux, macOS o 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
```

Per 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
```

L'aspetto dell'output di questa operazione è simile al seguente.

```
{  
  "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
  }
}

```

Dopo che lo stato del cluster è disponibile, crea almeno un'istanza per il cluster.

Per Linux, macOS o 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

```

Per 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

```

L'aspetto dell'output di questa operazione è simile al seguente.

```
{
  "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-ABCDEFGHIJKLMNQPQRSTUVWXYZ",
  }
}
```

```
"CACertificateIdentifier": "rds-ca-2019",
  "PromotionTier": 2,
  "DBInstanceArn": "arn:aws:rds:us-east-1:<accountID>:db:sample-cluster-
restore-instance"
}
```

Ripristino a un punto temporale specifico

Puoi ripristinare un cluster in qualsiasi momento che rientri nel periodo di conservazione del backup del cluster utilizzando AWS Management Console o AWS Command Line Interface (AWS CLI).

Note

Non è possibile eseguire un point-in-time ripristino di un cluster 3.6 su un cluster 4.0, ma è possibile migrare da una versione del cluster a un'altra. Per ulteriori informazioni, consulta [Migrazione ad Amazon DocumentDB](#).

Tieni presente quanto segue quando ripristini un cluster a un punto temporale specifico.

- Il nuovo cluster viene creato con la stessa configurazione del cluster di origine, ma utilizza il gruppo di parametri predefinito. Per impostare il gruppo di parametri del nuovo cluster su quello del cluster di origine, occorre modificare il cluster appena risulta disponibile. Per ulteriori informazioni sulla modifica di un cluster, consulta [Modifica di un cluster Amazon DocumentDB](#).

Using the AWS Management Console

È possibile ripristinare un cluster point-in-time entro il relativo periodo di conservazione dei backup completando le seguenti operazioni utilizzando il AWS Management Console

1. [Accedi a e apri AWS Management Console la console Amazon DocumentDB all'indirizzo https://console.aws.amazon.com/docdb](https://console.aws.amazon.com/docdb).
2. Nel pannello di navigazione scegliere Clusters (Cluster). Dall'elenco di cluster scegliere il pulsante a sinistra del cluster che si desidera ripristinare.


 Tip

Se il riquadro di navigazione non viene visualizzato sul lato sinistro della schermata, scegliere l'icona del menu (☰) nell'angolo in alto a sinistra della pagina.

3. Nel menu Actions (Operazioni) scegliere Restore to point in time (Esegui ripristino point in time).
4. Completare la sezione Restore time (Ora ripristino), in cui si specificano data e ora per il ripristino.
 - a. Data di ripristino: scegli o inserisci una data compresa tra la prima ora di ripristino e l'ora di ripristino più recente.
 - b. Ora di ripristino: scegli o inserisci l'ora, i minuti e i secondi compresi tra l'ora di ripristino più recente e l'ora di ripristino più recente.
5. Completare la sezione Configurazione.
 - a. Identificatore del cluster: accetta l'identificatore predefinito o inserisci un identificatore che preferisci.

Vincoli per la denominazione del cluster:

 - La lunghezza è di [1—63] lettere, numeri o trattini.
 - Il primo carattere deve essere una lettera.
 - Non può terminare con un trattino o contenere due trattini consecutivi.
 - Deve essere unico per tutti i cluster di Amazon RDS, Neptune e Amazon DocumentDB per regione. Account AWS
 - b. Classe di istanza: dall'elenco a discesa, scegli la classe di istanza che desideri per le istanze del cluster.
 - c. Numero di istanze: dall'elenco a discesa, scegli il numero di istanze che desideri creare quando il cluster viene ripristinato.
6. Per la configurazione dello storage del cluster, scegli un'opzione di archiviazione.

 Note

La configurazione di storage ottimizzata per l'I/O di Amazon DocumentDB è disponibile solo nella versione del motore Amazon DocumentDB 5.0.

7. Facoltativo. Per configurare le impostazioni di rete, le opzioni del cluster e abilitare le esportazioni dei log, scegliere Show advanced settings (Mostra impostazioni avanzate) e completare le sezioni seguenti. In alternativa, passare alla fase successiva.
 - Impostazioni di rete
 1. Virtual Private Cloud (VPC): dall'elenco a discesa, scegli il VPC che desideri utilizzare per questo cluster.
 2. Gruppo di sottoreti: dall'elenco a discesa, scegli il gruppo di sottoreti per questo cluster.
 3. Gruppi di sicurezza VPC: dall'elenco a discesa, scegli i gruppi di sicurezza VPC per questo cluster.
 - Cluster options (Opzioni cluster)
 1. Porta: accetta la porta predefinita (27017) o utilizza le frecce su e giù per impostare la porta per la comunicazione con questo cluster.
 - Log exports (Esportazioni log)
 1. Registri di controllo: seleziona questa opzione per abilitare l'esportazione dei log di controllo in Amazon Logs. CloudWatch Se selezioni questa opzione, devi abilitare `audit_logs` nel gruppo personalizzato dei parametri del cluster. Per ulteriori informazioni, consulta [Controllo degli eventi di Amazon DocumentDB](#).
 2. Registri del profiler: seleziona questa opzione per abilitare l'esportazione dei log del profiler operativo su Amazon Logs. CloudWatch Se selezioni questa opzione, devi anche modificare i seguenti parametri nel gruppo personalizzato dei parametri del cluster:
 - `profiler— enabled` Impostato su.
 - `profiler_threshold_ms`— Impostato su un valore `[0-INT_MAX]` per impostare la soglia per le operazioni di profilazione.
 - `profiler_sampling_rate`— Impostare su un valore `[0.0-1.0]` per impostare la percentuale di operazioni lente da profilare.

Per ulteriori informazioni, consulta [Profilazione delle operazioni di Amazon DocumentDB](#).

3. Registri del profiler: esporta i log del profiler su Amazon CloudWatch
 4. Ruolo IAM: dall'elenco a discesa, scegli RDS Service Linked Role.
- Tag
 1. Aggiungi tag: nella casella Chiave, inserisci il nome del tag per il tuo cluster. Nella casella Value (Valore) immetti facoltativamente il valore del tag. I tag vengono utilizzati con le policy AWS Identity and Access Management (IAM) per gestire l'accesso alle risorse di Amazon DocumentDB e per controllare quali azioni possono essere applicate alle risorse.
 - Deletion protection (Protezione da eliminazione)
 1. Abilita la protezione da eliminazione: protegge il cluster dall'eliminazione accidentale. Quando questa opzione è abilitata, non puoi eliminare il cluster.
8. Per ripristinare il cluster, scegliere Create cluster (Crea cluster). In alternativa, è possibile scegliere Cancel (Annulla) per annullare l'operazione.

Using the AWS CLI

Per ripristinare un cluster a un punto temporale specifico con il periodo di retention dei backup della snapshot, utilizza l'operazione `restore-db-cluster-to-point-in-time` con i parametri seguenti.

- **--db-cluster-identifier**— Obbligatorio. Il nome del nuovo cluster da creare. Questo cluster non può esistere prima di questa operazione. Il valore del parametro deve soddisfare i seguenti vincoli.

Vincoli per la denominazione del cluster:

- La lunghezza è di [1—63] lettere, numeri o trattini.
 - Il primo carattere deve essere una lettera.
 - Non può terminare con un trattino o contenere due trattini consecutivi.
 - Deve essere unico per tutti i cluster di Amazon RDS, Neptune e Amazon DocumentDB per regione. Account AWS
- **--restore-to-time**— La data e l'ora UTC a cui ripristinare il cluster. Ad esempio, `2018-06-07T23:45:00Z`.

Vincoli temporali:

- Deve essere prima dell'ultimo orario di ripristino per il cluster.
- Deve essere specificato se il parametro `--use-latest-restorable-time` non viene fornito.
- Non può essere specificato se il parametro `--use-latest-restorable-time` è `true`.
- Non può essere specificato se il valore del parametro `--restore-type` è `copy-on-write`.
- **`--source-db-cluster-identifier`**— Il nome del cluster di origine da cui eseguire il ripristino. Questo cluster deve esistere ed essere disponibile.
- **`--use-latest-restorable-time`** oppure **`--no-use-latest-restorable-time`** — Se ripristinare l'ultima data di backup ripristinabile. Non può essere specificato se il parametro `--restore-to-time` viene fornito.
- **`--storage-type standard | iopt1`**— Facoltativo. Default: `standard`.

L'AWS CLI operazione ripristina `restore-db-cluster-to-point-in-time` solo il cluster, non le relative istanze. È necessario utilizzare l'operazione `create-db-instance` per creare le istanze per il cluster ripristinato, specificandone l'identificatore in `--db-cluster-identifier`. Puoi creare le istanze solo dopo che l'operazione `restore-db-cluster-to-point-in-time` è terminata e il cluster ripristinato è disponibile.

Example

L'esempio seguente crea `sample-cluster-restored` dallo snapshot `sample-cluster-snapshot` all'ultimo orario di ripristino.

Per Linux, macOS o 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
```

Per 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

Nell'esempio seguente viene creato `sample-cluster-restored` dallo snapshot `sample-cluster-snapshot` delle 3:15 dell'11 dicembre 2018 (UTC), ovvero un orario incluso nel periodo di retention dei backup di `sample-cluster`.

Per Linux, macOS o 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
```

Per 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
```

L'aspetto dell'output di questa operazione è simile al seguente.

```
{  
  "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-ABCDEFGHIJKLMNQRSTUWXYZ",
"DBClusterArn": "arn:aws:rds:us-east-1:<accountID>:cluster:sample-cluster-restored",
"AssociatedRoles": [],
"ClusterCreateTime": "2020-04-24T20:14:36.713Z",
"DeletionProtection": false
}
}
```

Eliminazione di una snapshot del cluster

Uno snapshot manuale è un backup completo che viene eliminato solo quando viene eliminato manualmente utilizzando o. AWS Management Console AWS CLI Non è possibile eliminare manualmente una snapshot automatica, in quanto le snapshot automatiche vengono eliminate solo quando il periodo di retention delle snapshot scade o quando si elimina il rispettivo cluster.

Using the AWS Management Console

Per eliminare un'istantanea manuale del cluster utilizzando il AWS Management Console, completare la procedura seguente.

1. [Accedi a e apri AWS Management Console la console Amazon DocumentDB all'indirizzo https://console.aws.amazon.com/docdb](https://console.aws.amazon.com/docdb).
2. Nel pannello di navigazione, selezionare Snapshots (Snapshot).

i Tip

Se il riquadro di navigazione non viene visualizzato sul lato sinistro della schermata, scegliere l'icona del menu (☰) nell'angolo in alto a sinistra della pagina.

3. Nell'elenco delle snapshot scegli il pulsante a sinistra della snapshot da eliminare. Il tipo di snapshot deve essere manuale.
 1. È possibile verificare che il tipo di snapshot sia manual (manuale) controllando se è elencato come manual o automatic sotto la colonna Type (Tipo).
4. Nel menu Actions (Operazioni) selezionare Delete (Elimina). Se l'opzione Delete (Elimina) non è disponibile, probabilmente hai scelto una snapshot automatica.
5. Nella schermata di conferma dell'eliminazione, scegli Delete (Elimina) per eliminare la snapshot. Per mantenere la snapshot, scegli Cancel (Annulla).

Using the AWS CLI

Uno snapshot manuale del cluster di Amazon DocumentDB è un backup completo che puoi eliminare manualmente utilizzando AWS CLI. Non puoi eliminare manualmente una snapshot automatica.

Per eliminare uno snapshot manuale del cluster utilizzando il AWS CLI, utilizza l'operazione `delete-db-cluster-snapshot` con i seguenti parametri.

Parametri

- **`--db-cluster-snapshot-identifier`**: obbligatorio. Il nome della snapshot manuale da eliminare.

L'esempio seguente elimina la snapshot del cluster `sample-cluster-snapshot`.

Per Linux, macOS o Unix:

```
aws docdb delete-db-cluster-snapshot \
  --db-cluster-snapshot-identifier sample-cluster-snapshot
```

Per Windows:

```
aws docdb delete-db-cluster-snapshot ^  
  --db-cluster-snapshot-identifier sample-cluster-snapshot
```

L'output di questa operazione elenca i dettagli dello snapshot del cluster eliminato.

Gestione delle risorse di Amazon DocumentDB

Queste sezioni riguardano i vari componenti e le relative attività per la gestione dell'implementazione di Amazon DocumentDB (con compatibilità con MongoDB).

Argomenti

- [Panoramica sulle attività operative di](#)
- [Panoramica dei cluster globali di Amazon DocumentDB](#)
- [Gestione dei cluster Amazon DocumentDB](#)
- [Gestione delle istanze di Amazon DocumentDB](#)
- [Gestione dei gruppi di sottoreti Amazon DocumentDB](#)
- [Amazon DocumentDB](#)
- [Gestione degli indici Amazon DocumentDB](#)
- [Gestione della compressione dei documenti a livello di raccolta](#)
- [Gestione degli eventi Amazon DocumentDB](#)
- [Scelta di regioni e zone di disponibilità](#)
- [Gestione dei gruppi di parametri del cluster Amazon DocumentDB](#)
- [Comprendere gli endpoint di Amazon DocumentDB](#)
- [Informazioni su Amazon DocumentDB Amazon Resource Names \(ARN\)](#)
- [Etichettatura delle risorse Amazon DocumentDB](#)
- [Manutenzione di Amazon DocumentDB](#)
- [Comprendere i ruoli collegati ai servizi](#)

Panoramica sulle attività operative di

Questa sezione tratta delle attività operative per il cluster Amazon DocumentDB (con compatibilità MongoDB) e di come eseguirle utilizzando l'AWS CLI.

Argomenti

- [Aggiunta di una replica a un cluster Amazon DocumentDB](#)
- [Descrizione di cluster e istanze](#)

- [Creazione di una snapshot del cluster](#)
- [Ripristino da una snapshot](#)
- [Rimozione di un'istanza da un cluster](#)
- [Eliminazione di un cluster](#)

Aggiunta di una replica a un cluster Amazon DocumentDB

Una volta creata l'istanza primaria per il cluster Amazon DocumentDB, puoi aggiungere una o più istanze direpliche. Una replica è un'istanza di sola lettura che svolge due funzioni:

- Scalabilità— Se molti client devono accedere contemporaneamente, puoi aggiungere più repliche per il dimensionamento della lettura.
- Elevata disponibilità— Se l'istanza primaria non riesce, Amazon DocumentDB esegue automaticamente il failover a una determinata istanza di replica e la designa come nuova istanza primaria. Se una replica non riesce, le altre istanze nel cluster saranno ancora in grado di assolvere le richieste finché non viene ripristinato il nodo con l'errore.

Ogni cluster Amazon DocumentDB può supportare un massimo di 15 repliche.

Note

Per la massima tolleranza ai guasti, devi distribuire le repliche in zone di disponibilità separate. Questa configurazione garantisce che il cluster Amazon DocumentDB continui a funzionare anche se un'intera zona di disponibilità diventa non disponibile.

L'esempio seguente dell'AWS CLI mostra come aggiungere una nuova replica. Il parametro `--availability-zone` posiziona la replica nella zona di disponibilità specificata.

```
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
```

Descrizione di cluster e istanze

I seguenti AWS CLI esempio elenca tutti i cluster Amazon DocumentDB in una regione.

Per alcune funzionalità di gestione, come la gestione del ciclo di vita di cluster e istanze,

Amazon DocumentDB sfrutta la tecnologia operativa condivisa con Amazon RDS.

La `filterName=engine,Values=docdb` parametro filtro restituisce solo i cluster Amazon DocumentDB.

Per ulteriori informazioni sulla descrizione e la modifica dei cluster, consulta [Ciclo di vita del cluster Amazon DocumentDB](#).

```
aws docdb describe-db-clusters --filter Name=engine,Values=docdb
```

L'aspetto dell'output di questa operazione è simile al seguente.

```
{
  "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",
      ...
    }
  ]
}

```

I seguenti AWS CLI esempio elenca le istanze in un cluster Amazon DocumentDB. Per ulteriori informazioni sulla descrizione e la modifica dei cluster, consulta [Ciclo di vita delle istanze Amazon DocumentDB](#).

```

aws docdb describe-db-clusters \
  --db-cluster-identifier sample-cluster \
  --query 'DBClusters[*].[DBClusterMembers]'

```

L'aspetto dell'output è simile al seguente. In questo output, ci sono due istanze. L'istanza primaria è sample-instance-1 ("IsClusterWriter": true). È presente anche un'istanza di replica, 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
      }
    ]
  ]
}
```

Creazione di una snapshot del cluster

UNSnapshot del cluster è un backup completo dei dati nel cluster Amazon DocumentDB. Quando viene creato la snapshot, Amazon DocumentDB legge i dati direttamente dal volume cluster. Per questo motivo, puoi creare una snapshot anche se il cluster non contiene alcuna istanza attualmente in esecuzione. La quantità di tempo necessaria per creare una snapshot varia a seconda della dimensione del volume cluster.

Amazon DocumentDB supporta i backup automatici, che vengono eseguiti giornalmente durante la finestra di backup preferita, un intervallo di 30 minuti durante il giorno. L'esempio seguente dell'AWS CLI mostra come visualizzare la finestra di backup per il cluster:

```
aws docdb describe-db-clusters \  
  --db-cluster-identifier sample-cluster \  
  --query 'DBClusters[*].PreferredBackupWindow'
```

L'output mostra la finestra di backup (in UTC):

```
[  
  "00:18-00:48"  
]
```

Puoi definire la finestra di backup quando crei il cluster Amazon DocumentDB. Puoi anche modificare la finestra di backup, come nell'esempio seguente: Se non definisci una finestra di backup, Amazon DocumentDB ne assegna automaticamente una al cluster.

```
aws docdb modify-db-cluster \  
  --db-cluster-identifier sample-cluster \  
  --preferred-backup-window "02:00-02:30"
```

Oltre ai backup automatici, puoi creare manualmente una snapshot del cluster in qualsiasi momento. In questo caso, devi specificare il cluster di cui eseguire il backup e un nome univoco per la snapshot che consenta di ripristinarla in un secondo momento.

L'esempio seguente dell'AWS CLI mostra come creare una snapshot dei dati:

```
aws docdb create-db-cluster-snapshot \  
  --db-cluster-identifier sample-cluster \  
  --db-cluster-snapshot-identifier sample-cluster-snapshot
```

Ripristino da una snapshot

Puoi ripristinare una snapshot del cluster in un nuovo cluster Amazon DocumentDB. A tale scopo, devi specificare il nome della snapshot e il nome di un nuovo cluster. Non puoi eseguire il ripristino da una snapshot a un cluster esistente, ma Amazon DocumentDB crea un nuovo cluster al momento del ripristino e quindi lo popola con i dati della snapshot.

L'esempio seguente mostra tutte le snapshot per il cluster `sample-cluster`.

```
aws docdb describe-db-cluster-snapshots \  
  --db-cluster-identifier sample-cluster \  
  --query 'DBClusterSnapshots[*].[DBClusterSnapshotIdentifier,SnapshotType,Status]'
```

L'output è simile al seguente. Una snapshot manuale viene creata manualmente, mentre una snapshot automatica viene creata da Amazon DocumentDB all'interno della finestra di backup del cluster.

```
[  
  "sample-cluster-snapshot",  
  "manual",  
  "available"  
],  
 [  
  "rds:sample-cluster",  
  "automated",  
  "available"  
 ]  
]
```

Nell'esempio seguente viene illustrato come ripristinare un cluster Amazon DocumentDB da una snapshot.

```
aws docdb restore-db-cluster-from-snapshot \  
  --engine docdb \  
  --db-cluster-identifier sample-cluster
```

```
--db-cluster-identifier new-sample-cluster \  
--snapshot-identifier sample-cluster-snapshot
```

Il nuovo cluster non ha istanze associate, quindi per interagire con questo cluster devi aggiungervi un'istanza:

```
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
```

Puoi utilizzare le operazioni dell'AWS CLI seguenti per monitorare l'avanzamento della creazione del cluster e dell'istanza: Quando lo stato del cluster e delle istanze è disponibile, puoi connetterti all'endpoint del nuovo cluster e accedere ai dati.

```
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]'
```

Rimozione di un'istanza da un cluster

Amazon DocumentDB archivia tutti i dati nel volume cluster. I dati persistono nel volume cluster, anche se rimuovi tutte le istanze dal cluster. Se hai bisogno di accedere nuovamente ai dati, puoi aggiungere un'istanza al cluster in qualsiasi momento e riprendere da dove avevi lasciato.

Nell'esempio seguente viene illustrato come rimuovere un'istanza dal cluster Amazon DocumentDB.

```
aws docdb delete-db-instance \  
  --db-instance-identifier sample-instance
```

Eliminazione di un cluster

Per eliminare un cluster Amazon DocumentDB, devi rimuovere prima tutte le sue istanze. L'esempio seguente dell'AWS CLI restituisce informazioni sulle istanze in un cluster: Se questa operazione

restituisce uno o più identificatori di istanza, devi eliminare tutte le istanze. Per ulteriori informazioni, consultare [Rimozione di un'istanza da un cluster](#).

```
aws docdb describe-db-clusters \  
  --db-cluster-identifier sample-cluster \  
  --query 'DBClusters[*].DBClusterMembers[*].DBInstanceIdentifier'
```

Dopo aver rimosso tutte le istanze, puoi eliminare il cluster. A questo punto, devi scegliere una delle seguenti opzioni:

- Creazione di una snapshot finale— Acquisisci tutti i dati del cluster in una snapshot in modo da poter ricreare una nuova istanza con i dati. L'esempio seguente mostra la procedura per farlo:

```
aws docdb delete-db-cluster \  
  --db-cluster-identifier sample-cluster \  
  --final-db-snapshot-identifier sample-cluster-snapshot
```

- Ignora l'istantanea finale— Elimina definitivamente tutti i dati del cluster. Questa operazione non può essere annullata. L'esempio seguente mostra la procedura per farlo:

```
aws docdb delete-db-cluster \  
  --db-cluster-identifier sample-cluster \  
  --skip-final-snapshot
```

Panoramica dei cluster globali di Amazon DocumentDB

Cos'è un cluster globale?

Un cluster globale è composto da una regione principale e da un massimo di cinque aree secondarie di sola lettura. Le operazioni di scrittura vengono eseguite direttamente sul cluster primario nella regione primaria e Amazon DocumentDB replica automaticamente i dati nelle regioni secondarie utilizzando un'infrastruttura dedicata. La latenza è in genere inferiore a un secondo.

In che modo sono utili i cluster globali?

- Ripristino da interruzioni a livello regionale: in caso di interruzione a livello regionale, è possibile promuovere uno dei cluster secondari a cluster primario in pochi minuti, con un Recovery Time

Objective (RTO) tipico inferiore a un minuto. Il Recovery Point Objective (RPO) viene in genere misurato in secondi, ma dipende dal ritardo della rete al momento dell'errore.

- Letture globali con latenza locale: se hai uffici in tutto il mondo, puoi utilizzare un cluster globale per mantenere aggiornate le principali fonti di informazioni nella regione principale. Gli uffici delle altre aree geografiche possono accedere alle informazioni nella propria regione, con latenza locale.
- Cluster secondari scalabili: è possibile scalare i cluster secondari aggiungendo altre istanze di sola lettura a un'area secondaria. Il cluster secondario è di sola lettura, quindi può supportare fino a 16 istanze di replica in sola lettura anziché il normale limite di 15 per un singolo cluster.
- Replica rapida dai cluster primari a quelli secondari: la replica eseguita da un cluster globale ha un impatto minimo sulle prestazioni del cluster di database primario. Le risorse delle istanze database sono totalmente dedicate a servire carichi di lavoro di lettura e scrittura delle applicazioni.

Quali sono gli attuali limiti dei cluster globali?

- I cluster globali non sono supportati su Amazon DocumentDB v3.6.
- I cluster globali non sono supportati sui tipi di istanze t3, t4g e r4.
- I cluster globali non sono disponibili nelle seguenti regioni: Sud America (San Paolo), Europa (Milano), Cina (Pechino) e Cina (Ningxia).
- In caso di failover regionale, è necessario promuovere manualmente un cluster secondario affinché diventi cluster primario e modificare l'applicazione in modo che punti al nuovo cluster primario.
- Solo il cluster primario eseguire operazioni di scrittura. I client che eseguono operazioni di scrittura si connettono all'endpoint del cluster primario.
- È possibile disporre di un massimo di cinque regioni secondarie e una regione principale per il cluster.
- Un cluster secondario non può essere fermato. Un cluster primario non può essere interrotto se è associato a cluster secondari. È possibile interrompere solo un cluster regionale senza cluster secondari.
- Le repliche collegate al cluster secondario possono essere riavviate in determinate circostanze. Se l'istanza della regione primaria si riavvia o esegue il failover, vengono riavviate anche le repliche nell'area secondaria. Il cluster non sarà quindi disponibile finché tutte le repliche non saranno nuovamente sincronizzate con l'istanza writer del cluster di database primario. Si tratta di un comportamento normale. Assicurati di comprendere l'impatto sul cluster globale prima di apportare modifiche al cluster primario.
- Non è possibile utilizzare i flussi di modifica sui cluster secondari.

Argomenti

- [Guida introduttiva rapida: Cluster globali](#)
- [Gestione di un cluster globale Amazon DocumentDB](#)
- [Connect a un cluster globale di Amazon DocumentDB](#)
- [Monitoraggio dei cluster globali di Amazon DocumentDB](#)
- [Disaster Recovery e cluster globali Amazon DocumentDB](#)

Guida introduttiva rapida: Cluster globali

Argomenti

- [Configurazione](#)
- [Creazione di un cluster globale Amazon DocumentDB](#)
- [Aggiungere un file Regione AWS a un cluster globale Amazon DocumentDB](#)
- [Utilizzo di uno snapshot per il cluster globale Amazon DocumentDB](#)

Configurazione

Il cluster globale di Amazon DocumentDB si estende su almeno due. Regioni AWS La regione primaria supporta un cluster con un'istanza primaria (writer) e fino a quindici istanze di replica, mentre una regione secondaria gestisce un cluster di sola lettura composto interamente da un massimo di sedici istanze di replica. Un cluster globale può avere fino a cinque aree secondarie. La tabella elenca il numero massimo di cluster, istanze e repliche consentiti in un cluster globale.

Descrizione	Regione AWS principale	Regione AWS secondarie
Cluster	1	5 massimo
Istanze di scrittura	1	0
Istanze di sola lettura (repliche Amazon DocumentDB), per cluster	15 (massimo)	16 (totali)
Istanze di sola lettura (massimo consentito, dato	15 - s	s = numero totale di Regioni AWS secondarie

Descrizione	Regione AWS principale	Regione AWS secondarie
il numero effettivo di regioni secondarie)		

I cluster hanno i seguenti requisiti specifici:

- **Requisiti delle classi di istanze di database:** è possibile utilizzare solo le classi di db .r6 istanze db .r5 e.
- **Regione AWSrequisiti:** il cluster primario deve trovarsi in una regione e almeno un cluster secondario deve trovarsi in un'area diversa dello stesso account. È possibile creare fino a cinque cluster secondari (di sola lettura) e ognuno deve trovarsi in una regione diversa. In altre parole, non è possibile che due cluster si trovino nella stessa regione.
- **Requisiti di denominazione:** i nomi scelti per ogni cluster devono essere unici, in tutte le regioni. Non puoi utilizzare lo stesso nome per cluster diversi anche se si trovano in aree geografiche diverse.

Creazione di un cluster globale Amazon DocumentDB

Sei pronto a creare il tuo primo cluster globale? In questa sezione spiegheremo come creare un cluster globale nuovo di zecca con nuovi cluster e istanze di database, utilizzando AWS Management Console o AWS CLI con le seguenti istruzioni.

Utilizzo di AWS Management Console

1. NelAWS Management Console, accedi ad Amazon DocumentDB.
2. Quando accedi alla console Amazon DocumentDB, scegli Clusters.

The screenshot shows the AWS Management Console interface for Amazon DocumentDB. On the left, the navigation sidebar is visible with 'Clusters' highlighted in red. The main content area displays 'DocumentDB > Clusters' and a list of 11 clusters. A search bar labeled 'Filter Resources' is at the top. The cluster list includes columns for selection, cluster identifier, and a plus icon. The 'Create' button in the top right corner of the cluster list is circled in red.

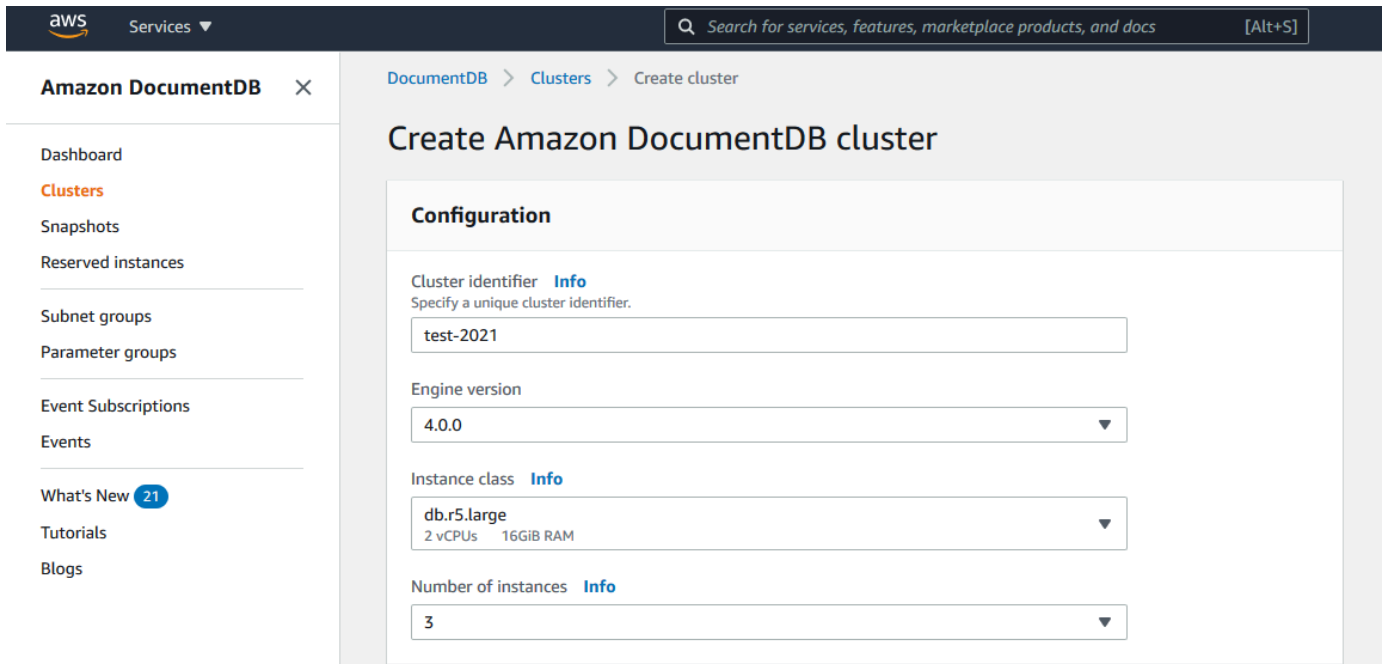
3. Scegli Crea.

The screenshot shows the 'Create cluster' configuration page in the AWS Management Console. The 'Create' button in the top right corner is circled in red. Below the button is a table with columns for Role, Engine version, Region & AZ, Status, Size, and Maintenance. The table contains three rows of cluster configurations.

Role	Engine version	Region & AZ	Status	Size	Maintenance
Global cluster	4.0.0	3 regions	available	3 clusters	-
Regional cluster	4.0.0	us-east-2	available	1 Instance	None
Global cluster	4.0.0	3 regions	available	3 clusters	-

4. Compila di conseguenza la sezione Configurazione del modulo Crea cluster Amazon DocumentDB:

- Identificatore del cluster: puoi inserire un identificatore univoco per questa istanza o consentire ad Amazon DocumentDB di fornire l'identificatore dell'istanza basato sull'identificatore del cluster.
- Versione del motore: scegli 4.0.0
- Classe di istanza: scegli db.r5.large
- Numero di istanze: scegli 3.

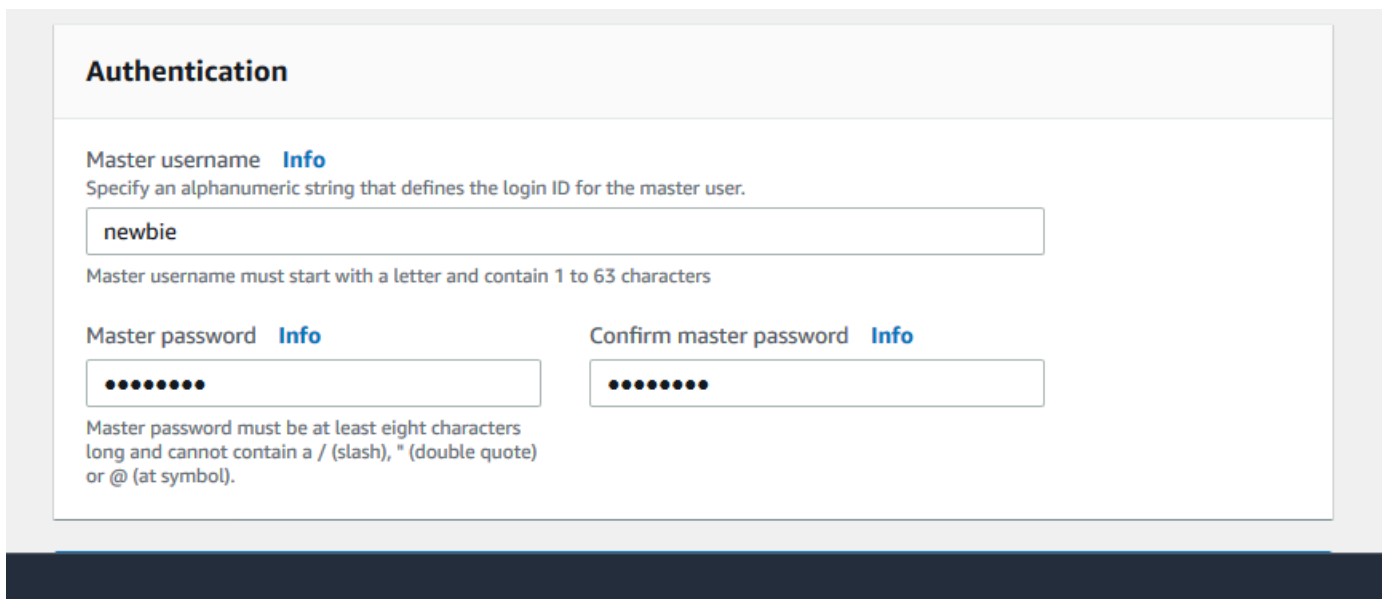


The screenshot shows the AWS Management Console interface for creating a new Amazon DocumentDB cluster. The breadcrumb navigation at the top indicates the path: DocumentDB > Clusters > Create cluster. The main heading is "Create Amazon DocumentDB cluster".

The "Configuration" section contains the following fields:

- Cluster identifier** (Info): Specify a unique cluster identifier. The value entered is "test-2021".
- Engine version**: A dropdown menu showing "4.0.0".
- Instance class** (Info): A dropdown menu showing "db.r5.large" with specifications "2 vCPUs" and "16GiB RAM".
- Number of instances** (Info): A dropdown menu showing "3".

5. Nella sezione Autenticazione, inserisci un nome utente e una password principali.

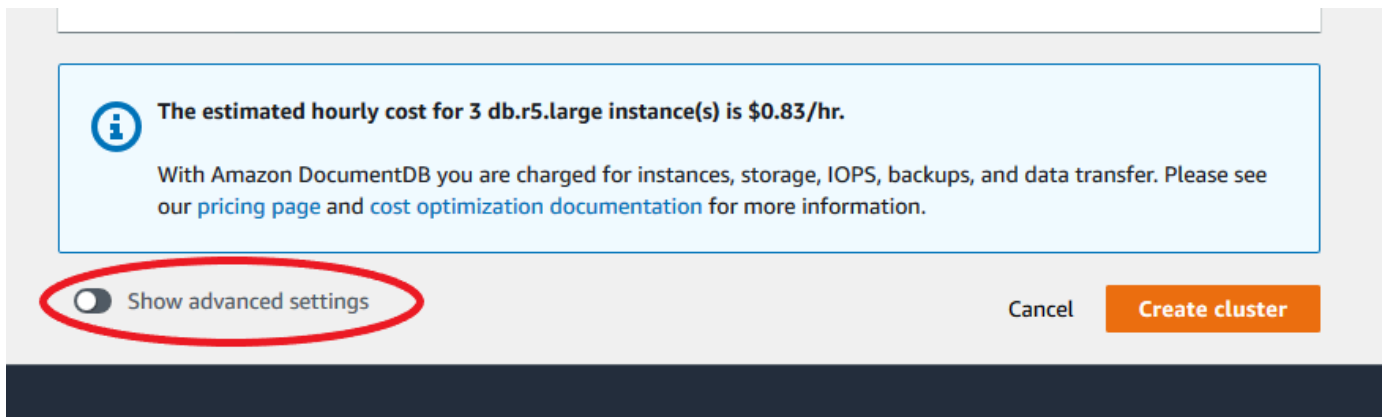


The screenshot shows the "Authentication" section of the AWS Management Console. It contains the following fields and instructions:

- Master username** (Info): Specify an alphanumeric string that defines the login ID for the master user. The value entered is "newbie". Below the field, it states: "Master username must start with a letter and contain 1 to 63 characters".
- Master password** (Info): A password field with masked characters (dots).
- Confirm master password** (Info): A second password field with masked characters (dots).

Below the password fields, it states: "Master password must be at least eight characters long and cannot contain a / (slash), " (double quote) or @ (at symbol)."

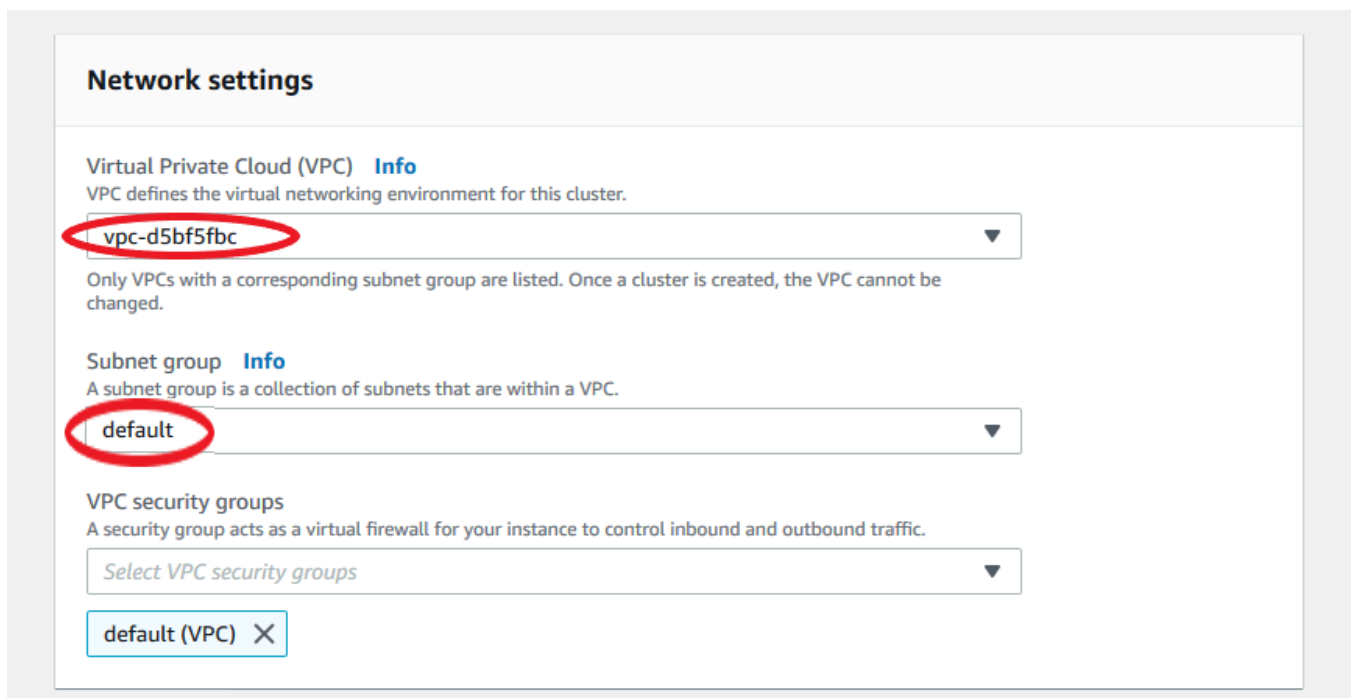
6. Scegli Mostra impostazioni avanzate.



The screenshot shows a light blue information box at the top with an 'i' icon. The text inside reads: "The estimated hourly cost for 3 db.r5.large instance(s) is \$0.83/hr. With Amazon DocumentDB you are charged for instances, storage, IOPS, backups, and data transfer. Please see our [pricing page](#) and [cost optimization documentation](#) for more information." Below this box is a toggle switch labeled "Show advanced settings" which is currently turned off and circled in red. To the right of the toggle are "Cancel" and "Create cluster" buttons.

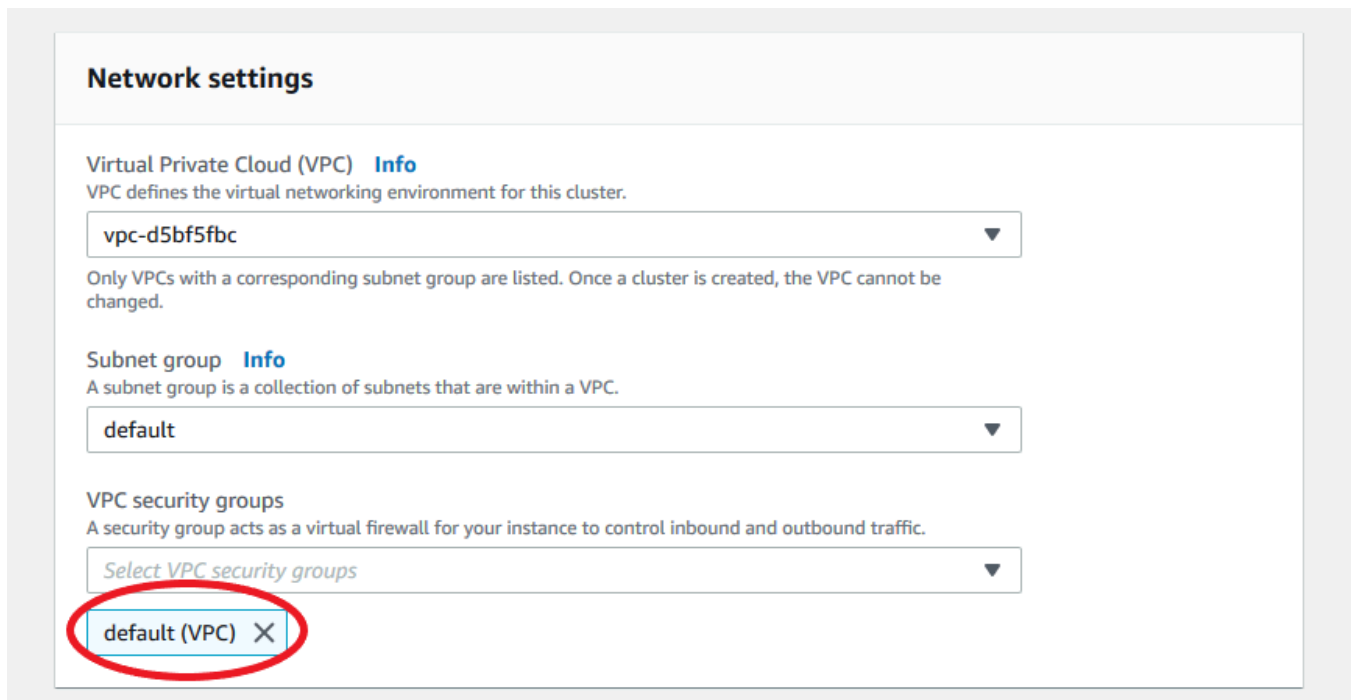
7. Nella sezione Impostazioni di rete:

- Mantieni le opzioni predefinite per Virtual Private Cloud e Subnet Group.

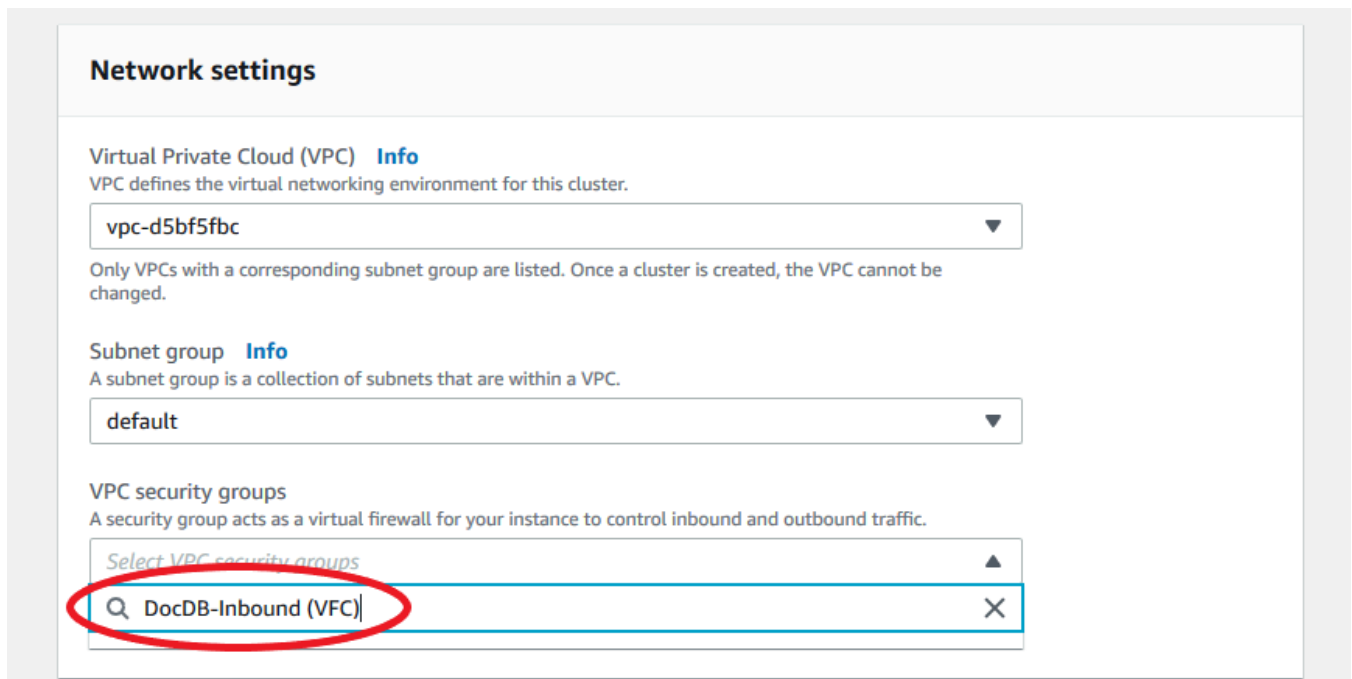


The screenshot shows the "Network settings" section. It includes three dropdown menus: "Virtual Private Cloud (VPC)", "Subnet group", and "VPC security groups". The "VPC" dropdown is set to "vpc-d5bf5fbc" and is circled in red. The "Subnet group" dropdown is set to "default" and is also circled in red. The "VPC security groups" dropdown is currently empty, showing the placeholder text "Select VPC security groups". Below the dropdowns, there is a button labeled "default (VPC) X".

- Per i gruppi di sicurezza VPC, il VPC predefinito dovrebbe già essere aggiunto.



- Digita DocDB nel campo Gruppi di sicurezza VPC e seleziona DOCDB-Inbound (VPC).



8. Per Cluster Options ed E, lascia le selezioni predefinite nryption-at-rest.

Cluster options

Port
TCP/IP port that is used to connect to the cluster.

27017

Cluster parameter group [Info](#)

default.docdb4.0

Encryption-at-rest

Encryption-at-rest [Info](#)

Enable encryption

Disable encryption

Master key

(default) aws/rds

Account

827630067164

KMS key ID

5e5dbe6b-e29d-4cfd-bfe5-585582908728

9. Per Backup ed Esportazioni di log, lascia le selezioni predefinite.

Backup

Backup retention period [Info](#)
A period between 1 and 35 days in which you can perform a point-in-time restore and for which automated backups are retained.

1 day ▼

Backup window
The daily time range (in UTC) during which automated backups are created.

Start time **Duration**

00 ▼ : 00 ▼ UTC 0.5 ▼ hours

Log exports

Select the log types to publish to Amazon CloudWatch Logs

Audit logs

Profiler logs

IAM role
The following service-linked role is used for publishing logs to CloudWatch Logs.

RDS Service Linked Role

i To enable auditing, ensure that both exporting auditing logs to Amazon CloudWatch is enabled and the Cluster Parameter "Auditing" is enabled.
[Learn more](#) ↗

10. Per la manutenzione, i tag e la protezione dall'eliminazione, lascia le selezioni predefinite.

Maintenance

Maintenance window [Info](#)
The period in which pending modifications or patches are applied to Instances in the cluster.

Select window

No preference

Tags

No tags

[Add tag](#)

Deletion protection

Enable deletion protection
Protects the cluster from being accidentally deleted. While this option is enabled, you can't delete the cluster.

11. Ora fai clic sul pulsante che dice Crea.

i The estimated hourly cost for 3 db.r5.large instance(s) is \$0.83/hr.

With Amazon DocumentDB you are charged for instances, storage, IOPS, backups, and data transfer. Please see our [pricing page](#) and [cost optimization documentation](#) for more information.

Show advanced settings

Cancel [Create cluster](#)

Utilizzo di AWS CLI

Per creare un cluster regionale Amazon DocumentDB, chiama il `create-db-cluster` AWS CLI II AWS CLI comando seguente crea un cluster Amazon DocumentDB denominato `global-cluster-id` Per ulteriori informazioni sulla protezione da eliminazione, consulta [Eliminazione di un cluster Amazon DocumentDB](#).

Inoltre, `--engine-version` è un parametro opzionale che utilizza per impostazione predefinita l'ultima versione principale del motore. L'attuale versione principale del motore è `4.0.0`. Quando vengono rilasciate nuove versioni principali del motore, la versione predefinita del motore viene aggiornata in modo da riflettere l'ultima versione principale del motore. `--engine-version` Di conseguenza, per i carichi di lavoro di produzione, in particolare quelli che dipendono da script, automazione o AWS CloudFormation modelli, si consiglia di specificare esplicitamente la versione principale `--engine-version` desiderata.

Se non `vpc-security-group-id` viene specificato un `db-subnet-group-name` or, Amazon DocumentDB utilizzerà il gruppo di sottoreti e il gruppo di sicurezza Amazon VPC predefiniti per la regione specificata.

Nell'esempio seguente, sostituisci ogni *segnaposto dell'input utente* con le tue informazioni.

Per Linux, macOS o 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
```

Per 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
```

L'aspetto dell'output di questa operazione è simile al seguente (formato JSON).

```
{  
  "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-KQSGI4MHU4NTDDRVLNTU7XVAY",
    "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"
  }
}

```

La creazione del cluster richiede diversi minuti. Puoi utilizzare la AWS Management Console o l'AWS CLI per monitorare lo stato del cluster. Per ulteriori informazioni, consulta [Monitoraggio dello stato di un cluster Amazon DocumentDB](#).

Important

Quando si utilizza AWS CLI per creare un cluster regionale Amazon DocumentDB, non viene creata alcuna istanza. Di conseguenza, devi creare esplicitamente un'istanza primaria e le eventuali istanze di replica di cui hai bisogno. Per creare le istanze puoi utilizzare la console o l'AWS CLI. Per ulteriori informazioni, consulta [Aggiungere un'istanza Amazon DocumentDB a un cluster](#) e [CreateDBCluster](#) consulta Amazon DocumentDB API Reference.

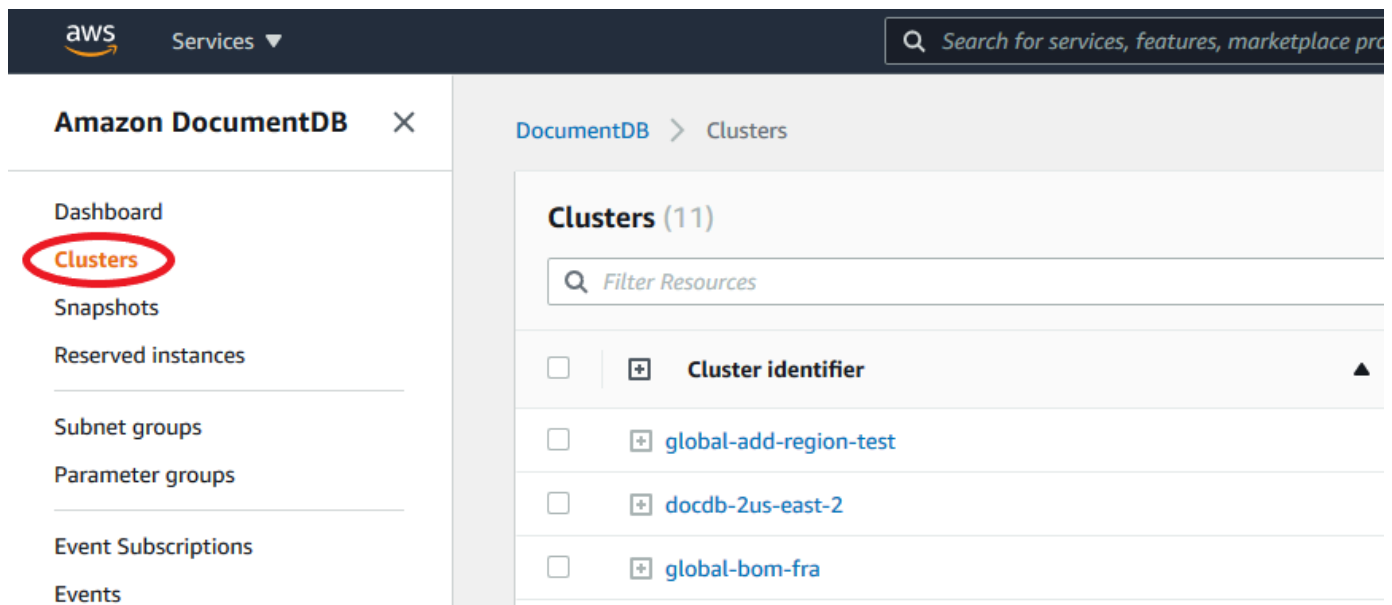
Una volta che il cluster regionale è disponibile, puoi aggiungere un cluster secondario in un'altra regione con le seguenti istruzioni:[Aggiungere un file Regione AWS a un cluster globale Amazon DocumentDB](#). Quando aggiungi una regione, il tuo cluster regionale diventa il cluster principale, e hai un nuovo cluster secondario nella regione che hai scelto.

Aggiungere un file Regione AWS a un cluster globale Amazon DocumentDB

Un cluster globale necessita di almeno un cluster secondario in una regione diversa da quella del cluster primario ed è possibile aggiungere fino a cinque cluster secondari. Tieni presente che per ogni cluster secondario che aggiungi, devi ridurre di una il numero di repliche consentite nel cluster primario. Ad esempio, se il cluster globale ha cinque regioni secondarie, il cluster primario può avere solo dieci (anziché quindici) repliche. Per ulteriori informazioni, consulta [Requisiti di configurazione di un cluster globale Amazon DocumentDB](#).

Utilizzo di AWS Management Console

1. Accedi AWS Management Console e apri la console Amazon DocumentDB.
2. Nel pannello di navigazione scegliere Clusters (Cluster).



3. Scegli il cluster a cui desideri aggiungere un cluster secondario. Assicurati che il cluster sia `Available`.

DocumentDB > Clusters

Clusters (10) Group Resources

Filter Resources

<input type="checkbox"/>	Cluster identifier	Role	Engine version	Region & AZ	Status
<input type="checkbox"/>	global-add-region-test	Global cluster	4.0.0	3 regions	available
<input type="checkbox"/>	docdb-2021-04-13-22-02-38	Regional cluster	4.0.0	us-east-1	available
<input type="checkbox"/>	global-bom-fra	Global cluster	4.0.0	3 regions	available
<input type="checkbox"/>	docdb-test	Regional cluster	4.0.0	us-east-1	available
<input checked="" type="checkbox"/>	mydocdbglobalcluster	Global cluster	4.0.0	2 regions	available

4. Seleziona il menu a discesa per Azioni, quindi scegli Aggiungi regione.

DocumentDB > Clusters

Clusters (10) Group Resources

Filter Resources

<input type="checkbox"/>	Cluster identifier	Role	Engine version	Region & AZ	Status	Actions	Maintenance
<input type="checkbox"/>	global-add-region-test	Global cluster	4.0.0	3 regions	available	3 clusters	-
<input type="checkbox"/>	docdb-2021-04-13-22-02-38	Regional cluster	4.0.0	us-east-1	available	0 Instances	None
<input type="checkbox"/>	global-bom-fra	Global cluster	4.0.0	3 regions	available	3 clusters	-
<input type="checkbox"/>	docdb-test	Regional cluster	4.0.0	us-east-1	available	0 Instances	None
<input checked="" type="checkbox"/>	mydocdbglobalcluster	Global cluster	4.0.0	2 regions	available	2 clusters	-

Actions menu: Add Region (circled), Modify, Delete, Create

5. Nella pagina Aggiungi una regione, scegli la regione secondaria. Tieni presente che non puoi scegliere una regione che abbia già un cluster secondario per lo stesso cluster globale. Inoltre, non può essere la stessa regione del cluster primario. Se questa è la prima regione che aggiungi, dovrai anche specificare un identificatore globale del cluster a tua scelta.

DocumentDB > Clusters > Add region

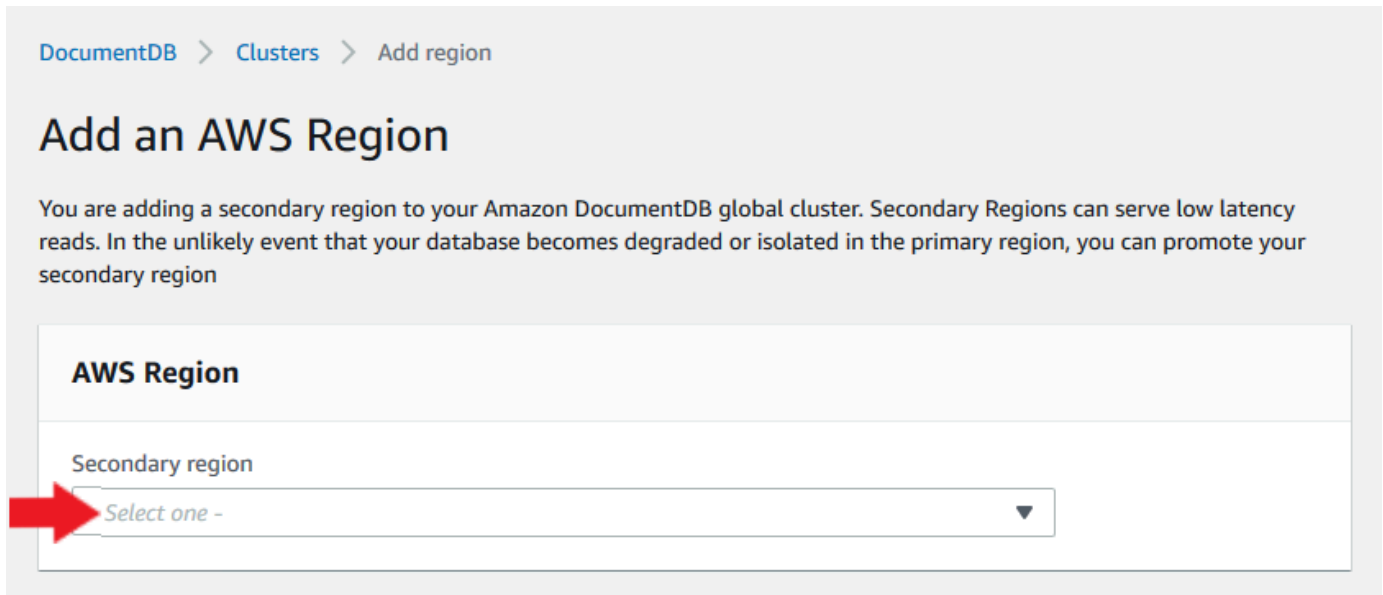
Add an AWS Region

You are adding a secondary region to your Amazon DocumentDB global cluster. Secondary Regions can serve low latency reads. In the unlikely event that your database becomes degraded or isolated in the primary region, you can promote your secondary region

AWS Region

Secondary region

Select one -



6. Completa i campi rimanenti per il cluster secondario nella nuova regione, quindi seleziona Crea cluster. Dopo aver aggiunto la regione, puoi visualizzarla nell'elenco dei cluster in. AWS Management Console

Configuration


Global Cluster Id
firstregion

Cluster identifier [Info](#)
Specify a unique cluster identifier.

Instance class [Info](#)

2 vCPUs 16GiB RAM

Number of instances [Info](#)

 **The estimated hourly cost for 3 db.r5.large instance(s) is \$0.83/hr.**

With Amazon DocumentDB you are charged for instances, storage, IOPS, backups, and data transfer. Please see our [pricing page](#) and [cost optimization documentation](#) for more information.

Show advanced settings

Cancel Create cluster

Utilizzo di AWS CLI

- Usa il comando `create-db-cluster` CLI con il nome (`--global-cluster-identifier`) del tuo cluster globale. Per gli altri parametri, effettuare le seguenti operazioni:
 - Perché `--region`, scegli una regione Regione AWS diversa da quella della tua regione principale.
 - Scegli i valori specifici per i parametri `--engine` e `--engine-version`.
 - Per un cluster crittografato, specificare la Regione AWS principale come `--source-region` per la crittografia.

L'esempio seguente crea un nuovo cluster Amazon DocumentDB e lo collega al cluster globale come cluster secondario di sola lettura. Nell'ultimo passaggio, l'istanza viene aggiunta al nuovo cluster.

Nell'esempio seguente, sostituisci ogni *segnaposto dell'input utente* con le tue informazioni.

Per Linux, macOS o 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
```

Per 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
```

Utilizzo di uno snapshot per il cluster globale Amazon DocumentDB

Puoi ripristinare uno snapshot di un cluster Amazon DocumentDB da utilizzare come punto di partenza per il tuo cluster globale. A tale scopo, è necessario ripristinare lo snapshot e creare un nuovo cluster. Questo fungerà da cluster principale del cluster globale. È quindi possibile aggiungere un'altra regione al cluster ripristinato, convertendola così in un cluster globale.

Gestione di un cluster globale Amazon DocumentDB

La maggior parte delle operazioni di gestione vengono eseguite sui singoli cluster che costituiscono un cluster globale. Quando scegli Risorse correlate al gruppo nella pagina Cluster della console, vedi il cluster primario e i cluster secondari raggruppati nel cluster globale associato.

La scheda Configurazione per un cluster globale mostra Regioni AWS dove vengono eseguiti i cluster, la versione e l'identificatore globale del cluster.

Argomenti

- [Modifica di un cluster globale Amazon DocumentDB](#)
- [Modifica dei parametri di un cluster globale Amazon DocumentDB](#)
- [Rimozione di un cluster da un cluster globale Amazon DocumentDB](#)
- [Eliminazione di un cluster da un cluster globale Amazon DocumentDB](#)
- [Creazione di un cluster Amazon DocumentDB headless in una regione secondaria](#)

Modifica di un cluster globale Amazon DocumentDB

La pagina Cluster AWS Management Console elenca tutti i cluster globali, mostrando il cluster primario e i cluster secondari per ciascuno di essi. Il cluster globale ha le proprie impostazioni di configurazione. In particolare, ha regioni associate ai suoi cluster primari e secondari.

Quando apporti modifiche al cluster globale, hai la possibilità di annullare le modifiche.

Quando si sceglie Continue (Continua), si confermano le modifiche.

Modifica dei parametri di un cluster globale Amazon DocumentDB

È possibile configurare i gruppi di parametri del cluster in modo indipendente per ogni cluster all'interno del cluster globale. La maggior parte dei parametri funziona come per altri tipi di cluster Amazon DocumentDB. Si consiglia di mantenere le impostazioni coerenti tra tutti i cluster di un database globale. In questo modo è possibile evitare modifiche impreviste del comportamento se si promuove un cluster secondario come primario.

Ad esempio, utilizzare le stesse impostazioni per fusi orari e set di caratteri per evitare comportamenti incoerenti se un cluster diverso diventa un cluster primario.

Rimozione di un cluster da un cluster globale Amazon DocumentDB

Esistono diverse situazioni in cui potresti voler rimuovere i cluster dal tuo cluster globale. Ad esempio, potresti voler rimuovere un cluster da un cluster globale se il cluster primario diventa degradato o isolato. Diventa quindi un cluster autonomo con provisioning che può essere utilizzato per creare un nuovo cluster globale. Per ulteriori informazioni, consulta Ripristino manuale di un cluster globale da un'interruzione non pianificata.

Potresti anche voler rimuovere i cluster perché desideri eliminare un cluster globale che non ti serve più. Puoi eliminare il cluster globale solo dopo aver scollegato tutti i cluster associati, lasciando il cluster primario per ultimo. Per ulteriori informazioni, consulta Eliminazione di un cluster globale Amazon DocumentDB.

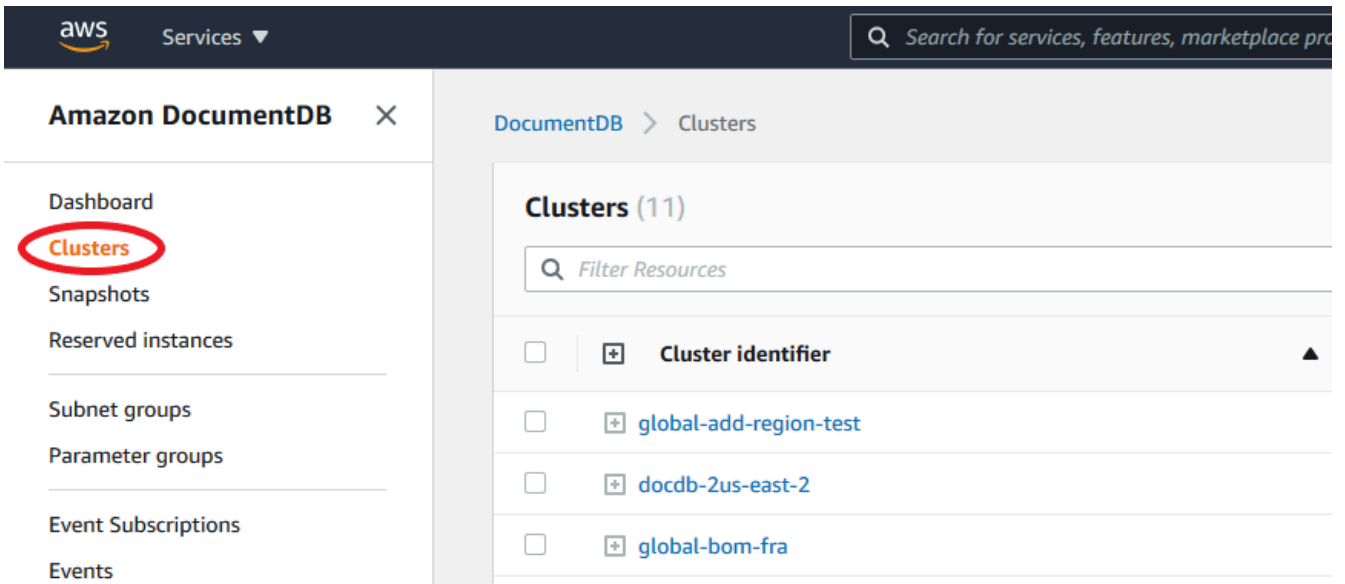
Note

Quando un cluster viene scollegato dal cluster globale, non è più sincronizzato con il cluster primario. Diventa un cluster autonomo con funzionalità complete di lettura/scrittura. Inoltre, non è più visibile nella console Amazon DocumentDB. È visibile solo quando si seleziona la regione nella console in cui si trovava il cluster.

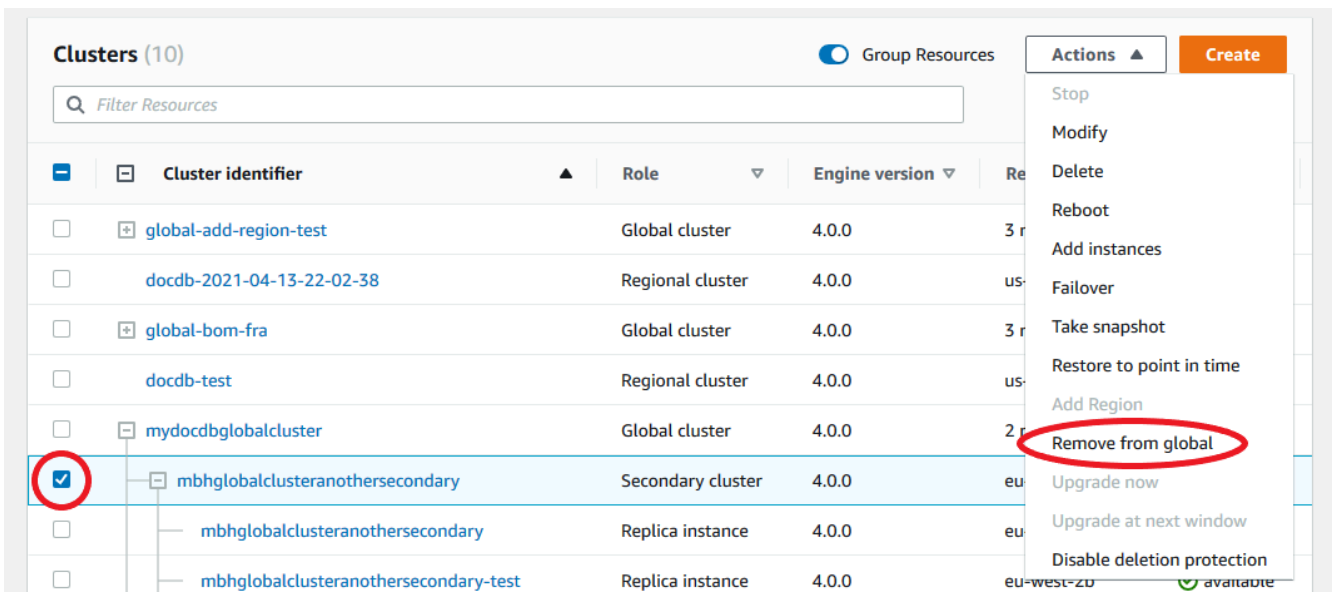
È possibile rimuovere i cluster dal cluster globale utilizzando l'AWS Management Console API RDS o AWS CLI l'API RDS.

Using the AWS Management Console

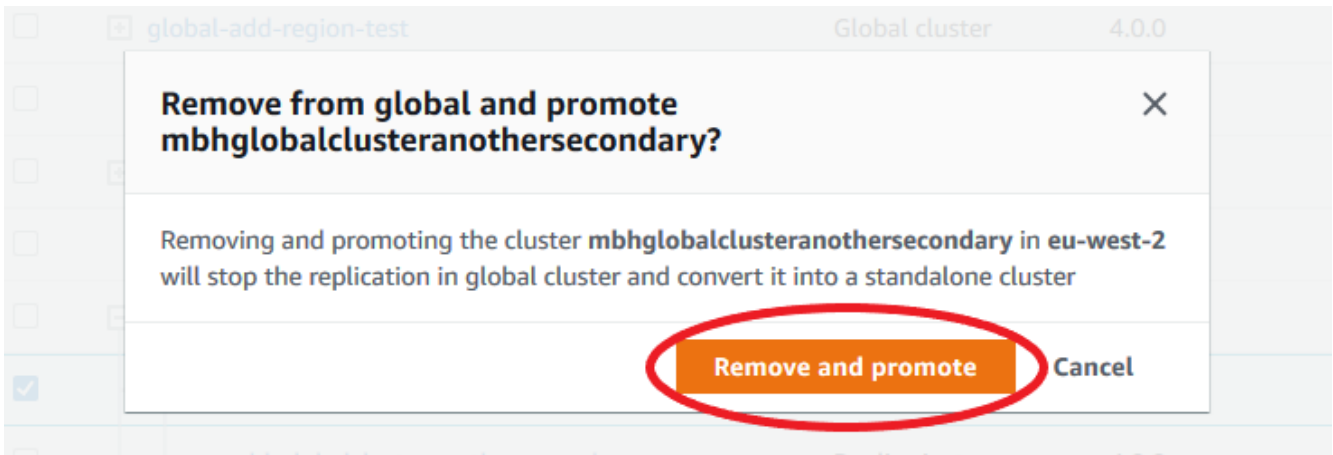
1. Accedi AWS Management Console e accedi alla console Amazon DocumentDB.
2. Scegli Clusters nella barra di navigazione a sinistra.



3. Espandi il cluster globale in modo da poter vedere tutti i cluster secondari. Seleziona i cluster secondari che desideri rimuovere. Scegli Azioni e, nel menu a discesa, scegli Rimuovi da globale.



4. Apparirà un messaggio che ti chiederà di confermare che desideri scollegare il secondario dal cluster globale. Scegli Rimuovi e promuovi per rimuovere il cluster dal cluster globale.



Ora quel cluster non funge più da secondario e non è più sincronizzato con il cluster primario. È un cluster autonomo con funzionalità di lettura/scrittura complete.

Dopo aver rimosso o eliminato tutti i cluster secondari, puoi rimuovere il cluster primario nello stesso modo. È possibile scollegare o rimuovere il cluster primario dal cluster globale solo dopo aver rimosso tutti i cluster secondari. Il cluster globale potrebbe rimanere nell'elenco dei cluster, con zero regioni e AZ. È possibile eliminare se non si desidera più utilizzare questo cluster globale.

Using the AWS CLI

Per rimuovere un cluster da un cluster globale, esegui il comando `remove-from-global-cluster` CLI con i seguenti parametri:

- `--global-cluster-identifier`— Il nome (identificatore) del cluster globale.
- `--db-cluster-identifier`— Il nome di ogni cluster da rimuovere dal cluster globale.

Gli esempi seguenti rimuovono prima un cluster secondario e poi il cluster primario da un cluster globale.

Per Linux, macOS o 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
```

Ripeti il `remove-from-global-cluster --db-cluster-identifier secondary_cluster_ARN` comando per ogni regione secondaria del cluster globale.

Per 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
```

Ripeti il `remove-from-global-cluster --db-cluster-identifier secondary_cluster_ARN` comando per ogni regione secondaria del cluster globale.

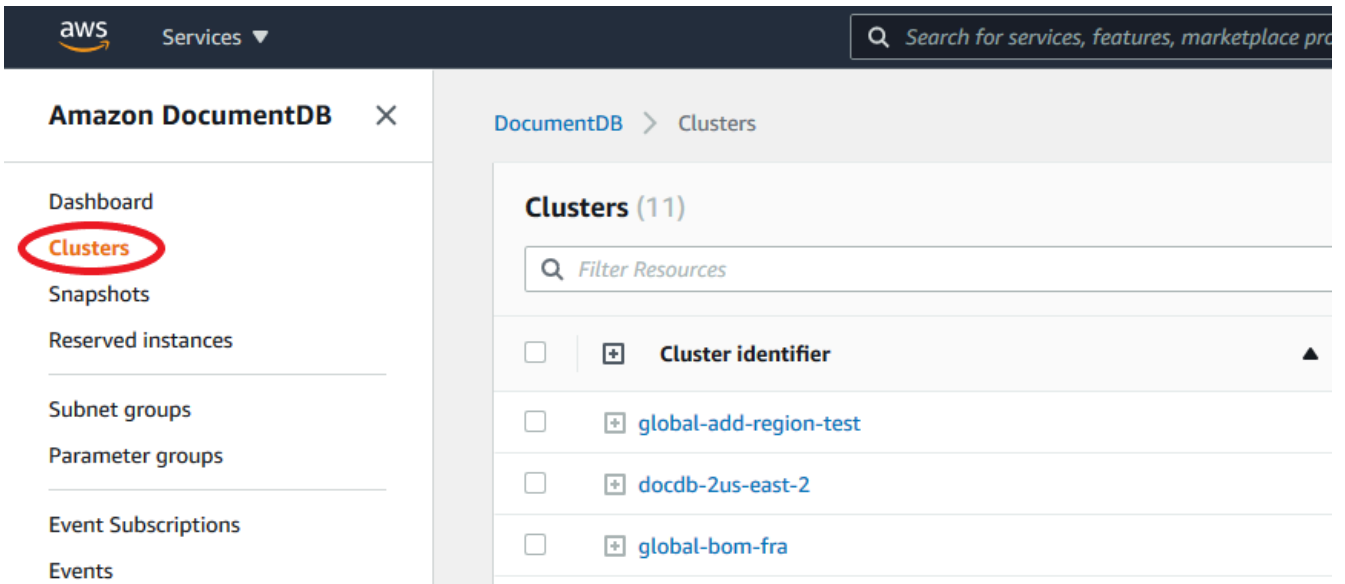
Eliminazione di un cluster da un cluster globale Amazon DocumentDB

Per eliminare un cluster globale, procedi come segue:

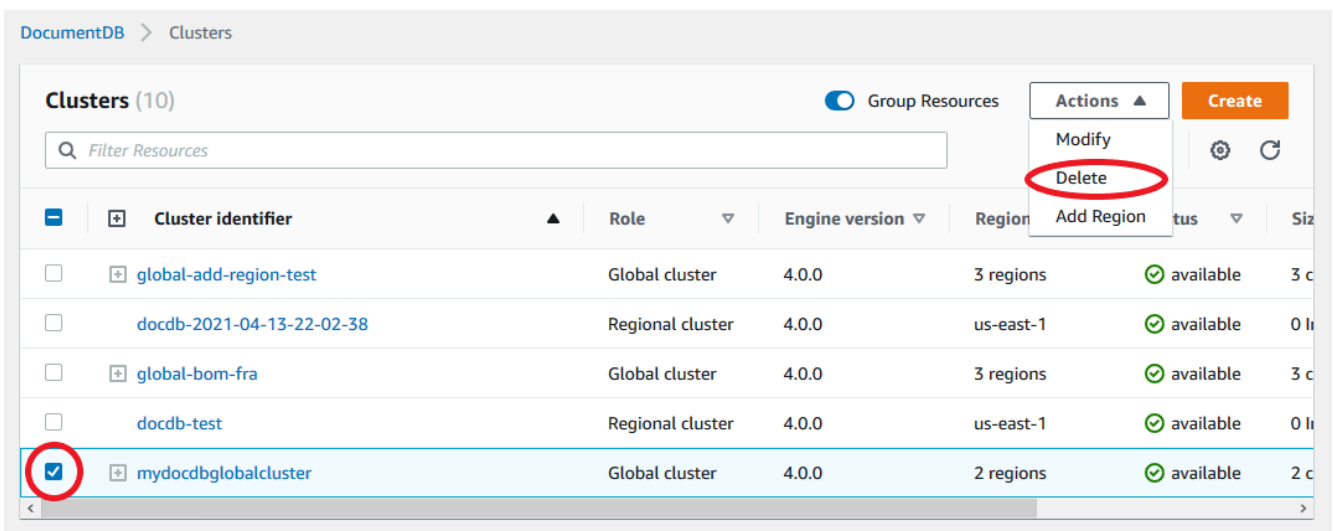
- Rimuovi tutti i cluster secondari dal cluster globale. Ogni cluster diventa un cluster autonomo. Vedi la sezione precedente, Rimozione dei cluster globali.
- Da ogni cluster autonomo, elimina tutte le repliche.
- Rimuovi il cluster primario dal cluster globale. Questo diventa un cluster autonomo.
- Dal cluster primario, elimina prima tutte le repliche, quindi elimina l'istanza principale. L'eliminazione dell'istanza primaria dal nuovo cluster autonomo in genere rimuove anche sia il cluster che il cluster globale.

Using the AWS Management Console

1. Accedi AWS Management Console e accedi alla console Amazon DocumentDB.
2. Scegli Clusters e trova il cluster globale che desideri eliminare.



- Con il cluster globale selezionato, scegli Elimina dal menu Azioni.



Verifica che tutti i cluster siano stati rimossi dal cluster globale. Il cluster globale dovrebbe mostrare zero regioni e AZ e una dimensione pari a zero cluster. Se il cluster globale contiene dei cluster, non puoi ancora eliminarlo. Dovrai prima seguire le istruzioni del passaggio precedente, Rimozione dei cluster globali.

Using the AWS CLI

Per eliminare un cluster globale, esegui il comando `delete-global-cluster` CLI con il nome Regione AWS e l'identificatore globale del cluster, come illustrato nell'esempio seguente.

Per Linux, macOS o Unix:

```
aws docdb --region primary_region delete-global-cluster \  
--global-cluster-identifier global_cluster_id
```

Per Windows:

```
aws docdb --region primary_region delete-global-cluster ^  
--global-cluster-identifier global_cluster_id
```

Creazione di un cluster Amazon DocumentDB headless in una regione secondaria

Sebbene un cluster globale Amazon DocumentDB richieda almeno un cluster secondario in un cluster Regione AWS diverso da quello primario, è possibile utilizzare una configurazione headless per il cluster secondario. Un cluster secondario headless di Amazon DocumentDB è un cluster senza istanza. Questo tipo di configurazione può ridurre le spese per un cluster globale. In un cluster Amazon DocumentDB, elaborazione e storage sono disaccoppiati. Senza l'istanza, non ti viene addebitato alcun costo per l'elaborazione, ma solo per lo storage. Se è configurato correttamente, il volume di archiviazione di un secondario headless viene mantenuto sincronizzato con il cluster primario.

Aggiungi il cluster secondario come fai normalmente quando crei un cluster globale Amazon DocumentDB. Tuttavia, dopo che il cluster primario inizia la replica sul cluster secondario, elimini l'istanza di sola lettura dal cluster secondario. Questo cluster secondario è ora considerato «headless» perché non dispone più di un'istanza. Tuttavia, il volume di storage viene mantenuto sincronizzato con il cluster Amazon DocumentDB principale.


Important

Consigliamo i cluster headless solo per i clienti che possono tollerare guasti a livello regionale per più di 15 minuti. Questo perché il ripristino da un errore a livello regionale con un cluster secondario headless richiederà all'utente di creare una nuova istanza dopo il failover. Una nuova istanza può impiegare circa 10-15 minuti per diventare disponibile.

Come aggiungere un cluster secondario headless al cluster globale

1. Accedi AWS Management Console e apri la console [Amazon DocumentDB](#).
2. Scegli Clusters nella barra di navigazione a sinistra.

3. Scegli il cluster globale che necessita di un cluster secondario. Assicurati che il cluster primario sia `Available`.
4. Per **Actions** (Operazioni), scegliere **Add region** (Aggiungi regione).
5. Nella pagina **Aggiungi una regione**, scegli la regione secondaria.

 **Note**


Non puoi scegliere una regione che abbia già un cluster secondario per lo stesso cluster globale. Inoltre, non può essere la stessa regione del cluster primario.

6. Completa i campi rimanenti per il cluster secondario nella nuova regione. Queste sono le stesse opzioni di configurazione di qualsiasi istanza del cluster.
7. **Aggiungi una regione**. Dopo aver aggiunto la regione al cluster globale, la vedrai nell'elenco di **Clusters** **AWS Management Console**.
8. Controlla lo stato del cluster secondario e della relativa istanza di lettura prima di continuare, utilizzando **AWS Management Console** o il **AWS CLI**. Ecco un esempio di comando se usi **AWS CLI**:

```
$ aws docdb describe-db-clusters --db-cluster-identifier secondary-cluster-id --query '*[].[Status]' --output text
```

Possono essere necessari diversi minuti prima che lo stato di un cluster secondario appena aggiunto cambi da **creazione** a **disponibile**. Quando il cluster è **disponibile**, puoi eliminare l'istanza del lettore.

9. Seleziona l'istanza del lettore nel cluster secondario, quindi scegli **Elimina**.
10. Dopo aver eliminato l'istanza del lettore, il cluster secondario rimane parte del cluster globale. Non dovrebbe avere alcuna istanza associata.

 **Note**

Puoi utilizzare questo cluster secondario **headless** di Amazon DocumentDB per ripristinare manualmente il cluster globale Amazon DocumentDB da un'interruzione non pianificata nella regione principale, se si verifica un'interruzione di questo tipo.

Connect a un cluster globale di Amazon DocumentDB

Il modo in cui ci si connette a un cluster globale dipende dal fatto che sia necessario scrivere sul cluster o leggere dal cluster:

- Per richieste o interrogazioni di sola lettura, ti connetti all'endpoint di lettura per il cluster del tuo. Regione AWS
- Per eseguire le istruzioni DML (Data Manipulation Language) o DDL (Data Definition Language), esegui la connessione all'endpoint del cluster per il cluster primario. Questo endpoint potrebbe trovarsi in una Regione AWS diversa rispetto all'applicazione.

Quando visualizzi un cluster globale nella console, puoi vedere tutti gli endpoint generici associati a tutti i relativi cluster.

Il modo in cui ci si connette a un cluster globale dipende dal fatto che sia necessario scrivere sul database o leggere dal database. Per le operazioni DDL, DML e di lettura che desideri eseguire dalla regione primaria, devi connetterti al cluster primario. Si consiglia di connettersi al cluster primario utilizzando l'endpoint del cluster in modalità set di replica, con una preferenza di lettura di `secondaryPreferred=true`. Questo indirizzerà il traffico di scrittura verso l'istanza writer del cluster primario e il traffico di lettura verso l'istanza di replica del cluster primario.

Per il traffico interregionale e di sola lettura, è necessario connettersi a uno dei cluster secondari. Ti consigliamo di connetterti al cluster secondario utilizzando l'endpoint del cluster in modalità set di repliche. Poiché tutte le istanze sono istanze di replica di sola lettura, non è necessario specificare una preferenza di lettura. Per ridurre al minimo la latenza, scegli l'endpoint di lettura che si trova nella tua regione o nella regione più vicina a te.

Monitoraggio dei cluster globali di Amazon DocumentDB

Amazon DocumentDB (con compatibilità con MongoDB) si integra per CloudWatch consentirti di raccogliere e analizzare i parametri operativi per i tuoi cluster. Puoi monitorare questi parametri utilizzando la CloudWatch console, la console Amazon DocumentDB, AWS Command Line Interface il AWS CLI () o CloudWatch l'API.

Per monitorare un cluster globale, utilizza le seguenti CloudWatch metriche.

Parametro	Descrizione
<code>GlobalClusterReplicatedWriteIO</code>	Il numero medio di operazioni di I/O di scrittura fatturate replicate dal volume del cluster nel volume primario Regione AWS al volume del cluster in un volume secondario Regione AWS, riportato a intervalli di 5 minuti. Il numero di repliche <code>ReplicatedWriteIOs</code> in ciascuna regione secondaria è uguale al numero di repliche interne eseguite dall'area principale e <code>VolumeWriteIOPs</code> .
<code>GlobalClusterDataTransferBytes</code>	La quantità di dati trasferiti dal cluster primario Regione AWS a quello secondario Regione AWS, misurata in byte.
<code>GlobalClusterReplicationLag</code>	La quantità di ritardo, in millisecondi, durante la replica degli eventi di modifica dal cluster primario a quello di un cluster secondario Regione AWS Regione AWS

[Per ulteriori informazioni su come visualizzare queste metriche, consulta Visualizzazione dei dati. CloudWatch](#)

Disaster Recovery e cluster globali Amazon DocumentDB

Utilizzando un cluster globale, puoi eseguire rapidamente il ripristino da disastri come i guasti regionali. Il ripristino da emergenza viene in genere misurato utilizzando i valori per RTO e RPO.

- Obiettivo del tempo di ripristino (RTO): il tempo necessario a un sistema per tornare in uno stato funzionante dopo un'emergenza. In altre parole, l'RTO misura i tempi di inattività. Per un cluster globale, l'RTO può essere dell'ordine dei minuti.
- Obiettivo del punto di ripristino (RPO): la quantità di dati che possono essere persi (misurata nel tempo). Per un cluster globale, l'RPO viene in genere misurato in secondi.
- Per ripristinare il sistema dopo un'interruzione non pianificata, è possibile eseguire un failover interregionale su uno dei sistemi secondari del cluster globale. Se il cluster globale ha più regioni secondarie, assicurati di scollegare tutte le aree secondarie se la principale presenta

un'interruzione. Regione AWS Quindi, promuovi una di queste regioni secondarie come nuova area principale. Regione AWS Infine, crei nuovi cluster in ciascuna delle altre regioni secondarie e colleghi tali cluster al tuo cluster globale.

- Quando promuovi un cluster secondario come cluster principale, devi anche aggiornare gli endpoint utilizzati dalle applicazioni per connettersi al cluster globale. Per ottenere un nuovo endpoint writer da un cluster appena promosso, è possibile convertire un precedente endpoint del lettore rimuovendo `-ro` dalla stringa dell'endpoint. Ad esempio, se un endpoint del lettore precedente è `global-16rr-test-cluster-1.cluster-ro-12345678901.us-west-2.docdb.amazonaws.com`, allora il nuovo endpoint di scrittura promosso è `global-16rr-test-cluster-1.cluster-cps2igpwyrra.us-west-2.rds.amazonaws.com`.

Failover per i cluster globali di Amazon DocumentDB

Se un intero cluster in una Regione AWS diventa non disponibile, puoi promuovere un altro cluster nel cluster globale affinché disponga di funzionalità di lettura/scrittura.

È possibile attivare manualmente il meccanismo di failover se un cluster in un'altra Regione AWS è la scelta migliore come cluster principale. Ad esempio, potrebbe essere necessario incrementare la capacità di uno dei cluster secondari e quindi promuoverlo a cluster primario. Oppure l'equilibrio delle attività tra i due Regioni AWS potrebbe cambiare, in modo che il passaggio dal cluster primario a un'altra Regione AWS potrebbe comportare una minore latenza per le operazioni di scrittura.

La procedura seguente descrive cosa fare per promuovere uno dei cluster secondari in un cluster globale DocumentDB.

Per promuovere un cluster secondario:

1. Interrompi l'emissione di istruzioni DML e altre operazioni di scrittura sul cluster primario in caso di interruzione Regione AWS.
2. Identifica un cluster da un cluster secondario da Regione AWS utilizzare come nuovo cluster primario. Se hai due (o più) cluster secondari Regioni AWS nel tuo cluster globale, scegli il cluster secondario con il minor ritardo.
3. Scollega il cluster secondario scelto dal cluster globale.

La rimozione di un cluster secondario da un cluster globale interrompe immediatamente la replica dal primario a questo secondario e la promuove in un cluster di cluster autonomo con funzionalità di lettura/scrittura complete. Qualsiasi altro cluster secondario associato al cluster

primario nella regione interessata dall'interruzione è ancora disponibile e può accettare chiamate dall'applicazione. Inoltre consumano risorse. Poiché state ricreando il cluster globale, per evitare problemi di tipo split-brain e di altro tipo, rimuovete gli altri cluster secondari prima di creare il nuovo cluster globale nei passaggi seguenti.

Per i passaggi dettagliati per lo scollegamento, consulta [Rimozione di un cluster da un cluster globale Amazon DocumentDB](#).

4. Riconfigura l'applicazione per inviare tutte le operazioni di scrittura a questo cluster ora autonomo utilizzando il suo nuovo endpoint. Se hai accettato i nomi forniti quando hai creato il cluster globale, puoi modificare l'endpoint rimuovendo `-ro` dalla stringa dell'endpoint del cluster nell'applicazione.

Ad esempio, l'endpoint del cluster secondario `my-global.cluster-ro-aaaaabbbbb.us-west-1.docdb.amazonaws.com` diventa `my-global.cluster-aaaaabbbbb.us-west-1.docdb.amazonaws.com` quando quel cluster viene scollegato dal cluster globale.

Questo cluster diventa il cluster principale di un nuovo cluster globale quando inizi ad aggiungervi regioni, nel passaggio successivo.

5. Aggiungi un Regione AWS al cluster. Quando esegui questa operazione, inizia il processo di replica da primario a secondario.
6. Aggiungine altre Regioni AWS se necessario per ricreare la topologia necessaria per supportare l'applicazione. Assicurati che le scritture delle applicazioni vengano inviate al cluster corretto prima, durante e dopo aver apportato modifiche come queste, per evitare incongruenze di dati tra i cluster del cluster globale (problemi di split-brain).
7. Quando l'interruzione è stata risolta e sei pronto a riassegnare il cluster originale Regione AWS come cluster primario, esegui la stessa procedura in senso inverso.
8. Rimuovi uno dei cluster secondari dal cluster globale. Ciò gli consentirà di servire traffico di lettura/scrittura.
9. Reindirizza tutto il traffico di scrittura al cluster primario dell'originale. Regione AWS
10. Aggiungi un Regione AWS per configurare uno o più cluster secondari Regione AWS come prima.

I cluster globali di Amazon DocumentDB possono essere gestiti tramite AWS SDK, che consentono di creare soluzioni per automatizzare il processo di failover globale dei cluster per i casi d'uso di Disaster Recovery e Business Continuity Planning. [Una di queste soluzioni è disponibile per i nostri clienti con licenza Apache 2.0 ed è accessibile dal nostro repository di strumenti qui](#). Questa

soluzione sfrutta Amazon Route53 per la gestione degli endpoint e fornisce funzioni AWS Lambda che possono essere attivate in base a eventi appropriati.

Gestione dei cluster Amazon DocumentDB

Per gestire un cluster Amazon DocumentDB, è necessario disporre di una policy IAM con le autorizzazioni appropriate del piano di controllo di Amazon DocumentDB. Queste autorizzazioni consentono di creare, modificare ed eliminare i cluster e le istanze. La `AmazonDocDBFullAccess` policy fornisce tutte le autorizzazioni necessarie per amministrare un cluster Amazon DocumentDB.

I seguenti argomenti mostrano come eseguire varie attività quando si lavora con i cluster Amazon DocumentDB, tra cui la creazione, l'eliminazione, la modifica, la connessione e la visualizzazione dei cluster.

Argomenti

- [Comprendere i cluster](#)
- [Impostazioni del cluster Amazon DocumentDB](#)
- [Configurazioni di storage in cluster Amazon DocumentDB](#)
- [Determinazione dello stato di un cluster](#)
- [Ciclo di vita del cluster Amazon DocumentDB](#)
- [Scalabilità dei cluster Amazon DocumentDB](#)
- [Clonazione di un volume per un cluster Amazon DocumentDB](#)
- [Comprendere la tolleranza agli errori del cluster Amazon DocumentDB](#)

Comprendere i cluster

Amazon DocumentDB separa elaborazione e storage e trasferisce la replica e il backup dei dati sul volume del cluster. Un volume cluster fornisce un servizio di storage durevole, affidabile e altamente disponibile che replica i dati in sei modi in tre zone di disponibilità. Le repliche consentono una maggiore disponibilità dei dati e il dimensionamento della lettura. Ogni cluster può scalare fino a 15 repliche.

Sostantivo	Descrizione	Operazioni API (verbi)
Cluster	È composto da una o più istanze e da un volume di	<code>create-db-cluster</code>

Sostantivo	Descrizione	Operazioni API (verbi)
	storage cluster per la gestione dei dati di tali istanze.	<code>delete-db-cluster</code> <code>describe-db-clusters</code> <code>modify-db-cluster</code>
Istanza	La lettura e la scrittura dei dati sul volume di storage cluster vengono eseguite mediante le istanze. In un determinato cluster sono disponibili due tipi di istanze: primaria e di replica. Un cluster ha sempre un'istanza principale e può avere da 0 a 15 repliche.	<code>create-db-instance</code> <code>delete-db-instance</code> <code>describe-db-instances</code> <code>modify-db-instance</code> <code>describe-orderable-db-instance-options</code> <code>reboot-db-instance</code>
Volume cluster	Un volume di storage per database virtuali che si estende su tre zone di disponibilità, ciascuna delle quali contiene due copie dei dati del cluster.	N/D
Istanza primaria	Supporta operazioni di lettura e scrittura ed esegue tutte le modifiche ai dati del volume cluster. Ogni cluster contiene un'istanza primaria.	N/D

Sostantivo	Descrizione	Operazioni API (verbi)
Istanza di replica	Supporta solo le operazioni di lettura. Ogni cluster Amazon DocumentDB può avere fino a 15 istanze di replica oltre all'istanza principale. Le repliche distribuiscono il carico di lavoro di lettura. Collocando le repliche in zone di disponibilità separate, puoi anche aumentare la disponibilità del database.	N/D
Endpoint del cluster	Un endpoint per un cluster Amazon DocumentDB che si connette all'istanza primaria corrente del cluster. Ogni cluster Amazon DocumentDB ha un endpoint del cluster e un'istanza principale.	N/D
Endpoint di lettura	Un endpoint per un cluster Amazon DocumentDB che si connette a una delle repliche disponibili per quel cluster. Ogni cluster Amazon DocumentDB dispone di un endpoint di lettura. Se esiste più di una replica, l'endpoint del lettore indirizza ogni richiesta di connessione a una delle repliche di Amazon DocumentDB.	N/D

Sostantivo	Descrizione	Operazioni API (verbi)
Endpoint dell'istanza	Un endpoint per un'istanza in un cluster Amazon DocumentDB che si connette a un'istanza specifica. Ogni istanza di un cluster, a prescindere dal tipo, ha un proprio endpoint dell'istanza esclusivo.	N/D

Impostazioni del cluster Amazon DocumentDB

Quando crei o modifichi un cluster, è importante comprendere quali siano i parametri immutabili e quali quelli modificabili dopo la creazione del cluster. La tabella seguente elenca tutte le impostazioni (parametri) specifiche di un cluster. Come specificato nella tabella, alcuni sono modificabili, altri no.

Note

Queste impostazioni non devono essere confuse con i gruppi di parametri del cluster Amazon DocumentDB e i relativi parametri. Per ulteriori informazioni sui gruppi di parametri del cluster, consulta [Gestione dei gruppi di parametri del cluster Amazon DocumentDB](#).

Parametro	Modificabile	Note
DBClusterIdentifier	Sì	Vincoli per la denominazione <ul style="list-style-type: none"> • La lunghezza è di [1—63] lettere, numeri o trattini. • Il primo carattere deve essere una lettera. • Non può terminare con un trattino o contenere due trattini consecutivi. • Deve essere unico per tutti i cluster di Amazon Amazon RDS, Amazon Neptune e

Parametro	Modificabile	Note
		Amazon DocumentDB per regione. Account AWS
Engine	No	Deve essere docdb.
BackupRetentionPeriod	Sì	Deve essere compreso tra [1 e 35] giorni.
DBClusterParameterGroupName	Sì	Vincoli per la denominazione <ul style="list-style-type: none"> • La lunghezza è di [1-255] caratteri alfanumerici. • Il primo carattere deve essere una lettera. • Non può terminare con un trattino o contenere due trattini consecutivi.
DBSubnetGroupName	No	Dopo aver creato un cluster, non puoi modificare la sottorete.
EngineVersion	No	Il valore può essere 5.0.0 (impostazione predefinita), o. 4.0.0 3.6.0
KmsKeyId	No	Se si sceglie di crittografare il cluster, non è possibile modificare la AWS KMS chiave utilizzata per crittografare il cluster.
MasterUsername	No	Dopo aver creato un cluster, non puoi modificare il MasterUsername . <p>Vincoli per la denominazione</p> <ul style="list-style-type: none"> • La lunghezza è di [1-63] caratteri alfanumerici. • Il primo carattere deve essere una lettera. • Non può essere una parola riservata del motore di database.

Parametro	Modificabile	Note
MasterUserPassword	Sì	<p>Vincoli:</p> <ul style="list-style-type: none"> • La lunghezza è di [8—100] caratteri ASCII stampabili. • È possibile utilizzare qualsiasi carattere ASCII stampabile eccetto i seguenti: <ul style="list-style-type: none"> • / (barra) • " (virgolette doppie) • @ (simbolo chiocciola)
Port	Sì	Il numero di porta è valido per tutte le istanze del cluster.
PreferredBackupWindow	Sì	
PreferredMaintenanceWindow	Sì	
StorageEncrypted	No	Se scegli di crittografare il cluster, non potrà essere decrittografato.
StorageType	Sì	<p>Il tipo di archiviazione per il cluster DB: Standard (standard) o I/O-Optimized (). iopt1</p> <p>Impostazione predefinita: standard</p> <p>Questo parametro può essere configurato con <code>CreateDBCluster</code> and. <code>ModifyDBCluster</code></p> <p>Per ulteriori informazioni, consulta Configurazioni di storage in cluster Amazon DocumentDB.</p>

Parametro	Modificabile	Note
Tags	Sì	
VpcSecurityGroupIds	No	Dopo aver creato un cluster, non puoi modificarlo e il VPC su cui risiede.

Configurazioni di storage in cluster Amazon DocumentDB

A partire da Amazon DocumentDB 5.0, i cluster basati su istanze supportano due tipi di configurazioni di storage:

- **Storage standard Amazon DocumentDB:** progettato per clienti con un consumo di I/O da basso a moderato. Se prevedi che i costi di I/O siano inferiori al 25% del totale del cluster Amazon DocumentDB, questa scelta potrebbe essere la soluzione ideale per te. Con la configurazione di storage standard di Amazon DocumentDB, ti vengono fatturati in base all' `pay-per-request` I/O oltre ai costi di istanza e storage. Ciò significa che la fatturazione potrebbe variare da un ciclo all'altro in base all'utilizzo. La configurazione è personalizzata per soddisfare le fluttuanti richieste di I/O dell'applicazione.
- **Storage ottimizzato per l'I/O di Amazon DocumentDB:** progettato per i clienti che danno priorità alla prevedibilità dei prezzi o hanno applicazioni a uso intensivo di I/O. La configurazione ottimizzata per l'I/O offre prestazioni migliorate, maggiore produttività e latenza ridotta per i clienti con carichi di lavoro I/O intensivi. Se prevedi che i costi di I/O superino il 25% dei costi totali del cluster Amazon DocumentDB, questa opzione offre un rapporto prezzo/prestazioni migliorato. Con la configurazione di storage ottimizzata per l'I/O di Amazon DocumentDB, non ti verrà addebitato alcun costo in base alle operazioni di I/O, garantendo costi prevedibili per ogni ciclo di fatturazione. La configurazione stabilizza i costi migliorando al contempo le prestazioni.

Puoi passare i cluster di database esistenti una volta ogni 30 giorni allo storage ottimizzato per l'I/O di Amazon DocumentDB. Puoi tornare allo storage standard di Amazon DocumentDB in qualsiasi momento. La data successiva per modificare la configurazione dello storage in modo da renderla ottimizzata per l'I/O può essere tracciata con il `describe-db-clusters` comando utilizzando AWS CLI o tramite la AWS Management Console pagina di configurazione del cluster.

[Puoi creare un nuovo cluster di database che include la configurazione ottimizzata per l'I/O di Amazon DocumentDB o convertire i cluster di database esistenti con pochi clic AWS Management](#)

[Console](#), [una singola modifica di parametro in AWS Command Line Interface \(AWS CLI\)](#) o [tramite SDK.AWS](#) Non sono necessari tempi di inattività o riavvio delle istanze durante o dopo la modifica della configurazione dello storage.

<u>Requirement</u>	<u>Standard</u>	<u>I/O-Optimized</u>	<u>Usage</u>
Default Storage Type	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Low to Moderate I/O Workload	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Best if expected I/O charges are less than or equal to 25%
Price Predictability	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
High I/O Workload	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Best if expected I/O charges are greater than or equal to 25%
High Write Throughput	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Average 30%-50% observed improvement

Creazione di un cluster ottimizzato per I/O

Using the AWS Management Console

Per creare o modificare un cluster ottimizzato per I/O utilizzando: AWS Management Console

1. Nella console di gestione di Amazon DocumentDB, in Clusters, scegli Crea o seleziona il cluster e scegli Azioni, quindi scegli Modifica.
2. Se stai creando un nuovo cluster, assicurati di scegliere Cluster basati su istanze nella sezione Tipo di cluster (questa è l'opzione predefinita).

Cluster type

Instance Based Cluster

Instance based cluster can scale your database to millions of reads per second and up to 64TB of storage capacity. With instance based clusters you can choose your instance type based on your requirements.

Elastic Cluster

Elastic clusters can scale your database to millions of reads and writes per second, with petabytes of storage capacity. Elastic clusters support MongoDB compatible sharding APIs. With Elastic Clusters, you do not need to choose, manage or upgrade instances.

3. Nella sezione Configurazione, in Configurazione dello storage del cluster, scegli Amazon DocumentDB I/O Optimized.

Cluster storage configuration - new [Info](#)

Choose the storage configuration for your Amazon DocumentDB cluster that best fits your application's price predictability and price performance needs.

Storage configuration
Database instance, storage, and I/O charges vary depending on the storage configuration

Amazon DocumentDB Standard

- Pay-per-request I/O charges apply. Instance and storage prices don't include I/O usage.
- Cost-effective pricing for many applications with low to moderate I/O usage.

Amazon DocumentDB I/O-Optimized

- No charges for I/O operations. Instance and storage prices include I/O usage.
- Predictable pricing for all applications. Improved price performance for I/O-intensive applications.

4. Completa la creazione o la modifica del cluster e scegli **Crea cluster** o **Modifica cluster**.

Per il processo completo di creazione del cluster, consulta [Creazione di un cluster e di un'istanza primaria utilizzando il AWS Management Console](#).

Per il processo completo di modifica del cluster, vedere [Modifica di un cluster Amazon DocumentDB](#).

Using the AWS CLI

Per creare un cluster ottimizzato per l'I/O utilizzando: AWS CLI

Negli esempi seguenti, sostituire ogni *segnaposto dell'input utente* con le proprie informazioni.

Per Linux, macOS o 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
```

Per 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
```

Analisi dei costi per determinare la configurazione dello storage

Con Amazon DocumentDB, hai la flessibilità di scegliere la configurazione di storage per ogni cluster di database di cui disponi. Per allocare correttamente i cluster tra standard e ottimizzati per l'I/O, puoi monitorare i costi di Amazon DocumentDB per cluster. A tale scopo, puoi aggiungere tag ai cluster esistenti, abilitare l'etichettatura per l'allocazione dei costi nella [AWS Billing and Cost Management dashboard](#) e analizzare i costi per un determinato cluster in [AWS Cost Explorer Service](#). Per informazioni sull'analisi dei costi, consulta il nostro blog [Utilizzo dei tag di allocazione dei costi](#).

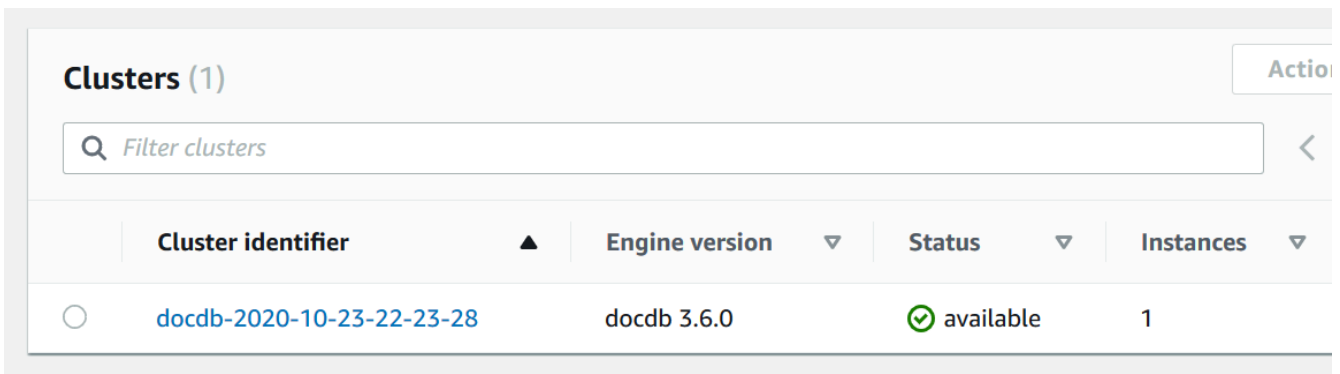
Determinazione dello stato di un cluster

È possibile determinare lo stato di un cluster utilizzando AWS Management Console o AWS CLI.

Using the AWS Management Console

Utilizza la seguente procedura per visualizzare lo stato del tuo cluster Amazon DocumentDB utilizzando il AWS Management Console

1. [Accedi a e apri AWS Management Console la console Amazon DocumentDB all'indirizzo `https://console.aws.amazon.com/docdb`.](https://console.aws.amazon.com/docdb)
2. Nel pannello di navigazione scegliere Clusters (Cluster).
3. Nella colonna Cluster identifier (Identificatore cluster) individua il nome del cluster desiderato. Quindi, per trovare lo stato del cluster, leggi la riga in corrispondenza della colonna Status (Stato), come illustrato di seguito.



Cluster identifier	Engine version	Status	Instances
docdb-2020-10-23-22-23-28	docdb 3.6.0	✔ available	1

Using the AWS CLI

Usa l'`describe-db-clusters` operazione per visualizzare lo stato del tuo cluster Amazon DocumentDB utilizzando il AWS CLI

Il codice seguente individua lo stato del cluster `sample-cluster`.

Per Linux, macOS o Unix:

```
aws docdb describe-db-clusters \  
  --db-cluster-identifier sample-cluster \  
  --query 'DBClusters[*].[DBClusterIdentifier,Status]'
```

Per Windows:

```
aws docdb describe-db-clusters ^  
  --db-cluster-identifier sample-cluster ^  
  --query 'DBClusters[*].[DBClusterIdentifier,Status]'
```

L'aspetto dell'output di questa operazione è simile al seguente (formato JSON).

```
[  
  [  
    "sample-cluster",  
    "available"  
  ]  
]
```

Ciclo di vita del cluster Amazon DocumentDB

Il ciclo di vita di un cluster Amazon DocumentDB include la creazione, la descrizione, la modifica e l'eliminazione del cluster. Questa sezione fornisce informazioni su come completare questi processi.

Argomenti

- [Creazione di un cluster Amazon DocumentDB](#)
- [Descrizione dei cluster Amazon DocumentDB](#)
- [Modifica di un cluster Amazon DocumentDB](#)
- [Determinazione della manutenzione in sospeso](#)
- [Esecuzione di un aggiornamento della patch alla versione del motore di un cluster](#)

- [Arresto e avvio di un cluster Amazon DocumentDB](#)
- [Eliminazione di un cluster Amazon DocumentDB](#)

Creazione di un cluster Amazon DocumentDB

Un cluster Amazon DocumentDB è composto da istanze e un volume di cluster che rappresenta i dati del cluster. Il volume cluster viene replicato in sei modi su tre zone di disponibilità come un unico volume virtuale. Il cluster contiene un'istanza primaria e, facoltativamente, fino a 15 istanze di replica.

Le seguenti sezioni mostrano come creare un cluster Amazon DocumentDB utilizzando il AWS Management Console o il. AWS CLI Puoi quindi aggiungere al cluster istanze di replica aggiuntive. Quando usi la console per creare il tuo cluster Amazon DocumentDB, contemporaneamente viene creata automaticamente un'istanza primaria per te. Se usi il AWS CLI per creare il tuo cluster Amazon DocumentDB, dopo che lo stato del cluster è disponibile, devi creare l'istanza principale per quel cluster.

Prerequisiti

Di seguito sono riportati i prerequisiti per la creazione di un cluster Amazon DocumentDB.

Se non ne hai uno Account AWS, completa i seguenti passaggi per crearne uno.

Per iscriverti a un Account AWS

1. Apri la pagina all'indirizzo <https://portal.aws.amazon.com/billing/signup>.
2. Segui le istruzioni online.

Nel corso della procedura di registrazione riceverai una telefonata, durante la quale sarà necessario inserire un codice di verifica attraverso la tastiera del telefono.

Quando ti iscrivi a un Account AWS, Utente root dell'account AWS viene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come best practice di sicurezza, [assegna l'accesso amministrativo a un utente amministrativo](#) e utilizza solo l'utente root per eseguire [attività che richiedono l'accesso di un utente root](#).

Prerequisiti per VPC

Puoi creare un cluster Amazon DocumentDB solo in un Amazon Virtual Private Cloud (Amazon VPC). Il tuo Amazon VPC deve avere almeno una sottorete in ciascuna di almeno due zone di disponibilità

per poterlo utilizzare con un cluster Amazon DocumentDB. Distribuendo le istanze del cluster tra le zone di disponibilità, ti assicuri che le istanze siano disponibili nel cluster nel caso improbabile di un errore nella zona di disponibilità.

Prerequisiti per la sottorete

Quando crei un cluster Amazon DocumentDB, devi scegliere un VPC e il gruppo di sottoreti corrispondente all'interno di quel VPC per avviare il cluster. Le sottoreti determinano la zona di disponibilità e l'intervallo IP all'interno della zona di disponibilità che desideri utilizzare per avviare un'istanza. In questa documentazione i termini sottorete e zona di disponibilità saranno utilizzati indifferentemente. Un gruppo di sottoreti è un set di sottoreti denominato (o zone di disponibilità). Ciò che un gruppo di sottoreti consente di fare è specificare le zone di disponibilità che si desidera utilizzare per avviare le istanze di Amazon DocumentDB. Ad esempio, per avere alta disponibilità in un cluster con tre istanze, è consigliabile effettuare il provisioning di ciascuna di queste istanze in zone di disponibilità separate. In questo modo, se una singola zona di disponibilità non funziona, sarà interessata solo una singola istanza.

Le istanze di Amazon DocumentDB possono attualmente essere fornite in un massimo di tre zone di disponibilità. Anche se un gruppo di sottoreti ha più di tre sottoreti, puoi utilizzarne solo tre per creare un cluster Amazon DocumentDB. Di conseguenza, quando crei un gruppo di sottoreti, è consigliabile scegliere solo le tre sottoreti in cui desideri distribuire le tue istanze. Negli Stati Uniti orientali (Virginia settentrionale), un gruppo di sottoreti può avere sei sottoreti (o zone di disponibilità). Tuttavia, quando viene effettuato il provisioning di un cluster Amazon DocumentDB, Amazon DocumentDB sceglie tre di quelle zone di disponibilità che utilizza per il provisioning delle istanze.

Ad esempio, supponiamo che durante la creazione di un cluster, Amazon DocumentDB scelga le zone di disponibilità {1A, 1B e 1C}. Se tenti di creare un'istanza nella zona di disponibilità {1D}, la chiamata API non riesce. Tuttavia, se scegli di creare un'istanza senza specificare una particolare zona di disponibilità, Amazon DocumentDB sceglie una zona di disponibilità per tuo conto. Amazon DocumentDB utilizza un algoritmo per bilanciare il carico delle istanze tra le zone di disponibilità per aiutarti a raggiungere un'elevata disponibilità. Ad esempio, se viene effettuato il provisioning di tre istanze, per impostazione predefinita il provisioning viene effettuato nelle tre zone di disponibilità e non in una sola di esse.

Raccomandazioni:

- A meno che non si abbia un motivo specifico, creare sempre un gruppo di sottoreti con tre sottoreti. In questo modo si assicura che i cluster con tre o più istanze possano ottenere una disponibilità più elevata in quanto ne verrà effettuato il provisioning su tre zone di disponibilità.

- Distribuisci sempre le istanze in più zone di disponibilità per ottenere una disponibilità più elevata. Non posizionare mai tutte le istanze di un cluster in una singola zona di disponibilità.
- Poiché gli eventi di failover possono verificarsi in qualsiasi momento, non devi presumere che un'istanza primaria o le istanze di replica siano sempre in una determinata zona di disponibilità.

Prerequisiti aggiuntivi

Di seguito sono riportati alcuni prerequisiti aggiuntivi per la creazione di un cluster Amazon DocumentDB:

- Se ti connetti AWS utilizzando credenziali AWS Identity and Access Management (IAM), il tuo account IAM deve disporre di politiche IAM che concedano le autorizzazioni necessarie per eseguire le operazioni di Amazon DocumentDB.

Se utilizzi un account IAM per accedere alla console Amazon DocumentDB, devi prima accedervi AWS Management Console con il tuo account IAM. [Quindi vai alla console Amazon DocumentDB all'indirizzo https://console.aws.amazon.com/docdb](https://console.aws.amazon.com/docdb).

- Per personalizzare i parametri di configurazione per il cluster, devi specificare un gruppo di parametri del cluster e un gruppo di parametri con le impostazioni dei parametri richieste. Per informazioni sulla creazione o la modifica di un gruppo di parametri del cluster o un gruppo di parametri, consulta [Gestione dei gruppi di parametri del cluster Amazon DocumentDB](#).
- Devi determinare il numero di porta TCP/IP da specificare per il cluster. I firewall di alcune aziende bloccano le connessioni alle porte predefinite per Amazon DocumentDB. Se il firewall della tua azienda blocca la porta predefinita, scegli un'altra porta per il cluster. Tutte le istanze in un cluster utilizzano la stessa porta.

Creazione di un cluster e di un'istanza primaria utilizzando il AWS Management Console

Le seguenti procedure descrivono come utilizzare la console per avviare un cluster Amazon DocumentDB con una o più istanze.

Creare un cluster: utilizzando le impostazioni predefinite

Per creare un cluster con istanze utilizzando le impostazioni predefinite utilizzando il AWS Management Console

1. [Accedi a e apri AWS Management Console la console Amazon DocumentDB all'indirizzo https://console.aws.amazon.com/docdb](https://console.aws.amazon.com/docdb).

2. Se desideri creare il cluster in una regione AWS diversa da quella degli Stati Uniti orientali (Virginia settentrionale), scegli la regione dall'elenco nella sezione in alto a destra della console.
3. Nel riquadro di navigazione scegliere Clusters (Cluster), quindi Create (Crea).

 Tip

Se il riquadro di navigazione non viene visualizzato sul lato sinistro della schermata, scegliere l'icona del menu (☰) nell'angolo in alto a sinistra della pagina.

4. Nella pagina Crea cluster Amazon DocumentDB, completa il riquadro Configurazione.
 - a. Identificatore del cluster: accetta il nome fornito da Amazon DocumentDB o immetti un nome per il cluster, ad esempio. **sample-cluster**

Vincoli per la denominazione del cluster:
 - La lunghezza è di [1—63] lettere, numeri o trattini.
 - Il primo carattere deve essere una lettera.
 - Non può terminare con un trattino o contenere due trattini consecutivi.
 - Deve essere unico per tutti i cluster di Amazon RDS, Neptune e Amazon DocumentDB per regione. Account AWS
 - b. Versione del motore: accetta la versione predefinita del motore 4.0.0 o, facoltativamente, scegli 3.6.0.
 - c. Classe di istanza: accetta l'impostazione predefinita o scegli db.r5.large la classe di istanza che desideri dall'elenco.
 - d. Numero di istanze: nell'elenco, scegliete il numero di istanze che desiderate creare con questo cluster. La prima istanza è l'istanza primaria, tutte le altre sono istanze di replica di sola lettura. È possibile aggiungere ed eliminare le istanze in un secondo momento, se necessario. Per impostazione predefinita, un cluster Amazon DocumentDB viene avviato con tre istanze (una principale e due repliche).
5. Completa la sezione Configurazione dello storage del cluster.

Scegli tra Amazon DocumentDB Standard (impostazione predefinita) o Amazon DocumentDB I/O Optimized. Per ulteriori informazioni, consulta [Configurazioni di storage in cluster Amazon DocumentDB](#).

6. Compila il riquadro Authentication (Autenticazione).

- a. Nome utente: immetti un nome per l'utente principale. Per accedere al cluster, è necessario utilizzare il nome utente principale.

Vincoli principali di denominazione degli utenti:

- La lunghezza è di [1-63] caratteri alfanumerici.
- Il primo carattere deve essere una lettera.
- Non può essere una parola riservata del motore di database.

- b. Password: immetti una password per l'utente principale, quindi confermalà. Per accedere al cluster, è necessario utilizzare la password dell'utente principale.

Vincoli per la password:

- La lunghezza è di [8-100] caratteri ASCII stampabili.
- È possibile utilizzare qualsiasi carattere ASCII stampabile eccetto i seguenti:
 - / (barra)
 - " (virgolette doppie)
 - @ (simbolo chiocciola)

7. Nella parte inferiore della schermata, scegli uno dei seguenti:

- Per creare subito il cluster, scegli Create cluster (Crea cluster).
- Per non creare il cluster, scegli Cancel (Annulla).
- Per configurare ulteriormente il cluster prima di crearlo, scegliere Show additional configurations (Mostra configurazioni aggiuntive), quindi continuare in [Creare un cluster: configurazioni aggiuntive](#).

Le configurazioni comprese nella sezione Additional Configurations (Configurazioni aggiuntive) sono:

- Impostazioni di rete: l'impostazione predefinita prevede l'utilizzo del gruppo di default sicurezza VPC.

- Opzioni del cluster: l'impostazione predefinita prevede l'utilizzo della porta 27017 e il gruppo di parametri predefinito.
- Crittografia: l'impostazione predefinita è abilitare la crittografia utilizzando la chiave. (default) `aws/rds`

 Important

Una volta che un cluster è crittografato, non può essere decrittografato.

- Backup: l'impostazione predefinita prevede di conservare i backup per 1 giorno e lasciare che Amazon DocumentDB scelga la finestra di backup.
- Esportazioni di log: l'impostazione predefinita prevede di non esportare i log di controllo in Logs. CloudWatch
- Manutenzione: l'impostazione predefinita prevede che Amazon DocumentDB scelga la finestra di manutenzione.
- Protezione dall'eliminazione: protegge il cluster dall'eliminazione accidentale. L'impostazione predefinita per i cluster creati utilizzando la console è abilitata.

Se accetti le impostazioni predefinite ora, potrai modificare la maggior parte di esse successivamente modificando il cluster.

8. Abilita la connessione in entrata per il gruppo di sicurezza del cluster.

Se non sono state modificate le impostazioni predefinite per il cluster, questo è stato creato utilizzando il gruppo di sicurezza predefinito per il VPC predefinito nella regione selezionata. Per connetterti ad Amazon DocumentDB, devi abilitare le connessioni in entrata sulla porta 27017 (o sulla porta di tua scelta) per il gruppo di sicurezza del cluster.

Per aggiungere una connessione in entrata al gruppo di sicurezza del cluster

- a. [Accedi AWS Management Console e apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.](https://console.aws.amazon.com/ec2/)
- b. Nella sezione Resources (Risorse) della finestra principale, selezionare Security groups (Gruppi di sicurezza).

Resources

You are using the following Amazon EC2 resources in the EU West (Ireland) region:

0 Running Instances	0 Elastic IPs
0 Dedicated Hosts	0 Snapshots
0 Volumes	0 Load Balancers
0 Key Pairs	1 Security Groups
0 Placement Groups	

- c. Dall'elenco di gruppi di sicurezza, individuare il gruppo di sicurezza utilizzato quando si crea il cluster (è probabile che il gruppo di sicurezza predefinito) e scegliere la casella a sinistra del nome del gruppo di sicurezza.

	Name	Group ID	Group Name	VPC ID
<input checked="" type="checkbox"/>		sg-06b2ad61	default	vpc-d833a4bc
<input type="checkbox"/>		sg-07443a112c70a5282	test-sg	vpc-d833a4bc

- d. Dal menu Actions (Operazioni), scegliere Edit inbound rules (Modifica regole in entrata), quindi scegliere o inserire i vincoli della regola.
- i. Tipo: dall'elenco, scegli il protocollo da aprire al traffico di rete.
 - ii. Protocollo: dall'elenco, scegli il tipo di protocollo.
 - iii. Intervallo di porte: per una regola personalizzata, inserisci un numero di porta o un intervallo di porte. Assicurati che il numero di porta o l'intervallo includa la porta specificata quando hai creato il cluster (valore predefinito: 27017).
 - iv. Fonte: specifica il traffico che può raggiungere l'istanza. Dall'elenco, scegliere l'origine del traffico. Se si sceglie Custom (Personalizzata), specificare un solo indirizzo IP o un intervallo di indirizzi IP nella notazione CIDR (ad es., 203.0.113.5/32).
 - v. Descrizione: inserisci una descrizione per questa regola.
 - vi. Dopo aver creato la regola, scegliere Save (Salva).

Creare un cluster: configurazioni aggiuntive

Se desideri accettare le impostazioni predefinite per il cluster, puoi ignorare le seguenti fasi e scegliere Create cluster (Crea cluster).

1. Completa il riquadro Network settings (Impostazioni di rete).

Network settings

a Virtual Private Cloud (VPC) [Info](#)
VPC defines the virtual networking environment for this cluster.

vpc-91280df6 ▼

Only VPCs with a corresponding subnet group are listed. Once a cluster is created, the VPC cannot be changed.

b Subnet group [Info](#)
A subnet group is a collection of subnets that are within a VPC.

default ▼

c VPC security groups
A security group acts as a virtual firewall for your instance to control inbound and outbound traffic.

Select VPC security groups ▼

default (VPC) ✕

- a. Virtual Private Cloud (VPC): nell'elenco, scegli l'Amazon VPC in cui desideri avviare questo cluster.
 - b. Gruppo di sottoreti: nell'elenco, scegli il gruppo di sottoreti che desideri utilizzare per questo cluster.
 - c. Gruppi di sicurezza VPC: nell'elenco, scegli il gruppo di sicurezza VPC per questo cluster.
2. Completa il riquadro Cluster options (Opzioni cluster).

Cluster options

Port
TCP/IP port that is used to connect to the cluster.

27017

Cluster parameter group [Info](#)

default.docdb4.0 ▼

- a. Porta database: utilizza le frecce su e giù per impostare la porta TCP/IP che le applicazioni utilizzeranno per connettersi all'istanza.
 - b. Gruppo di parametri del cluster: nell'elenco dei gruppi di parametri, scegli il gruppo di parametri del cluster per questo cluster.
3. Completa il riquadro Encryption (Crittografia).

Encryption-at-rest

Encryption-at-rest [Info](#)

Enable encryption
 Disable encryption

AWS KMS Key

Account
713738290397

KMS key ID
32d28de3-8254-4597-a3da-571ddc95b76f

a. Encryption-at-rest —Scegliete una delle seguenti opzioni:

- Abilita crittografia: impostazione predefinita. Tutti i dati inattivi vengono crittografati. Se scegli di crittografare i dati, non è possibile annullare questa operazione.
- Disattiva la crittografia: i dati non sono crittografati.

b. AWS Chiave KMS: disponibile solo se si crittografano i dati. Scegliere nell'elenco la chiave che si desidera utilizzare per crittografare i dati nel cluster. Il valore predefinito è (default) aws/rds.

Se si sceglie Enter a key ARN (Immetti ARN chiave), è necessario immettere un Amazon Resource Name (ARN) per la chiave.

4. Completa il riquadro Backup.

Backup

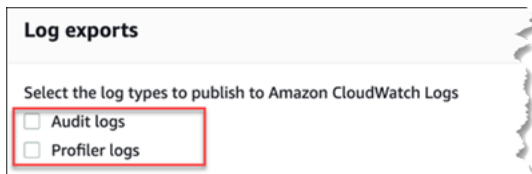
a Backup retention period [Info](#)
A period between 1 and 35 days in which you can perform a point-in-time restore and for which automated backups are retained.

b Backup window
The daily time range (in UTC) during which automated backups are created.

Start time : UTC Duration hours

- a. Periodo di conservazione dei backup: nell'elenco, scegli il numero di giorni in cui conservare i backup automatici di questo cluster prima di eliminarli.
- b. Finestra di backup: imposta l'ora e la durata giornaliera durante le quali Amazon DocumentDB deve effettuare i backup di questo cluster.

- i. Ora di inizio: nel primo elenco, scegli l'ora di inizio (UTC) per avviare i backup automatici. Dal secondo elenco scegli il minuto dell'ora in cui desideri inizino i backup automatici.
 - ii. Durata: nell'elenco, scegli il numero di ore da assegnare alla creazione di backup automatici.
5. Completa il riquadro Esportazioni dei log selezionando i tipi di log che desideri esportare in Logs. CloudWatch



Log exports

Select the log types to publish to Amazon CloudWatch Logs

Audit logs

Profiler logs

- Registri di controllo: seleziona questa opzione per abilitare l'esportazione dei log di controllo in Amazon Logs. CloudWatch Se selezioni Audit logs (Log di audit), devi abilitare `audit_logs` nel gruppo personalizzato di parametri del cluster. Per ulteriori informazioni, consulta [Controllo degli eventi di Amazon DocumentDB](#).
- Registri del profiler: seleziona questa opzione per abilitare l'esportazione dei log del profiler operativo su Amazon Logs. CloudWatch Se selezioni Profiler logs (Log del profiler), devi anche modificare i seguenti parametri nel gruppo personalizzato dei parametri del cluster:
 - `profilerenabled`—Imposta su.
 - `profiler_threshold_ms`—Imposta su un valore `[0-INT_MAX]` per impostare la soglia per le operazioni di profilatura.
 - `profiler_sampling_rate`—Imposta su un valore `[0.0-1.0]` per impostare la percentuale di operazioni lente da profilare.

Per ulteriori informazioni, consulta [Profilazione delle operazioni di Amazon DocumentDB](#).

6. Compilare il riquadro Maintenance (Manutenzione).

- Scegli una delle seguenti opzioni
 - Seleziona finestra: puoi specificare il giorno della settimana, l'ora di inizio UTC e la durata affinché Amazon DocumentDB esegua la manutenzione del cluster.
 - a. Giorno di inizio: nell'elenco, scegli il giorno della settimana in cui iniziare la manutenzione del cluster.
 - b. Ora di inizio: negli elenchi, scegli l'ora e il minuto (UTC) per avviare la manutenzione.
 - c. Durata: nell'elenco, scegli quanto tempo dedicare alla manutenzione del cluster. Se la manutenzione non può essere completata nel tempo specificato, il processo di manutenzione proseguirà oltre l'orario indicato fino al completamento.
 - Nessuna preferenza: Amazon DocumentDB sceglie il giorno della settimana, l'ora di inizio e la durata per eseguire la manutenzione.

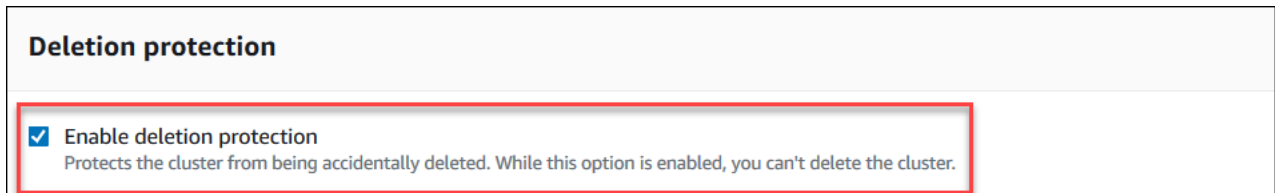
7. Per aggiungere uno o più tag a questo cluster, completare il riquadro Tags (Tag).

Per ogni tag che si desidera aggiungere al cluster, ripetere i seguenti passaggi. È possibile averne fino a 10 in un cluster.

- a. Scegli Aggiungi tag.
- b. Digita il tag Key (Chiave).
- c. Opzionalmente digita il Value (Valore) del tag.

Per rimuovere un tag, scegli Remove (Rimuovi).

- Quando si crea un cluster utilizzando la console, la Deletion Protection (Protezione dall'eliminazione) viene abilitata per impostazione predefinita. Per disabilitare la protezione dall'eliminazione, deseleziona Enable deletion protection (Abilita la protezione dall'eliminazione). Quando abilitata, la protezione dall'eliminazione impedisce che un cluster venga eliminato. Per eliminare un cluster protetto dall'eliminazione, è necessario prima modificare il cluster per disabilitare la protezione dall'eliminazione.



Per ulteriori informazioni sulla protezione dall'eliminazione, consultare [Eliminazione di un cluster Amazon DocumentDB](#).

- Per creare il cluster, scegli Create cluster (Crea cluster). Altrimenti, scegli Cancel (Annulla).

Creazione di un cluster utilizzando il AWS CLI

Le seguenti procedure descrivono come utilizzare AWS CLI per avviare un cluster Amazon DocumentDB e creare una replica Amazon DocumentDB.

Parametri

- db-cluster-identifier**: obbligatorio. Una stringa di lettere minuscole che identifica il cluster.

Vincoli per la denominazione del cluster:

- La lunghezza è di [1—63] lettere, numeri o trattini.
 - Il primo carattere deve essere una lettera.
 - Non può terminare con un trattino o contenere due trattini consecutivi.
 - Deve essere unico per tutti i cluster (tra Amazon RDS, Amazon Neptune e Amazon DocumentDB) per account e per regione. AWS
- engine**: obbligatorio. Deve essere **docdb**.

- **--deletion-protection | --no-deletion-protection**—Facoltativo. Quando è abilitata la protezione dall'eliminazione, questa impedisce che il cluster venga eliminato. Quando si utilizza AWS CLI, l'impostazione predefinita prevede che la protezione da eliminazione sia disabilitata.

Per ulteriori informazioni sulla protezione dall'eliminazione, consultare [Eliminazione di un cluster Amazon DocumentDB](#).

- **--storage-type standard | iopt1**—Facoltativo. Default: **standard**. La configurazione di archiviazione del cluster. I valori validi sono **standard** (Standard) o **iopt1** (ottimizzato per l'I/O).
- **--master-username**: obbligatorio. Il nome utilizzato per autenticare l'utente.

Vincoli per la denominazione dell'utente master:

- La lunghezza è compresa tra 1 e 63 caratteri alfanumerici.
 - Il primo carattere deve essere una lettera.
 - Non può essere una parola riservata del motore di database.
- **--master-user-password**: obbligatorio. La password utilizzata per autenticare l'utente.

Vincoli per la password master:

- La lunghezza è di [8-100] caratteri ASCII stampabili.
- È possibile utilizzare qualsiasi carattere ASCII stampabile eccetto i seguenti:
 - / (barra)
 - " (virgolette doppie)
 - @ (simbolo chiocciola)

Per altri parametri, vedi [CreateDBCluster](#).

Per avviare un cluster Amazon DocumentDB utilizzando AWS CLI

Per creare un cluster Amazon DocumentDB, chiama il `create-db-cluster` AWS CLI o il comando seguente crea un cluster Amazon DocumentDB denominato `sample-cluster` con la protezione da eliminazione abilitata. Per ulteriori informazioni sulla protezione da eliminazione, consulta [Eliminazione di un cluster Amazon DocumentDB](#).

Inoltre, `--engine-version` è un parametro opzionale che utilizza per impostazione predefinita l'ultima versione principale del motore. L'attuale versione principale del motore è la 4.0.0. Quando vengono rilasciate nuove versioni principali del motore, la versione predefinita del motore viene aggiornata in modo da riflettere l'ultima versione principale del motore. `--engine-version` Di conseguenza, per i carichi di lavoro di produzione, in particolare quelli che dipendono da script, automazione o AWS CloudFormation modelli, si consiglia di specificare esplicitamente la versione principale `--engine-version` desiderata.

Note

Se non `vpc-security-group-id` viene specificato un `db-subnet-group-name` or, Amazon DocumentDB utilizzerà il gruppo di sottoreti e il gruppo di sicurezza Amazon VPC predefiniti per la regione specificata.

Per Linux, macOS o Unix:

```
aws docdb create-db-cluster \  
  --db-cluster-identifier sample-cluster \  
  --engine docdb \  
  --engine-version 4.0.0 \  
  --deletion-protection \  
  --master-username masteruser \  
  --master-user-password password
```

Per Windows:

```
aws docdb create-db-cluster ^  
  --db-cluster-identifier sample-cluster ^  
  --engine docdb ^  
  --engine-version 4.0.0 ^  
  --deletion-protection ^  
  --master-username masteruser ^  
  --master-user-password password
```

L'aspetto dell'output di questa operazione è simile al seguente (formato JSON).

```
{  
  "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:sample-cluster",
    "DBClusterIdentifier": "sample-cluster",
    "MultiAZ": false,
    "DBClusterParameterGroup": "default.docdb4.0",
    "PreferredBackupWindow": "09:12-09:42",
    "DbClusterResourceId": "cluster-KQSGI4MHU4NTDDRVLNTU7XVAY",
    "PreferredMaintenanceWindow": "tue:04:17-tue:04:47",
    "Port": 27017,
    "Status": "creating",
    "ReaderEndpoint": "sample-cluster.cluster-ro-sfcrlcjcjcoroz.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-sfcrlcjcjcoroz.us-east-1.docdb.amazonaws.com"
  }
}

```

La creazione del cluster richiede diversi minuti. Puoi usare AWS Management Console o AWS CLI per monitorare lo stato del tuo cluster. Per ulteriori informazioni, consulta [Monitoraggio dello stato di un cluster Amazon DocumentDB](#).

⚠ Important

Quando si utilizza AWS CLI per creare un cluster Amazon DocumentDB, non viene creata alcuna istanza. Di conseguenza, devi creare esplicitamente un'istanza primaria e le eventuali istanze di replica di cui hai bisogno. È possibile utilizzare la console o AWS CLI creare le istanze. Per ulteriori informazioni, consulta [Aggiungere un'istanza Amazon DocumentDB a un cluster](#).

Per ulteriori informazioni, consulta [CreateDBCluster](#) Amazon DocumentDB API Reference.

Descrizione dei cluster Amazon DocumentDB

Puoi utilizzare la Console di gestione Amazon DocumentDB o AWS CLI visualizzare dettagli come endpoint di connessione, gruppi di sicurezza, VPC e gruppi di parametri relativi ai cluster Amazon DocumentDB.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- [Monitoraggio dello stato di un cluster Amazon DocumentDB](#)
- [Ricerca degli endpoint del cluster](#)

Using the AWS Management Console

Utilizza la seguente procedura per visualizzare i dettagli di un cluster Amazon DocumentDB specificato utilizzando la console.

1. [Accedi a e apri AWS Management Console la console Amazon DocumentDB all'indirizzo https://console.aws.amazon.com/docdb](https://console.aws.amazon.com/docdb).
2. Nel pannello di navigazione scegliere Clusters (Cluster).

i Tip

Se il riquadro di navigazione non viene visualizzato sul lato sinistro della schermata, scegliere l'icona del menu (☰) nell'angolo in alto a sinistra della pagina.

3. Nell'elenco dei cluster scegli il nome del cluster di cui desideri visualizzare i dettagli. Le informazioni sul cluster vengono organizzate nei seguenti gruppi:
 - **Riepilogo:** informazioni generali sul cluster, tra cui la versione del motore, lo stato del cluster, la manutenzione in corso e lo stato del relativo gruppo di parametri.
 - **Connettività e sicurezza:** la sezione Connect elenca gli endpoint di connessione per connettersi a questo cluster con la shell mongo o con un'applicazione. Nella sezione Security Groups (Gruppi di sicurezza) sono elencati i gruppi di protezione associati a questo cluster e l'ID VPC e le descrizioni.
 - **Configurazione:** la sezione dei dettagli del cluster elenca i dettagli sul cluster, inclusi l'Amazon Resource Name (ARN), l'endpoint e il gruppo di parametri del cluster. Vengono inoltre elencate le informazioni di backup del cluster, i dettagli di manutenzione e le impostazioni di sicurezza e di rete. La sezione Cluster instances (Istanze del cluster) elenca le istanze che appartengono a questo cluster con lo stato del ruolo e del gruppo di parametri del cluster di ogni istanza.
 - **Monitoraggio:** i parametri di Amazon CloudWatch Logs per questo cluster. Per ulteriori informazioni, consulta [Monitoraggio di Amazon DocumentDB con CloudWatch](#).
 - **Eventi e tag:** la sezione Eventi recenti elenca gli eventi recenti per questo cluster. Amazon DocumentDB registra gli eventi relativi a cluster, istanze, snapshot, gruppi di sicurezza e gruppi di parametri del cluster. Queste informazioni includono la data, l'ora e il messaggio associati a ciascun evento. La sezione Tag elenca i tag allegati al cluster.

Using the AWS CLI

Per visualizzare i dettagli dei tuoi cluster Amazon DocumentDB utilizzando il AWS CLI, usa il `describe-db-clusters` comando come mostrato negli esempi seguenti. Per ulteriori informazioni, consulta [DescribeDBClusters](#) Amazon DocumentDB Resource Management API Reference.

Note

Per alcune funzionalità di gestione come la gestione del ciclo di vita di cluster e istanze, Amazon DocumentDB sfrutta la tecnologia operativa condivisa con Amazon RDS. Il parametro `filterName=engine,Values=docdb` filter restituisce solo cluster Amazon DocumentDB.

Example

Esempio 1: elenca tutti i cluster Amazon DocumentDB

Il AWS CLI codice seguente elenca i dettagli per tutti i cluster Amazon DocumentDB in una regione.

```
aws docdb describe-db-clusters --filter Name=engine,Values=docdb
```

L'aspetto dell'output di questa operazione è simile al seguente.

```
{
  "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

Esempio 2: elenca tutti i dettagli per un cluster Amazon DocumentDB specificato

Il AWS CLI codice seguente elenca i dettagli del cluster `sample-cluster`.

Per Linux, macOS o Unix:

```

aws docdb describe-db-clusters \
  --filter Name=engine,Values=docdb \
  --db-cluster-identifier sample-cluster

```

Per Windows:

```

aws docdb describe-db-clusters ^
  --filter Name=engine,Values=docdb ^
  --db-cluster-identifier sample-cluster

```

L'aspetto dell'output di questa operazione è simile al seguente.

```

{
  "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

Esempio 3: elenca dettagli specifici per un cluster Amazon DocumentDB

Per elencare un sottoinsieme dei dettagli dei cluster utilizzando il AWS CLI, aggiungi un elenco `--query` che specifichi quali membri del cluster l'`describe-db-clusters` operazione deve elencare. Il parametro `--db-cluster-identifier` è l'identificatore per il particolare cluster del quale desideri visualizzare i dettagli. Per ulteriori informazioni sulle interrogazioni, consulta [Come filtrare l'output con l'--query opzione nella Guida per l'utente AWS Command Line Interface](#)

L'esempio seguente elenca le istanze in un cluster Amazon DocumentDB.

Per Linux, macOS o Unix:

```

aws docdb describe-db-clusters \
  --filter Name=engine,Values=docdb \
  --db-cluster-identifier sample-cluster \
  --query 'DBClusters[*].[DBClusterMembers]'

```

Per Windows:

```

aws docdb describe-db-clusters ^
  --filter Name=engine,Values=docdb ^
  --db-cluster-identifier sample-cluster ^
  --query 'DBClusters[*].[DBClusterMembers]'

```

L'aspetto dell'output di questa operazione è simile al seguente.

```
[
  [
    [
      {
        "DBInstanceIdentifier": "sample-instance-1",
        "IsClusterWriter": true,
        "DBClusterParameterGroupStatus": "in-sync",
        "PromotionTier": 1
      },
      {
        "DBInstanceIdentifier": "sample-instance-2",
        "IsClusterWriter": false,
        "DBClusterParameterGroupStatus": "in-sync",
        "PromotionTier": 1
      }
    ]
  ]
]
```

Modifica di un cluster Amazon DocumentDB

Per modificare un cluster, il cluster deve essere nello stato disponibile. Non è possibile modificare un cluster arrestato. Se il cluster viene arrestato, per prima cosa avviare il cluster, attendere che diventi disponibile, quindi apportare le modifiche desiderate. Per ulteriori informazioni, consulta [Arresto e avvio di un cluster Amazon DocumentDB](#).

Using the AWS Management Console

Utilizza la seguente procedura per modificare uno specifico cluster Amazon DocumentDB utilizzando la console.

Per modificare un cluster Amazon DocumentDB

1. [Accedi a e apri AWS Management Console la console Amazon DocumentDB all'indirizzo `https://console.aws.amazon.com/docdb`.](https://console.aws.amazon.com/docdb)
2. Nel pannello di navigazione scegliere Clusters (Cluster).

 Tip

Se il riquadro di navigazione non viene visualizzato sul lato sinistro della schermata, scegliere l'icona del menu (☰) nell'angolo in alto a sinistra della pagina.

3. Specifica il cluster da modificare scegliendo il pulsante a sinistra del nome del cluster.
4. Scegli Actions (Operazioni), quindi Modify (Modifica).
5. Nel riquadro Modify Cluster: cluster-name (Modifica cluster: cluster-name) apporta le modifiche desiderate. È possibile modificare le seguenti aree:
 - Specifiche del cluster: nome, gruppi di sicurezza e password del cluster.
 - Configurazione dello storage del cluster: la modalità di archiviazione dei dati del cluster. Scegli tra la configurazione standard e quella ottimizzata per l'I/O.
 - Opzioni del cluster: la porta e il gruppo di parametri del cluster.
 - Backup: il periodo di conservazione dei backup e la finestra di backup del cluster.
 - Esportazioni di log: abilita o disabilita l'esportazione dei log di controllo o del profiler.
 - Manutenzione: imposta la finestra di manutenzione del cluster.
 - Protezione dall'eliminazione: abilita o disabilita la protezione da eliminazione sul cluster. Per impostazione predefinita, la protezione da eliminazione è abilitata.
6. Al termine, scegli Continue (Continua) per visualizzare un riepilogo delle modifiche.
7. Se accetti le modifiche, puoi scegliere Modify cluster (Modifica cluster) per modificare il cluster. In alternativa, puoi scegliere Back (Indietro) o Cancel (Annulla) per modificare o annullare le modifiche, rispettivamente.

L'applicazione delle modifiche richiede qualche minuto. Puoi utilizzare il cluster solo quando ha lo stato disponibile. Puoi monitorare lo stato del cluster con la console o l' AWS CLI. Per ulteriori informazioni, consulta [Monitoraggio dello stato di un cluster Amazon DocumentDB](#).

Using the AWS CLI

Utilizzare l'operazione `modify-db-cluster` per modificare il cluster specificato utilizzando il comando AWS CLI. Per ulteriori informazioni, consulta [ModifyDBCluster](#) Amazon DocumentDB API Reference.

Parametri

- **--db-cluster-identifier**: obbligatorio. L'identificatore del cluster Amazon DocumentDB che intendi modificare.
- **--backup-retention-period**—Facoltativo. Il numero di giorni durante i quali vengono conservati i backup automatici. I valori validi sono compresi tra 1 e 35.
- **--storage-type**—Facoltativo. La configurazione di archiviazione del cluster. I valori validi sono `standard` (Standard) o `iopt1` (ottimizzato per l'I/O).
- **--db-cluster-parameter-group-name**—Facoltativo. Il nome del gruppo di parametri del cluster da utilizzare per il cluster.
- **--master-user-password**—Facoltativo. La nuova password per l'utente principale del database.

Vincoli per la password:

- La lunghezza è di [8—100] caratteri ASCII stampabili.
- È possibile utilizzare qualsiasi carattere ASCII stampabile eccetto i seguenti:
 - / (barra)
 - " (virgolette doppie)
 - @ (simbolo chiocciola)
- **--new-db-cluster-identifier**—Facoltativo. Il nuovo identificatore per il cluster quando un cluster viene rinominato. Questo valore è archiviato come stringa in caratteri minuscoli.

Vincoli per la denominazione

- La lunghezza è di [1—63] lettere, numeri o trattini.
- Il primo carattere deve essere una lettera.
- Non può terminare con un trattino o contenere due trattini consecutivi.
- Deve essere unico per tutti i cluster di Amazon RDS, Amazon Neptune e Amazon DocumentDB per regione. Account AWS
- **--preferred-backup-window**—Facoltativo. L'intervallo temporale giornaliero durante il quale vengono creati i backup automatici, in UTC.
 - Formato: `hh24:mm-hh24:mm`
- **--preferred-maintenance-window**—Facoltativo. L'intervallo temporale settimanale durante il quale può avvenire la manutenzione dei sistemi, in UTC.
 - Formato: `ddd:hh24:mm-ddd:hh24:mm`

- Giorni validi: Sun, Mon, Tue, Wed, Thu, Fri e Sat.
- **--deletion-protection** o **--no-deletion-protection** —Facoltativo. Se la protezione dall'eliminazione deve essere abilitata su questo cluster. La protezione dall'eliminazione impedisce che un cluster venga accidentalmente eliminato finché il cluster non viene modificato per disabilitare la protezione dall'eliminazione. Per ulteriori informazioni, consulta [Eliminazione di un cluster Amazon DocumentDB](#).
- **--apply-immediately** o **--no-apply-immediately**: **--apply-immediately** da utilizzare per apportare immediatamente la modifica. Utilizzare **--no-apply-immediately** per apportare la modifica durante la finestra di manutenzione successiva del cluster.

Example

Il codice seguente cambia il periodo di retention dei backup per il cluster `sample-cluster`.

Per Linux, macOS o Unix:

```
aws docdb modify-db-cluster \
  --db-cluster-identifier sample-cluster \
  --apply-immediately \
  --backup-retention-period 7
```

Per Windows:

```
aws docdb modify-db-cluster ^
  --db-cluster-identifier sample-cluster ^
  --apply-immediately ^
  --backup-retention-period 7
```

L'aspetto dell'output di questa operazione è simile al seguente.

```
{
  "DBCluster": {
    "BackupRetentionPeriod": 7,
    "DbClusterResourceId": "cluster-VDP53QEWST7YHM36TTX0PJT5YE",
    "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
}
}

```

L'applicazione delle modifiche richiede qualche minuto. Puoi utilizzare il cluster solo quando ha lo stato disponibile. Puoi monitorare lo stato del cluster con la console o l' AWS CLI. Per ulteriori informazioni, consulta [Monitoraggio dello stato di un cluster Amazon DocumentDB](#).

Determinazione della manutenzione in sospeso

Puoi determinare se disponi della versione più recente del motore Amazon DocumentDB determinando se hai una manutenzione del cluster in sospeso.

Using the AWS Management Console

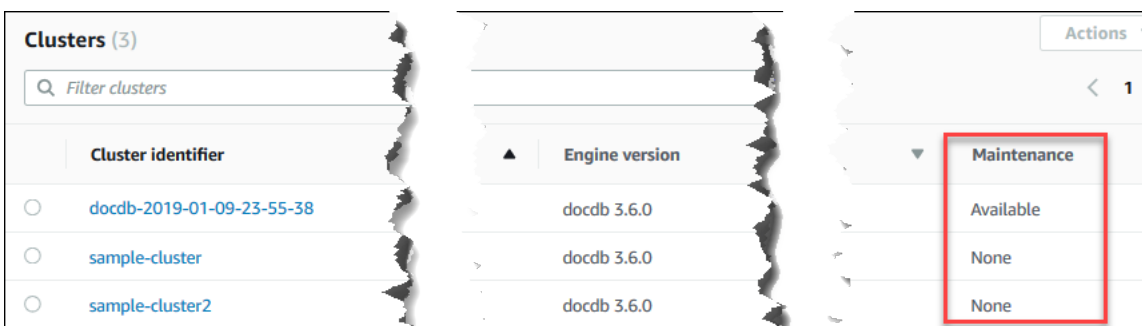
Puoi usare il AWS Management Console per determinare se un cluster ha una manutenzione in sospeso.

1. [Accedi a e apri AWS Management Console la console Amazon DocumentDB all'indirizzo https://console.aws.amazon.com/docdb](https://console.aws.amazon.com/docdb).
2. Nel pannello di navigazione scegliere Clusters (Cluster).

Tip

Se il riquadro di navigazione non viene visualizzato sul lato sinistro della schermata, scegliere l'icona del menu (☰) nell'angolo in alto a sinistra della pagina.

3. Individuare la colonna Maintenance (Manutenzione) per determinare se un cluster è in attesa di manutenzione.



None (Nessuno) indica che sul cluster è in esecuzione l'ultima versione del motore. Available (Disponibile) indica che il cluster è in attesa di manutenzione, il che potrebbe significare che è necessario l'aggiornamento del motore.

4. Se il cluster è in attesa di manutenzione, continuare con la procedura in [Esecuzione di un aggiornamento della patch alla versione del motore di un cluster](#).

Using the AWS CLI

Puoi utilizzare il AWS CLI per determinare se un cluster dispone della versione più recente del motore utilizzando l'`describe-pending-maintenance-actions` operazione con i seguenti parametri.

Parametri

- **--resource-identifier**—Facoltativo. L'ARN per la risorsa (cluster). Se questo parametro viene omesso, vengono elencate le operazioni di manutenzione in attesa per tutti i cluster.
- **--region**—Facoltativo. L'endpoint della regione AWS in cui eseguire l'operazione, ad esempio `us-east-1`.

Example

Per Linux, macOS o Unix:

```
aws docdb describe-pending-maintenance-actions \  
  --resource-identifier arn:aws:rds:us-east-1:123456789012:cluster:sample-cluster \  
  --region us-east-1
```

Per Windows:

```
aws docdb describe-pending-maintenance-actions ^  
  --resource-identifier arn:aws:rds:us-east-1:123456789012:cluster:sample-cluster ^  
  --region us-east-1
```

L'aspetto dell'output di questa operazione è simile al seguente.

```
{  
  "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"  
  }  
]
```

Se il cluster è in attesa di manutenzione, continuare con la procedura in [Esecuzione di un aggiornamento della patch alla versione del motore di un cluster](#).

Esecuzione di un aggiornamento della patch alla versione del motore di un cluster

In questa sezione, spiegheremo come distribuire un aggiornamento di patch utilizzando AWS Management Console o il AWS CLI. Un aggiornamento patch è un aggiornamento all'interno della stessa versione del motore (ad esempio, l'aggiornamento di una versione del motore 3.6 a una versione più recente del motore 3.6). Puoi aggiornarlo immediatamente o durante la prossima finestra di manutenzione del cluster. Per determinare se il motore necessita di un aggiornamento, consulta [Determinazione della manutenzione in sospeso](#). Tieni presente che quando applichi l'aggiornamento, il cluster subirà dei tempi di inattività.

Note

Se stai cercando di eseguire l'aggiornamento da una versione principale del motore a un'altra, ad esempio dalla 3.6 alla 5.0, consulta una delle due versioni oppure [Aggiornamento immediato della versione principale di Amazon DocumentDB](#). [Aggiornamento del cluster Amazon DocumentDB tramite AWS Database Migration Service](#) Un aggiornamento immediato della versione principale supporta solo docdb 5.0 come versione del motore di destinazione.

Esistono due requisiti di configurazione per ottenere gli ultimi aggiornamenti delle patch per la versione del motore di un cluster:

- Lo stato del cluster deve essere disponibile.
- Il cluster deve eseguire una versione precedente del motore.

Using the AWS Management Console

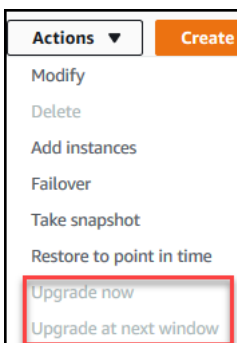
La procedura seguente applica gli aggiornamenti delle patch alla versione del motore del cluster utilizzando la console. Hai la possibilità di eseguire l'aggiornamento immediatamente o durante la prossima finestra di manutenzione del cluster.

1. [Accedi a e apri AWS Management Console la console Amazon DocumentDB all'indirizzo https://console.aws.amazon.com/docdb](https://console.aws.amazon.com/docdb).
2. Nel pannello di navigazione scegliere Clusters (Cluster). Dall'elenco di cluster scegliere il pulsante a sinistra del cluster che si desidera aggiornare. Lo stato del cluster deve essere disponibile.

Tip

Se il riquadro di navigazione non viene visualizzato sul lato sinistro della schermata, scegliere l'icona del menu (☰) nell'angolo in alto a sinistra della pagina.

3. Nel menu Actions (Operazioni) scegliere una delle opzioni indicate di seguito. Queste opzioni di menu sono selezionabili solo se sul cluster scelto non è in esecuzione la versione più recente del motore.



- **Aggiorna ora:** avvia immediatamente il processo di aggiornamento. Il cluster sarà temporaneamente offline durante l'aggiornamento alla versione più recente del motore.

- **Aggiorna alla finestra successiva:** avvia il processo di aggiornamento durante la successiva finestra di manutenzione del cluster. Il cluster sarà temporaneamente offline durante l'aggiornamento del cluster alla versione più recente del motore.
4. Quando si apre la finestra di conferma, scegliere una delle seguenti opzioni:
- **Aggiornamento:** per aggiornare il cluster alla versione più recente del motore in base alla pianificazione scelta nel passaggio precedente.
 - **Annulla:** per annullare l'aggiornamento del motore del cluster e continuare con la versione corrente del motore del cluster.

Using the AWS CLI

È possibile applicare gli aggiornamenti delle patch al cluster utilizzando l'`apply-pending-maintenance-action` operazione AWS CLI and con i seguenti parametri.

Parametri

- **--resource-identifier:** obbligatorio. L'ARN del cluster Amazon DocumentDB che intendi aggiornare.
- **--apply-action:** obbligatorio. Sono consentiti i seguenti valori. Per aggiornare la versione del motore di un cluster, utilizzare `db-upgrade`.
 - **db-upgrade**
 - **system-update**
- **--opt-in-type:** obbligatorio. Sono consentiti i seguenti valori.
 - `immediate`—Applica immediatamente l'azione di manutenzione.
 - `next-maintenance`—Applica l'azione di manutenzione durante la finestra di manutenzione successiva.
 - `undo-opt-in`—Annulla tutte le richieste di `next-maintenance opt-in` esistenti.

Example

La seguente patch di esempio aggiorna la versione del motore `sample-cluster` alla versione 4.0.0.

Per Linux, macOS o 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
```

Per 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
```

L'aspetto dell'output di questa operazione è simile al seguente.

```
{  
  "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"  
      }  
    ]  
  }  
}
```

Arresto e avvio di un cluster Amazon DocumentDB

L'interruzione e l'avvio dei cluster Amazon DocumentDB può aiutarti a gestire i costi per gli ambienti di sviluppo e test. Invece di creare ed eliminare cluster e istanze ogni volta che usi Amazon DocumentDB, puoi interrompere temporaneamente tutte le istanze del cluster quando non sono necessarie. È quindi possibile avviarle nuovamente quando è necessario riprendere il testing.

Argomenti

- [Panoramica dell'avvio e dell'arresto di un cluster.](#)
- [Operazioni che è possibile eseguire su un cluster interrotto](#)

Panoramica dell'avvio e dell'arresto di un cluster.

Nei periodi in cui non è necessario un cluster Amazon DocumentDB, è possibile interrompere tutte le istanze in quel cluster contemporaneamente. È possibile avviare nuovamente il cluster ogni volta che è necessario utilizzarlo. L'avvio e l'arresto semplificano i processi di impostazione e rimozione dei cluster utilizzati per lo sviluppo, i test o attività analoghe che non richiedono una disponibilità continua. Puoi arrestare e avviare un cluster utilizzando il AWS Management Console o AWS CLI con una singola azione, indipendentemente dal numero di istanze nel cluster.

Quando il cluster viene arrestato, il volume di archiviazione associato al cluster rimane invariato. Vengono addebitati solo i costi per lo storage, gli snapshot manuali e lo storage di backup automatici all'interno della finestra di retention specificata. Non ti viene addebitato alcun costo per le ore di utilizzo delle istanze. Amazon DocumentDB avvia automaticamente il cluster dopo sette giorni in modo da non rimanere indietro rispetto agli aggiornamenti di manutenzione richiesti. Quando il cluster viene avviato dopo 7 giorni, avrà nuovamente inizio l'addebito relativo alle istanze del cluster. Mentre il cluster viene arrestato, non è possibile eseguire query sul volume di archiviazione perché l'esecuzione di query richiede che le istanze siano nello stato disponibile.

Quando un cluster Amazon DocumentDB viene arrestato, né il cluster né le relative istanze possono essere modificati in alcun modo. Ciò include l'aggiunta o la rimozione di istanze o l'eliminazione del cluster.

Using the AWS Management Console

La seguente procedura mostra come arrestare un cluster con una o più istanze in stato disponibile o avviare un cluster arrestato.

Per arrestare o avviare un cluster Amazon DocumentDB

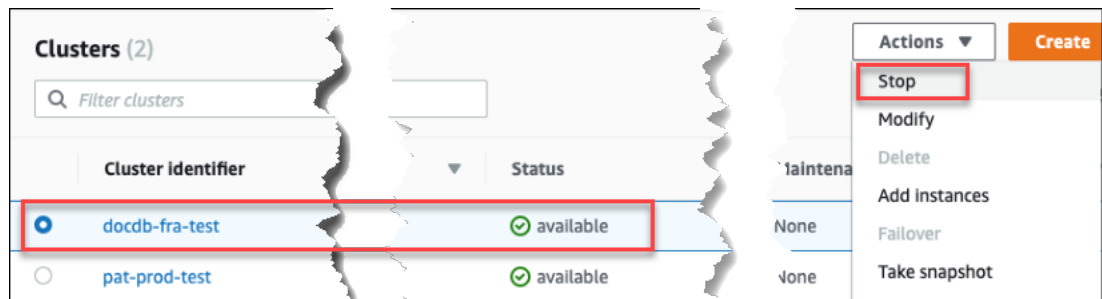
1. [Accedi a e apri AWS Management Console la console Amazon DocumentDB all'indirizzo https://console.aws.amazon.com/docdb.](https://console.aws.amazon.com/docdb)
2. Nel pannello di navigazione scegliere Clusters (Cluster).

Tip

Se il riquadro di navigazione non viene visualizzato sul lato sinistro della schermata, scegliere l'icona del menu (☰) nell'angolo in alto a sinistra della pagina.

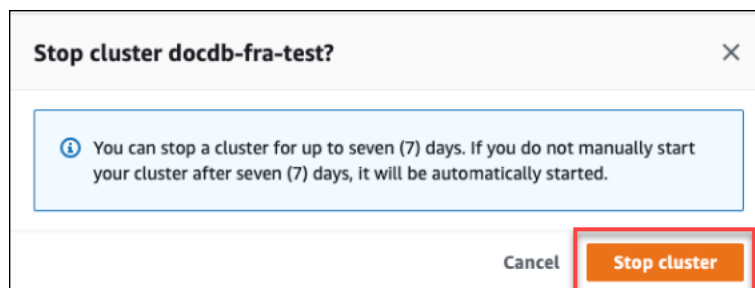
3. Quindi, nell'elenco dei cluster, scegliere il pulsante a sinistra del nome del cluster che si desidera arrestare o avviare.
4. Scegliere Actions (Operazioni) e quindi scegliere l'operazione che si desidera eseguire sul cluster.
 - Se si desidera arrestare il cluster e il cluster è disponibile:

a. Scegli Stop (Arresta).

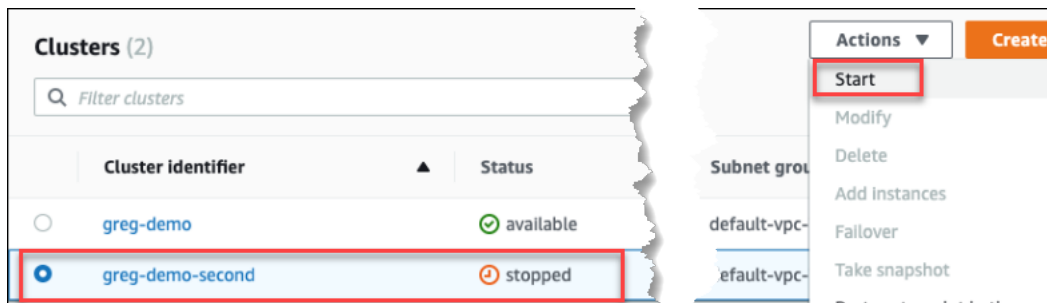


Per evitare l'attivazione del meccanismo di failover, l'operazione di arresto interrompe prima le istanze di replica e poi l'istanza primaria.

- b. Nella finestra di dialogo di conferma, confermare che si desidera arrestare il cluster scegliendo Stop cluster (Arresta cluster) oppure, per mantenere il cluster in esecuzione, scegliere Cancel (Annulla).



- Se si desidera avviare il cluster e il cluster è arrestato, scegliere Start (Avvia).



5. Monitorare lo stato del cluster e delle relative istanze. Se si avvia il cluster, è possibile riprendere ad utilizzare il cluster quando il cluster e le relative istanze risultano disponibili. Per ulteriori informazioni, consulta [Determinazione dello stato di un cluster](#).



Using the AWS CLI

I seguenti codici di esempio illustrano come arrestare un cluster con una o più istanze in stato disponibile o avviare un cluster arrestato.

Per arrestare un cluster con una o più istanze disponibili utilizzando il AWS CLI, usa l'`stop-db-cluster` operazione. Per avviare un cluster arrestato, utilizzare l'operazione `start-db-cluster`. Entrambe le operazioni consentono di utilizzare il parametro `--db-cluster-identifier`.

Parametro:

- **`--db-cluster-identifier`**: obbligatorio. Il nome del cluster da arrestare o avviare.

Example — Per arrestare un cluster utilizzando il AWS CLI

Il codice seguente arresta il cluster `sample-cluster`. Il cluster deve avere una o più istanze in stato disponibile.

Per Linux, macOS o Unix:


```
aws docdb stop-db-cluster \  
  --db-cluster-identifier sample-cluster
```

Per Windows:

```
aws docdb stop-db-cluster ^  
  --db-cluster-identifier sample-cluster
```

Example — Per avviare un cluster utilizzando il AWS CLI

Il codice seguente avvia il cluster `sample-cluster`. Il cluster deve attualmente essere arrestato.

Per Linux, macOS o Unix:

```
aws docdb start-db-cluster \  
  --db-cluster-identifier sample-cluster
```

Per Windows:

```
aws docdb start-db-cluster ^  
  --db-cluster-identifier sample-cluster
```

Operazioni che è possibile eseguire su un cluster interrotto

Mentre un cluster Amazon DocumentDB è fermo, puoi eseguire un point-in-time ripristino in qualsiasi punto all'interno della finestra di conservazione dei backup automatizzata specificata. Per informazioni dettagliate su come eseguire un point-in-time ripristino, consulta [Ripristino a un punto temporale specifico](#).

Non è possibile modificare la configurazione di un cluster Amazon DocumentDB o di nessuna delle sue istanze mentre il cluster è fermo. Inoltre, non è possibile aggiungere o rimuovere istanze di database dal cluster o eliminarlo se possiede ancora istanze di database associate. Devi avviare il cluster prima di eseguire questo tipo di operazioni amministrative.

Amazon DocumentDB applica qualsiasi manutenzione programmata al cluster interrotto solo dopo che è stato riavviato. Dopo sette giorni, Amazon DocumentDB avvia automaticamente un cluster interrotto in modo che non rimanga troppo indietro nello stato di manutenzione. Quando il cluster viene riavviato, avrà nuovamente inizio l'addebito relativo alle istanze del cluster.

Mentre un cluster è fermo, Amazon DocumentDB non esegue backup automatici né estende il periodo di conservazione dei backup.

Eliminazione di un cluster Amazon DocumentDB

Puoi eliminare un cluster Amazon DocumentDB utilizzando AWS Management Console o il AWS CLI. Per eliminare un cluster, il cluster deve trovarsi nello stato disponibile e non deve avere alcuna istanza associata. Se il cluster viene arrestato, per prima cosa avviare il cluster, attendere che diventi disponibile, quindi eliminarlo. Per ulteriori informazioni, consulta [Arresto e avvio di un cluster Amazon DocumentDB](#).

Deletion protection (Protezione da eliminazione)

Per proteggere il cluster dall'eliminazione accidentale, è possibile abilitare la protezione dall'eliminazione. Quando si crea un cluster utilizzando la console, la protezione dall'eliminazione viene abilitata per impostazione predefinita. Tuttavia, la protezione dall'eliminazione è disabilitata per impostazione predefinita se si crea un cluster utilizzando la AWS CLI.

Amazon DocumentDB applica la protezione da eliminazione per un cluster indipendentemente dal fatto che l'operazione di eliminazione venga eseguita utilizzando la console o il AWS CLI. Se la protezione dall'eliminazione è abilitata, non puoi eliminare un cluster. Per eliminare un cluster con la protezione dall'eliminazione abilitata, devi modificare il cluster e disabilitare la protezione dall'eliminazione.

Quando si utilizza la console con la protezione dall'eliminazione abilitata su un cluster, non è possibile eliminare l'ultima istanza del cluster perché questa operazione elimina anche il cluster. È possibile eliminare l'ultima istanza di un cluster con protezione dall'eliminazione attiva utilizzando la AWS CLI. Il cluster, tuttavia, è ancora esistente e i dati sono conservati. È possibile accedere ai dati mediante la creazione di nuove istanze per il cluster. Per ulteriori informazioni sull'abilitazione e la disabilitazione della protezione dall'eliminazione, consulta:

- [Creazione di un cluster Amazon DocumentDB](#)
- [Modifica di un cluster Amazon DocumentDB](#)

Using the AWS Management Console

Per eliminare un cluster utilizzando la AWS Management Console, la protezione dall'eliminazione deve essere disabilitata.

Per determinare se la protezione dall'eliminazione di un cluster è abilitata:

1. [Accedi a e apri AWS Management Console la console Amazon DocumentDB all'indirizzo `https://console.aws.amazon.com/docdb`.](https://console.aws.amazon.com/docdb)
2. Nel pannello di navigazione scegliere Clusters (Cluster).

Tip

Se il riquadro di navigazione non viene visualizzato sul lato sinistro della schermata, scegliere l'icona del menu (☰) nell'angolo in alto a sinistra della pagina.

3. Tieni presente che nella casella di navigazione Cluster, la colonna Cluster Identifier mostra sia i cluster che le istanze. Le istanze sono elencate sotto i cluster, in modo simile alla schermata seguente.

<input type="checkbox"/>	<input type="checkbox"/>	Cluster identifier	Role	Engine version	Region & AZ
<input type="checkbox"/>	<input type="checkbox"/>	docdb-cloud9-getstarted	Cluster	3.6.0	us-east-1
<input type="checkbox"/>	<input type="checkbox"/>	docdb-cloud9-getstarted	Primary	3.6.0	us-east-1f
<input type="checkbox"/>	<input type="checkbox"/>	robo3t	Cluster	3.6.0	us-east-1
<input type="checkbox"/>	<input type="checkbox"/>	robo3t	Primary	3.6.0	us-east-1d

4. Scegliere il nome del cluster e selezionare la scheda Configuration (Configurazione) . Nella sezione Cluster details (Dettagli cluster) individuare l'opzione Deletion protection (Protezione dall'eliminazione). Se la protezione dall'eliminazione è abilitata, modificare il cluster per disabilitarla. Per ulteriori informazioni sulla modifica di un cluster database, consultare [Modifica di un cluster Amazon DocumentDB](#).

Dopo aver eliminato la Deletion protection (Protezione dall'eliminazione), è possibile eliminare il cluster.

Per eliminare un cluster:

1. Nel pannello di navigazione scegliere Clusters (Cluster).

2. Determinare se il cluster dispone di qualche istanza selezionando la colonna Instances (Istanze). Per eliminare un cluster, devi eliminare tutte le sue istanze. Per ulteriori informazioni, consulta [Eliminazione di un'istanza Amazon DocumentDB](#).
3. A seconda che il cluster disponga o meno di qualche istanza, eseguire una delle seguenti operazioni.
 - Se il cluster non dispone di istanze, selezionare il pulsante a sinistra del nome del cluster e scegliere Actions (Operazioni). Dal menu a discesa, scegli Delete (Elimina). Completare la finestra di dialogo Delete <cluster-name> (Elimina <cluster-name>) e quindi scegliere Delete (Elimina).
 - Se il cluster dispone di una o più istanze, eseguire le operazioni descritte qui di seguito:
 - a. Nel riquadro di navigazione, seleziona Istanze.
 - b. Eliminare tutte le istanze del cluster. Quando si elimina l'ultima istanza, anche il cluster viene eliminato. Per ulteriori informazioni sull'eliminazione delle istanze, consultare [Eliminazione di un'istanza Amazon DocumentDB](#).

Sono necessari alcuni minuti per l'eliminazione del cluster. Per monitorare lo stato del cluster, consulta [Monitoraggio dello stato di un cluster Amazon DocumentDB](#).

Using the AWS CLI

Non puoi eliminare un cluster a cui sono associate delle istanze. Per determinare quali istanze sono associate al cluster, esegui il comando `describe-db-clusters` ed elimina tutte le istanze del cluster. Quindi, se necessario, disattiva la protezione dell'eliminazione nel cluster e, infine, elimina il cluster.

1. In primo luogo, elimina tutte le istanze del cluster.

Per determinare quali istanze eliminare, esegui il comando seguente.

```
aws docdb describe-db-clusters \
  --db-cluster-identifier sample-cluster \
  --query 'DBClusters[*].
  [DBClusterIdentifier,DBClusterMembers[*].DBInstanceIdentifier]'
```

L'aspetto dell'output di questa operazione è simile al seguente (formato JSON).

```
[
```

```
[
  "sample-cluster",
  [
    "sample-instance-1",
    "sample-instance-2"
  ]
]
```

Se il cluster da eliminare possiede delle istanze associate, elimina tali istanze prima di continuare.

```
aws docdb delete-db-instance \
  --db-instance-identifier sample-instance
```

2. In secondo luogo, disabilita la protezione da eliminazione.

L'utilizzo AWS CLI di per eliminare tutte le istanze di un cluster non elimina il cluster. È anche necessario eliminare il cluster, ma è possibile eseguire questa operazione solo se la protezione dall'eliminazione è disattivata.

Per determinare se la protezione dall'eliminazione per il cluster è attivata, eseguire il seguente comando.

Tip

Per visualizzare lo stato di protezione dall'eliminazione di tutti i cluster Amazon DocumentDB, ometti il parametro. `--db-cluster-identifier`

```
aws docdb describe-db-clusters \
  --db-cluster-identifier sample-cluster \
  --query 'DBClusters[*].[DBClusterIdentifier,DeletionProtection]'
```

L'aspetto dell'output di questa operazione è simile al seguente.

```
[
  [
    "sample-cluster",
```

```

        "true"
    ]
]

```

Se la protezione dall'eliminazione per il cluster è abilitata, modificare il cluster e disabilitare la protezione dall'eliminazione. Per disabilitare la protezione dall'eliminazione del cluster, utilizzare il seguente codice.

```

aws docdb modify-db-cluster \
  --db-cluster-identifier sample-cluster \
  --no-deletion-protection \
  --apply-immediately

```

3. Infine, eliminare il cluster.

Dopo la disattivazione della protezione dall'eliminazione, è possibile eliminare il cluster. Per eliminare un cluster, utilizzare l'operazione `delete-db-cluster` con i parametri elencati di seguito.

- **--db-cluster-identifier**: obbligatorio. L'identificatore del cluster da eliminare.
- **--final-db-snapshot-identifier**—Facoltativo. Se desideri uno snapshot finale, devi includere questo parametro con un nome per l'ultimo snapshot. È necessario includere `--final-db-snapshot-identifier` o `--skip-final-snapshot`.

Vincoli per la denominazione

- La lunghezza è di [1—63] lettere, numeri o trattini.
- Il primo carattere deve essere una lettera.
- Non può terminare con un trattino o contenere due trattini consecutivi.
- Deve essere unico per tutti i cluster di Amazon RDS, Amazon Neptune e Amazon DocumentDB per regione. Account AWS
- **--skip-final-snapshot**—Facoltativo. Utilizzare questo parametro solo se non si desidera acquisire uno snapshot finale prima di eliminare il cluster. L'impostazione predefinita prevede l'acquisizione di uno snapshot finale. È necessario includere `--final-db-snapshot-identifier` o `--skip-final-snapshot`.

Il AWS CLI codice seguente elimina il cluster `sample-cluster` con un'istantanea finale. L'operazione ha esito negativo se vi sono istanze associate al cluster o se è abilitata la protezione dall'eliminazione.

Example

Per Linux, macOS o Unix:

```
aws docdb delete-db-cluster \  
  --db-cluster-identifier sample-cluster \  
  --final-db-snapshot-identifier sample-cluster-final-snapshot
```

Per Windows:

```
aws docdb delete-db-cluster ^  
  --db-cluster-identifier sample-cluster ^  
  --final-db-snapshot-identifier sample-cluster-final-snapshot
```

Example

Il AWS CLI codice seguente elimina il cluster `sample-cluster` senza scattare un'istantanea finale.

Per Linux, macOS o Unix:

```
aws docdb delete-db-cluster \  
  --db-cluster-identifier sample-cluster \  
  --skip-final-snapshot
```

Per Windows:

```
aws docdb delete-db-cluster ^  
  --db-cluster-identifier sample-cluster ^  
  --skip-final-snapshot
```

L'output dell'operazione `delete-db-cluster` è il cluster che stai eliminando.

Sono necessari alcuni minuti per l'eliminazione del cluster. Per monitorare lo stato del cluster, consulta [Monitoraggio dello stato di un cluster](#).

Scalabilità dei cluster Amazon DocumentDB

Amazon DocumentDB ti consente di scalare lo storage e l'elaborazione nei cluster in base alle tue esigenze. Questa sezione descrive come utilizzare la scalabilità dello storage, la scalabilità delle istanze e la scalabilità della lettura per gestire le prestazioni e la scalabilità per i cluster e le istanze di Amazon DocumentDB.

Argomenti

- [Dimensionamento dello storage](#)
- [Dimensionamento delle istanze](#)
- [Dimensionamento della lettura](#)
- [Ridimensionamento della scrittura](#)

Dimensionamento dello storage

Lo storage Amazon DocumentDB si ridimensiona automaticamente in base ai dati nel volume del cluster. Man mano che i dati crescono, lo storage del volume del cluster cresce con incrementi di 10 GiB, fino a 128 TiB.

Dimensionamento delle istanze

Puoi scalare il tuo cluster Amazon DocumentDB secondo necessità modificando la classe di istanza per ogni istanza del cluster. Amazon DocumentDB supporta diverse classi di istanze ottimizzate per Amazon DocumentDB.

Per ulteriori informazioni, consulta [Modifica di un'istanza Amazon DocumentDB](#).

Dimensionamento della lettura

Puoi ottenere la scalabilità di lettura per il tuo cluster Amazon DocumentDB creando fino a 15 repliche Amazon DocumentDB nel cluster. Ogni replica di Amazon DocumentDB restituisce gli stessi dati dal volume del cluster con un ritardo di replica minimo, in genere meno di 100 millisecondi dopo che l'istanza principale ha scritto un aggiornamento. Man mano che il traffico di lettura aumenta, puoi creare repliche di Amazon DocumentDB aggiuntive e connetterti direttamente ad esse per distribuire

il carico di lettura per il tuo cluster. Le repliche di Amazon DocumentDB non devono necessariamente appartenere alla stessa classe di istanza dell'istanza principale.

Per ulteriori informazioni, consulta [Aggiungere un'istanza Amazon DocumentDB a un cluster](#).

Per leggere in scala con Amazon DocumentDB, ti consigliamo di connetterti al cluster come set di repliche e di distribuire le letture sulle istanze di replica utilizzando le funzionalità di preferenza di lettura integrate del driver. Per ulteriori informazioni, consulta [Connessione ad Amazon DocumentDB come set di repliche](#).


Ridimensionamento della scrittura

Puoi scalare la capacità di scrittura sul tuo cluster Amazon DocumentDB aumentando le dimensioni dell'istanza principale del cluster. Questa sezione fornisce due metodi per dimensionare l'istanza primaria del cluster in base alle proprie esigenze. La prima opzione cerca di ridurre al minimo l'impatto delle applicazioni, ma richiede più fasi per il complemento. La seconda opzione ottimizza la semplicità in quanto ha meno fasi, ma ha un impatto potenziale maggiore sull'applicazione.

A seconda dell'applicazione, è possibile scegliere l'approccio più adatto alle proprie esigenze. Per ulteriori informazioni sulle dimensioni e sui costi delle istanze disponibili, consulta la pagina dei [prezzi di Amazon DocumentDB](#).

1. Ottimizza per garantire disponibilità e prestazioni elevate: se ti connetti al cluster in [modalità set di repliche](#) (consigliata), puoi utilizzare il seguente processo per ridurre al minimo l'impatto sull'applicazione durante il ridimensionamento dell'istanza primaria. Questo metodo riduce al minimo l'impatto perché mantiene il cluster pari o superiore all'elevata disponibilità e le destinazioni di dimensionamento in lettura vengono aggiunte al cluster come istanze, anziché essere aggiornate.
 - a. Aggiunta di una o più repliche del tipo di istanza più grande al cluster (consulta [???](#)). È consigliabile che tutte le repliche siano dello stesso tipo o di dimensioni maggiori dell'istanza primaria. Ciò evita il fileover di una riduzione involontaria delle prestazioni di scrittura su un tipo di istanza più piccolo. Per la maggior parte dei clienti, ciò significa raddoppiare temporaneamente il numero di istanze nel cluster, quindi la rimozione delle repliche più piccole al termine del dimensionamento.
 - b. Impostare il livello di failover su tutte le nuove repliche su priorità zero, assicurando che una replica del tipo di istanza più piccolo abbia la priorità di failover più alta. Per ulteriori informazioni, consulta [???](#).

- c. Avviare un failover manuale, che promuoverà una delle nuove repliche come istanza primaria. Per ulteriori informazioni, consulta [???](#).

 Note

Ciò comporterà circa 30 secondi di tempo di inattività per il cluster. Pianificare le attività di conseguenza.

- d. Rimuovere tutte le repliche di un tipo di istanza di dimensioni inferiori alla nuova istanza primaria dal cluster.
- e. Reimpostare il livello di failover di tutte le istanze sulla stessa priorità (in genere, ciò significa impostarle nuovamente su 1).

Supponiamo, ad esempio, di disporre di un cluster che attualmente contiene tre istanze `r5.large` (una primaria e due repliche) e di voler dimensionare su un tipo di istanza `r5.xlarge`. A tale scopo, è necessario innanzitutto aggiungere al cluster tre istanze di replica `r5.xlarge` e quindi impostare il livello di failover delle nuove repliche `r5.xlarge` su zero. Successivamente, è necessario avviare un failover manuale (tenendo conto che l'applicazione avrà circa 30 secondi di inattività). Una volta completato il failover, è necessario rimuovere dal cluster tutte e tre le istanze `r5.large`, lasciando il cluster dimensionato sulle istanze `r5.xlarge`.

Per aiutare a ottimizzare i costi, le istanze di Amazon DocumentDB vengono fatturate in incrementi di un secondo, con un addebito minimo di dieci minuti a seguito di una modifica dello stato fatturabile, come la creazione, la modifica o l'eliminazione di un'istanza. Per ulteriori informazioni, consulta [Ottimizzazione dei costi](#) nella documentazione relativa alle best practice.

2. Ottimizza per la semplicità: questo approccio ottimizza per la semplicità. Non espande e contrae il cluster, ma potrebbe ridurre temporaneamente la capacità di lettura.

È possibile che la modifica della classe di istanza di una replica impedisca all'istanza di soddisfare le richieste per un breve periodo di tempo, da pochi secondi a meno di 30 secondi. Se ci si connette al cluster in [modalità set di repliche](#) (consigliata), ciò ridurrebbe la capacità di lettura di una replica (ad esempio, al 66% della capacità in un cluster a 3 nodi o al 75% della capacità in un cluster a 4 nodi, ecc.) durante l'operazione di scalabilità.

- a. Scalate una delle istanze di replica del cluster. Per ulteriori informazioni, consulta [Gestione delle classi delle istanze](#).

- b. Attendi che l'istanza sia disponibile (vedi [Monitoraggio dello stato di un'istanza Amazon DocumentDB](#)).

Note

Ciò comporterà circa 30 secondi di tempo di inattività per il cluster. Pianificare le attività di conseguenza.

- c. Continuate a eseguire i passaggi 1 e 2 fino a scalare tutte le istanze di replica, una per una.
- d. Avvia un failover manuale. Ciò promuoverà una delle repliche a diventare l'istanza principale. Per ulteriori informazioni, consulta [Failover di Amazon DocumentDB](#).

Note

Ciò comporterà fino a 30 secondi di inattività per il cluster, ma spesso richiede meno tempo. Pianificare le attività di conseguenza.

- e. Ridimensiona la precedente istanza primaria (ora una replica).

Clonazione di un volume per un cluster Amazon DocumentDB

Utilizzando la clonazione di Amazon DocumentDB, puoi creare un nuovo cluster che utilizza lo stesso volume del cluster Amazon DocumentDB e contiene gli stessi dati dell'originale. Il processo è progettato per essere veloce e conveniente. Il nuovo cluster con il relativo volume di dati associato è noto come clone. La creazione di un clone è più veloce ed efficiente in termini di spazio rispetto alla copia fisica dei dati utilizzando una tecnica diversa, ad esempio con il ripristino di uno snapshot.

Amazon DocumentDB supporta la creazione di un clone con provisioning di Amazon DocumentDB da un cluster Amazon DocumentDB fornito. Quando crei un clone utilizzando una configurazione di distribuzione diversa da quella di origine, il clone viene creato utilizzando la versione più recente del motore Amazon DocumentDB del codice sorgente.

Quando crei cloni dai tuoi cluster Amazon DocumentDB, i cloni vengono creati nel AWS tuo account, lo stesso account proprietario del cluster Amazon DocumentDB di origine.

Argomenti

- [Panoramica della clonazione di Amazon DocumentDB](#)
- [Limitazioni della clonazione di Amazon DocumentDB](#)

- [Come funziona la clonazione di Amazon DocumentDB](#)
- [Creazione di un clone di Amazon DocumentDB](#)

Panoramica della clonazione di Amazon DocumentDB

Amazon DocumentDB utilizza un copy-on-write protocollo per creare un clone. Questo meccanismo utilizza uno spazio aggiuntivo minimo per creare un clone iniziale. Quando il clone viene creato per la prima volta, Amazon DocumentDB conserva una singola copia dei dati utilizzati dal cluster DB di origine e dal nuovo cluster Amazon DocumentDB (clonato). Lo storage aggiuntivo viene allocato solo quando vengono apportate modifiche ai dati (sul volume di storage Amazon DocumentDB) dal cluster Amazon DocumentDB di origine o dal clone del cluster Amazon DocumentDB. Per ulteriori informazioni sul protocollo, consulta [copy-on-write Come funziona la clonazione di Amazon DocumentDB](#)

La clonazione di Amazon DocumentDB è particolarmente utile per configurare rapidamente ambienti di test utilizzando i dati di produzione, senza rischiare il danneggiamento dei dati. È possibile utilizzare i cloni per molti tipi di applicazioni di breve durata, ad esempio:

- Sperimenta potenziali cambiamenti (modifiche allo schema e modifiche ai gruppi di parametri, ad esempio) per valutare tutti gli impatti.
- Esegui operazioni che utilizzano in modo intensivo i carichi di lavoro, come l'esportazione di dati o l'esecuzione di query analitiche sul clone.
- Creare una copia del cluster database di produzione per lo sviluppo, il test o altri scopi.

Puoi creare più di un clone dallo stesso cluster Amazon DocumentDB. È anche possibile creare più cloni da un altro clone.

Dopo aver creato un clone di Amazon DocumentDB, puoi configurare le istanze di Amazon DocumentDB in modo diverso dal cluster Amazon DocumentDB di origine. Ad esempio, potrebbe non essere necessario un clone per scopi di sviluppo per soddisfare gli stessi requisiti di alta disponibilità del cluster Amazon DocumentDB di produzione di origine. In questo caso, puoi configurare il clone con una singola istanza Amazon DocumentDB anziché con più istanze DB utilizzate dal cluster Amazon DocumentDB.

Una volta terminato di utilizzare il clone per test, sviluppo o altri scopi, è possibile eliminarlo.

Limitazioni della clonazione di Amazon DocumentDB

Amazon DocumentDB; la clonazione presenta attualmente le seguenti limitazioni:

- Puoi creare tutti i cloni che desideri, fino al numero massimo di cluster database consentito nella Regione AWS. Tuttavia, dopo aver creato 15 cloni, il clone successivo è una copia completa. L'operazione di clonazione funziona come un ripristino. point-in-time
- Non è possibile creare un clone in una AWS regione diversa dal cluster Amazon DocumentDB di origine.
- Non è possibile creare un clone da un cluster Amazon DocumentDB senza istanze DB. Puoi clonare solo cluster Amazon DocumentDB che hanno almeno un'istanza DB.
- Puoi creare un clone in un cloud privato virtuale (VPC) diverso da quello del cluster Amazon DocumentDB. Tuttavia, le sottoreti in quei VPC devono essere associate alle stesse zone di disponibilità.

Come funziona la clonazione di Amazon DocumentDB

La clonazione di Amazon DocumentDB funziona a livello di storage di un cluster Amazon DocumentDB. Utilizza un copy-on-write protocollo rapido ed efficiente in termini di supporti durevoli sottostanti che supportano il volume di storage Amazon DocumentDB. Puoi saperne di più sui volumi del cluster Amazon DocumentDB in [Gestione dei cluster Amazon DocumentDB](#)

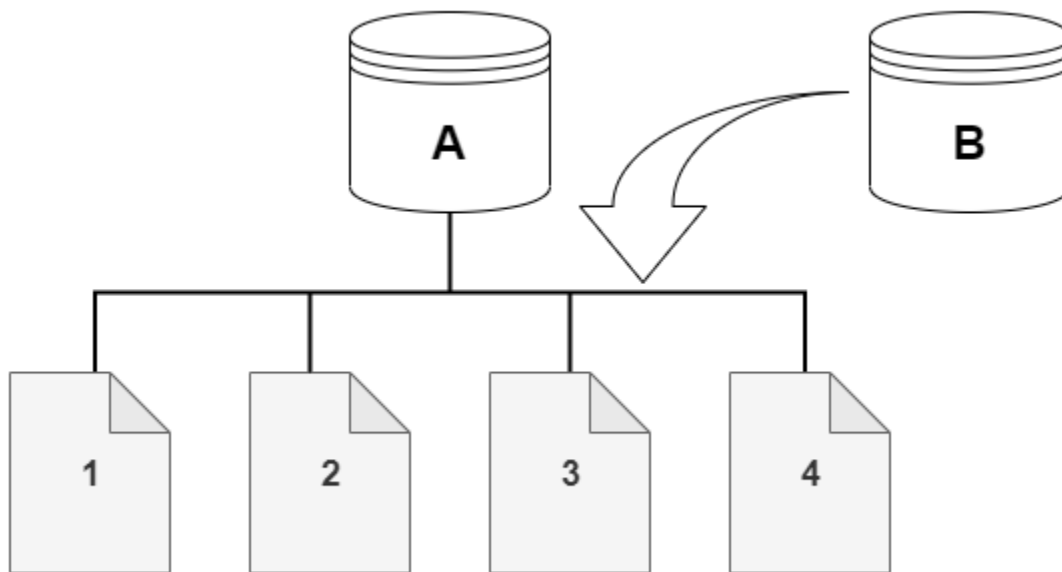
Argomenti

- [Comprendere il protocollo copy-on-write](#)
- [Eliminazione di un volume cluster di origine](#)

Comprendere il protocollo copy-on-write

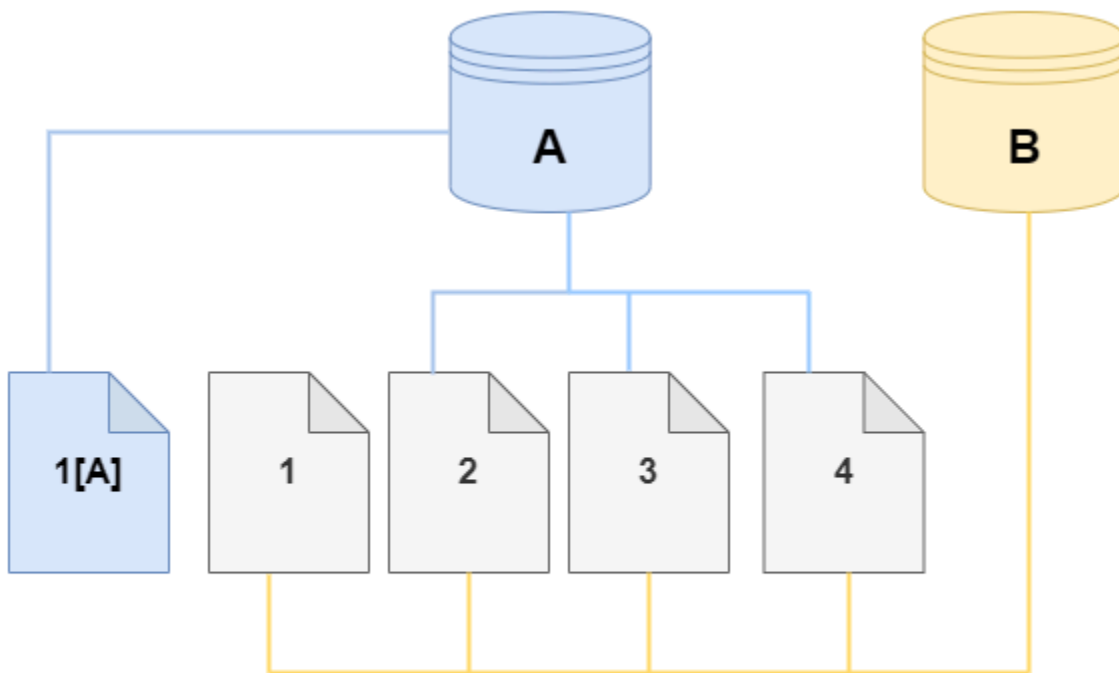
Un cluster Amazon DocumentDB archivia i dati in pagine nel volume di storage Amazon DocumentDB sottostante.

Ad esempio, nel diagramma seguente puoi trovare un cluster Amazon DocumentDB (A) con quattro pagine di dati, 1, 2, 3 e 4. Immagina che un clone, B, venga creato dal cluster Amazon DocumentDB. Quando viene creato il clone, non viene copiato alcun dato. Piuttosto, il clone punta allo stesso set di pagine del cluster Amazon DocumentDB di origine.

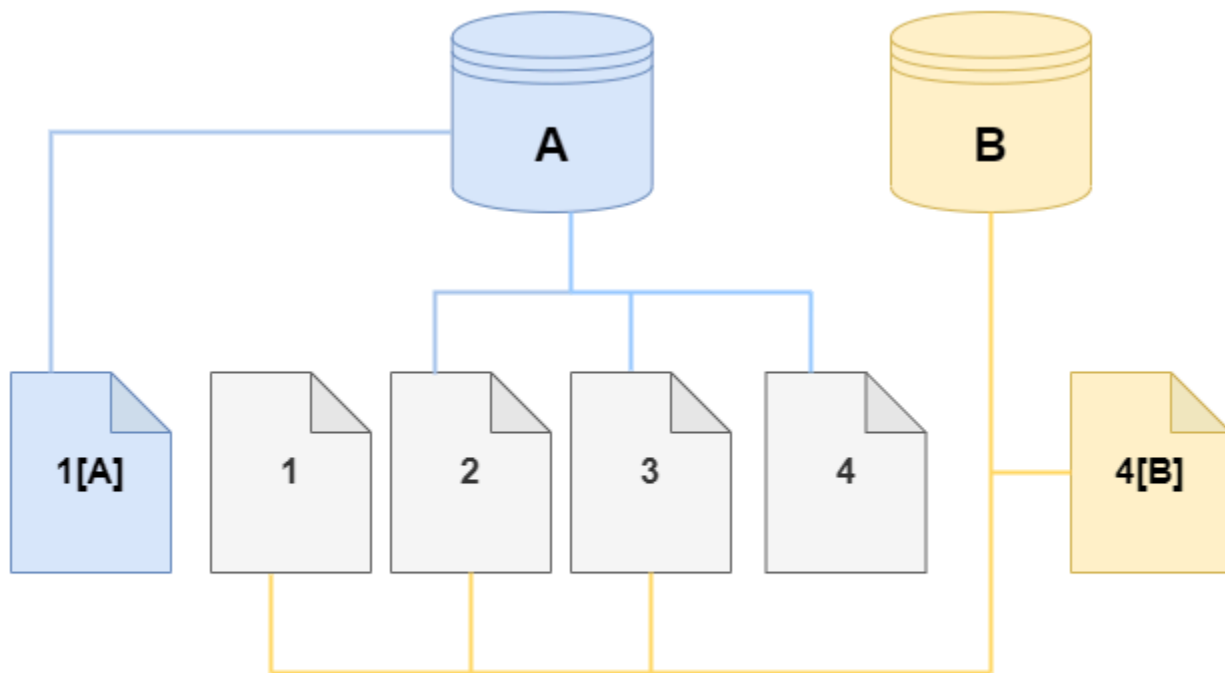


Quando viene creato il clone, in genere non è necessario alcuno spazio di archiviazione aggiuntivo. Il copy-on-write protocollo utilizza lo stesso segmento sul supporto di archiviazione fisico del segmento di origine. Lo spazio di archiviazione aggiuntivo è necessario solo se la capacità del segmento di origine non è sufficiente per l'intero segmento di clone. In questo caso, il segmento di origine viene copiato su un altro dispositivo fisico.

Nei diagrammi seguenti, è possibile trovare un esempio del copy-on-write protocollo in azione che utilizza lo stesso cluster A e il suo clone, B, come mostrato in precedenza. Supponiamo che tu apporti una modifica al tuo cluster Amazon DocumentDB (A) che comporti una modifica ai dati contenuti nella pagina 1. Invece di scrivere sulla pagina 1 originale, Amazon DocumentDB crea una nuova pagina 1 [A]. Il volume del cluster Amazon DocumentDB per cluster (A) ora punta alle pagine 1 [A], 2, 3 e 4, mentre il clone (B) fa ancora riferimento alle pagine originali.



Sul clone, viene apportata una modifica a pagina 4 sul volume di archiviazione. Invece di scrivere sulla pagina 4 originale, Amazon DocumentDB crea una nuova pagina, 4 [B]. Il clone punta ora alle pagine 1, 2, 3 e alla pagina 4[B], mentre il cluster (A) continua a puntare a 1[A], 2, 3 e 4.



Man mano che nel tempo si verificano più modifiche sia nel volume del cluster Amazon DocumentDB di origine che nel clone, è necessario più storage per acquisire e archiviare le modifiche.

Eliminazione di un volume cluster di origine

Quando si elimina un volume cluster di origine a cui sono associati uno o più cloni, i cloni non sono interessati. I database clone continuano a rimandare alle pagine precedentemente di proprietà del volume del cluster di origine.

Creazione di un clone di Amazon DocumentDB

Puoi creare un clone nello stesso AWS account del cluster Amazon DocumentDB di origine. A tale scopo, è possibile utilizzare AWS Management Console o AWS CLI le procedure seguenti.

Utilizzando la clonazione di Amazon DocumentDB, puoi creare un clone di cluster Amazon DocumentDB fornito da un cluster Amazon DocumentDB fornito.

Using the AWS Management Console

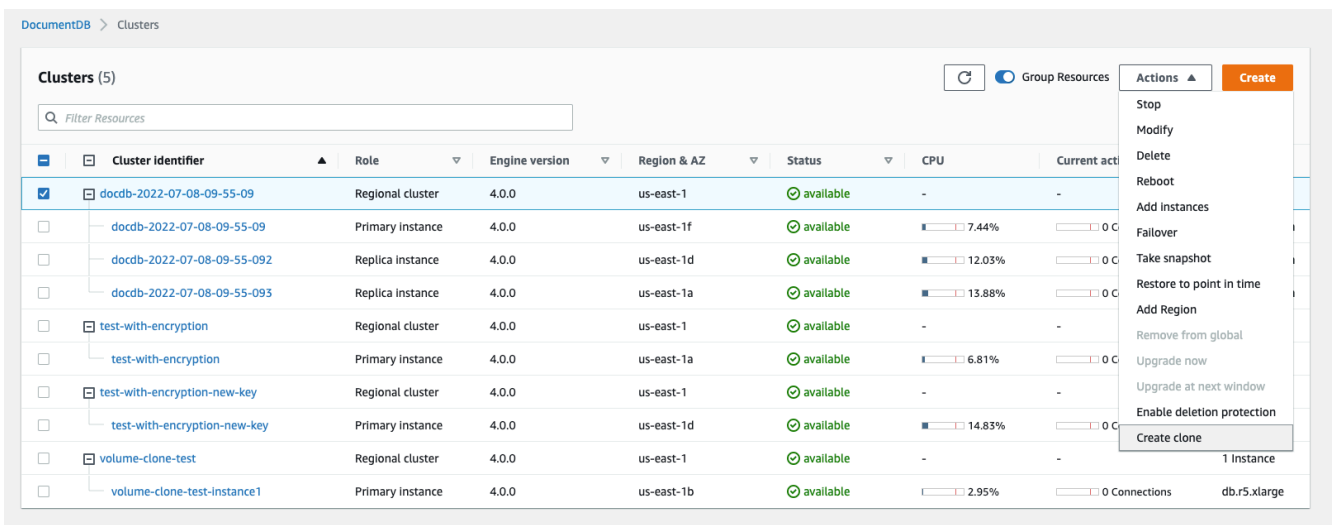
La procedura seguente descrive come clonare un cluster Amazon DocumentDB utilizzando AWS Management Console

Creazione di un clone utilizzando i AWS Management Console risultati in un cluster Amazon DocumentDB con un'istanza Amazon DocumentDB.

Queste istruzioni si applicano ai cluster DB di proprietà dello stesso AWS account che sta creando il clone. Il cluster DB deve appartenere allo stesso AWS account poiché la clonazione tra account non è supportata in Amazon DocumentDB.

Per creare un clone di un cluster DB di proprietà del tuo account, utilizza AWS Management Console

1. [Accedi a e apri AWS Management Console la console Amazon DocumentDB all'indirizzo https://console.aws.amazon.com/docdb.](https://console.aws.amazon.com/docdb)
2. Nel pannello di navigazione scegliere Clusters (Cluster).
3. Scegli il tuo cluster Amazon DocumentDB dall'elenco e, per Azioni, scegli Crea clone.



Viene visualizzata la pagina Crea clone, in cui è possibile configurare un identificatore di cluster e una classe di istanza e altre opzioni per il clone del cluster Amazon DocumentDB.

4. Nella sezione Rule settings (Impostazioni regole), procedi nel seguente modo:
 - a. Per l'identificatore del cluster, inserisci il nome che desideri assegnare al cluster Amazon DocumentDB clonato.

- b. Per la configurazione dell'istanza, seleziona una classe di istanza appropriata per il cluster Amazon DocumentDB clonato.

Create Clone

You are cloning a DocumentDB cluster. This will create a new DB cluster that includes all of the data from the existing database as well as a writer DB instance.

Settings

Source cluster identifier
docdb-2022-07-08-09-55-09

Cluster identifier
Specify a unique cluster identifier.

Instance configuration

Instance class

db.r6g.large
2 vCPUs 16GiB RAM

▼

- c. Per le impostazioni di rete, scegli un gruppo di sottoreti per il tuo caso d'uso e i gruppi di sicurezza VPC associati.
- d. Per Encryption-at-rest, se il cluster di origine (il cluster che viene clonato) ha la crittografia abilitata, anche il cluster clonato deve avere la crittografia abilitata. Se questo scenario è vero, le opzioni Abilita crittografia sono disattivate (disattivate) ma con l'opzione Abilita crittografia selezionata. Al contrario, se il cluster di origine non ha la crittografia abilitata, sono disponibili le opzioni Abilita crittografia ed è possibile scegliere di abilitare o disabilitare la crittografia.

Network settings

Subnet group
A subnet group is a collection of subnets that are within a VPC.

default ▼

VPC security groups
A security group acts as a virtual firewall for your instance to control inbound and outbound traffic.

Select VPC security groups ▼

default ✕

Encryption-at-rest

Enable encryption

Enable encryption
 Disable encryption

KMS key ID

(default) aws/rds ▼

Account
12345678910

KMS key ID
example-key-abcdef123

- e. Completa la nuova configurazione del clone del cluster selezionando il tipo di log da esportare (opzionale), inserendo una porta specifica utilizzata per la connessione al cluster e attivando la protezione dall'eliminazione accidentale del cluster (abilitata per impostazione predefinita).

Log exports

Select the log types to publish to Amazon CloudWatch Logs

Audit logs

Profiler logs

Cluster options

Port
TCP/IP port that is used to connect to the cluster.

Deletion protection

Enable deletion protection
Protects the cluster from being accidentally deleted. While this option is enabled, you can't delete the cluster.

Tags

No tags associated with the cluster.

You can add 50 more tags.

- f. Completa l'immissione di tutte le impostazioni per il clone del cluster Amazon DocumentDB. Per ulteriori informazioni sulle impostazioni di cluster e istanze di Amazon DocumentDB, consulta. [Gestione dei cluster Amazon DocumentDB](#)
5. Scegli Crea clone per avviare il clone Amazon DocumentDB del cluster Amazon DocumentDB scelto.

Quando il clone viene creato, viene elencato con gli altri cluster Amazon DocumentDB nella sezione Databases della console e mostra il suo stato corrente. Il clone è pronto per l'utilizzo quando lo stato diventa Disponibile.

Using the AWS CLI

L'utilizzo di AWS CLI per la clonazione del cluster Amazon DocumentDB richiede un paio di passaggi.

Il `restore-db-cluster-to-point-in-time` AWS CLI comando utilizzato genera un cluster Amazon DocumentDB vuoto con 0 istanze Amazon DocumentDB. Cioè, il comando ripristina solo il cluster Amazon DocumentDB, non le istanze DB per quel cluster. Sarà possibile farlo separatamente una volta che il clone è disponibile. Le due fasi del processo sono descritte di seguito:

1. Crea il clone utilizzando il comando [restore-db-cluster-to-point-in-time](#) CLI. I parametri utilizzati con questo comando controllano il tipo di capacità e altri dettagli del cluster Amazon DocumentDB vuoto (clone) che viene creato.
2. Crea l'istanza Amazon DocumentDB per il clone utilizzando il comando [create-db-instance](#) CLI per ricreare l'istanza Amazon DocumentDB nel cluster Amazon DocumentDB ripristinato.

I comandi seguenti presuppongono che AWS CLI sia impostato con la tua regione come impostazione predefinita. AWS Questo approccio ti evita di dover inviare il nome `--region` in ciascuno dei comandi. Per ulteriori informazioni, consultare la pagina relativa alla [configurazione di AWS CLI](#). È anche possibile specificare la `--region` in ciascuno dei comandi della CLI che seguono.

Creare il clone

I parametri specifici che vengono inviati al comando della CLI [restore-db-cluster-to-point-in-time](#) variano. Ciò che passi dipende dal tipo di clone che desideri creare.

Utilizza la seguente procedura per creare un clone Amazon DocumentDB fornito da un cluster Amazon DocumentDB fornito.

Per creare un clone della stessa modalità motore del cluster Amazon DocumentDB di origine

- Utilizzare il comando [restore-db-cluster-to-point-in-time](#) della CLI e specificare i valori per i seguenti parametri:

- `--db-cluster-identifier`: scegliere un nome significativo per il clone. Assegnate un nome al clone quando utilizzate il comando [restore-db-cluster-to-point-in-time](#) CLI.
- `--restore-type`: utilizza `copy-on-write` per creare un clone del cluster database di origine. Senza questo parametro, `restore-db-cluster-to-point-in-time` ripristina il cluster Amazon DocumentDB anziché creare un clone. L'impostazione predefinita per è `restore-type full-copy`
- `--source-db-cluster-identifier`— Usa il nome del cluster Amazon DocumentDB di origine che desideri clonare.
- `--use-latest-restorable-time`: questo valore punta ai dati del volume ripristinabile più recenti per il clone. Questo parametro è obbligatorio `restore-type copy-on-write`, tuttavia, non è possibile utilizzarlo `restore-to-time` parameter con esso.

Nell'esempio seguente viene creato un clone denominato `my-clone` da un cluster denominato `my-source-cluster`.

Per Linux, macOS o 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
```

Per 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
```

Il comando restituisce l'oggetto JSON contenente i dettagli del clone. Prima di provare a creare l'istanza database per il clone, verificare che il cluster database clonato sia disponibile. Per ulteriori informazioni, consulta [Verifica dello stato e acquisizione dei dettagli del clone](#) di seguito:

Verifica dello stato e ottenimento dei dettagli del clone

È possibile utilizzare il seguente comando per controllare lo stato del cluster database vuoto appena creato.

```
$ aws docdb describe-db-clusters --db-cluster-identifier my-clone --query '*[].[Status]' --output text
```

Oppure puoi ottenere lo stato e gli altri valori necessari per creare l'istanza DB per il tuo clone utilizzando la seguente query: AWS CLI

Per Linux, macOS o Unix:

```
aws docdb describe-db-clusters --db-cluster-identifier my-clone \  
  --query '*[].{Status:Status,Engine:Engine,EngineVersion:EngineVersion}'
```

Per Windows:

```
aws docdb describe-db-clusters --db-cluster-identifier my-clone ^  
  --query '*[].{Status:Status,Engine:Engine,EngineVersion:EngineVersion}'
```

Questa query restituisce un output simile al seguente:

```
[  
  {  
    "Status": "available",  
    "Engine": "docdb",  
    "EngineVersion": "4.0.0",  
  }  
]
```

Creazione dell'istanza Amazon DocumentDB per il tuo clone

Usa il comando [create-db-instance](#) CLI per creare l'istanza DB per il tuo clone.

Il `--db-instance-class` parametro viene utilizzato solo per i cluster Amazon DocumentDB forniti.

Per Linux, macOS o Unix:

```
aws docdb create-db-instance \  
  --db-instance-identifier my-new-db \  
  --db-cluster-identifier my-clone \  
  --db-instance-class db.r5.4xlarge \  
  --db-subnet-group my-subnet-group
```

```
--engine docdb
```

Per 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
```

Parametri da utilizzare per la clonazione

La tabella seguente riassume i vari parametri utilizzati per `restore-db-cluster-to-point-in-time` clonare i cluster Amazon DocumentDB.

Parametro	Descrizione
<code>--source-db-cluster-identifier</code>	Usa il nome del cluster Amazon DocumentDB di origine che desideri clonare.
<code>--db-cluster-identifier</code>	Scegliere un nome significativo per il clone. È possibile assegnare un nome al clone con il comando <code>restore-db-cluster-to-point-in-time</code> . Quindi questo nome viene inviato al comando <code>create-db-instance</code> .
<code>--restore-type</code>	<code>--restore-type</code> Specificare <code>copy-on-write</code> come creare un clone del cluster DB di origine anziché ripristinare il cluster Amazon DocumentDB di origine.
<code>--use-latest-restorable-time</code>	Questo valore punta ai dati del volume ripristinabile più recenti per il clone.

Comprendere la tolleranza agli errori del cluster Amazon DocumentDB

I cluster Amazon DocumentDB sono progettati per essere tolleranti ai guasti. Il volume di ogni cluster si estende su più zone di disponibilità in un'unica Regione AWS zona e ogni zona di disponibilità contiene una copia dei dati del volume del cluster. Questa funzionalità consente al cluster di tollerare il guasto di una zona di disponibilità senza perdita di dati e con solo una breve interruzione del servizio.

Se l'istanza primaria di un cluster si guasta, Amazon DocumentDB esegue automaticamente un failover su una nuova istanza primaria in due modi:

- Promuovendo una replica Amazon DocumentDB esistente sulla nuova istanza principale scelta in base all'impostazione del livello di promozione di ciascuna replica e quindi creando una replica sostitutiva per la precedente principale. Un failover sull'istanza di replica richiede in genere meno di 30 secondi. Le operazioni di lettura e scrittura potrebbero subire brevi interruzioni durante questo periodo. Per aumentare la disponibilità del cluster, ti consigliamo di creare almeno una o più repliche di Amazon DocumentDB in due o più zone di disponibilità diverse.
- Creando una nuova istanza primaria. Ciò accade solo se non disponi di un'istanza di replica nel cluster e il completamento può richiedere alcuni minuti.

Se il cluster dispone di una o più repliche di Amazon DocumentDB, una replica di Amazon DocumentDB viene promossa all'istanza principale durante un evento di errore. Un evento di errore ha come conseguenza una breve interruzione, durante la quale le operazioni di lettura e scrittura inviate all'istanza primaria falliscono con un'eccezione. Tuttavia, il servizio viene in genere ripristinato in meno di 120 secondi e spesso in meno di 60 secondi. Per aumentare la disponibilità del cluster, ti consigliamo di creare almeno una o più repliche di Amazon DocumentDB in due o più zone di disponibilità diverse.

È possibile personalizzare l'ordine in cui le repliche di Amazon DocumentDB vengono promosse all'istanza principale dopo un errore assegnando a ciascuna replica una priorità. Le priorità vanno da 0, quella massima, a 15, quella minima. Se l'istanza primaria fallisce, la replica di Amazon DocumentDB con la priorità più alta viene promossa alla nuova istanza primaria. Puoi modificare la priorità di una replica di Amazon DocumentDB in qualsiasi momento. Modificando una priorità non attiverai un failover. Puoi utilizzare l'operazione `modify-db-instance` con il parametro `--promotion-tier`. Per ulteriori informazioni sulla personalizzazione della priorità di failover di un'istanza, consulta [Failover di Amazon DocumentDB](#).

Più di una replica di Amazon DocumentDB può condividere la stessa priorità, con conseguenti livelli di promozione. Se due o più repliche di Amazon DocumentDB condividono la stessa priorità, la replica di dimensioni maggiori viene promossa a principale. Se due o più repliche di Amazon DocumentDB condividono la stessa priorità e dimensione, viene promossa una replica arbitraria nello stesso livello di promozione.

Se il cluster non contiene repliche di Amazon DocumentDB, l'istanza principale viene ricreata durante un evento di errore. Un evento di errore ha come conseguenza un'interruzione, durante la quale le operazioni di lettura e scrittura falliscono con un'eccezione. Il servizio viene ripristinato quando crei

la nuova istanza primaria. In genere, ciò richiede meno di 10 minuti. La promozione di una replica di Amazon DocumentDB sull'istanza principale è molto più rapida rispetto alla creazione di una nuova istanza primaria.

Gestione delle istanze di Amazon DocumentDB

I seguenti argomenti forniscono informazioni per aiutarti a gestire le istanze di Amazon DocumentDB. Includono dettagli sulle classi e gli stati delle istanze e su come creare, eliminare e modificare un'istanza.

Argomenti

- [Gestione delle classi delle istanze](#)
- [Determinazione dello stato di un'istanza](#)
- [Ciclo di vita delle istanze Amazon DocumentDB](#)

Gestione delle classi delle istanze

La classe di istanza determina la capacità di calcolo e memoria di un'istanza Amazon DocumentDB (con compatibilità con MongoDB). La classe di istanza di cui hai bisogno dipende dai requisiti in termini di potenza di elaborazione e memoria.

Amazon DocumentDB supporta le famiglie di classi di istanze R4, R5, R6G, T3 e T4G. ovvero classi di istanze della generazione attuale ottimizzate per applicazioni a elevato utilizzo di memoria. Per le specifiche relative a tali classi, consulta [Specifiche per la classe di istanza](#).

Argomenti

- [Determinare una classe di istanza](#)
- [Modifica della classe di un'istanza](#)
- [Classi di istanze supportate per regione](#)
- [Specifiche per la classe di istanza](#)

Determinare una classe di istanza

Per determinare la classe di un'istanza, è possibile utilizzare l'`describe-db-instances` AWS CLI operazione AWS Management Console o.

Using the AWS Management Console

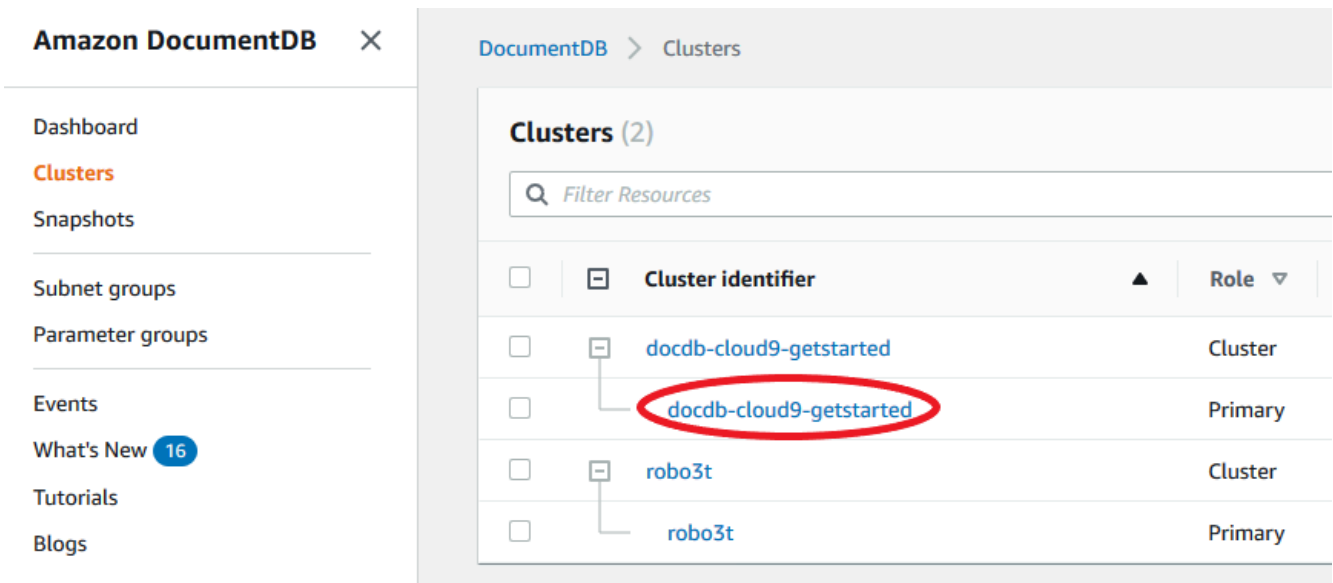
Per determinare la classe di istanza per le istanze del cluster, completa i seguenti passaggi nella console.

1. [Accedi a e apri AWS Management Console la console Amazon DocumentDB all'indirizzo `https://console.aws.amazon.com/docdb`.](https://console.aws.amazon.com/docdb)
2. Nel pannello di navigazione, scegli Clusters per trovare l'istanza che ti interessa.

Tip

Se il riquadro di navigazione non viene visualizzato sul lato sinistro della schermata, scegliere l'icona del menu (☰) nell'angolo in alto a sinistra della pagina.

3. Nella casella di navigazione Clusters, vedrai la colonna Cluster Identifier. Le tue istanze sono elencate in cluster, in modo simile alla schermata seguente.



<input type="checkbox"/>	<input type="checkbox"/>	Cluster identifier	Role
<input type="checkbox"/>	<input type="checkbox"/>	docdb-cloud9-getstarted	Cluster
<input type="checkbox"/>	<input type="checkbox"/>	docdb-cloud9-getstarted	Primary
<input type="checkbox"/>	<input type="checkbox"/>	robo3t	Cluster
<input type="checkbox"/>	<input type="checkbox"/>	robo3t	Primary

4. Nell'elenco delle istanze, espandi il cluster per trovare le istanze che ti interessano. Trova l'istanza che desideri. Quindi, guarda la colonna Size della riga dell'istanza per vedere la sua classe di istanza.

Nell'immagine seguente, la classe per l'istanza robo3t è `db.r5.4xlarge`.

DocumentDB > Clusters

Clusters (2) Group Resources Actions Create

Filter Resources

Cluster identifier	Role	Engine version	Region & AZ	Status	Size	Maintenance
docdb-cloud9-getstarted	Cluster	3.6.0	us-east-1	available	1 Instance	None
docdb-cloud9-getstarted	Primary	3.6.0	us-east-1f	available	db.r5.large	None
robo3t	Cluster	3.6.0	us-east-1	available	1 Instance	None
robo3t	Primary	3.6.0	us-east-1d	available	db.r5.large	None

Using the AWS CLI

Per determinare la classe di un'istanza utilizzando il AWS CLI, utilizzate l'`describe-db-instances` operazione con i seguenti parametri.

- **--db-instance-identifier**— Facoltativo. Specifica l'istanza della quale desideri trovare la classe. Se questo parametro viene omesso, `describe-db-instances` restituisce una descrizione per un massimo di 100 istanze.
- **--query**— Facoltativo. Specifica i membri dell'istanza da includere nei risultati. Se questo parametro viene omesso, vengono restituiti tutti i membri dell'istanza.

Example

L'esempio seguente trova il nome e la classe dell'istanza `sample-instance-1`.

Per Linux, macOS o Unix:

```
aws docdb describe-db-instances \
  --query 'DBInstances[*].[DBInstanceIdentifier,DBInstanceClass]' \
  --db-instance-identifier sample-instance-1
```

Per Windows:

```
aws docdb describe-db-instances ^
  --query 'DBInstances[*].[DBInstanceIdentifier,DBInstanceClass]' ^
  --db-instance-identifier sample-instance-1
```

L'aspetto dell'output di questa operazione è simile al seguente.

```
[
  [
    "sample-instance-1",
    "db.r5.large"
  ]
]
```

Example

L'esempio seguente trova il nome e la classe dell'istanza per un massimo di 100 istanze di Amazon DocumentDB.

Per Linux, macOS o Unix:

```
aws docdb describe-db-instances \
  --query 'DBInstances[*].[DBInstanceIdentifier,DBInstanceClass]' \
  --filter Name=engine,Values=docdb
```

Per Windows:

```
aws docdb describe-db-instances ^
  --query 'DBInstances[*].[DBInstanceIdentifier,DBInstanceClass]' ^
  --filter Name=engine,Values=docdb
```

L'aspetto dell'output di questa operazione è simile al seguente.

```
[
  [
    "sample-instance-1",
    "db.r5.large"
  ],
  [
    "sample-instance-2",
    "db.r5.large"
  ],
  [
    "sample-instance-3",
    "db.r5.4xlarge"
  ],
  [
    "sample-instance-4",
    "db.r5.4xlarge"
  ]
]
```

```
] ]
```

Per ulteriori informazioni, consulta [Descrizione delle istanze di Amazon DocumentDB](#).

Modifica della classe di un'istanza

Puoi modificare la classe dell'istanza utilizzando AWS Management Console o il AWS CLI Per ulteriori informazioni, consulta [Modifica di un'istanza Amazon DocumentDB](#).

Classi di istanze supportate per regione

Amazon DocumentDB supporta le seguenti classi di istanze:

- R6G—Istanze ottimizzate per la memoria di ultima generazione basate su processori AWS Graviton2 basati su ARM che offrono prestazioni fino al 30% migliori rispetto alle istanze R5 a un costo inferiore del 5%.
- R5—Istanze ottimizzate per la memoria che offrono prestazioni fino al 100% migliori rispetto alle istanze R4 allo stesso costo di istanza.
- R4—Generazione precedente di istanze ottimizzate per la memoria.
- T4G—Tipo di istanza generica, sostenibile e a basso costo di ultima generazione, alimentata da processori AWS Graviton2 basati su ARM che fornisce un livello base di prestazioni della CPU, offre un rapporto prezzo/prestazioni fino al 35% migliore rispetto alle istanze T3 ed è ideale per l'esecuzione di applicazioni con un utilizzo moderato della CPU che presentano picchi temporanei di utilizzo.
- T3—Tipo di istanza generica espandibile a basso costo che fornisce un livello base di prestazioni della CPU con la possibilità di aumentare l'utilizzo della CPU in qualsiasi momento per tutto il tempo necessario.

Per specifiche dettagliate relative alle classi di istanze, consulta [Specifiche per la classe di istanza](#).

Una particolare classe di istanza può essere supportata o meno in una determinata regione. La tabella seguente specifica quali classi di istanze sono supportate da Amazon DocumentDB in ciascuna regione.

Classi di istanze supportate per regione

Regione	R6G	R5	R4	T4G	T3
Stati Uniti orientali (Ohio)	Supportato	Supportato	Supportato	Supportato	Supportato
Stati Uniti orientali (Virginia settentrionale)	Supportato	Supportato	Supportato	Supportato	Supportato
US West (Oregon)	Supportato	Supportato	Supportato	Supportato	Supportato
Sud America (San Paolo)	Supportato	Supportato		Supportato	Supportato
Asia Pacifico (Hong Kong)	Supportato	Supportato		Supportato	Supportato
Asia Pacifico (Hyderabad)		Supportato			Supportato
Asia Pacifico (Mumbai)	Supportato	Supportato		Supportato	Supportato
Asia Pacifico (Seul)	Supportato	Supportato		Supportato	Supportato
Asia Pacifico (Sydney)	Supportato	Supportato		Supportato	Supportato
Asia Pacifico (Singapore)	Supportato	Supportato		Supportato	Supportato
Asia Pacifico (Tokyo)	Supportato	Supportato		Supportato	Supportato

Regione	R6G	R5	R4	T4G	T3
Canada (Centrale)	Supportato	Supportato		Supportato	Supportato
Europa (Francoforte)	Supportato	Supportato		Supportato	Supportato
Europa (Irlanda)	Supportato	Supportato	Supportato	Supportato	Supportato
Europa (Londra)	Supportato	Supportato		Supportato	Supportato
Europa (Milano)	Supportato	Supportato		Supportato	Supportato
Europa (Parigi)	Supportato	Supportato		Supportato	Supportato
Medio Oriente (Emirati Arabi Uniti)	Supportato	Supportato		Supportato	Supportato
Regione Cina (Pechino)	Supportato	Supportato		Supportato	Supportato
Cina (Ningxia)	Supportato	Supportato		Supportato	Supportato
AWS GovCloud (Stati Uniti occidentali)	Supportato	Supportato		Supportato	Supportato
AWS GovCloud (Stati Uniti orientali)	Supportato	Supportato		Supportato	Supportato

Specifiche per la classe di istanza

La tabella seguente fornisce dettagli sulle classi di istanze di Amazon DocumentDB. Puoi trovare spiegazioni su ogni colonna della tabella nella sezione sotto la tabella.

Classi di istanze Amazon DocumentDB supportate

Classe di istanza	vCPU ¹	Memoria (GiB) 2	Temperatura massima di archiviazione (GiB) ³	Larghezza di banda massima (Mbps) ⁴	Prestazioni di rete ⁵	Motori di supporto ⁶
-------------------	-------------------	--------------------	---	--	----------------------------------	---------------------------------

R6G — Classe di istanza ottimizzata per la memoria di attuale generazione basata su Graviton2

db.r6g.large	2	16	32	Fino a 4.750	Fino a 10 Gb/s	4.0.0 e 5.0.0
db.r6g.xlarge	4	32	63	Fino a 4.750	Fino a 10 Gb/s	4.0.0 e 5.0.0
db.r6g.2xlarge	8	64	126	Fino a 4.750	Fino a 10 Gb/s	4.0.0 e 5.0.0
db.r6g.4xlarge	16	128	252	4.750	Fino a 10 Gb/s	4.0.0 e 5.0.0
db.r6g.8xlarge	32	256	504	9.000	12 GBps	4.0.0 e 5.0.0
db.r6g.12xlarge	48	384	756	13.500	20 Gb/s	4.0.0 e 5.0.0
db.r6g.16xlarge	64	512	1008	19.000	25 Gb/s	4.0.0 e 5.0.0

R5 — Classe di istanza ottimizzata per la memoria della generazione precedente

db.r5.large	2	16	31	Fino a 3.500	Fino a 10 Gb/s	3.6.0, 4.0.0 e 5.0.0
-------------	---	----	----	--------------	----------------	----------------------

Classe di istanza	vCPU ¹	Memoria (GiB) 2	Temperatura massima di archiviazione (GiB) ³	Larghezza di banda massima (Mbps) ⁴	Prestazioni di rete ⁵	Motori di supporto ⁶
db.r5.xlarge	4	32	62	Fino a 3.500	Fino a 10 Gb/s	3.6.0, 4.0.0 e 5.0.0
db.r5.2xlarge	8	64	124	Fino a 3.500	Fino a 10 Gb/s	3.6.0, 4.0.0 e 5.0.0
db.r5.4xlarge	16	128	249	3,500	Fino a 10 Gb/s	3.6.0, 4.0.0 e 5.0.0
db.r5.8xlarge	32	256	504	6.800	10 Gb/s	3.6.0, 4.0.0 e 5.0.0
db.r5.12xlarge	48	384	748	7,000	10 Gb/s	3.6.0, 4.0.0 e 5.0.0
db.r5.16xlarge	64	512	1008	13.600	20 Gb/s	3.6.0, 4.0.0 e 5.0.0
db.r5.24xlarge	96	768	1500	14.000	25 Gb/s	3.6.0, 4.0.0 e 5.0.0
R4 — Classe di istanza ottimizzata per la memoria della generazione precedente						
db.r4.large	2	15,25	30	437	Fino a 10 Gb/s	Solo 3.6.0
db.r4.xlarge	4	30,5	60	875	Fino a 10 Gb/s	solo 3.6.0
db.r4.2xlarge	8	61	120	875	Fino a 10 Gb/s	solo 3.6.0
db.r4.4xlarge	16	122	240	875	Fino a 10 Gb/s	solo 3.6.0

Classe di istanza	vCPU ¹	Memoria (GiB) ²	Temperatura massima di archiviazione (GiB) ³	Larghezza di banda massima (Mbps) ⁴	Prestazioni di rete ⁵	Motori di supporto ⁶
db.r4.8xlarge	32	244	480	875	10 Gb/s	solo 3.6.0
db.r4.16xlarge	64	488	960	14.000	25 Gb/s	solo 3.6.0

T4G: classi di istanze Burstable Performance di ultima generazione basate su Graviton2

db.t4g.medium	2	4	8.13	Fino a 2.085	Fino a 5 Gb/s	4.0.0 e 5.0.0
---------------	---	---	------	--------------	---------------	---------------

T3 — Classi di istanze Burstable Performance della generazione precedente

db.t3.medium	2	4	7.5	Fino a 1.536	Fino a 5 Gb/s	3.6.0, 4.0.0 e 5.0.0
--------------	---	---	-----	--------------	---------------	----------------------

1. vCPU: il numero di unità di elaborazione centrale virtuali (CPU). Una CPU virtuale è un'unità di capacità che puoi utilizzare per confrontare le classi di istanza. Invece di acquistare o affittare un determinato processore da utilizzare per vari mesi o anni, si affitta la capacità su base oraria. Il nostro obiettivo è fornire una quantità coerente di capacità di CPU, indipendentemente dall'hardware reale alla base.
2. Memoria (GiB): la RAM, in gigabyte, allocata all'istanza. Spesso c'è un rapporto costante tra memoria e vCPU.
3. Max. temp. storage (GiB): la RAM, in gigabyte, che viene allocata all'istanza per l'archiviazione temporanea non persistente dei file.
4. Larghezza di banda massima (Mbps): la larghezza di banda massima in megabit al secondo. Dividendo il valore per 8, puoi ottenere il throughput previsto in megabyte al secondo.
5. Prestazioni di rete: la velocità della rete rispetto ad altre classi di istanze.
6. Motori di supporto: i motori di Amazon DocumentDB che supportano la classe di istanze.

Determinazione dello stato di un'istanza

Per visualizzare gli stati validi di un'istanza, il loro significato e come determinare lo stato delle istanze, consulta [Monitoraggio dello stato di un'istanza Amazon DocumentDB](#).

Ciclo di vita delle istanze Amazon DocumentDB

Il ciclo di vita di un'istanza Amazon DocumentDB include la creazione, la modifica, la manutenzione e l'aggiornamento, l'esecuzione di backup e ripristini, il riavvio e l'eliminazione dell'istanza. Questa sezione fornisce informazioni su come completare questi processi.

Argomenti

- [Aggiungere un'istanza Amazon DocumentDB a un cluster](#)
- [Descrizione delle istanze di Amazon DocumentDB](#)
- [Modifica di un'istanza Amazon DocumentDB](#)
- [Riavvio di un'istanza Amazon DocumentDB](#)
- [Eliminazione di un'istanza Amazon DocumentDB](#)

Puoi creare una nuova istanza di Amazon DocumentDB utilizzando AWS Management Console o il CLI. Per aggiungere un'istanza a un cluster, il cluster deve essere nello stato disponibile. Non è possibile aggiungere un'istanza a un cluster arrestato. Se il cluster viene arrestato, per prima cosa avviare il cluster, attendere che diventi disponibile, quindi aggiungere un'istanza. Per ulteriori informazioni, consulta [Arresto e avvio di un cluster Amazon DocumentDB](#).

Note

Se crei un cluster Amazon DocumentDB utilizzando la console, contemporaneamente viene creata automaticamente un'istanza per te. Per creare altre istanze, utilizza una delle procedure riportate di seguito.

Aggiungere un'istanza Amazon DocumentDB a un cluster

Using the AWS Management Console

Utilizza la seguente procedura per creare un'istanza per il tuo cluster utilizzando la console Amazon DocumentDB.

1. [Accedi a e apri AWS Management Console la console Amazon DocumentDB all'indirizzo https://console.aws.amazon.com/docdb](https://console.aws.amazon.com/docdb).
2. Nel pannello di navigazione scegliere Clusters (Cluster).

 Tip

Se il riquadro di navigazione non viene visualizzato sul lato sinistro della schermata, scegliere l'icona del menu (☰) nell'angolo in alto a sinistra della pagina.

3. Per scegliere il cluster a cui aggiungere un'istanza, seleziona il pulsante a sinistra del nome del cluster.
4. Scegli Actions (Operazioni), quindi Add instance (Aggiungi istanza).
5. Nella pagina Add instance to: (Aggiungi istanza a:)<cluster-name> ripetere i seguenti passaggi per ogni istanza che si desidera aggiungere al cluster. Puoi averne fino a 15.
 - a. Identificatore dell'istanza: puoi inserire un identificatore univoco per questa istanza o consentire ad Amazon DocumentDB di fornire l'identificatore dell'istanza basato sull'identificatore del cluster.

Vincoli per la denominazione di un'istanza:

- La lunghezza è di [1—63] lettere, numeri o trattini.
 - Il primo carattere deve essere una lettera.
 - Non può terminare con un trattino o contenere due trattini consecutivi.
 - Deve essere unico per tutte le istanze in Amazon RDS, Neptune e Amazon DocumentDB per regione. Account AWS
- b. Classe di istanza: dall'elenco a discesa, scegli il tipo di istanza che desideri per questa istanza.
 - c. Livello di promozione: dall'elenco a discesa, scegli il livello di promozione per la tua istanza o scegli Nessuna preferenza per consentire ad Amazon DocumentDB di impostare il livello di promozione per la tua istanza. Un numero minore indica una priorità più elevata. Per ulteriori informazioni, consulta [Controllo della destinazione di failover](#).
 - d. Per aggiungere ulteriori istanze, scegliere Add additional instances (Aggiungi istanze aggiuntive) e ripetere i passaggi a, b e c.

6. Terminare l'operazione.

- Per aggiungere istanze al cluster, scegliere Crea.
- Per annullare l'operazione, scegli Cancel (Annulla).

La creazione dell'istanza richiede diversi minuti. Puoi usare la console o AWS CLI visualizzare lo stato dell'istanza. Per ulteriori informazioni, consulta [Monitoraggio dello stato di un'istanza](#).

Using the AWS CLI

Utilizza l'`create-db-instance` AWS CLI operazione con i seguenti parametri per creare l'istanza principale per il tuo cluster.

- **--db-instance-class**: obbligatorio. La capacità di calcolo e di memoria dell'istanza, ad esempio `db.m4.large`. Non tutte le classi di istanze sono disponibili in tutte Regioni AWS.
- **--db-instance-identifier**: obbligatorio. Una stringa di lettere minuscole che identifica l'istanza.

Vincoli per la denominazione di un'istanza:

- La lunghezza è di [1—63] lettere, numeri o trattini.
- Il primo carattere deve essere una lettera.
- Non può terminare con un trattino o contenere due trattini consecutivi.
- Deve essere unico per tutte le istanze in Amazon RDS, Neptune e Amazon DocumentDB per regione. Account AWS
- **--engine**: obbligatorio. Deve essere `docdb`.
- **--availability-zone**— Facoltativo. La zona di disponibilità in cui verrà creata l'istanza. Utilizza questo parametro per trovare le istanze in diverse zone di disponibilità per aumentare la tolleranza ai guasti. Per ulteriori informazioni, consulta [Amazon DocumentDB](#).
- **--promotion-tier**— Facoltativo. Il livello di priorità di failover per l'istanza. Il valore deve essere compreso tra 0 e 15 con i numeri più bassi che corrispondono a una priorità maggiore. Per ulteriori informazioni, consulta [Controllo della destinazione di failover](#).

1. Innanzitutto, determina in quali zone di disponibilità puoi creare l'istanza.

Se desideri specificare la zona di disponibilità prima di creare l'istanza, esegui il comando seguente per determinare quali zone di disponibilità sono disponibili per il tuo cluster Amazon DocumentDB.

Per Linux, macOS o Unix:

```
aws docdb describe-db-clusters \  
  --query 'DBClusters[*].[DBClusterIdentifier,AvailabilityZones[*]]'
```

Per Windows:

```
aws docdb describe-db-clusters ^\  
  --query 'DBClusters[*].[DBClusterIdentifier,AvailabilityZones[*]]'
```

L'aspetto dell'output di questa operazione è simile al seguente.

```
[  
  [  
    "sample-cluster",  
    [  
      "us-east-1c",  
      "us-east-1b",  
      "us-east-1a"  
    ]  
  ]  
]
```

2. In secondo luogo, determina quali classi di istanza puoi creare nella regione.

Per determinare le classi di istanze disponibili nella tua regione, esegui il comando seguente. Dall'output, scegli una classe di istanza per l'istanza che desideri aggiungere al tuo cluster Amazon DocumentDB.

Per Linux, macOS o Unix:

```
aws docdb describe-orderable-db-instance-options \  
  --engine docdb \  
  --query 'OrderableDBInstanceOptions[*].DBInstanceClass'
```

Per Windows:

```
aws docdb describe-orderable-db-instance-options ^\  
  --engine docdb ^
```

```
--query 'OrderableDBInstanceOptions[*].DBInstanceClass'
```

L'aspetto dell'output di questa operazione è simile al seguente.

```
[
  "db.r5.16xlarge",
  "db.r5.2xlarge",
  "db.r5.4xlarge",
  "db.r5.8xlarge",
  "db.r5.large",
  "db.r5.xlarge"
]
```

3. Infine, aggiungi un'istanza al tuo cluster Amazon DocumentDB.

Per aggiungere un'istanza al tuo cluster Amazon DocumentDB, esegui il comando seguente.

Per Linux, macOS o 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
```

Per 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
```

L'aspetto dell'output di questa operazione è simile al seguente.

```
{
  "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"
}
}
```

La creazione dell'istanza richiede diversi minuti. Puoi usare la console o AWS CLI visualizzare lo stato dell'istanza. Per ulteriori informazioni, consulta [Monitoraggio dello stato di un'istanza Amazon DocumentDB](#).

Descrizione delle istanze di Amazon DocumentDB

Puoi utilizzare la console di gestione di Amazon DocumentDB o visualizzare dettagli come endpoint di connessione, gruppi di sicurezza VPC, autorità di certificazione e gruppi di parametri relativi alle tue istanze di Amazon DocumentDB. AWS CLI

Using the AWS Management Console

Per visualizzare i dettagli delle istanze utilizzando la AWS Management Console, segui la procedura riportata di seguito.

1. [Accedi a e apri AWS Management Console la console Amazon DocumentDB all'indirizzo https://console.aws.amazon.com/docdb](https://console.aws.amazon.com/docdb).
2. Nel pannello di navigazione scegliere Clusters (Cluster).

Tip

Se il riquadro di navigazione non viene visualizzato sul lato sinistro della schermata, scegliere l'icona del menu (☰) nell'angolo in alto a sinistra della pagina.

3. Nella casella di navigazione Clusters, vedrai la colonna Cluster Identifier. Le tue istanze sono elencate in cluster, in modo simile alla schermata seguente.

The screenshot shows the Amazon DocumentDB console interface. On the left is a navigation menu with options: Dashboard, Clusters (highlighted), Snapshots, Subnet groups, Parameter groups, Events, What's New (16), Tutorials, and Blogs. The main content area is titled 'DocumentDB > Clusters' and shows a list of clusters under the heading 'Clusters (2)'. There is a search bar labeled 'Filter Resources'. The list has columns for 'Cluster identifier' and 'Role'. The following table represents the data shown in the screenshot:

<input type="checkbox"/>	<input type="checkbox"/>	Cluster identifier	Role
<input type="checkbox"/>	<input type="checkbox"/>	docdb-cloud9-getstarted	Cluster
<input type="checkbox"/>	<input type="checkbox"/>	docdb-cloud9-getstarted	Primary
<input type="checkbox"/>	<input type="checkbox"/>	robo3t	Cluster
<input type="checkbox"/>	<input type="checkbox"/>	robo3t	Primary

4. Nell'elenco delle istanze, scegli il nome dell'istanza di cui desideri visualizzarne i dettagli. Le informazioni sull'istanza sono organizzate nei seguenti raggruppamenti:
- Riepilogo: informazioni generali sull'istanza, tra cui la versione del motore, la classe, lo stato e qualsiasi manutenzione in sospeso.
 - Connettività e sicurezza: la sezione Connect elenca gli endpoint di connessione per connettersi a questa istanza con la shell mongo o con un'applicazione. Nella sezione Security Groups (Gruppi di sicurezza) sono elencati i gruppi di sicurezza associati a questa istanza, l'ID VPC e le descrizioni.
 - Configurazione: la sezione Dettagli elenca le configurazioni e lo stato dell'istanza, inclusi l'Amazon Resource Name (ARN), l'endpoint, il ruolo, la classe e l'autorità di certificazione dell'istanza. Vengono inoltre elencate le impostazioni di sicurezza e di rete dell'istanza e le informazioni di backup. La sezione Cluster details (Dettagli cluster) elenca i dettagli del cluster a cui appartiene questa istanza. La sezione Istanze del cluster elenca tutte le istanze che appartengono al cluster con lo stato del ruolo e del gruppo di parametri del cluster di ogni istanza.

Note

Puoi modificare il cluster associato all'istanza selezionando **Modify** (Modifica) accanto all'istanza **Cluster details** (Dettagli cluster). Per ulteriori informazioni, consulta [Modifica di un cluster Amazon DocumentDB](#).

- **Monitoraggio:** i parametri dei CloudWatch log per questa istanza. Per ulteriori informazioni, consulta [Monitoraggio di Amazon DocumentDB con CloudWatch](#).
- **Eventi e tag:** la sezione Eventi recenti elenca gli eventi recenti per questa istanza. Amazon DocumentDB registra gli eventi relativi a cluster, istanze, snapshot, gruppi di sicurezza e gruppi di parametri del cluster. Queste informazioni includono la data, l'ora e il messaggio associati a ciascun evento. La sezione Tag elenca i tag allegati al cluster. Per ulteriori informazioni, consulta [Etichettatura delle risorse Amazon DocumentDB](#).

Using the AWS CLI

Per visualizzare i dettagli delle tue istanze di Amazon DocumentDB utilizzando il AWS CLI, usa il `describe-db-clusters` comando come mostrato negli esempi seguenti. Per ulteriori informazioni, consulta [DescribeDBInstances](#) Amazon DocumentDB Resource Management API Reference.

Note

Per alcune funzionalità di gestione come la gestione del ciclo di vita di cluster e istanze, Amazon DocumentDB sfrutta la tecnologia operativa condivisa con Amazon RDS. Il parametro `filterName=engine,Values=docdb` filter restituisce solo cluster Amazon DocumentDB.

1. Elenca tutte le istanze di Amazon DocumentDB.

Il AWS CLI codice seguente elenca i dettagli per tutte le istanze di Amazon DocumentDB in una regione.

Per Linux, macOS o Unix:

```
aws docdb describe-db-instances \  
  --filter Name=engine,Values=docdb
```

Per Windows:

```
aws docdb describe-db-instances \  
  --filter Name=engine,Values=docdb
```

2. Elenca tutti i dettagli per un'istanza Amazon DocumentDB specificata

Il codice seguente consente di elencare i dettagli per `sample-cluster-instance`. Se includi il parametro `--db-instance-identifier` nel nome di un'istanza, puoi limitare l'output alle sole informazioni su quella specifica istanza.

Per Linux, macOS o Unix:

```
aws docdb describe-db-instances \  
  --db-instance-identifier sample-cluster-instance
```

Per Windows:

```
aws docdb describe-db-instances \  
  --db-instance-identifier sample-cluster-instance
```

L'aspetto dell'output di questa operazione è simile al seguente.

```
{  
  "DBInstances": [  
    {  
      "DbiResourceId": "db-BJKKB54PIDV5QFKGV5T3S6GM",  
      "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"
}
]
```

Modifica di un'istanza Amazon DocumentDB

Puoi modificare la tua istanza di Amazon DocumentDB utilizzando AWS Management Console o AWS CLI. Per modificare un'istanza, questa deve essere nello stato disponibile. Non è possibile modificare un'istanza arrestata. Se il cluster viene arrestato, per prima cosa avviare il cluster, attendere che l'istanza diventi disponibile, quindi apportare le modifiche desiderate. Per ulteriori informazioni, consulta [Arresto e avvio di un cluster Amazon DocumentDB](#).

Using the AWS Management Console

Per modificare un'istanza specifica di Amazon DocumentDB utilizzando la console, completa i seguenti passaggi.

1. [Accedi a e apri AWS Management Console la console Amazon DocumentDB all'indirizzo https://console.aws.amazon.com/docdb](https://console.aws.amazon.com/docdb).
2. Nel pannello di navigazione scegliere Clusters (Cluster).

Tip

Se il riquadro di navigazione non viene visualizzato sul lato sinistro della schermata, scegliere l'icona del menu

(≡

nell'angolo in alto a sinistra della pagina.

)

- Nella casella di navigazione Clusters, vedrai la colonna Cluster Identifier. Le tue istanze sono elencate in cluster, in modo simile alla schermata seguente.

- Seleziona la casella a sinistra dell'istanza che desideri modificare.
- Scegli Actions (Operazioni), quindi Modify (Modifica).
- Nel riquadro Modify instance: <instance-name>(Modifica istanza: instance-name) apporta le modifiche desiderate. È possibile apportare le seguenti modifiche.
 - Specifiche dell'istanza: l'identificatore e la classe dell'istanza. Vincoli di denominazione dell'identificatore di istanza:
 - Identificatore dell'istanza: inserisci un nome univoco per tutte le istanze di tua proprietà Account AWS nell'area corrente. L'identificatore di istanza deve contenere [1–63] caratteri alfanumerici o trattini, avere una lettera come primo carattere e non può terminare con un trattino o contenere due trattini consecutivi.
 - Classe di istanza: dal menu a discesa, seleziona una classe di istanza per la tua istanza Amazon DocumentDB. Per ulteriori informazioni, consulta [Gestione delle classi delle istanze](#).
 - Autorità di certificazione: certificato del server per questa istanza. Per ulteriori informazioni, consulta [Aggiornamento dei certificati TLS di Amazon DocumentDB](#).
 - Failover: durante il failover, l'istanza con il livello di promozione più alto verrà promossa a principale. Per ulteriori informazioni, consulta [Failover di Amazon DocumentDB](#).

- **Manutenzione:** la finestra di manutenzione in cui le modifiche o le patch in sospeso vengono applicate alle istanze del cluster.
7. Al termine, scegli Continue (Continua) per visualizzare un riepilogo delle modifiche.
 8. Dopo aver verificato le modifiche, è possibile applicarle immediatamente o durante la successiva finestra di manutenzione in Scheduling of modifications (Pianificazione delle modifiche). Scegli Instance (Modifica istanza) per salvare le modifiche. In alternativa, puoi selezionare Cancel (Annulla) per eliminare le modifiche.

L'applicazione delle modifiche richiede qualche minuto. Puoi utilizzare l'istanza solo quando ha lo stato disponibile. Puoi monitorare lo stato dell'istanza con la console o l' AWS CLI. Per ulteriori informazioni, consulta [Monitoraggio dello stato di un'istanza Amazon DocumentDB](#).

Using the AWS CLI

Per modificare un'istanza specifica di Amazon DocumentDB utilizzando il AWS CLI, utilizza `modify-db-instance` i seguenti parametri. Per ulteriori informazioni, vedete [ModifyDbInstance](#). Il codice seguente modifica la classe di istanza in `db.r5.large` per l'istanza `sample-instance`.

Parametri

- **--db-instance-identifier:** obbligatorio. L'identificatore dell'istanza da modificare.
- **--db-instance-class**— Facoltativo. La nuova capacità di calcolo e memoria dell'istanza, `db.r5.large` ad esempio. Non tutte le classi di istanze sono disponibili in tutte Regioni AWS. Se si modifica la classe dell'istanza, si verifica un'interruzione durante la modifica. La modifica viene applicata durante la finestra di manutenzione successiva, a meno che non `ApplyImmediately` sia specificata come `true` per questa richiesta.
- **--apply-immediately** o **--no-apply-immediately** — Facoltativo. Specifica se questa modifica debba essere applicata subito o alla prossima finestra di manutenzione. Se questo parametro viene omissso, la modifica viene eseguita durante la finestra di manutenzione successiva.

Example

Per Linux, macOS o Unix:

```
aws docdb modify-db-instance \
```

```
--db-instance-identifier sample-instance \  
--db-instance-class db.r5.large \  
--apply-immediately
```

Per Windows:

```
aws docdb modify-db-instance ^  
  --db-instance-identifier sample-instance ^  
  --db-instance-class db.r5.large ^  
  --apply-immediately
```

L'aspetto dell'output di questa operazione è simile al seguente.

```
{  
  "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-ABCDEFGHIJKLMNQPQRSTUVWXYZ",
"CACertificateIdentifier": "rds-ca-2019",
"PromotionTier": 1,
"DBInstanceArn": "arn:aws:rds:us-east-1:123456789012:db:sample-
instance-1",
"EnabledCloudwatchLogsExports": [
    "profiler"
]
}
]
}

```

L'applicazione delle modifiche richiede qualche minuto. Puoi utilizzare l'istanza solo quando ha lo stato disponibile. È possibile monitorare lo stato dell'istanza utilizzando AWS Management Console o AWS CLI. Per ulteriori informazioni, consulta [Monitoraggio dello stato di un'istanza Amazon DocumentDB](#).

Riavvio di un'istanza Amazon DocumentDB

Occasionalmente, potrebbe essere necessario riavviare l'istanza di Amazon DocumentDB, di solito per motivi di manutenzione. Se apporti alcune modifiche, ad esempio la modifica del gruppo di parametri del cluster associato a un cluster, devi riavviare le istanze del cluster affinché le modifiche abbiano effetto. È possibile riavviare un'istanza specificata utilizzando o il AWS Management Console . AWS CLI

Il riavvio di un'istanza comporta il riavvio del servizio del motore di database. Il riavvio comporta un'interruzione temporanea, durante la quale lo stato dell'istanza viene impostato `rebooting`. Un evento Amazon DocumentDB viene creato al termine del riavvio.

Il riavvio di un'istanza non comporta un failover. Per eseguire il failover di un cluster Amazon DocumentDB, usa AWS Management Console l'operazione o AWS CLI `failover-db-cluster`. Per ulteriori informazioni, consulta [Failover di Amazon DocumentDB](#).


Non puoi riavviare l'istanza se il suo stato non è disponibile. Il database può non essere disponibile per diversi motivi, ad esempio una modifica richiesta in precedenza o un'operazione della finestra di manutenzione. Per ulteriori informazioni sugli stati delle istanze, consulta [Monitoraggio dello stato di un'istanza Amazon DocumentDB](#).

Using the AWS Management Console

La procedura seguente riavvia un'istanza specificata utilizzando la console.

1. [Accedi a e apri AWS Management Console la console Amazon DocumentDB all'indirizzo `https://console.aws.amazon.com/docdb`.](https://console.aws.amazon.com/docdb)
2. Nel pannello di navigazione scegliere Clusters (Cluster).

Tip

Se il riquadro di navigazione non viene visualizzato sul lato sinistro della schermata, scegliere l'icona del menu () nell'angolo in alto a sinistra della pagina.

3. Nella casella di navigazione Clusters, vedrai la colonna Cluster Identifier. Le tue istanze sono elencate in cluster, in modo simile alla schermata seguente.

The screenshot shows the Amazon DocumentDB console interface. On the left is a navigation menu with options like Dashboard, Clusters, Snapshots, Subnet groups, Parameter groups, Events, What's New (16), Tutorials, and Blogs. The main content area is titled 'DocumentDB > Clusters' and displays a table of clusters. The table has columns for 'Cluster identifier' and 'Role'. The cluster 'docdb-cloud9-getstarted' is highlighted with a red circle, and its role is 'Primary'. Other clusters shown include 'robo3t' with a 'Cluster' role and another 'robo3t' with a 'Primary' role.

<input type="checkbox"/>	<input type="checkbox"/>	Cluster identifier	Role
<input type="checkbox"/>	<input type="checkbox"/>	docdb-cloud9-getstarted	Cluster
<input type="checkbox"/>	<input type="checkbox"/>	docdb-cloud9-getstarted	Primary
<input type="checkbox"/>	<input type="checkbox"/>	robo3t	Cluster
<input type="checkbox"/>	<input type="checkbox"/>	robo3t	Primary

4. Seleziona la casella a sinistra dell'istanza che desideri riavviare.
5. Scegli Actions (Operazioni), scegli Reboot (Riavvia) e quindi Reboot (Riavvia) per confermare il riavvio.

Per il riavvio dell'istanza sono necessari alcuni minuti. Puoi utilizzare l'istanza solo quando ha lo stato disponibile. Puoi monitorare lo stato dell'istanza con la console o l' AWS CLI. Per ulteriori informazioni, consulta [Monitoraggio dello stato di un'istanza Amazon DocumentDB](#).

Using the AWS CLI

Per riavviare un'istanza Amazon DocumentDB, utilizza l'operazione con `reboot-db-instance` e il parametro `--db-instance-identifier` per specificare l'identificatore per l'istanza da riavviare.

Il codice seguente riavvia l'istanza `sample-instance`.

Example

Per Linux, macOS o Unix:

```
aws docdb reboot-db-instance \
  --db-instance-identifier sample-instance
```

Per Windows:

```
aws docdb reboot-db-instance ^
```

```
--db-instance-identifier sample-instance
```

L'aspetto dell'output di questa operazione è simile al seguente.

```
{
  "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-ABCDEFGHIJKLMNQPQRSTUVWXYZ",
  "CACertificateIdentifier": "rds-ca-2019",
  "PromotionTier": 1,
  "DBInstanceArn": "arn:aws:rds:us-east-1:<accountID>:db:sample-instance",
  "EnabledCloudwatchLogsExports": [
    "profiler"
  ]
}
}
```

Per il riavvio dell'istanza sono necessari alcuni minuti. Puoi utilizzare l'istanza solo quando ha lo stato disponibile. Puoi monitorare lo stato dell'istanza con la console o l' AWS CLI. Per ulteriori informazioni, consulta [Monitoraggio dello stato di un'istanza Amazon DocumentDB](#).

Eliminazione di un'istanza Amazon DocumentDB

Puoi eliminare la tua istanza di Amazon DocumentDB utilizzando AWS Management Console o AWS CLI. Per eliminare un'istanza, questa deve essere nello stato disponibile. Non è possibile eliminare un'istanza arrestata. Se il cluster Amazon DocumentDB che contiene l'istanza viene interrotto, avvia prima il cluster, attendi che l'istanza diventi disponibile, quindi elimina l'istanza. Per ulteriori informazioni, consulta [Arresto e avvio di un cluster Amazon DocumentDB](#).

Note

Amazon DocumentDB archivia tutti i dati nel volume del cluster. I dati persistono nel volume cluster, anche se rimuovi tutte le istanze dal cluster. Se hai bisogno di accedere nuovamente

ai dati, puoi aggiungere un'istanza al cluster in qualsiasi momento e riprendere da dove avevi lasciato.

Using the AWS Management Console

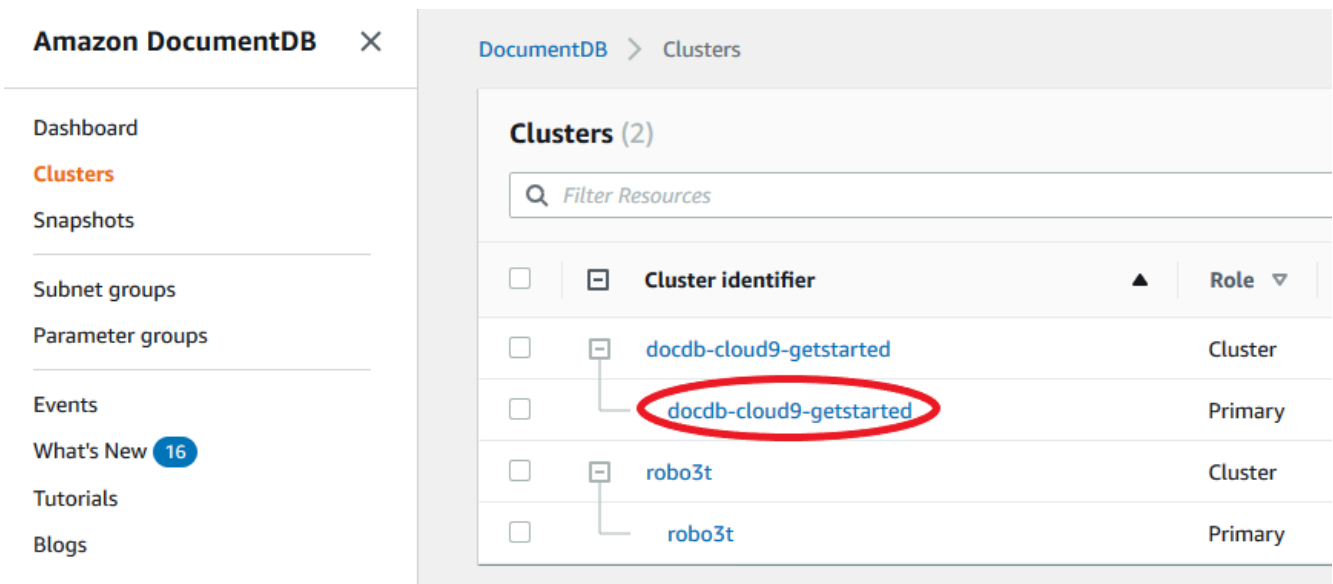
La procedura seguente elimina un'istanza Amazon DocumentDB specificata utilizzando la console.

1. [Accedi a e apri AWS Management Console la console Amazon DocumentDB all'indirizzo https://console.aws.amazon.com/docdb](https://console.aws.amazon.com/docdb).
2. Nel pannello di navigazione scegliere Clusters (Cluster).

Tip

Se il riquadro di navigazione non viene visualizzato sul lato sinistro della schermata, scegliere l'icona del menu (☰) nell'angolo in alto a sinistra della pagina.

3. Nella casella di navigazione Clusters, vedrai la colonna Cluster Identifier. Le tue istanze sono elencate in cluster, in modo simile alla schermata seguente.



<input type="checkbox"/>	<input type="checkbox"/>	Cluster identifier	Role
<input type="checkbox"/>	<input type="checkbox"/>	docdb-cloud9-getstarted	Cluster
<input type="checkbox"/>	<input type="checkbox"/>	docdb-cloud9-getstarted	Primary
<input type="checkbox"/>	<input type="checkbox"/>	robo3t	Cluster
<input type="checkbox"/>	<input type="checkbox"/>	robo3t	Primary

4. Seleziona la casella a sinistra dell'istanza che desideri eliminare.
5. Scegli Actions (Operazioni), quindi Delete (Elimina).

1. Se stai eliminando l'ultima istanza nel cluster:
 - Create final cluster snapshot? (Crea la snapshot del cluster finale?) — Scegliete Sì se desiderate creare un'istantanea finale prima dell'eliminazione del cluster. Altrimenti, scegliere No.
 - Nome dell'istantanea finale: se scegli di creare un'istantanea finale, inserisci l'identificatore dell'istantanea del cluster della nuova istantanea del cluster creata.
 - Delete <instance-name> instance? (Elimina istanza <nome-istanza>?) — Inserisci la frase delete entire cluster nel campo per confermare l'eliminazione.
2. Se non stai eliminando l'ultima istanza nel cluster:
 - Delete <instance-name> instance? (Elimina istanza <nome-istanza>?) — Inserisci la frase delete me nel campo per confermare l'eliminazione.
6. Seleziona Delete (Elimina) per eliminare l'istanza.

Sono necessari alcuni minuti per l'eliminazione dell'istanza. Per monitorare lo stato di un'istanza, consulta [Monitoraggio dello stato di un'istanza Amazon DocumentDB](#).

Using the AWS CLI

La procedura seguente elimina un'istanza di Amazon DocumentDB utilizzando AWS CLI

1. Innanzitutto, determina quante istanze ci sono nel tuo cluster Amazon DocumentDB:

Per determinare il numero di istanze presenti nel cluster, esegui il comando `describe-db-clusters` come indicato di seguito.

```
aws docdb describe-db-clusters \
  --db-cluster-identifier sample-cluster \
  --query 'DBClusters[*].
  [DBClusterIdentifier,DBClusterMembers[*].DBInstanceIdentifier]'
```

L'aspetto dell'output di questa operazione è simile al seguente.

```
[
  [
    "sample-cluster",
    [
      "sample-instance-1",
      "sample-instance-2"
    ]
  ]
]
```

```
]
  ]
]
```

2. Se nel cluster Amazon DocumentDB sono presenti più di un'istanza:

Per eliminare un'istanza Amazon DocumentDB specificata, usa il `delete-db-instance` comando con il `--db-instance-identifier` parametro, come illustrato di seguito. Sono necessari alcuni minuti per l'eliminazione dell'istanza. Per monitorare lo stato di un'istanza, consulta [Monitoraggio dello stato di un'istanza Amazon DocumentDB](#).

```
aws docdb delete-db-instance \
    --db-instance-identifier sample-instance-2
```

L'aspetto dell'output di questa operazione è simile al seguente.

```
{
  "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-ABCDEFGHIJKLMNQRSTUWXYZ",
    "CACertificateIdentifier": "rds-ca-2019",
    "PromotionTier": 1,
    "DBInstanceArn": "arn:aws:rds:us-east-1:<accountID>:db:sample-instance-2",
    "EnabledCloudwatchLogsExports": [
      "profiler"
    ]
  }
}

```

3. Se l'istanza che desideri eliminare è l'ultima istanza del tuo cluster Amazon DocumentDB:

Se elimini l'ultima istanza in un cluster Amazon DocumentDB, elimini anche quel cluster e gli snapshot automatici e i backup continui associati a quel cluster.

Per eliminare l'ultima istanza del cluster, puoi eliminare il cluster e, facoltativamente, creare uno snapshot finale. Per ulteriori informazioni, consulta [Eliminazione di un cluster Amazon DocumentDB](#).

Deletion protection (Protezione da eliminazione)

L'eliminazione dell'ultima istanza di un cluster Amazon DocumentDB comporta anche l'eliminazione del cluster, nonché gli snapshot automatici e i backup continui associati a tale cluster. Amazon DocumentDB applica la protezione da eliminazione per un cluster indipendentemente dal fatto che l'operazione di eliminazione venga eseguita utilizzando o il AWS Management Console . AWS CLI Se la protezione dall'eliminazione è abilitata, non puoi eliminare un cluster.

Per eliminare un cluster con la protezione dall'eliminazione abilitata, devi modificare il cluster e disabilitare la protezione dall'eliminazione. Per ulteriori informazioni, consulta [Eliminazione di un cluster Amazon DocumentDB](#).

Gestione dei gruppi di sottoreti Amazon DocumentDB

Un cloud privato virtuale (Virtual Private Cloud, VPC, Virtual Cloud) è una rete virtuale dedicata a teAccount AWS. Il VPC è isolato a livello logico dalle altre reti virtuali del cloud AWS. Puoi avviare leAWS risorse, ad esempio i cluster Amazon DocumentDB, nel VPC Amazon. Puoi specificare un intervallo di indirizzi IP per il VPC, aggiungere sottoreti, associare gruppi di sicurezza e configurare tabelle di routing.

Una sottorete è un intervallo di indirizzi IP nel VPC Amazon. È possibile avviare le risorse AWS in una sottorete specifica. Utilizza una sottorete pubblica per le risorse che devono essere connesse a Internet. Utilizza una sottorete privata per le risorse che non saranno connesse a Internet. Per ulteriori informazioni sulle sottoreti pubbliche e private, consulta Nozioni di [base su VPC e sottoreti](#) nella Guida per l'utente di Amazon Virtual Private Cloud.

Un gruppo di sottoreti del database è una raccolta di sottoreti creata in un VPC, che è possibile indicare per i cluster. Un gruppo di sottoreti consente di specificare un determinato VPC quando si creano i cluster. Se usi il gruppo di sottoreti default, esso include tutte le sottoreti nel VPC.

Ogni gruppo di sottoreti database dovrebbe avere almeno due zone di disponibilità in una data regione . Quando crei un cluster database in un VPC, devi selezionare un gruppo di sottoreti database. Amazon DocumentDB utilizza tale gruppo di sottoreti del database e la zona di disponibilità preferita per selezionare una sottorete e un indirizzo IP all'interno della sottorete da associare al

cluster. Se l'istanza primaria non riesce, Amazon DocumentDB può promuovere un'istanza di replica corrispondente a diventare la nuova istanza primaria. È possibile creare una nuova istanza di replica usando un indirizzo IP della sottorete in cui si trovava l'istanza primaria precedente.

Quando Amazon DocumentDB crea un'istanza in un VPC, assegna un'interfaccia di rete al cluster usando un indirizzo IP selezionato dal gruppo di sottoreti del database. È consigliabile utilizzare il nome DNS, perché l'indirizzo IP sottostante può variare durante il failover. Per ulteriori informazioni, consulta [Endpoint Amazon DocumentDB](#).

Per informazioni sulla creazione di VPC e sottoreti personalizzati, consulta [Working with VPC and Subnet](#) in the Amazon Virtual Private Cloud User Guide.

Argomenti

- [Creazione di un gruppo di sottoreti Amazon DocumentDB](#)
- [Descrizione di un gruppo di sottoreti Amazon DocumentDB](#)
- [Modifica di un gruppo di sottoreti Amazon DocumentDB](#)
- [Eliminazione di un gruppo di sottoreti Amazon DocumentDB](#)

Creazione di un gruppo di sottoreti Amazon DocumentDB

Quando crei un cluster Amazon DocumentDB, devi scegliere un Amazon VPC e un gruppo di sottorete corrispondente all'interno di quel VPC Amazon per avviare il cluster. Le sottoreti determinano la zona di disponibilità e l'intervallo IP all'interno della zona di disponibilità che si desidera utilizzare per avviare un'istanza.

Un gruppo di sottoreti è un set denominato di sottoreti (o AZ) che consente di specificare le zone di disponibilità da utilizzare per avviare istanze Amazon DocumentDB. Ad esempio, in un cluster con tre istanze, si consiglia di eseguire il provisioning di ciascuna di queste istanze in AZ separati, in modo da ottimizzare l'elevata disponibilità. Pertanto, se una singola AZ fallisce, influirà solo su una singola istanza.

Attualmente, le istanze di Amazon DocumentDB possono essere fornite in un massimo di tre AZ. Anche se un gruppo di sottoreti ha più di tre sottoreti, potrai utilizzarne solo tre per creare un cluster Amazon DocumentDB. Pertanto, quando si crea un gruppo di sottoreti, si consiglia di scegliere solo le tre sottoreti di cui distribuire le istanze.

Ad esempio: viene creato un cluster e Amazon DocumentDB sceglie AzS {1A, 1B e 1C}. Se tenti di creare un'istanza in AZ {1D} la chiamata API non riuscirà. Tuttavia, se scegli di creare un'istanza,

senza specificare una determinata AZ, Amazon DocumentDB sceglierà una AZ per tuo conto. Amazon DocumentDB utilizza un algoritmo per bilanciare il carico delle istanze tra gli AZ per aiutarti a ottenere un'elevata disponibilità. Se vengono fornite tre istanze, per impostazione predefinita, verranno eseguite su tre AZ e non verranno eseguite tutte in un'unica AZ.

Best practice

- A meno che non si abbia un motivo specifico, creare sempre un gruppo di sottoreti con tre sottoreti. Ciò garantisce che i cluster con tre o più istanze saranno in grado di raggiungere una maggiore disponibilità poiché le istanze verranno distribuite su tre AZ.
- Distribuisci sempre le istanze su più AZ per ottenere una disponibilità più elevata. Non posizionare mai tutte le istanze di un cluster in una singola AZ.
- Poiché gli eventi di failover possono verificarsi in qualsiasi momento, non devi presumere che un'istanza primaria o le istanze di replica siano sempre in una determinata AZ.

Come creare un gruppo di sottoreti

Puoi usare AWS Management Console o AWS CLI per creare un gruppo di sottorete Amazon DocumentDB:



Using the AWS Management Console

Utilizza la procedura seguente per creare un gruppo di sottoreti Amazon DocumentDB.

Per creare un gruppo di sottoreti Amazon DocumentDB

1. Accedi alla e apri la console Amazon DocumentDB all'[indirizzo https://console.aws.amazon.com/docdb](https://console.aws.amazon.com/docdb). AWS Management Console
2. Dal riquadro di navigazione, scegliere Subnet group (Gruppo di sottoreti), quindi scegliere Create (Crea).

Tip

Se il riquadro di navigazione non viene visualizzato sul lato sinistro della schermata, scegliere l'icona del menu () nell'angolo in alto a sinistra della pagina. 

3. Dalla pagina Create subnet group (Crea gruppo di sottorete):

- a. Nella sezione Subnet group details (Dettagli del gruppo di sottoreti):
 - i. Nome: immettere un nome specifico per il gruppo di sottoreti.
 - ii. Descrizione: immettere una descrizione del gruppo di sottoreti.
 - b. Nella sezione Add subnets (Aggiungi sottoreti):
 - i. VPC: nell'elenco, scegli un VPC per questo gruppo di sottoreti.
 - ii. Completa una delle seguenti operazioni:
 - Per includere tutte le sottoreti nel VPC selezionato, scegliere Add all the subnets related to this VPC (Aggiungi tutte le sottoreti correlate a questo VPC).
 - Per specificare le sottoreti per questo gruppo di sottoreti, eseguire la procedura seguente per ogni zona di disponibilità in cui si desidera includere le sottoreti. È necessario includere almeno due zone di disponibilità.
 - A. Zona di disponibilità: nell'elenco, selezionare una zona di disponibilità.
 - B. Sottorete: nell'elenco, selezionare una sottorete dalla zona di disponibilità scelta per questo gruppo di sottoreti.
 - C. Scegliere Add subnet (Aggiungi sottorete).
4. Seleziona Create (Crea). Quando viene creato, il gruppo di sottoreti viene elencato con gli altri gruppi di sottoreti.

Name	Description	Status	VPC
default	default	Complete	vpc-91280df6
sample-subnet-group	A sample subnet group	Complete	vpc-91280df6

Using the AWS CLI

Prima di creare un gruppo di sottoreti utilizzando l'AWS CLI, è necessario stabilire quali sottoreti sono disponibili. Per elencare le zone di disponibilità e le relative sottoreti, eseguire questa operazione AWS CLI.

Parametri:

- **--db-subnet-group**—Opzionale. L'indicazione di un determinato gruppo di sottoreti elencherà le zone di disponibilità e le sottoreti per quel gruppo. L'omissione di questo parametro

elencherà zone di disponibilità e le sottoreti per tutti i gruppi di sottoreti. L'indicazione del gruppo di sottoreti `default` elenca tutte le sottoreti del VPC.

Example

Per Linux, macOS o Unix:

```
aws docdb describe-db-subnet-groups \  
  --db-subnet-group-name default \  
  --query 'DBSubnetGroups[*].[DBSubnetGroupName,Subnets[*].  
[SubnetAvailabilityZone.Name,SubnetIdentifier]]'
```

Per Windows:

```
aws docdb describe-db-subnet-groups ^  
  --db-subnet-group-name default ^  
  --query 'DBSubnetGroups[*].[DBSubnetGroupName,Subnets[*].  
[SubnetAvailabilityZone.Name,SubnetIdentifier]]'
```

L'aspetto dell'output di questa operazione è simile al seguente (formato JSON).

```
[  
  [  
    "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"
    ]
  ]
]

```

Utilizzando l'output dall'operazione precedente, è possibile creare un nuovo gruppo di sottoreti. Il nuovo gruppo di sottoreti deve includere sottoreti da almeno due zone di disponibilità.

Parametri:

- **--db-subnet-group-name**: obbligatorio. Il nome di questo gruppo di sottoreti.
- **--db-subnet-group-description**: obbligatorio. La descrizione di questo gruppo di sottoreti.
- **--subnet-ids**: obbligatorio. Un elenco di sottoreti da includere in questo gruppo di sottoreti. Esempio: `subnet-53ab3636`.
- **--Etichette** —Facoltativo. Un elenco di tag (coppie chiave/valore) da collegare a questo gruppo di sottoreti.

Il codice seguente crea il gruppo di sottoreti `sample-subnet-group` con tre sottoreti `subnet-4e26d263`, `subnet-afc329f4` e `subnet-b3806e8f`.

Per Linux, macOS o 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

```

Per 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
```

L'aspetto dell'output di questa operazione è simile al seguente (formato JSON).

```
{  
  "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"  
  }  
}
```

Descrizione di un gruppo di sottoreti Amazon DocumentDB

È possibile utilizzare AWS Management Console o il AWS CLI per ottenere i dettagli di un gruppo di sottorete Amazon DocumentDB.

Using the AWS Management Console

La procedura seguente illustra come ottenere i dettagli di un gruppo di sottoreti Amazon DocumentDB.

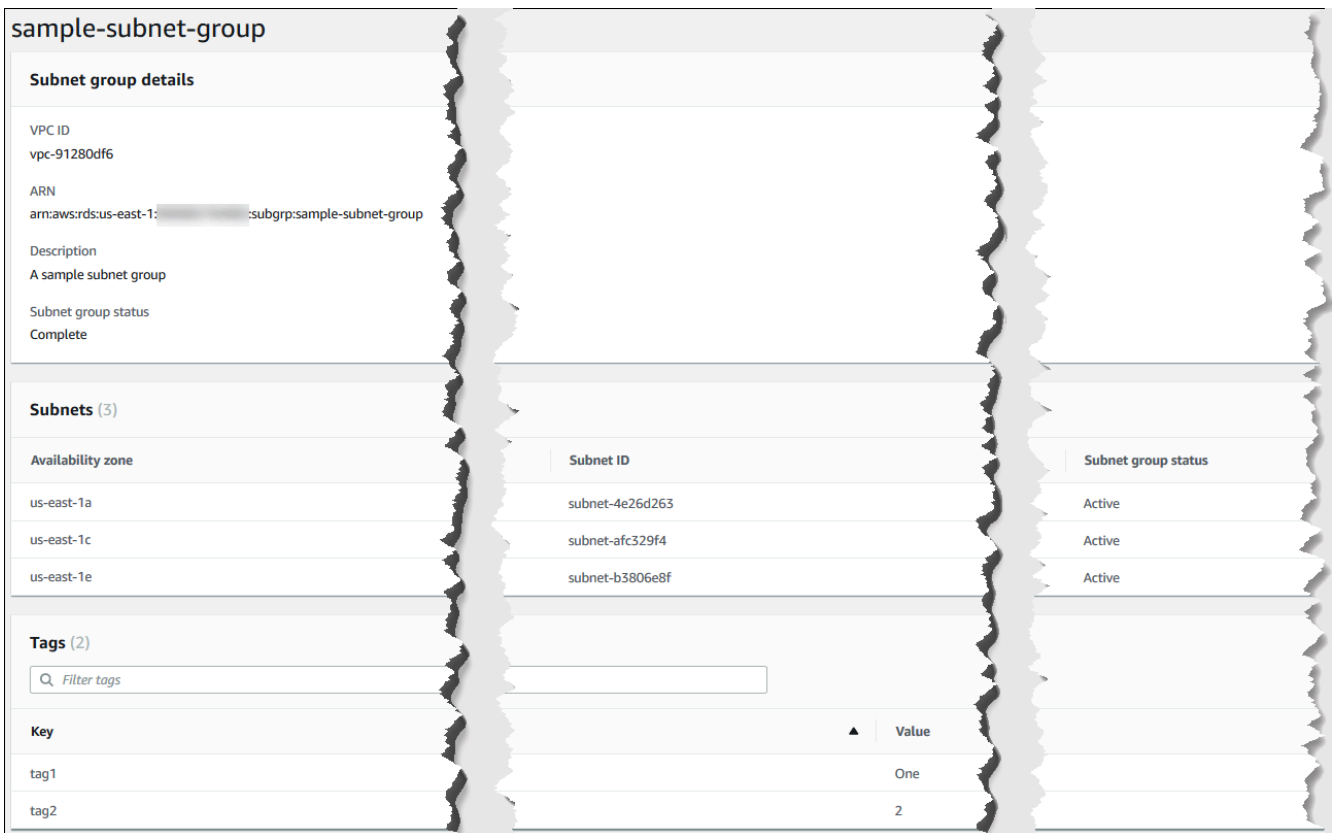
Per individuare i dettagli di un gruppo di sottoreti

1. Accedi alla e apri la console Amazon DocumentDB all'[indirizzo https://console.aws.amazon.com/docdb](https://console.aws.amazon.com/docdb). AWS Management Console
2. Nel pannello di navigazione selezionare Subnet groups (Gruppi di sottoreti).

Tip

Se il riquadro di navigazione non viene visualizzato sul lato sinistro della schermata, scegliere l'icona del menu (☰) nell'angolo in alto a sinistra della pagina.

3. Per vedere i dettagli di un gruppo di sottoreti, selezionare il nome di tale gruppo di sottoreti.



Using the AWS CLI

Per trovare i dettagli di un gruppo di sottorete Amazon DocumentDB, utilizza l'`describe-db-subnet-groups` operazione con il seguente parametro.

Parametro

- `--db-subnet=group-name`—Opzionale. Se incluso, sono elencati i dettagli per il gruppo di sottoreti designato. Se omesso, sono elencati i dettagli di un massimo di 100 gruppi di sottoreti.

Example

Il codice seguente elenca i dettagli per il gruppo di sottoreti `sample-subnet-group` che abbiamo creato nella sezione [Creazione di un gruppo di sottoreti Amazon DocumentDB](#).

Per Linux, macOS o Unix:

```
aws docdb describe-db-subnet-groups \
  --db-subnet-group-name sample-subnet-group
```

Per Windows:

```
aws docdb describe-db-subnet-groups ^  
  --db-subnet-group-name sample-subnet-group
```

L'aspetto dell'output di questa operazione è simile al seguente (formato JSON).

```
{  
  "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"  
  }  
}
```

Modifica di un gruppo di sottoreti Amazon DocumentDB

Puoi utilizzare AWS Management Console o AWS CLI per modificare la descrizione di un gruppo di sottoreti o per aggiungere o rimuovere sottoreti da un gruppo di sottoreti Amazon DocumentDB. Tuttavia, non è possibile modificare il gruppo di sottoreti default.

Using the AWS Management Console

È possibile utilizzare l'AWS Management Console per modificare la descrizione di un gruppo di sottoreti o per aggiungere e rimuovere le sottoreti. Ricorda che, al termine di questa operazione è necessario disporre di almeno due zone di disponibilità associate al gruppo di sottoreti.

Per modificare il gruppo di sottoreti

1. Accedi alla e apri la console Amazon DocumentDB all'[indirizzo https://console.aws.amazon.com/docdb](https://console.aws.amazon.com/docdb). AWS Management Console
2. Nel pannello di navigazione selezionare Subnet groups (Gruppi di sottoreti). Quindi scegliere il pulsante a sinistra del nome del gruppo di sottoreti. Ricorda che non è possibile modificare il gruppo di sottoreti default.

Tip

Se il riquadro di navigazione non viene visualizzato sul lato sinistro della schermata, scegliere l'icona del menu (☰) nell'angolo in alto a sinistra della pagina.

3. Scegli Actions (Operazioni), quindi Modify (Modifica).
4. Descrizione: per modificare la descrizione del gruppo di sottoreti, inserisci una nuova descrizione.
5. Per modificare le sottoreti associate al gruppo di sottoreti, nella sezione Add subnets (Aggiungi sottoreti) , eseguire una o più delle operazioni seguenti:
 - Per rimuovere tutte le sottoreti da questo gruppo di sottoreti, scegliere Remove all (Rimuovi tutte).
 - Per rimuovere sottoreti specifiche da questo gruppo di sottoreti, scegliere Remove (Rimuovi) per ciascuna sottorete da rimuovere.

- Per aggiungere tutte le sottoreti associate a questo VPC, scegliere **Add all the subnets related to this VPC** (Aggiungi tutte le sottoreti correlate a questo VPC).
 - Per aggiungere sottoreti specifiche a questo gruppo di sottoreti, eseguire la procedura seguente per ogni zona di disponibilità a cui si desidera aggiungere una sottorete.
 - a. Zona di disponibilità: nell'elenco, scegli una nuova zona di disponibilità.
 - b. Sottorete: nell'elenco, selezionare una sottorete dalla zona di disponibilità scelta per questo gruppo di sottoreti.
 - c. Scegliere **Add subnet** (Aggiungi sottorete).
6. Nella finestra di dialogo di conferma:
- Per apportare tali modifiche al gruppo di sottoreti, scegliere **Modify** (Modifica).
 - Per mantenere il gruppo di sottoreti invariato, scegliere **Cancel** (Annulla).

Using the AWS CLI

È possibile utilizzare l'AWS CLI per modificare la descrizione di un gruppo di sottoreti o per aggiungere e rimuovere le sottoreti. Ricorda che, al termine di questa operazione è necessario disporre di almeno due zone di disponibilità associate al gruppo di sottoreti. Non è possibile modificare il gruppo di sottoreti `default`.

Parametri:

- `--db-subnet-group-name`: obbligatorio. Il nome del gruppo di sottorete Amazon DocumentDB che stai modificando.
- `--subnet-ids`: obbligatorio. Un elenco di tutte le sottoreti che vuoi aggiungere al gruppo di sottoreti al completamento di questa modifica.

Important

Tutte le sottoreti attualmente nel gruppo di sottoreti che non vengono incluse in questo elenco vengono rimosse dal gruppo di sottoreti. Se si desidera conservare le sottoreti attualmente nel gruppo di sottoreti, è necessario includerle in questo elenco.

- `--db-subnet-group-description`—Opzionale. La descrizione del gruppo di sottoreti.

Example

Il codice seguente modifica la descrizione e sostituisce le sottoreti esistenti con le sottoreti `subnet-991cb8d0`, `subnet-53ab3636` e `subnet-29ab1025`.

Per Linux, macOS o 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"
```

Per 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"
```

L'aspetto dell'output di questa operazione è simile al seguente (formato JSON). Questo è lo stesso gruppo di sottoreti che è stato creato nella sezione [Creazione di un gruppo di sottoreti Amazon DocumentDB](#). Tuttavia, le sottoreti nel gruppo di sottoreti vengono sostituite da quelle elencate nell'operazione `modify-db-subnet-group`.

```
{  
  "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"
}
```

Eliminazione di un gruppo di sottoreti Amazon DocumentDB

Puoi usare AWS Management Console o AWS CLI per eliminare un gruppo di sottoreti Amazon DocumentDB. Tuttavia, non è possibile eliminare il gruppo di sottoreti default.

Using the AWS Management Console

È possibile utilizzare AWS Management Console per eliminare un gruppo di sottoreti. Tuttavia, non è possibile eliminare il gruppo di sottoreti default.

Per eliminare un gruppo di sottoreti

1. Accedi alla e apri la console Amazon DocumentDB all'[indirizzo https://console.aws.amazon.com/docdb](https://console.aws.amazon.com/docdb). AWS Management Console
2. Nel pannello di navigazione selezionare Subnet groups (Gruppi di sottoreti). Quindi scegliere il pulsante a sinistra del nome del gruppo di sottoreti. Ricorda che non è possibile eliminare il gruppo di sottoreti default.

Tip

Se il riquadro di navigazione non viene visualizzato sul lato sinistro della schermata, scegliere l'icona del menu

(☰)
nell'angolo in alto a sinistra della pagina.

3. Scegli Actions (Operazioni), quindi Delete (Elimina).
4. Nella finestra di dialogo di conferma:
 - Per eliminare il gruppo di sottoreti, scegliere Delete (Elimina).
 - Per mantenere il gruppo di sottoreti, scegliere Cancel (Annulla).

Using the AWS CLI

Per eliminare un gruppo di sottorete Amazon DocumentDB utilizzando ilAWS CLI, utilizza l'`delete-db-subnet-group`operazione con il seguente parametro.

Parametro

- `--db-subnet-group-name`: obbligatorio. Nome del gruppo di sottoreti Amazon DocumentDB da eliminare. Ricorda che non è possibile eliminare il gruppo di sottoreti default.

Example

Il codice seguente consente di eliminare `sample-subnet-group`.

Per Linux, macOS o Unix:

```
aws docdb delete-db-subnet-group \  
  --db-subnet-group-name sample-subnet-group
```

Per Windows:

```
aws docdb delete-db-subnet-group ^  
  --db-subnet-group-name sample-subnet-group
```

L'operazione non produce alcun output.

Amazon DocumentDB

Puoi ottenere un'alta disponibilità e dimensionamento della lettura in Amazon DocumentDB (con compatibilità MongoDB) utilizzando istanze di replica. Un singolo cluster Amazon DocumentDB

supporta una singola istanza primaria e fino a 15 istanze di replica. Queste istanze possono essere distribuite tra le zone di disponibilità all'interno della regione del cluster. L'istanza primaria accetta il traffico in lettura e in scrittura, mentre le istanze di replica accettano solo richieste di lettura.

Il volume cluster si compone di più copie dei dati per il cluster. Tuttavia, i dati nel volume cluster sono rappresentati come singolo volume logico all'istanza primaria e alle repliche Amazon DocumentDB nel cluster. Le istanze di replica sono consistenti finali. Restituiscono risultati di query con un ritardo di replica minimo, generalmente inferiore a 100 millisecondi dopo che l'istanza primaria ha scritto un aggiornamento. Il ritardo di replica varia in base alla velocità di modifica del database. In altre parole, nei periodi in cui si verificano numerose operazioni di scrittura nel database, potresti riscontrare un aumento del ritardo di replica.

Dimensionamento della lettura

Le repliche Amazon DocumentDB funzionano bene per il dimensionamento della lettura perché sono dedicate completamente a operazioni di lettura nel volume cluster. Le operazioni di lettura sono gestite dall'istanza primaria. Il volume del cluster è condiviso tra tutte le istanze del cluster. Pertanto, non è necessario replicare e conservare una copia dei dati per ciascuna replica Amazon DocumentDB.

Elevata disponibilità

Quando crei un cluster Amazon DocumentDB, effettua il provisioning delle istanze nelle zone di disponibilità a seconda del loro numero nel gruppo di sottorete (devono essere almeno due). Quando crei le istanze nel cluster, Amazon DocumentDB distribuisce automaticamente le istanze nelle zone di disponibilità in un gruppo di sottorete per bilanciare il cluster. Questa azione impedisce inoltre che tutte le istanze si trovino nella stessa zona di disponibilità.

Esempio

Per illustrare meglio questo punto, si supponga di creare un cluster che abbia un gruppo di sottorete con tre zone di disponibilità: AZ1, AZ2, e AZ3.

Una volta creata, la prima istanza all'interno del cluster si trova in una delle zone di disponibilità. In questo esempio, si trova nella zona AZ1. La seconda istanza creata è un'istanza di replica e si trova in una delle altre due zone di disponibilità, ad esempio AZ2. La terza istanza creata è un'istanza di replica e si trova nella zona di disponibilità restante, AZ3. Se crei più istanze, queste sono distribuite tra le zone di disponibilità in modo da ottenere il bilanciamento del cluster.

Se si verifica un errore nell'istanza primaria (AZ1), viene attivato un failover e una delle repliche esistenti viene promossa a primaria. Quando la vecchia istanza primaria viene ripristinata, diventa una replica nella stessa zona di disponibilità in cui è stata assegnata (AZ1). Quando effettui il provisioning di un cluster a tre istanze, Amazon DocumentDB continua per preservare il cluster a tre istanze. Amazon DocumentDB gestisce automaticamente il rilevamento, il failover e il ripristino degli errori di istanza senza alcun intervento manuale.

Quando Amazon DocumentDB esegue un failover e ripristina un'istanza, l'istanza recuperata rimane nella zona di disponibilità in cui è stata originariamente assegnata. Tuttavia, il ruolo dell'istanza potrebbe cambiare da primaria a replica. Questa operazione viene eseguita per evitare lo scenario in cui una serie di failover provoca il posizionamento di tutte le istanze nella stessa zona di disponibilità.

È possibile specificare le repliche Amazon DocumentDB come destinazioni di failover. Cioè, se l'istanza primaria ha esito negativo, la replica o la replica Amazon DocumentDB specificata da un livello specificata viene promossa a primaria. Si verifica una breve interruzione durante la quale le richieste di lettura e scrittura inviate all'istanza primaria falliscono con un'eccezione. Se il cluster Amazon DocumentDB non include repliche Amazon DocumentDB, l'istanza primaria viene ricreata in caso si verifichi un evento di errore. La promozione di una replica Amazon DocumentDB è un'operazione molto più veloce rispetto alla ricreazione dell'istanza primaria.

Per gli scenari di disponibilità elevata, è consigliato creare una o più repliche Amazon DocumentDB. Queste repliche dovrebbero essere della stessa classe di istanza dell'istanza primaria e in zone di disponibilità diverse per il cluster Amazon DocumentDB.

Per ulteriori informazioni, consulta quanto segue:

- [Comprendere la tolleranza agli errori del cluster Amazon DocumentDB](#)
- [Failover di Amazon DocumentDB](#)
 - [Controllo della destinazione di failover](#)

Elevata disponibilità con i cluster globali

Per un'elevata disponibilità su piùRegioni AWS, puoi configurare [Cluster globali Amazon DocumentDB](#). Ciascun cluster globale si estende su più regioni, consentendo letture globali a bassa latenza e il disaster recovery da interruzioni a livello di Regione AWS. Amazon DocumentDB gestisce automaticamente la replica di tutti i dati e gli aggiornamenti dalla regione primaria a ciascuna delle regioni secondarie.

Aggiunta di repliche di

L'istanza primaria è la prima istanza aggiunta al cluster. Ogni istanza aggiunta dopo la prima è un'istanza di replica. Oltre all'istanza primaria, ogni cluster può avere fino a 15 istanze di replica.

Se crei un cluster utilizzando la AWS Management Console, nello stesso momento viene creata automaticamente anche un'istanza primaria. Per creare una replica nello stesso momento in cui viene creato il cluster e l'istanza primaria, scegli `Create replica in different zone` (Crea replica in una zona diversa). Per ulteriori informazioni, consulta la fase 4.d in [Creazione di un cluster Amazon DocumentDB](#). Per aggiungere più repliche a un cluster Amazon DocumentDB, consulta [Aggiungere un'istanza Amazon DocumentDB a un cluster](#).

Quando utilizzi l'AWS CLI per creare il cluster, devi creare in modo esplicito l'istanza primaria e le istanze di replica. Per ulteriori informazioni, consulta la sezione "Utilizzo dell'AWS CLI" dei seguenti argomenti:

- [Creazione di un cluster Amazon DocumentDB](#)
- [Aggiungere un'istanza Amazon DocumentDB a un cluster](#)

Failover di Amazon DocumentDB

In alcuni casi, ad esempio per alcuni tipi di manutenzione programmata o nel caso poco probabile di un errore in un nodo primario o in una zona di disponibilità, Amazon DocumentDB (con compatibilità con MongoDB) rileva l'errore e sostituisce il nodo primario. Durante un failover, il tempo di inattività di scrittura è ridotto al minimo. Questo perché il ruolo del nodo principale esegue il failover in una delle repliche di lettura invece di creare ed eseguire il provisioning di un nuovo nodo principale. Questa individuazione degli errori e promozione delle repliche garantisce la possibilità di ricominciare a scrivere nel nuovo nodo primario non appena la promozione è terminata.

Perché il failover sia efficace, il cluster deve contenere almeno due istanze, una istanza primaria e almeno un'istanza di replica.

Controllo della destinazione di failover

Amazon DocumentDB fornisce livelli di failover con cui controllare quale istanza di replica promuovere a istanza primaria quando si verifica un failover.

Livelli di failover

Ogni istanza di replica è associata a un livello di failover (0-15). Quando si verifica un failover a causa di operazioni di manutenzione o, in casi rari, di un guasto all'hardware, l'istanza primaria esegue il failover su una replica con la massima priorità (il numero di livello più basso). Se più repliche hanno stesso livello di priorità, l'istanza primaria esegue il failover su una replica nello stesso livello con le dimensioni più vicine a quelle dell'istanza primaria precedente.

Impostando il livello di failover per un gruppo di repliche selezionate su 0 (priorità massima), puoi assicurare che un failover promuoverà una delle repliche in tale gruppo. Inoltre, per evitare che delle repliche specifiche vengano promosse a istanza primaria in caso di failover, puoi assegnare un livello di priorità basso (numero alto) a queste repliche. Questa funzione è utile nei casi in cui repliche specifiche siano particolarmente utilizzate da un'applicazione e il failover di una di esse potrebbe influire negativamente su un'applicazione critica.

Puoi impostare il livello di failover di un'istanza quando la crei o puoi modificarlo successivamente. Il failover non viene attivato se imposti il livello di failover di un'istanza modificando l'istanza. Per ulteriori informazioni, consulta gli argomenti seguenti:

- [Aggiungere un'istanza Amazon DocumentDB a un cluster](#)
- [Modifica di un'istanza Amazon DocumentDB](#)

Quando avvii manualmente un failover, puoi controllare quale istanza di replica viene promossa a primaria in due modi: i livelli di failover descritti in precedenza e il parametro `--target-db-instance-identifier`.

`--target-db-instance-identifier`

Per il testing, puoi forzare un evento di failover utilizzando l'operazione `failover-db-cluster`. Puoi utilizzare il parametro `--target-db-instance-identifier` per specificare quale replica promuovere a istanza primaria. L'utilizzo del parametro `--target-db-instance-identifier` sostituisce il livello di priorità di failover. Se non specifichi il parametro `--target-db-instance-identifier`, il failover primario si conforma al livello di priorità di failover.

Cosa accade durante un failover

Il failover viene gestito automaticamente da Amazon DocumentDB, in modo che le applicazioni possano riprendere le operazioni database il più rapidamente possibile, senza alcun intervento amministrativo.

- Se hai un'istanza di replica Amazon DocumentDB nella stessa zona di disponibilità o in un'altra zona di disponibilità durante il failover: Amazon DocumentDB fa in modo che il record di nome canonico (CNAME) dell'istanza punti alla replica integra, che a sua volta viene alzata di livello e impostata come nuova replica primaria. In genere, l'esecuzione completa dell'intero processo di failover impiega meno di 30 secondi.
- Se non disponi di un'istanza di replica di Amazon DocumentDB (ad esempio, un cluster a istanza singola): Amazon DocumentDB tenterà di creare una nuova istanza nella stessa zona di disponibilità dell'istanza originale. Questa sostituzione dell'istanza originale viene eseguita in base al tentativo migliore e potrebbe non avvenire, ad esempio, se si verifica un problema che interessa in qualche modo la zona di disponibilità.

L'applicazione deve provare a ristabilire le connessioni al database in caso di perdita della connessione.

Verifica del Failover

Un failover di un cluster promuove una delle repliche di Amazon DocumentDB (istanze di sola lettura) nel cluster a istanza primaria (cluster di scrittura).

esegue automaticamente il failover in una replica Amazon DocumentDB, se disponibile, quando l'istanza primaria non riesce. Puoi forzare un failover per simulare un guasto di un'istanza primaria per scopi di testing. Ogni istanza in un cluster ha il proprio indirizzo di endpoint. Pertanto, è necessario eliminare e ristabilire tutte le connessioni esistenti che utilizzano tali indirizzi una volta completato il failover..

Per forzare un failover, utilizza l'operazione `failover-db-cluster` con questi parametri.

- `--db-cluster-identifier`: obbligatorio. Il nome del cluster di cui eseguire il failover.
- `--target-db-instance-identifier`—Opzionale. Il nome dell'istanza da promuovere a istanza primaria.

Example

L'operazione seguente forza un failover del cluster `sample-cluster`. Non specifica l'istanza da promuovere a nuova istanza primaria, pertanto Amazon DocumentDB sceglie l'istanza in base alla priorità del livello di failover.

Per Linux, macOS o Unix:

```
aws docdb failover-db-cluster \  
  --db-cluster-identifier sample-cluster
```

Per Windows:

```
aws docdb failover-db-cluster ^  
  --db-cluster-identifier sample-cluster
```

L'operazione seguente forza un failover del cluster `sample-cluster`, specificando che `sample-cluster-instance` deve essere promosso al ruolo primario. Annota il valore `"IsClusterWriter": true` nell'output.

Per Linux, macOS o Unix:

```
aws docdb failover-db-cluster \  
  --db-cluster-identifier sample-cluster \  
  --target-db-instance-identifier sample-cluster-instance
```

Per Windows:

```
aws docdb failover-db-cluster ^  
  --db-cluster-identifier sample-cluster ^  
  --target-db-instance-identifier sample-cluster-instance
```

L'aspetto dell'output di questa operazione è simile al seguente (formato JSON).

```
{  
  "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-ABCDEFGHIJKLMNQRSTUWXYZ"
}
```

}

Ritardo di replica

Il ritardo di replica è in genere pari o inferiore a 50 ms. I motivi più comuni per un aumento del ritardo di replica sono:

- Una velocità di scrittura elevata sul primario che fa sì che le repliche di lettura rimangano indietro rispetto al primario.
- Contention sulle repliche di lettura tra query di lunga durata (ad esempio, scansioni sequenziali di grandi dimensioni, query di aggregazione) e replica in scrittura in entrata.
- Numero molto elevato di query simultanee sulle repliche di lettura.

Per ridurre al minimo il ritardo di replica, prova le seguenti tecniche di risoluzione dei problemi:

- Se si dispone di una velocità di scrittura elevata o di un utilizzo elevato della CPU, si consiglia di ridimensionare le istanze nel cluster.
- Se sono presenti query di lunga durata sulle repliche di lettura e aggiornamenti molto frequenti ai documenti sottoposti a query, prendere in considerazione la possibilità di modificare le query di lunga durata o eseguirle con la replica primaria/scrittura per evitare contese sulle repliche di lettura.
- Se esiste un numero molto elevato di query simultanee o un elevato utilizzo della CPU solo nelle repliche di lettura, un'altra opzione è ridimensionare il numero di repliche di lettura per distribuire il carico di lavoro.
- Poiché il ritardo di replica è il risultato dell'elevato throughput di scrittura e di query di lunga durata, si consiglia di risolvere il ritardo di replica utilizzando la metrica `dbClusterReplicaLAGMaximumCW` in combinazione con il logger di query lento `writeThroughput/writeIOPS` Parametri di

In generale, è consigliabile che tutte le repliche siano dello stesso tipo di istanza, in modo che un failover del cluster non provochi un deterioramento delle prestazioni.

Se si sceglie tra scaling up e scaling out (ad esempio sei istanze più piccole rispetto a tre istanze più grandi), generalmente consigliamo di provare a scalare prima (istanze più grandi) prima di eseguire il ridimensionamento, poiché si otterrà una buffer cache più grande per istanza DB.

In modo proattivo, è necessario impostare un allarme di ritardo di replica e impostare la sua soglia su un valore che si ritiene sia il limite superiore per quanto siano lontani (o «obsoleti») i dati sulle istanze di replica prima che inizino a influenzare la funzionalità dell'applicazione. In generale, consigliamo di

superare la soglia di ritardo di replica per diversi punti dati prima di allarmarsi, a causa di carichi di lavoro transitori.

Note

Inoltre, si consiglia di impostare un altro allarme per i ritardi di replica che superano i 10 secondi. Se si supera questa soglia per più punti dati, si consiglia di aumentare le istanze o ridurre il throughput di scrittura sull'istanza principale.

Gestione degli indici Amazon DocumentDB

Creazione di indici Amazon DocumentDB

La creazione di indici in Amazon DocumentDB richiede l'adozione di una serie di decisioni:

- Quanto velocemente deve essere completato?
- La raccolta può essere inaccessibile durante la compilazione?
- Quanta potenza di calcolo di un'istanza può essere allocata alla build?
- Che tipo di indice deve essere creato?

Questa sezione ti aiuta a rispondere a queste domande e fornisce i comandi e gli esempi di monitoraggio per creare un indice Amazon DocumentDB sulla tua raccolta di cluster basata su istanze.

Linee guida

Le seguenti linee guida includono limiti di base e compromessi di configurazione per la creazione di nuovi indici:

- Supporto della versione di Amazon DocumentDB - Mentre l'indicizzazione a singolo worker è supportata su tutte le versioni di Amazon DocumentDB, l'indicizzazione di più worker è supportata solo nelle versioni 4.0 e 5.0 di Amazon DocumentDB.
- Compromesso in termini di prestazioni: l'aumento del numero di lavoratori nel processo di creazione dell'indice aumenta l'utilizzo della CPU e l'IO di lettura sull'istanza principale del database Amazon DocumentDB. Le risorse necessarie per creare un nuovo indice non saranno disponibili per il carico di lavoro in esecuzione.

- Cluster elastici: l'indicizzazione parallela non è supportata sui cluster elastici di Amazon DocumentDB.
- Numero massimo di lavoratori: il numero massimo di worker che è possibile configurare dipende dalla dimensione dell'istanza principale nel cluster di database. È la metà del numero totale di vCPU sull'istanza principale del cluster di database. Ad esempio, è possibile eseguire un massimo di 32 worker su un'istanza db.r6g.16xlarge con 64 vCPU.

Note

I worker paralleli non sono supportati su classi di istanze 2xlarge e inferiori.

- Numero minimo di lavoratori: il numero minimo di lavoratori che è possibile configurare è uno. L'impostazione predefinita per la creazione di indici su cluster basati su istanze è di due worker. Tuttavia, è possibile ridurre il numero di lavoratori a uno utilizzando l'opzione «worker threads». Questo eseguirà il processo con un solo lavoratore.
- Compressione dell'indice: Amazon DocumentDB non supporta la compressione degli indici. Le dimensioni dei dati per gli indici potrebbero essere maggiori rispetto a quando utilizzi altre opzioni.
- Indicizzazione di più raccolte: metà delle vCPU sull'istanza principale del cluster di database può essere utilizzata per i lavoratori configurati che eseguono la creazione di indici su più raccolte.
- Tipi di indice: consulta [questo post di blog](#) per una spiegazione completa dei tipi di indice supportati su Amazon DocumentDB.

Nozioni di base

Per avviare la creazione dell'indice su una raccolta, usa il `createIndexes` comando. Per impostazione predefinita, il comando eseguirà due worker paralleli che aumentano di due volte la velocità del processo di creazione dell'indice.

Ad esempio, il seguente processo di comando dimostra come creare un indice per il campo «user_name» in un documento e aumentare la velocità del processo di indicizzazione a quattro worker:

1. Crea indici utilizzando due worker paralleli sul cluster:

```
db.runCommand({"createIndexes":"test","indexes":[{"key":{"user_name":1},  
"name":"username_idx"}]})
```

2. Per ottimizzare la velocità del processo di creazione dell'indice, è possibile specificare il numero di worker utilizzando l'opzione «worker threads» ("workers": <number>) nel comando.

```
db.runCommand createIndexes
```

Aumenta la velocità del processo a quattro lavoratori paralleli:

```
db.runCommand({"createIndexes":"test","indexes":[{"key": {"user_name":1},  
"name":"username_idx", "workers":4}]})
```

Note

Maggiore è il numero di lavoratori, più velocemente avanza la creazione dell'indice. Tuttavia, più aumenta il numero di lavoratori, maggiore è il carico sulle vCPU e sull'IO di lettura dell'istanza principale. Assicurati che il cluster disponga di risorse sufficienti per gestire l'aumento del carico di lavoro senza compromettere gli altri carichi di lavoro.

Indicizzazione dello stato di avanzamento

Il processo di creazione dell'indice funziona iniziando, scansionando le raccolte, ordinando le chiavi e, infine, inserendo le chiavi tramite un generatore di indici. Il processo prevede fino a sei fasi se viene eseguito in primo piano e fino a nove fasi quando viene eseguito in background. È possibile visualizzare le metriche di stato come la percentuale di completamento, il numero totale di blocchi di archiviazione scansionati, le chiavi ordinate e le chiavi inserite fase per fase.

Monitora l'avanzamento del processo di indicizzazione utilizzando il `db.currentOp()` comando nella shell mongo. Un completamento al 100% dell'ultima fase mostra che tutti gli indici sono stati creati con successo:

```
db.currentOp({"command.createIndexes": { $exists : true } })
```

Tipi di compilazione dell'indice

I quattro tipi di build di indici sono:

- **Foreground**: la build dell'indice in primo piano blocca tutte le altre operazioni del database fino alla creazione dell'indice. La build in primo piano di Amazon DocumentDB è composta da cinque fasi.
- **Foreground (unique)**: le build di indici in primo piano a documento singolo (univoco) bloccano altre operazioni di database, come le normali compilazioni in primo piano. A differenza della build di

base in primo piano, la build unica utilizza una fase aggiuntiva (ordinamento delle chiavi 2) per cercare le chiavi duplicate. La build in primo piano (unica) è composta da sei fasi.

- **Sfondo:** la creazione dell'indice in background consente l'esecuzione in primo piano di altre operazioni del database durante la creazione dell'indice. La build in background di Amazon DocumentDB è composta da otto fasi.
- **Background (unico):** le build di indici in background a documento singolo (univoco) consentono l'esecuzione di altre operazioni del database in primo piano durante la creazione dell'indice. A differenza della build di base in background, la build unica utilizza una fase aggiuntiva (ordinamento delle chiavi 2) per cercare le chiavi duplicate. La build in background (unica) è composta da nove fasi.

Fasi di creazione dell'indice

Stage	Primo piano	Primo piano (unico)	Contesto	Sfondo (unico)
Inizializzazione	1	1	1	1
indice di costruzione: inizializzazione	2	2	2	2
indice di costruzione: scansione della raccolta	3	3	3	3
indice dell'edificio: ordinamento delle chiavi 1	4	4	4	4
indice dell'edificio: ordinamento delle chiavi 2		5		5
indice di costruzione:	5	6	5	6

Stage	Primo piano	Primo piano (unico)	Contesto	Sfondo (unico)
inserimento di chiavi				
convalida: indice di scansione			6	7
convalida: ordinamento delle tuple			7	8
convalida: scansione della raccolta			8	9

- **inizializzazione: createIndex** sta preparando il generatore di indici. Questa fase dovrebbe essere molto breve.
- **building index: inizializzazione** - Il generatore di indici si sta preparando a creare l'indice. Questa fase dovrebbe essere molto breve.
- **building index: scanning collection** - Il generatore di indici sta eseguendo una scansione della raccolta per raccogliere le chiavi dell'indice. L'unità di misura è «blocchi».

Note

Se più di un worker è configurato per la creazione dell'indice, questo viene visualizzato in questa fase. La fase di «scansione della raccolta» è l'unica fase che utilizza più worker durante il processo di creazione dell'indice. Tutte le altre fasi mostreranno un solo lavoratore.

- **indice di ordinamento: chiavi di ordinamento 1** - Il generatore di indici sta ordinando le chiavi dell'indice raccolte. L'unità di misura è «chiavi».
- **building index: sorting keys 2** - Il generatore di indici sta ordinando le chiavi di indice raccolte che corrispondono a tuple morte. Questa fase esiste solo per la creazione di indici unici. L'unità di misura è la «chiave».

- **building index:** inserimento di chiavi - Il generatore di indici inserisce le chiavi dell'indice nel nuovo indice. L'unità di misura è «chiavi».
- **convalida:** indice di scansione - CreateIndex sta scansionando l'indice per trovare le chiavi che devono essere convalidate. L'unità di misura è «blocchi».
- **convalida:** ordinamento delle tuple - CreateIndex sta ordinando l'output della fase di scansione dell'indice.
- **convalida:** scansione della raccolta - CreateIndex sta scansionando la raccolta per convalidare le chiavi dell'indice trovate nelle due fasi precedenti. L'unità di misura è «blocchi».

Esempio di output di compilazione dell'indice

Nell'esempio di output riportato di seguito (creazione dell'indice in primo piano), viene mostrato lo stato della creazione dell'indice. Il campo «msg» riassume l'avanzamento della compilazione indicando la fase e la percentuale di completamento della build. Il campo «workers» indica il numero di lavoratori utilizzati durante quella fase della creazione dell'indice. Il campo «avanzamento» mostra i numeri effettivi utilizzati per calcolare la percentuale di completamento.

Note

I campi «currentIndexBuildName», «msg» e «progress» non sono supportati su Amazon DocumentDB versione 4.0.

```
{
  "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
}
```

Gestione della compressione dei documenti a livello di raccolta

La compressione dei documenti a livello di raccolta di Amazon DocumentDB ti consente di ridurre i costi di storage e di I/O comprimendo i documenti nelle tue raccolte. Puoi abilitare la compressione dei documenti a livello di raccolta e visualizzare le metriche di compressione in base alle esigenze misurando i guadagni in termini di spazio di archiviazione tramite metriche di compressione come la dimensione di archiviazione dei documenti compressi e lo stato della compressione. Amazon DocumentDB utilizza l'algoritmo di compressione LZ4 per comprimere i documenti.

Linee guida

Le seguenti linee guida si applicano alla compressione dei documenti a livello di raccolta:

- La compressione dei documenti è disattivata per impostazione predefinita
- La compressione dei documenti non può essere applicata alle raccolte esistenti.
- La compressione dei documenti è supportata solo su Amazon DocumentDB versione 5.0 e successive.
- Amazon DocumentDB comprime solo documenti di dimensioni pari o superiori a 2 KB.

Attivazione della compressione dei documenti

Abilita la compressione dei documenti durante la creazione di una raccolta su Amazon DocumentDB utilizzando il `db.createCollection()` metodo:

```
db.createCollection( sample_collection,{
  storageEngine : {
    documentDB: {
      compression:{
        enable: <true | false>
      }
    }
  }
})
```

Monitoraggio della compressione dei documenti

Puoi verificare se una raccolta è compressa e calcolarne il rapporto di compressione come segue.

Visualizza le statistiche di compressione eseguendo il `db.collection.stats()` comando `db.printCollectionStats()` or dalla shell mongo. L'output mostra le dimensioni originali e le dimensioni compresse che è possibile confrontare per analizzare i vantaggi in termini di spazio di archiviazione derivanti dalla compressione dei documenti. In questo esempio, vengono mostrate le statistiche per una raccolta denominata «sample_collection»:

```
db.sample_collection.stats(1024*1024)

{
  "ns" : "test.sample_collection",
  "count" : 1000000,
  "size" : 3906.3,
  "avgObjSize" : 4096,
  "storageSize" : 1953.1,
  compression:{
    "enabled" : true,
    "threshold" : 2032
  }
  ...
}
```

- `size` - La dimensione originale della raccolta di documenti.
- `avgObjSize`- La dimensione media del documento prima della compressione è arrotondata al primo decimale. L'unità di misura è il byte.
- `StorageSize`: la dimensione di archiviazione della raccolta dopo la compressione. L'unità di misura è il byte.

Visualizzazione Amazon DocumentDB

Ogni tipo di risorsa Amazon DocumentDB ha tipi specifici di eventi che possono essere associati ad esso. È possibile utilizzare l'AWS CLI `describe-event-categories` operazione per visualizzare la mappatura tra i tipi di evento e i tipi di risorse Amazon DocumentDB.

Parametri

- **--source-type**—Opzionale. Utilizzare il parametro `--source-type` per visualizzare le categorie di eventi per un determinato tipo di origine. Di seguito sono elencati i valori consentiti:
 - `db-cluster`
 - `db-instance`
 - `db-parameter-group`
 - `db-security-group`
 - `db-cluster-snapshot`
- **--filters**—Opzionale. Per visualizzare le categorie di eventi solo per Amazon DocumentDB, utilizza il filtro `--filter Name=engine,Values=docdb`.

Example

Il codice seguente elenca le categorie di eventi associati ai cluster.

Per Linux, macOS o Unix:

```
aws docdb describe-event-categories \  
  --filter Name=engine,Values=docdb \  
  --source-type db-cluster
```

Per Windows:

```
aws docdb describe-event-categories ^  
  --filter Name=engine,Values=docdb ^  
  --source-type db-cluster
```

L'aspetto dell'output di questa operazione è simile al seguente (formato JSON).

```
{  
  "EventCategoriesMapList": [  
    {
```

```

        "EventCategories": [
            "notification",
            "failure",
            "maintenance",
            "failover"
        ],
        "SourceType": "db-cluster"
    }
]
}

```

Il codice seguente elenca le categorie di eventi associate a ciascun tipo di origine Amazon DocumentDB.

```
aws docdb describe-event-categories
```

L'aspetto dell'output di questa operazione è simile al seguente (formato JSON).

```

{
  "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"
      ]
    }
  ]
}
```

Visualizzazione Amazon DocumentDB

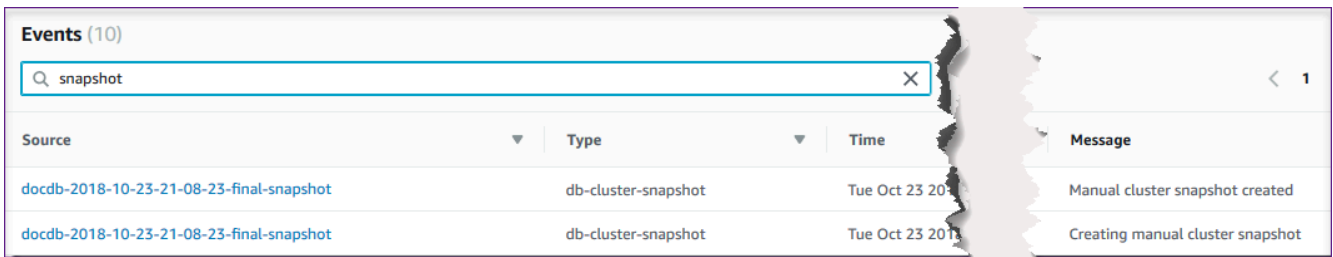
Puoi recuperare gli eventi delle risorse Amazon DocumentDB [Puoi anche recuperare eventi per le risorse AmazonAWS CLI DocumentDB DescribeEventsAmazon DocumentDB](#) Se utilizzi laAWS CLI o l'API Amazon DocumentDB per visualizzare gli eventi, puoi recuperare gli eventi fino agli ultimi 14 giorni.

Using the AWS Management Console

Per visualizzare tutti gli eventi dell'istanza Amazon DocumentDB

1. [Accedere allaAWS Management Console e aprire la console Amazon DocumentDB](https://console.aws.amazon.com/docdb) <https://console.aws.amazon.com/docdb>
2. Nel pannello di navigazione selezionare Events (Eventi). Gli eventi disponibili sono indicati all'interno di un elenco.

- Utilizza l'elenco Filter (Filtra) per filtrare gli eventi per tipo. Inserisci un termine nella casella di testo per filtrare ulteriormente i risultati. Ad esempio, il seguente screenshot mostra il filtraggio di tutti gli eventi Amazon DocumentDB



Source	Type	Time	Message
docdb-2018-10-23-21-08-23-final-snapshot	db-cluster-snapshot	Tue Oct 23 2018	Manual cluster snapshot created
docdb-2018-10-23-21-08-23-final-snapshot	db-cluster-snapshot	Tue Oct 23 2018	Creating manual cluster snapshot

Using the AWS CLI

Per visualizzare tutti gli eventi dell'istanza Amazon DocumentDB

Puoi visualizzare tutti gli eventi [dell'AWS CLI](#) istanza Amazon DocumentDB `--duration 10080`

```
aws docdb describe-events --duration 10080
```

Filtraggio per gli eventi Amazon DocumentDB

Per visualizzare eventi Amazon DocumentDB specifici, utilizza l'`describe-events` operazione con i seguenti parametri.

Parametri

- `--filter`**—Necessario per limitare i valori restituiti agli eventi Amazon DocumentDB. **Name=engine, Values=docdb** Da utilizzare per filtrare tutti gli eventi solo per Amazon DocumentDB.
- `--source-identifier`**—Opzionale. L'identificatore dell'origine dell'evento in base a cui vengono restituiti gli eventi. Se omissso, nei risultati sono inclusi gli eventi provenienti da tutte le origini.
- `--source-type`**—Facoltativo, a meno che non `--source-identifier` venga fornito, quindi obbligatorio. Se viene fornito `--source-identifier`, `--source-type` deve concordare con il tipo di `--source-identifier`. Di seguito sono elencati i valori consentiti:
 - `db-cluster`
 - `db-instance`
 - `db-parameter-group`

- db-security-group
- db-cluster-snapshot

Nell'esempio seguente sono elencati tutti gli eventi Amazon DocumentDB

```
aws docdb describe-events --filters Name=engine,Values=docdb
```

L'aspetto dell'output di questa operazione è simile al seguente (formato JSON).

```
{
  "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"
      ]
    }
  ]
}
```



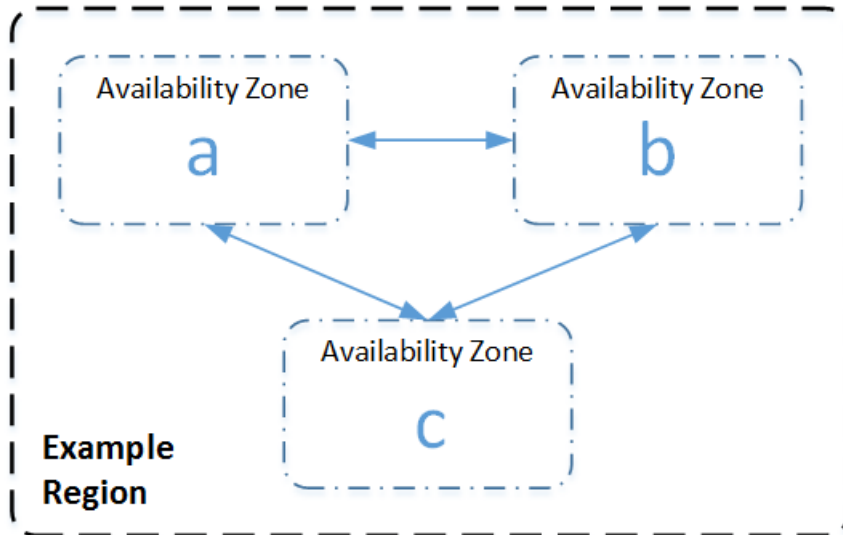
```
    ]  
  }  
]  
}
```

Per ulteriori informazioni, consulta [Controllo degli eventi di Amazon DocumentDB](#).

Scelta di regioni e zone di disponibilità

Le risorse di cloud computing Amazon sono ospitate in più ubicazioni in tutto il mondo. Queste sedi sono costituite da zone di Regioni AWS disponibilità. Ciascuna Regione AWS è un'area geografica separata. Ciascuna regione presenta più località isolate, conosciute come zone di disponibilità. Amazon DocumentDB offre la possibilità di collocare risorse, come istanze e dati, in più posizioni. Le risorse non vengono replicate tra di loro Regioni AWS a meno che tu non lo faccia in modo specifico.

Amazon gestisce data center avanzati e ad alta disponibilità. Anche se rari, i guasti che compromettono la disponibilità di istanze nella stessa ubicazione possono verificarsi. Se ospiti tutte le istanze in un'unica ubicazione colpita da tale guasto, nessuna di esse risulterà disponibile. Il diagramma seguente mostra una Regione AWS con tre zone di disponibilità.



È importante ricordare che ogni regione è indipendente. Qualsiasi attività di Amazon DocumentDB avviata (ad esempio, la creazione di istanze o l'elenco delle istanze disponibili) viene eseguita solo nell'impostazione predefinita corrente. Regione AWS Puoi modificare la regione predefinita nella console impostando la variabile di ambiente EC2_REGION. In alternativa, puoi sostituirla utilizzando il parametro `--region` nell'AWS CLI. Per ulteriori informazioni, consulta [Configurazione, in particolare](#)

[AWS Command Line Interface, delle](#) sezioni sulle variabili di ambiente e sulle opzioni della riga di comando.

Quando crei un cluster utilizzando la console Amazon DocumentDB e scegli di creare una replica in una zona di disponibilità diversa, Amazon DocumentDB crea due istanze. Crea l'istanza primaria in una zona di disponibilità e l'istanza di replica in un'altra zona di disponibilità. Il volume cluster viene sempre replicato nelle tre zone di disponibilità.

Per creare o utilizzare un'istanza Amazon DocumentDB in una specifica istanza Regione AWS, utilizza l'endpoint di servizio regionale corrispondente.

Disponibilità nelle regioni

Amazon DocumentDB è disponibile nelle seguenti AWS regioni.

Regioni supportate da Amazon DocumentDB

Nome della regione	Regione	Zone di disponibilità (elaborazione)
Stati Uniti orientali (Ohio)	us-east-2	3
Stati Uniti orientali (Virginia settentrionale)	us-east-1	6
US West (Oregon)	us-west-2	4
Sud America (São Paulo)	sa-east-1	3
Asia Pacifico (Hong Kong)	ap-east-1	3
Asia Pacific (Hyderabad)	ap-south-2	3
Asia Pacifico (Mumbai)	ap-south-1	3

Nome della regione	Regione	Zone di disponibilità (elaborazione)
Asia Pacifico (Seul)	ap-northeast-2	4
Asia Pacifico (Singapore)	ap-southeast-1	3
Asia Pacifico (Sydney)	ap-southeast-2	3
Asia Pacifico (Tokyo)	ap-northeast-1	3
Canada (Centrale)	ca-central-1	3
Regione Cina (Pechino)	cn-north-1	3
Cina (Ningxia)	cn-northwest-1	3
Europa (Francoforte)	eu-central-1	3
Europa (Irlanda)	eu-west-1	3
Europa (Londra)	eu-west-2	3
Europa (Milano)	eu-south-1	3
Europa (Parigi)	eu-west-3	3
Medio Oriente (Emirati Arabi Uniti)	me-central-1	3
AWS GovCloud (Stati Uniti occidentali)	us-gov-west-1	3
AWS GovCloud (Stati Uniti orientali)	us-gov-east-1	3

Per impostazione predefinita, il fuso orario per un cluster Amazon DocumentDB è Universal Time Coordinated (UTC).

Per ulteriori informazioni su come trovare gli endpoint di connessione per i cluster e le istanze in una specifica regione, consulta [Comprendere gli endpoint di Amazon DocumentDB](#).

Gestione dei gruppi di parametri del cluster Amazon DocumentDB

Puoi gestire la configurazione del motore Amazon DocumentDB utilizzando i parametri in un gruppo di parametri del cluster. Un gruppo di parametri del cluster è una raccolta di valori di configurazione di Amazon DocumentDB che semplificano la gestione dei parametri dei cluster Amazon DocumentDB. I gruppi di parametri del cluster fungono da container per i valori di configurazione del motore applicati a tutte le istanze nel cluster.

In questa sezione viene descritto come creare, visualizzare e modificare i gruppi di parametri del cluster. Viene inoltre illustrato come puoi individuare a quale gruppo di parametri è associato a un determinato cluster.

Argomenti

- [Descrizione dei gruppi di parametri del cluster Amazon DocumentDB](#)
- [Creazione di gruppi di parametri del cluster Amazon DocumentDB](#)
- [Modifica dei gruppi di parametri del cluster Amazon DocumentDB](#)
- [Modifica dei cluster Amazon DocumentDB per utilizzare gruppi di parametri di cluster personalizzati](#)
- [Copia dei gruppi di parametri del cluster Amazon DocumentDB](#)
- [Reimpostazione dei gruppi di parametri del cluster Amazon DocumentDB](#)
- [Eliminazione di gruppi di parametri del cluster Amazon DocumentDB](#)
- [Riferimento ai parametri del cluster Amazon DocumentDB](#)

Descrizione dei gruppi di parametri del cluster Amazon DocumentDB

Un gruppo di parametri del default cluster viene creato automaticamente quando si crea il primo cluster Amazon DocumentDB in una nuova regione o si utilizza un nuovo motore. I cluster successivi, creati nella stessa regione e con la stessa versione del motore, vengono creati con il default gruppo di parametri del cluster.

Argomenti

- [Descrizione dei dettagli di un gruppo di parametri del cluster Amazon DocumentDB](#)
- [Determinazione del gruppo di parametri di un cluster Amazon DocumentDB](#)


Descrizione dei dettagli di un gruppo di parametri del cluster Amazon DocumentDB

Per descrivere i dettagli di un determinato gruppo di parametri del cluster, attieniti alla procedura seguente utilizzando la AWS Management Console o AWS Command Line Interface (AWS CLI).

Using the AWS Management Console

1. [Accedi a e apri AWS Management Console la console Amazon DocumentDB all'indirizzo `https://console.aws.amazon.com/docdb`.](https://console.aws.amazon.com/docdb)
2. Nel riquadro di navigazione scegliere Parameter groups (Gruppi di parametri).

Tip

Se il riquadro di navigazione non viene visualizzato sul lato sinistro della schermata, scegliere l'icona del menu () nell'angolo in alto a sinistra della pagina.

3. Nel riquadro Parameter groups (Gruppi di parametri), selezionare il gruppo di parametri del cluster di cui si desidera visualizzare i dettagli.
4. La pagina risultante mostra i parametri, l'attività recente e i tag del gruppo di parametri.
 - In Cluster parameters (Parametri cluster) puoi vedere il nome, il valore corrente, i valori consentiti, il tipo di dati e la descrizione del parametro e specifica se il parametro è modificabile. Puoi modificare i singoli parametri selezionando il parametro e scegliendo Edit (Modifica) nella sezione Cluster parameters (Parametri cluster). Per ulteriori informazioni, consulta [Modifica dei parametri del cluster Amazon DocumentDB](#).
 - In Recent events (Eventi recenti), puoi vedere gli eventi più recenti per questo gruppo di parametri. Puoi filtrare questi eventi utilizzando la barra di ricerca in questa sezione. Per ulteriori informazioni, consulta [Gestione degli eventi Amazon DocumentDB](#).
 - In Tags (Tag) puoi visualizzare i tag di questo gruppo di parametri del cluster. Puoi aggiungere o rimuovere i tag scegliendo Edit (Modifica) nella sezione Tags (Tag). Per ulteriori informazioni, consulta [Etichettatura delle risorse Amazon DocumentDB](#).

Using the AWS CLI

Puoi utilizzare il `describe-db-cluster-parameter-groups` AWS CLI comando per visualizzare Amazon Resource Name (ARN), famiglia, descrizione e nome di un singolo gruppo di parametri del cluster o di tutti i gruppi di parametri del cluster di cui disponi per Amazon DocumentDB. Inoltre puoi utilizzare il comando `describe-db-cluster-parameters` dell'AWS CLI per visualizzare i parametri e i relativi dettagli all'interno di un singolo gruppo di parametri del cluster.

- **--describe-db-cluster-parameter-groups**— Per visualizzare un elenco di tutti i gruppi di parametri del cluster e i relativi dettagli.
 - **--db-cluster-parameter-group-name**— Facoltativo. Il nome del gruppo di parametri del cluster da descrivere. Se questo parametro viene omesso, vengono descritti tutti i gruppi di parametri del cluster.
- **--describe-db-cluster-parameters**— Per elencare tutti i parametri all'interno di un gruppo di parametri e i relativi valori.
 - **--db-cluster-parameter-group name**: obbligatorio. Il nome del gruppo di parametri del cluster da descrivere.

Example

Il codice seguente elenca fino a 100 gruppi di parametri del cluster con relativi ARN, famiglia, descrizione e nome.

```
aws docdb describe-db-cluster-parameter-groups
```

L'aspetto dell'output di questa operazione è simile al seguente (formato JSON).

```
{
  "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

Il codice seguente elenca l'ARN, la famiglia, la descrizione e il nome per `sample-parameter-group`.

Per Linux, macOS o Unix:

```

aws docdb describe-db-cluster-parameter-groups \
    --db-cluster-parameter-group-name sample-parameter-group

```

Per Windows:

```

aws docdb describe-db-cluster-parameter-groups ^
    --db-cluster-parameter-group-name sample-parameter-group

```

L'aspetto dell'output di questa operazione è simile al seguente (formato JSON).

```

{
    "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

Il codice seguente elenca i valori dei parametri in `sample-parameter-group`.

Per Linux, macOS o Unix:

```
aws docdb describe-db-cluster-parameters \  
  --db-cluster-parameter-group-name sample-parameter-group
```

Per Windows:

```
aws docdb describe-db-cluster-parameters ^  
  --db-cluster-parameter-group-name sample-parameter-group
```

L'aspetto dell'output di questa operazione è simile al seguente (formato JSON).

```
{  
  "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"  
    }  
  ]  
}
```



```
}
```

Determinazione del gruppo di parametri di un cluster Amazon DocumentDB

Per determinare a quale gruppo di parametri è associato un determinato cluster, attieniti alla procedura seguente utilizzando la AWS Management Console o l'AWS CLI.

Using the AWS Management Console

1. [Accedi a e apri AWS Management Console la console Amazon DocumentDB all'indirizzo https://console.aws.amazon.com/docdb](https://console.aws.amazon.com/docdb).
2. Nel pannello di navigazione a sinistra, seleziona Cluster.
3. Dall'elenco dei cluster seleziona il nome del cluster desiderato.
4. La pagina risultante mostra i dettagli del cluster selezionato. Scorri verso il basso fino a Cluster details (Dettagli del cluster). Nella parte inferiore della sezione, individua il nome del gruppo di parametri sotto Cluster parameter group (Gruppo di parametri del cluster).

Cluster details

Configurations and status

ARN

arn:aws:rds: [redacted] :cluster:sample-cluster

Cluster identifier

sample-cluster (available)

Cluster creation time

1/10/2020, 2:13:38 PM UTC-8

Cluster endpoint

sample-cluster. [redacted]
[redacted].docdb.amazonaws.com

Reader endpoint

sample-cluster. [redacted]
[redacted].docdb.amazonaws.com

Master username

[redacted]

Port

27017

Status

available

Cluster parameter group

sample-parameter-group

Deletion protection

Enabled

CloudWatch logs enabled

None

Using the AWS CLI

Il seguente codice dell'AWS CLI determina il gruppo di parametri che regola il cluster `sample-cluster`.

```
aws docdb describe-db-clusters \  
  --db-cluster-identifier sample-cluster \  
  --query 'DBClusters[*].[DBClusterIdentifier,DBClusterParameterGroup]'
```

L'aspetto dell'output di questa operazione è simile al seguente (formato JSON).

```
[  
  [  
    "sample-cluster",  
    "sample-parameter-group"  
  ]  
]
```

Creazione di gruppi di parametri del cluster Amazon DocumentDB

Gruppi di parametri di cluster predefiniti come `default.docdb5.0default.docdb4.0`, `default.docdb3.6`, vengono creati quando crei un cluster con una nuova versione del motore e in una nuova regione. I cluster successivi creati in questa regione e con la stessa versione del motore ereditano il gruppo di parametri del default cluster. Una volta creati, i gruppi di default parametri non possono essere eliminati o rinominati. Puoi modificare il comportamento del motore delle istanze del cluster creando un gruppo di parametri personalizzato con valori di parametri preferiti e collegandolo al tuo cluster Amazon DocumentDB.

La seguente procedura ti guida nella creazione di un gruppo di parametri del cluster personalizzato. Quindi puoi [modificare i parametri all'interno del gruppo](#).

Note

Dopo aver creato un gruppo di parametri del cluster, devi attendere almeno 5 minuti prima di poterlo utilizzare. Ciò consente ad Amazon DocumentDB di completare completamente l'creazione prima che il gruppo di parametri del cluster venga utilizzato per un nuovo cluster. Puoi utilizzare la AWS Management Console o l'operazione `describe-db-cluster-parameter-groups` dell'AWS CLI per verificare che il gruppo di parametri del

cluster sia stato creato. Per ulteriori informazioni, consulta [Descrizione dei gruppi di parametri del cluster Amazon DocumentDB](#).

Using the AWS Management Console

Per creare un gruppo di parametri del cluster

1. [Accedi a e apri AWS Management Console la console Amazon DocumentDB all'indirizzo `https://console.aws.amazon.com/docdb`](https://console.aws.amazon.com/docdb).
2. Nel riquadro di navigazione scegliere Parameter groups (Gruppi di parametri).

Tip

Se il riquadro di navigazione non viene visualizzato sul lato sinistro della schermata, scegliere l'icona del menu (☰) nell'angolo in alto a sinistra della pagina.

3. Nel riquadro Cluster parameter groups (Gruppi di parametri del cluster), scegliere Create (Crea).
4. Nel riquadro Create cluster parameter group (Crea gruppo di parametri del cluster) immettere quanto segue:
 - a. Nome del gruppo: inserisci un nome per il gruppo di parametri del cluster. Ad esempio, `sample-parameter-group`. I gruppi di parametri del cluster hanno i seguenti vincoli di denominazione:
 - La lunghezza è compresa tra 1 e 255 caratteri alfanumerici.
 - Il primo carattere deve essere una lettera.
 - Non può terminare con un trattino o contenere due trattini consecutivi.
 - b. Descrizione: fornire una descrizione per questo gruppo di parametri del cluster.
5. Per creare il gruppo di parametri del cluster, scegli Create (Crea). Per annullare l'operazione, scegli Cancel (Annulla).
6. Dopo aver scelto Create (Crea), nella parte superiore della pagina viene visualizzato il testo seguente per verificare che il gruppo di parametri del cluster sia stato creato:

```
Successfully created cluster parameter group 'sample-parameter-group'.
```

Using the AWS CLI

Per creare un nuovo gruppo di parametri del cluster per i cluster Amazon DocumentDB 4.0, utilizza l'AWS CLI `create-db-cluster-parameter-group` operazione con i seguenti parametri:

- **--db-cluster-parameter-group-name**— Il nome del gruppo di parametri del cluster personalizzato. Ad esempio, `sample-parameter-group`.
- **--db-cluster-parameter-group-family**— La famiglia di gruppi di parametri del cluster utilizzata come modello per il gruppo di parametri di cluster personalizzato. Al momento, il valore deve essere `docdb4.0`.
- **--description**— La descrizione fornita dall'utente per questo gruppo di parametri del cluster. L'esempio seguente utilizza `"Custom docdb4.0 parameter group"`.

Per Linux, macOS o Unix:

Example

```
aws docdb create-db-cluster-parameter-group \  
  --db-cluster-parameter-group-name sample-parameter-group \  
  --db-parameter-group-family docdb4.0 \  
  --description "Custom docdb4.0 parameter group"
```

Per Windows:

```
aws docdb create-db-cluster-parameter-group ^  
  --db-cluster-parameter-group-name sample-parameter-group ^  
  --db-parameter-group-family docdb4.0 ^  
  --description "Custom docdb4.0 parameter group"
```

L'aspetto dell'output di questa operazione è simile al seguente (formato JSON).

```
{  
  "DBClusterParameterGroup": {  
    "DBClusterParameterGroupName": "sample-parameter-group",  
    "DBParameterGroupFamily": "docdb4.0",
```

```
    "Description": "Custom docdb4.0 parameter group",  
    "DBClusterParameterGroupArn": "sample-parameter-group-arn"  
  }  
}
```

Modifica dei gruppi di parametri del cluster Amazon DocumentDB

Questa sezione spiega come modificare un gruppo di parametri Amazon DocumentDB personalizzato. In Amazon DocumentDB, non è possibile modificare un gruppo di parametri del default cluster creato quando si crea per la prima volta un cluster con una nuova versione del motore in una nuova regione. Se il tuo cluster Amazon DocumentDB utilizza il gruppo di parametri del cluster predefinito e desideri modificare un valore al suo interno, devi prima [creare un nuovo gruppo di parametri](#) o [copiare un gruppo di parametri esistente](#), modificarlo e quindi applicare il gruppo di parametri modificato al cluster.

Completa i seguenti passaggi per modificare un gruppo di parametri del cluster personalizzato. La propagazione delle azioni di modifica potrebbe richiedere del tempo. Attendi che il gruppo di parametri del cluster modificato sia disponibile prima di collegarlo al cluster. Puoi utilizzare la AWS Management Console o l'operazione `describe-db-cluster-parameters` dell'AWS CLI per verificare che il gruppo di parametri del cluster sia stato modificato. Per ulteriori informazioni, consulta [Descrizione dei gruppi di parametri del cluster](#).

Using the AWS Management Console

Segui questi passaggi per modificare un gruppo di parametri Amazon DocumentDB personalizzato. Non puoi modificare un gruppo di parametri default. Se desideri modificare un valore nel gruppo di parametri default, puoi [copiare il gruppo di parametri del cluster predefinito](#), modificarlo e quindi applicare il gruppo di parametri modificato al cluster. Per ulteriori informazioni sull'applicazione dei gruppi di parametri al cluster, consulta [Modifica di un cluster Amazon DocumentDB](#).

Per modificare un gruppo di parametri del cluster personalizzato

1. [Accedi a e apri AWS Management Console la console Amazon DocumentDB all'indirizzo `https://console.aws.amazon.com/docdb`](https://console.aws.amazon.com/docdb).
2. Nel riquadro di navigazione sul lato sinistro della console scegli Parameter groups (Gruppi di parametri). Nell'elenco dei gruppi di parametri, scegli il nome del gruppo di parametri da modificare.

 Tip

Se il riquadro di navigazione non viene visualizzato sul lato sinistro della schermata, scegliere l'icona del menu (☰) nell'angolo in alto a sinistra della pagina.

3. Per ogni parametro nel gruppo di parametri che desideri modificare, procedi nel seguente modo:
 - a. Individua il parametro che vuoi modificare e verifica che sia modificabile controllando se è elencato come `true` nella colonna Modifiable (Modificabile).
 - b. Se è modificabile, seleziona il parametro e scegli Edit (Modifica) in alto a destra nella pagina della console.
 - c. Nella finestra di dialogo Modify **<parameter-name>** (Modifica), apporta le modifiche desiderate. Quindi scegli Modify cluster parameter (Modifica parametro del cluster) oppure scegli Cancel (Annulla) per annullare le modifiche.


Using the AWS CLI

Puoi modificare o modificare qualsiasi parametro modificabile in un gruppo ApplyMethod di parametri del cluster Amazon DocumentDB personalizzato utilizzando il `ParameterValue` `Description` AWS CLI. Non puoi apportare modifiche direttamente in un gruppo di parametri del cluster predefinito.

Per modificare i parametri di un gruppo di parametri del cluster personalizzato, utilizza l'operazione `modify-db-cluster-parameter-group` con i parametri seguenti.

- **--db-cluster-parameter-group-name**: obbligatorio. Il nome del gruppo di parametri del cluster che stai modificando.
- **--parameters**: obbligatorio. I parametri che stai modificando. Per un elenco dei parametri che si applicano a tutte le istanze in un cluster Amazon DocumentDB, consulta la [Riferimento ai parametri del cluster Amazon DocumentDB](#). Ogni voce del parametro deve includere:
 - **ParameterName**— Il nome del parametro che stai modificando.
 - **ParameterValue**— Il nuovo valore per questo parametro.

- **ApplyMethod**— Come si desidera applicare le modifiche a questo parametro. I valori consentiti sono `immediate` e `pending-reboot`.

 Note

I parametri con `ApplyType` per `static` devono avere `ApplyMethod` per `pending-reboot`.

Example - Modifica del valore di un parametro

In questo esempio, puoi elencare i valori dei parametri di `sample-parameter-group` e modificare il parametro `tls`. Quindi, dopo 5 minuti, puoi elencare di nuovo i valori dei parametri di `sample-parameter-group` per visualizzare i valori modificati.

1. Elenca i parametri e i relativi valori di `sample-parameter-group`.

Per Linux, macOS o Unix:

```
aws docdb describe-db-cluster-parameters \  
  --db-cluster-parameter-group-name sample-parameter-group
```

Per Windows:

```
aws docdb describe-db-cluster-parameters ^  
  --db-cluster-parameter-group-name sample-parameter-group
```

L'aspetto dell'output di questa operazione è simile al seguente (formato JSON).

```
{  
  "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. Modifica il parametro `tls` in modo che il valore sia `disabled`.

Non puoi modificare `ApplyMethod` perché `ApplyType` è `static`.

Per Linux, macOS o Unix:

```

aws docdb modify-db-cluster-parameter-group \
  --db-cluster-parameter-group-name sample-parameter-group \
  --parameters
  "ParameterName=tls,""ParameterValue=disabled,""ApplyMethod=pending-reboot

```

Per Windows:

```

aws docdb modify-db-cluster-parameter-group ^
  --db-cluster-parameter-group-name sample-parameter-group ^
  --parameters
  "ParameterName=tls,""ParameterValue=disabled,""ApplyMethod=pending-reboot

```

L'aspetto dell'output di questa operazione è simile al seguente (formato JSON).

```

{
  "DBClusterParameterGroupName": "sample-parameter-group"
}

```

3. Attendi almeno 5 minuti.

4. Elenca i valori dei parametri di `sample-parameter-group` per verificare che il parametro `tls` sia stato modificato.

Per Linux, macOS o Unix:

```
aws docdb describe-db-cluster-parameters \  
  --db-cluster-parameter-group-name sample-parameter-group
```

Per Windows:

```
aws docdb describe-db-cluster-parameters ^  
  --db-cluster-parameter-group-name sample-parameter-group
```

L'aspetto dell'output di questa operazione è simile al seguente (formato JSON).

```
{  
  "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"  
    }  
  ]  
}
```

Modifica dei cluster Amazon DocumentDB per utilizzare gruppi di parametri di cluster personalizzati

Quando crei un cluster Amazon DocumentDB, viene creato automaticamente un gruppo di `default.docdb4.0` parametri per quel cluster. Non è consentito modificare il gruppo di parametri `default`. Puoi invece modificare il tuo cluster Amazon DocumentDB per associarvi un nuovo gruppo di parametri personalizzato.

Questa sezione spiega come modificare un cluster Amazon DocumentDB esistente per utilizzare un gruppo di parametri del cluster personalizzato utilizzando AWS Management Console and the AWS Command Line Interface (AWS CLI).

Using the AWS Management Console

Per modificare un cluster Amazon DocumentDB per utilizzare un nuovo gruppo di parametri di cluster non predefinito

1. Prima di iniziare, assicurati di aver creato un cluster Amazon DocumentDB e un gruppo di parametri del cluster. Vedere [Creazione di un cluster Amazon DocumentDB](#) e [Creazione di gruppi di parametri del cluster Amazon DocumentDB](#) per ulteriori istruzioni.
2. Dopo aver creato il gruppo di parametri del cluster, apri la console Amazon DocumentDB all'indirizzo. <https://console.aws.amazon.com/docdb> Nel riquadro di navigazione scegliere Clusters (Cluster) per aggiungere il nuovo gruppo di parametri a un cluster.
3. Scegliere il cluster a cui si desidera associare il gruppo di parametri. Scegliere Actions (Operazioni), quindi scegliere Modify (Modifica) per modificare il cluster.
4. In Cluster options (Opzioni cluster), scegliere il nuovo gruppo di parametri a cui si desidera associare il cluster.
5. Scegliere Continue (Continua) per visualizzare un riepilogo delle modifiche.
6. Dopo aver verificato le modifiche, è possibile applicarle immediatamente o durante la successiva finestra di manutenzione in Scheduling of modifications (Pianificazione delle modifiche).
7. Scegliere Modify cluster (Modifica cluster) per aggiornare il cluster con il nuovo gruppo di parametri.

Using the AWS CLI

Prima di iniziare, assicurati di aver creato un cluster Amazon DocumentDB e un gruppo di parametri del cluster. È possibile [creare un cluster Amazon DocumentDB](#) utilizzando l'AWS CLI `create-db-cluster` operazione. Puoi [creare un gruppo di parametri del cluster](#) utilizzando l'operazione `create-db-cluster-parameter-group` dell'AWS CLI.

Per aggiungere il nuovo gruppo di parametri cluster al cluster, utilizza l'operazione `modify-db-cluster` dell'AWS CLI con i parametri seguenti.

- `--db-cluster-identifier` — Il nome del cluster (ad esempio, `sample-cluster`).
- `--db-cluster-parameter-group-name` — Il nome del gruppo di parametri a cui desiderate associare il cluster (ad esempio, `sample-parameter-group`).

Example

```
aws docdb modify-db-cluster \  
  --db-cluster-identifier sample-cluster \  
  --db-cluster-parameter-group-name sample-parameter-group
```

L'aspetto dell'output di questa operazione è simile al seguente (formato JSON).

```
"DBCluster": {  
  "AvailabilityZones": [  
    "us-west-2c",  
    "us-west-2b",  
    "us-west-2a"  
  ],  
  "BackupRetentionPeriod": 1,  
  "DBClusterIdentifier": "sample-cluster",  
  "DBClusterParameterGroup": "sample-parameter-group",  
  "DBSubnetGroup": "default",  
  ...  
}
```

Copia dei gruppi di parametri del cluster Amazon DocumentDB

Puoi creare una copia di un gruppo di parametri del cluster in Amazon DocumentDB utilizzando AWS Management Console o il AWS Command Line Interface (AWS CLI).

Using the AWS Management Console

La procedura seguente ti guida nella creazione di un nuovo gruppo di parametri del cluster eseguendo una copia di un gruppo di parametri cluster esistente.

Per copiare un gruppo di parametri del cluster

1. [Accedi a e apri AWS Management Console la console Amazon DocumentDB all'indirizzo https://console.aws.amazon.com/docdb](https://console.aws.amazon.com/docdb).
2. Nel riquadro di navigazione scegliere Parameter groups (Gruppi di parametri).
3. Nel riquadro Cluster parameter groups (Gruppi di parametri del cluster), scegliere il nome del gruppo di parametri del cluster di cui si desidera visualizzare i dettagli.
4. Scegliere Actions (Operazioni), quindi scegliere Copy (Copia) per copiare il gruppo di parametri.
5. In Copy options (Opzioni copia), immettere un nome e una descrizione per il nuovo gruppo di parametri del cluster. Quindi scegliere Copy (Copia) per salvare le modifiche.

Using the AWS CLI

Per copiare un gruppo di parametri del cluster, utilizza l'operazione `copy-db-cluster-parameter-group` con i parametri seguenti.

- **--source-db-cluster-parameter-group-identifier**: obbligatorio. Il nome o l'Amazon Resource Name (ARN) del gruppo di parametri del cluster da copiare.

Se i gruppi di parametri del cluster di origine e di destinazione coincidono Regione AWS, l'identificatore può essere un nome o un ARN.

Se i gruppi di parametri del cluster di origine e di destinazione sono diversi Regioni AWS, l'identificatore deve essere un ARN.

- **--target-db-cluster-parameter-group-identifier**: obbligatorio. Il nome o l'ARN della copia del gruppo di parametri del cluster.

Vincoli:

- Non può essere null o vuoto.
- Deve contenere da 1 a 255 lettere, numeri o trattini.
- Il primo carattere deve essere una lettera.

- Non può terminare con un trattino o contenere due trattini consecutivi.
- **--target-db-cluster-parameter-group-description**: obbligatorio. Una descrizione per la copia del gruppo di parametri del cluster fornita dall'utente.

Example

Il codice seguente crea una copia di `sample-parameter-group`, denominandola `sample-parameter-group-copy`.

Per Linux, macOS o 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"
```

Per 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"
```

L'aspetto dell'output di questa operazione è simile al seguente (formato JSON).

```
{  
  "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"  
  }  
}
```

Reimpostazione dei gruppi di parametri del cluster Amazon DocumentDB

Puoi ripristinare alcuni o tutti i valori dei parametri di un gruppo di parametri del cluster Amazon DocumentDB ai valori predefiniti utilizzando AWS Management Console o the AWS Command Line Interface (AWS CLI) per reimpostare il gruppo di parametri del cluster.

Using the AWS Management Console

Atteniti alla seguente procedura per reimpostare alcuni o tutti i valori di un parametro di un gruppo di parametri del cluster ai valori predefiniti.

Per reimpostare i valori dei parametri di un gruppo di parametri del cluster

1. [Accedi a e apri AWS Management Console la console Amazon DocumentDB all'indirizzo `https://console.aws.amazon.com/docdb`.](https://console.aws.amazon.com/docdb)
2. Nel riquadro di navigazione sul lato sinistro della console scegli Parameter groups (Gruppi di parametri).
3. Nel riquadro Cluster parameter groups (Gruppi di parametri del cluster), scegliere il nome del gruppo di parametri del cluster da reimpostare.
4. Scegliere Actions (Operazioni), quindi scegliere Reset (Reimposta) per reimpostare il gruppo di parametri.
5. Nella pagina di conferma della reimpostazione del gruppo di parametri del cluster restituita, confermare che si desidera reimpostare i valori predefiniti di tutti i parametri del cluster per il gruppo di parametri. Quindi scegliere Reset (Reimposta) per reimpostare il gruppo di parametri. È anche possibile selezionare Cancel (Annulla) per annullare le modifiche.

Using the AWS CLI

Per reimpostare alcuni o tutti i valori di un parametro di un gruppo di parametri del cluster ai valori predefiniti, puoi utilizzare l'operazione `reset-db-cluster-parameter-group` con i parametri seguenti.

- **`--db-cluster-parameter-group-name`**: obbligatorio. Il nome del gruppo di parametri del cluster da reimpostare.
- **`--parameters`**— Facoltativo. Un elenco di `ParameterName` e `ApplyMethod` nel gruppo di parametri del cluster da ripristinare ai valori predefiniti. I parametri statici devono essere impostati su `pending-reboot` per essere applicati al successivo riavvio dell'istanza o quando

viene eseguita la richiesta `reboot-db-instance`. Devi chiamare `reboot-db-instance` per ogni istanza nel cluster a cui desideri applicare il parametro statico aggiornato.

Questo parametro e `--reset-all-parameters` sono reciprocamente esclusivi: puoi utilizzarne uno solo, non entrambi.

- **`--reset-all-parameters`** oppure **`--no-reset-all-parameters`** — Facoltativo. Specifica se ripristinare tutti i parametri (`--reset-all-parameters`) o solo alcuni (`--no-reset-all-parameters`) ai valori predefiniti. Il parametro `--reset-all-parameters` e `--parameters` sono reciprocamente esclusivi: puoi utilizzarne uno solo, non entrambi.

Quando reimposti l'intero gruppo, i parametri dinamici vengono aggiornati immediatamente. I parametri statici devono essere impostati su `pending-reboot` per essere applicati al successivo riavvio dell'istanza o quando viene eseguita la richiesta `reboot-db-instance`. Devi chiamare `reboot-db-instance` per ogni istanza nel cluster a cui desideri applicare il parametro statico aggiornato.

Example

Esempio 1: reimpostazione di tutti i parametri ai valori predefiniti

Il codice seguente reimposta tutti i parametri nel gruppo di parametri del cluster `sample-parameter-group` ai valori predefiniti.

Per Linux, macOS o Unix:

```
aws docdb reset-db-cluster-parameter-group \  
  --db-cluster-parameter-group-name sample-parameter-group \  
  --reset-all-parameters
```

Per Windows:

```
aws docdb reset-db-cluster-parameter-group ^  
  --db-cluster-parameter-group-name sample-parameter-group ^  
  --reset-all-parameters
```

Esempio 2: reimpostazione di parametri specifici ai valori predefiniti

Il codice seguente reimposta il parametro `tls` nel gruppo di parametri del cluster `sample-parameter-group` al valore predefinito.

Per Linux, macOS o 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
```

Per 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
```

L'aspetto dell'output di questa operazione è simile al seguente (formato JSON).

```
{  
  "DBClusterParameterGroupName": "sample-parameter-group"  
}
```

Riavvio di un'istanza cluster

Prima di modificare il valore di un parametro statico, l'istanza cluster deve essere riavviata. Riavvia ogni istanza nel cluster a cui desideri applicare il parametro statico aggiornato.

Per Linux, macOS o Unix:

```
aws docdb reboot-db-instance \  
  --db-instance-identifier sample-cluster-instance
```

Per Windows:

```
aws docdb reboot-db-instance ^  
  --db-instance-identifier sample-cluster-instance
```

Eliminazione di gruppi di parametri del cluster Amazon DocumentDB


È possibile eliminare un gruppo di parametri del cluster Amazon DocumentDB personalizzato utilizzando AWS Management Console o il AWS Command Line Interface (AWS CLI). Non è possibile eliminare il gruppo di parametri del cluster `default.docdb4.0`.

Using the AWS Management Console

Per eliminare un gruppo di parametri del cluster

1. [Accedi a e apri AWS Management Console la console Amazon DocumentDB all'indirizzo `https://console.aws.amazon.com/docdb`.](https://console.aws.amazon.com/docdb)
2. Nel riquadro di navigazione scegliere Parameter groups (Gruppi di parametri).

Tip

Se il riquadro di navigazione non viene visualizzato sul lato sinistro della schermata, scegliere l'icona del menu () nell'angolo in alto a sinistra della pagina.

3. Nel riquadro Parameter groups (Gruppi di parametri) scegli il pulsante di opzione a sinistra del gruppo di parametri del cluster da eliminare.
4. Scegli Actions (Operazioni), quindi Delete (Elimina).
5. Nel riquadro di conferma Delete (Elimina) scegliere Delete (Elimina) per eliminare il gruppo di parametri del cluster. Per mantenere il gruppo di parametri del cluster, scegli Annulla.

Using the AWS CLI

Per eliminare un gruppo di parametri del cluster, utilizza l'operazione `delete-db-cluster-parameter-group` con il parametro seguente.

- **`--db-cluster-parameter-group-name`**: obbligatorio. Il nome del gruppo di parametri del cluster da eliminare. Deve essere un gruppo di parametri del cluster esistente. Non è possibile eliminare il gruppo di parametri del cluster `default.docdb4.0`.

Example - Eliminazione di un gruppo di parametri del cluster

L'esempio seguente descrive le tre fasi che consentono di eliminare un gruppo di parametri del cluster:

1. Ricerca del nome del gruppo di parametri del cluster da eliminare.
2. Eliminazione del gruppo di parametri del cluster specificato.
3. Verifica dell'avvenuta eliminazione del gruppo di parametri del cluster.

1. Cerca il nome del gruppo di parametri del cluster da eliminare.

Il codice seguente elenca i nomi di tutti i gruppi di parametri del cluster.

Per Linux, macOS o Unix:

```
aws docdb describe-db-cluster-parameter-groups \  
    --query 'DBClusterParameterGroups[*].[DBClusterParameterGroupName]'
```

Per Windows:

```
aws docdb describe-db-cluster-parameter-groups ^  
    --query 'DBClusterParameterGroups[*].[DBClusterParameterGroupName]'
```

L'output dell'operazione precedente è un elenco dei nomi dei gruppi di parametri del cluster simile al seguente (formato JSON).

```
[  
  [  
    "default.docdb4.0"  
  ],  
  [  
    "sample-parameter-group"  
  ],  
  [  
    "sample-parameter-group-copy"  
  ]  
]
```

2. Elimina un gruppo di parametri del cluster specifico.

Il codice seguente elimina il gruppo di parametri del cluster `sample-parameter-group-copy`.

Per Linux, macOS o Unix:

```
aws docdb delete-db-cluster-parameter-group \  
    --db-cluster-parameter-group-name sample-parameter-group-copy
```

Per Windows:

```
aws docdb delete-db-cluster-parameter-group ^
```

```
--db-cluster-parameter-group-name sample-parameter-group-copy
```

Questa operazione non produce alcun output.

3. Verifica dell'avvenuta eliminazione del gruppo di parametri del cluster specificato.

Il codice seguente elenca i nomi di tutti i gruppi di parametri del cluster rimanenti.

Per Linux, macOS o Unix:

```
aws docdb describe-db-cluster-parameter-groups \  
  --query 'DBClusterParameterGroups[*].[DBClusterParameterGroupName]'
```

Per Windows:

```
aws docdb describe-db-cluster-parameter-groups ^  
  --query 'DBClusterParameterGroups[*].[DBClusterParameterGroupName]'
```

L'output dell'operazione precedente è un elenco dei gruppi di parametri del cluster simile al seguente (formato JSON). Il gruppo di parametri del cluster appena eliminato non deve comparire nell'elenco.

L'aspetto dell'output di questa operazione è simile al seguente (formato JSON).

```
[  
  [  
    "default.docdb4.0"  
  ],  
  [  
    "sample-parameter-group"  
  ]  
]
```

Riferimento ai parametri del cluster Amazon DocumentDB

Quando modifichi un parametro dinamico e salvi il gruppo di parametri del cluster, la modifica viene applicata immediatamente, indipendentemente dall'impostazione Apply Immediately (Applica immediatamente). Quando modifichi un parametro statico e salvi il gruppo di parametri del cluster, la modifica del parametro viene applicata dopo che avrai riavviato manualmente l'istanza. Puoi riavviare

un'istanza utilizzando la console Amazon DocumentDB o chiamando esplicitamente `reboot-db-instance`

La tabella seguente mostra i parametri che si applicano a tutte le istanze in un cluster Amazon DocumentDB.

Parametri a livello di cluster Amazon DocumentDB

Parametro	Valore predefinito	Valori validi	Modificabile	Applica tipo	Tipo di dati	Descrizione
<code>audit_logs</code>	<code>disabled</code>	abilitati, disabilitati, ddl, dml_read, dml_write, all, none	Sì	Dinamico	Stringa	<p>Definisce se i log CloudWatch di controllo di Amazon sono abilitati.</p> <ul style="list-style-type: none"> • enabled— i log CloudWatch di controllo sono abilitati. • disabled— i registri CloudWatch di controllo sono disabilitati. • ddl— il controllo degli

Parametro	Valore predefinito	Valori validi	Modificabile	Applica tipo	Tipo di dati	Descrizione
						<p>eventi DDL è abilitato.</p> <ul style="list-style-type: none"> • dml_read—il controllo degli eventi di lettura DML è abilitato. • dml_write—il controllo per gli eventi di scrittura DML è abilitato. • all—il controllo per tutti gli eventi del database è abilitato. • none—il controllo è disabilitato.

Parametro	Valore predefinito	Valori validi	Modificabile	Applica tipo	Tipo di dati	Descrizione
<code>change_stream_log_retention_duration</code>	10800	3600-604800	Sì	Dinamico	Numero intero	Definisce la durata del tempo (in secondi) in cui il registro del flusso di modifiche viene mantenuto e può essere consumato.

Parametro	Valore predefinito	Valori validi	Modificabile	Applica tipo	Tipo di dati	Descrizione
<code>profiler</code>	<code>disabled</code>	abilitato, disabilitato	Sì	Dinamico	Stringa	<p>Abilita il profiling per operazioni lente.</p> <ul style="list-style-type: none"> • enabled— le operazioni che richiedono o più tempo di un valore di soglia definito dal cliente (ad esempio 100 ms) vengono registrate in Amazon Logs. CloudWatch • disabled— le operazioni lente non vengono

Parametro	Valore predefinito	Valori validi	Modificabile	Applica tipo	Tipo di dati	Descrizione
						registrate e nei log. CloudWatch
profiler_sampling_rate	1.0	0,0 - 1,0	Sì	Dinamico	Float	Definisce la frequenza di campionamento per le operazioni registrate.
profiler_threshold_ms	100	50-2147483646	Sì	Dinamico	Numero intero	Definisce la soglia per profiler. <ul style="list-style-type: none"> Tutte le operazioni superiori a 1 profiler_threshold_ms vengono registrate e nei registri. CloudWatch

Parametro	Valore predefinito	Valori validi	Modificabile	Applica tipo	Tipo di dati	Descrizione
<code>tls</code>	abilitato	abilitato, disabilitato, fips-140-3	Sì	Statico	Stringa	<p>Definisce se sono necessarie connessioni Transport Layer Security (TLS).</p> <ul style="list-style-type: none"> • enabled — Le connessioni TLS sono necessari e per la connessione. • disabled — Le connessioni TLS non possono essere utilizzate per la connessione. • fips-140-3 — Per la

Parametro	Valore predefinito	Valori validi	Modificabile	Applica tipo	Tipo di dati	Descrizione
						<p>connessioni sono necessari e le connessioni TLS con gli attributi FIPS (Federal Information Processing Standards). Il cluster accetta solo connessioni sicure secondo la pubblicazione FIPS 140-3. È supportato solo a partire dai cluster Amazon DocumentDB</p>

Parametro	Valore predefinito	Valori validi	Modificabile	Applica tipo	Tipo di dati	Descrizione
						B 5.0 (versione del motore 3.0.3727) in queste regioni: ca-central-1, us-west-2, us-east-1, us-east-2, -1, -1. us-gov-east us-gov-west

Parametro	Valore predefinito	Valori validi	Modificabile	Applica tipo	Tipo di dati	Descrizione
<code>ttl_monitor</code>	abilitato	abilitato, disabilitato	Sì	Dinamico	Stringa	<p>Definisce se il monitoraggio Time to Live (TTL) è abilitato per il cluster.</p> <ul style="list-style-type: none"> • enabled— Il monitoraggio TTL è abilitato. • disabled— Il monitoraggio TTL è disabilitato.

Modifica dei parametri del cluster Amazon DocumentDB

In Amazon DocumentDB, i gruppi di parametri del cluster sono costituiti da parametri che si applicano a tutte le istanze create nel cluster. Per i gruppi di parametri del cluster personalizzati, puoi modificare un valore di parametro in qualsiasi momento o reimpostare tutti i valori dei parametri sulle impostazioni predefinite per i gruppi di parametri creati. Questa sezione descrive come visualizzare i parametri che costituiscono un gruppo di parametri del cluster Amazon DocumentDB e i relativi valori e come modificare o aggiornare questi valori.

I parametri possono essere dinamici o statici. Quando modifichi un parametro dinamico e salvi il gruppo di parametri del cluster, la modifica viene applicata immediatamente, indipendentemente

dall'impostazione `Apply Immediately`. Quando modifichi un parametro statico e salvi il gruppo di parametri del cluster, la modifica del parametro viene applicata solo dopo che avrai riavviato manualmente le istanze.

Visualizzazione dei parametri di un gruppo di parametri del cluster Amazon DocumentDB


Puoi visualizzare i parametri di un cluster Amazon DocumentDB e i relativi valori utilizzando o. AWS Management Console AWS CLI

Using the AWS Management Console

Per visualizzare i dettagli di un gruppo di parametri del cluster

1. [Accedi a e apri AWS Management Console la console Amazon DocumentDB all'indirizzo `https://console.aws.amazon.com/docdb`.](https://console.aws.amazon.com/docdb)
2. Nel riquadro di navigazione scegliere `Parameter groups` (Gruppi di parametri).

Tip

Se il riquadro di navigazione non viene visualizzato sul lato sinistro della schermata, scegliere l'icona del menu () nell'angolo in alto a sinistra della pagina.

3. Nel riquadro `Parameter groups` (Gruppi di parametri), scegli il nome del gruppo di parametri del cluster di cui desideri visualizzare i dettagli.
4. La pagina risultante mostra i seguenti valori per ciascun parametro: nome del parametro, valore corrente, valori consentiti, se il parametro è modificabile, tipo di applicazione, tipo di dati e descrizione.

	Cluster parameter name ▲	Values ▼	Allowed values
<input type="radio"/>	audit_logs	disabled	enabled,disabled
<input type="radio"/>	tls	enabled	disabled,enabled
<input type="radio"/>	ttl_monitor	enabled	disabled,enabled

Using the AWS CLI

Per visualizzare i parametri e i valori di un gruppo di parametri del cluster, utilizza l'operazione `describe-db-cluster-parameters` con i parametri seguenti.

- **--db-cluster-parameter-group-name**: obbligatorio. Il nome del gruppo di parametri del cluster di cui ottenere un elenco di parametri dettagliato.
- **--source**— Facoltativo. Se fornito, restituisce solo i parametri per una determinata origine. Le origini dei parametri possono essere `engine-default`, `system` o `user`.

Example

Il codice seguente elenca i parametri e i relativi valori per il gruppo di parametri `custom3-6-param-grp`. Per ulteriori informazioni sul gruppo di parametri, ometti la riga `--query`. Per informazioni su tutti i gruppi di parametri, ometti la riga `--db-cluster-parameter-group-name`.

Per Linux, macOS o Unix:

```
aws docdb describe-db-cluster-parameters \
  --db-cluster-parameter-group-name custom3-6-param-grp \
  --query 'Parameters[*].[ParameterName,ParameterValue]'
```

Per Windows:

```
aws docdb describe-db-cluster-parameters ^
  --db-cluster-parameter-group-name custom3-6-param-grp ^
  --query 'Parameters[*].[ParameterName,ParameterValue]'
```

L'aspetto dell'output di questa operazione è simile al seguente (formato JSON).

```
[
  [
    "audit_logs",
    "disabled"
  ],
  [
    "tls",
    "enabled"
  ],
  [
    "ttl_monitor",
    "enabled"
  ]
]
```

Modifica dei parametri di un gruppo di parametri del cluster Amazon DocumentDB

Puoi modificare i parametri di un gruppo di parametri utilizzando la AWS Management Console o l'AWS CLI.

Using the AWS Management Console

Per aggiornare i parametri di un gruppo di parametri del cluster

1. [Accedi a e apri AWS Management Console la console Amazon DocumentDB all'indirizzo `https://console.aws.amazon.com/docdb`.](https://console.aws.amazon.com/docdb)
2. Nel riquadro di navigazione scegliere Parameter groups (Gruppi di parametri).

Tip

Se il riquadro di navigazione non viene visualizzato sul lato sinistro della schermata, scegliere l'icona del menu (☰) nell'angolo in alto a sinistra della pagina.

3. Nel riquadro Parameter groups (Gruppi di parametri) scegliere il gruppo di parametri del cluster di cui si desidera aggiornare i parametri.
4. La pagina risultante mostra i parametri e i relativi dettagli corrispondenti per questo gruppo di parametri del cluster. Selezionare un parametro da aggiornare.
5. In alto a destra della pagina, scegliere Edit (Modifica) per modificare il valore del parametro. Per ulteriori informazioni sui tipi di parametri del cluster, consulta [Riferimento ai parametri del cluster Amazon DocumentDB](#).
6. Apportare la modifica, quindi scegliere Modify cluster parameter (Modifica parametro cluster) per salvare le modifiche. Per annullare le modifiche, selezionare Cancel (Annulla).

Using the AWS CLI

Per modificare i parametri di un gruppo di parametri del cluster, utilizzare l'operazione `modify-db-cluster-parameter-group` con i parametri seguenti.

- **`--db-cluster-parameter-group-name`**: obbligatorio. Il nome del gruppo di parametri del cluster che stai modificando.

- **--parameters**: obbligatorio. Il parametro o i parametri che stai modificando. Ogni voce del parametro deve includere:
 - **ParameterName**— Il nome del parametro che stai modificando.
 - **ParameterValue**— Il nuovo valore per questo parametro.
 - **ApplyMethod**— Come si desidera applicare le modifiche a questo parametro. I valori consentiti sono `immediate` e `pending-reboot`.

 Note

I parametri con `ApplyType` per `static` devono avere `ApplyMethod` per `pending-reboot`.

Per modificare i valori dei parametri di un gruppo di parametri del cluster (AWS CLI)

L'esempio seguente cambia il parametro `tls`.

1. Elenca i parametri e i relativi valori di **sample-parameter-group**.

Per Linux, macOS o Unix:

```
aws docdb describe-db-cluster-parameters \  
  --db-cluster-parameter-group-name sample-parameter-group
```

Per Windows:

```
aws docdb describe-db-cluster-parameters ^  
  --db-cluster-parameter-group-name sample-parameter-group
```

L'aspetto dell'output di questa operazione è simile al seguente (formato JSON).

```
{  
  "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. Modifica il parametro **tls** in modo che il relativo valore sia **disabled**. Non puoi modificare `ApplyMethod` perché `ApplyType` è static.

Per Linux, macOS o Unix:

```

aws docdb modify-db-cluster-parameter-group \
  --db-cluster-parameter-group-name sample-parameter-group \
  --parameters
  "ParameterName=tls,ParameterValue=disabled,ApplyMethod=pending-reboot"

```

Per Windows:

```

aws docdb modify-db-cluster-parameter-group ^
  --db-cluster-parameter-group-name sample-parameter-group ^
  --parameters "ParameterName=tls,ParameterValue=disabled,ApplyMethod=pending-
reboot"

```

L'aspetto dell'output di questa operazione è simile al seguente (formato JSON).

```

{
  "DBClusterParameterGroupName": "sample-parameter-group"
}

```

3. Attendi almeno 5 minuti.
4. Elenca i valori dei parametri di **sample-parameter-group**.

Per Linux, macOS o Unix:

```
aws docdb describe-db-cluster-parameters \  
  --db-cluster-parameter-group-name sample-parameter-group
```

Per Windows:

```
aws docdb describe-db-cluster-parameters ^  
  --db-cluster-parameter-group-name sample-parameter-group
```

L'aspetto dell'output di questa operazione è simile al seguente (formato JSON).

```
{  
  "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"  
    }  
  ]  
}
```

Comprendere gli endpoint di Amazon DocumentDB

Puoi utilizzare gli endpoint Amazon DocumentDB (con compatibilità con MongoDB) per connetterti a un cluster o a un'istanza. Amazon DocumentDB ha tre diversi tipi di endpoint, ciascuno con un proprio scopo.

Argomenti

- [Ricerca degli endpoint del cluster](#)
- [Ricerca di un endpoint dell'istanza](#)
- [Connessione agli endpoint](#)

Endpoint del cluster

Un endpoint del cluster è un endpoint per un cluster Amazon DocumentDB che si connette all'istanza principale corrente del cluster. Ogni cluster Amazon DocumentDB ha un singolo endpoint del cluster e un'istanza principale. Nel caso di un failover, l'endpoint del cluster viene rimappato alla nuova istanza primaria.

Endpoint di lettura

Un endpoint reader è un endpoint per un cluster Amazon DocumentDB che si connette a una delle repliche disponibili per quel cluster. Ogni cluster Amazon DocumentDB dispone di un endpoint di lettura. Se esiste più di una replica, l'endpoint di lettura indirizza ogni richiesta di connessione a una delle repliche di Amazon DocumentDB.

Endpoint dell'istanza

Per endpoint dell'istanza si intende un endpoint che si connette a un'istanza specifica. Ogni istanza in un cluster, a prescindere che sia primaria o di replica, ha un proprio endpoint dell'istanza esclusivo. Si consiglia di non utilizzare gli endpoint dell'istanza nell'applicazione. Questo perché possono variare ruoli in caso di un failover, richiedendo in tal modo modifiche del codice nell'applicazione.

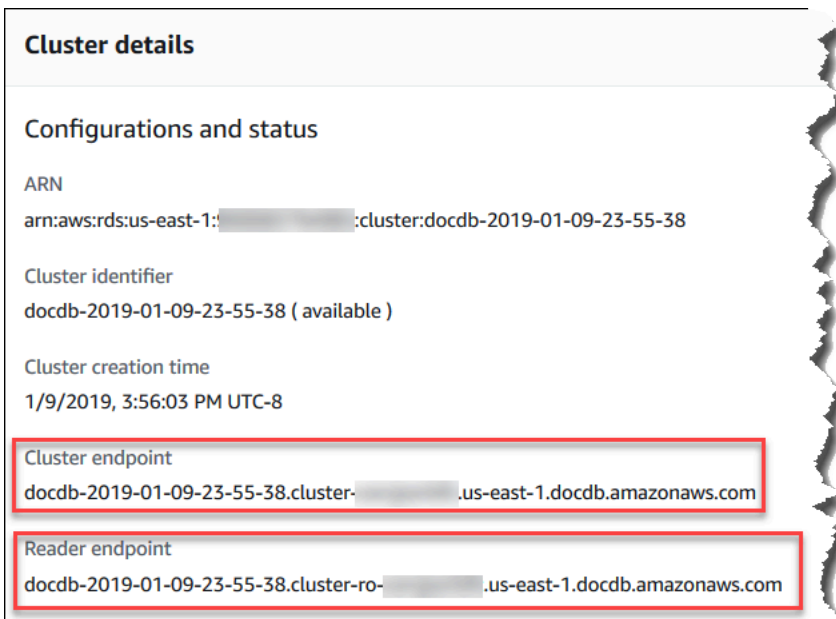
Ricerca degli endpoint del cluster

Puoi trovare l'endpoint del cluster e l'endpoint di lettura di un cluster utilizzando la console Amazon DocumentDB o AWS CLI.

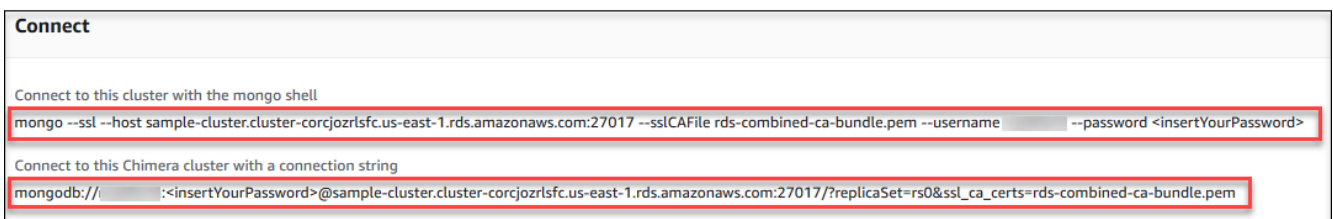
Using the AWS Management Console

Per trovare gli endpoint del cluster con la console

1. Accedi al AWS Management Console e apri la console Amazon DocumentDB all'indirizzo <https://console.aws.amazon.com/docdb>.
2. Nel riquadro di navigazione scegli Clusters (Cluster).
3. Dall'elenco dei cluster scegli il nome del cluster desiderato.
4. Scorri la sezione Details (Dettagli) e individua l'endpoint del cluster e l'endpoint lettore.



5. Per connettersi a questo cluster, scorri fino alla sezione Connect (Connetti). Individua la stringa di connessione per la shell mongo e una stringa di connessione che può essere utilizzata nel codice dell'applicazione per connetterti al cluster.



Using the AWS CLI

Per trovare gli endpoint del cluster e lettore per il tuo cluster con l'AWS CLI, esegui il comando `describe-db-clusters` con questi parametri.

Parametri

- **--db-cluster-identifier**—Facoltativo. Specifica il cluster per il quale restituire l'endpoint. Se omissso, restituisce gli endpoint per un massimo di 100 cluster.
- **--query**—Facoltativo. Specifica i campi da visualizzare. È utile per ridurre la quantità di dati da visualizzare per trovare gli endpoint. Se omissso, vengono restituite tutte le informazioni su un cluster.
- **--region**—Facoltativo. Il parametro `--region` consente di specificare la regione a cui applicare il comando. Se omissso, viene usata la regione predefinita.

Example

L'esempio seguente restituisce l'endpoint `DBClusterIdentifier` (endpoint del cluster) e `ReaderEndpoint` per `sample-cluster`.

Per Linux, macOS o Unix:

```
aws docdb describe-db-clusters \
  --region us-east-1 \
  --db-cluster-identifier sample-cluster \
  --query 'DBClusters[*].[DBClusterIdentifier,Port,Endpoint,ReaderEndpoint]'
```

Per Windows:

```
aws docdb describe-db-clusters ^
  --region us-east-1 ^
  --db-cluster-identifier sample-cluster ^
  --query 'DBClusters[*].[DBClusterIdentifier,Port,Endpoint,ReaderEndpoint]'
```

L'aspetto dell'output di questa operazione è simile al seguente (formato JSON).

```
[
  [
    "sample-cluster",
    27017,
    "sample-cluster.cluster-corlsfccjozr.us-east-1.docdb.amazonaws.com",
    "sample-cluster.cluster-ro-corlsfccjozr.us-east-1.docdb.amazonaws.com"
  ]
]
```

Dopo aver installato l'endpoint del cluster, puoi connetterti al cluster con mongo o mongod. Per ulteriori informazioni, consulta [Connessione agli endpoint](#).

Ricerca di un endpoint dell'istanza

Puoi trovare l'endpoint per un'istanza utilizzando la console Amazon DocumentDB o ilAWS CLI.

Using the AWS Management Console

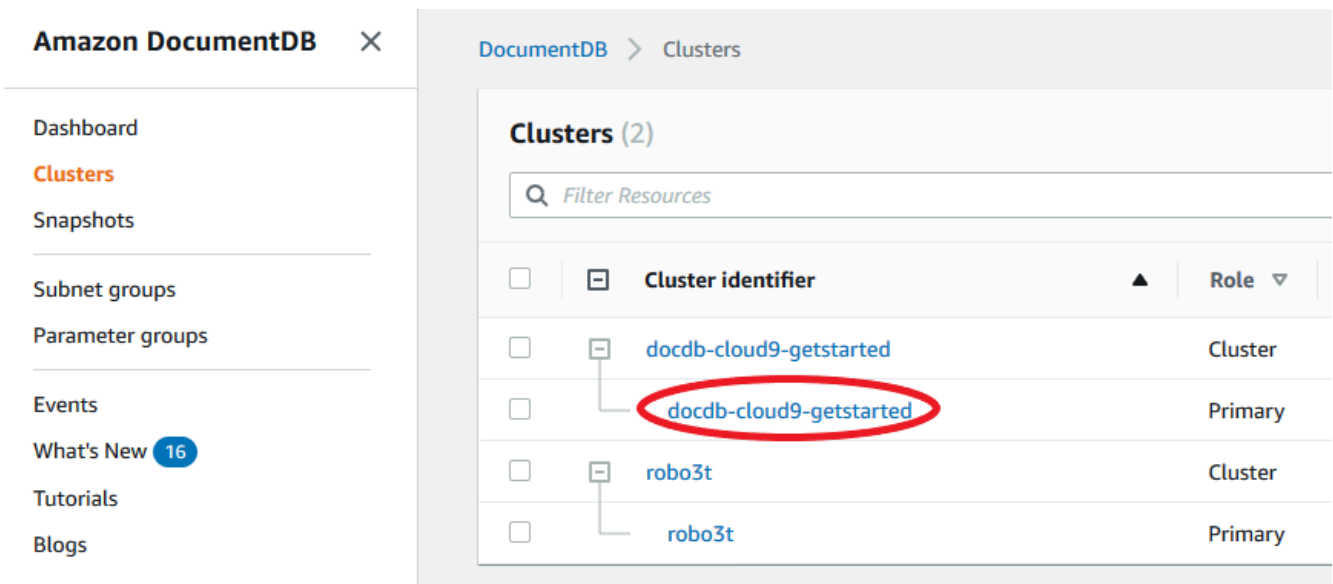
Per trovare l'endpoint dell'istanza con la console

1. Accedi aAWS Management Consolee apri la console Amazon DocumentDB all'indirizzo<https://console.aws.amazon.com/docdb>.
2. Nel pannello di navigazione scegliere Clusters (Cluster).

Tip

Se il riquadro di navigazione non viene visualizzato sul lato sinistro della schermata, scegliere l'icona del menu (☰) nell'angolo in alto a sinistra della pagina.

3. Nella casella di navigazione Clusters, vedrai la colonnaIdentificatore del cluster. Le tue istanze sono elencate in cluster, in modo simile alla schermata seguente.

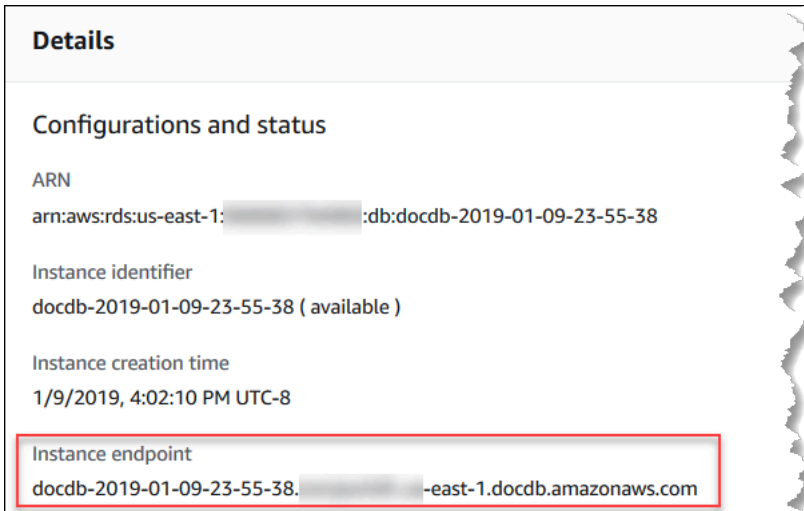


The screenshot shows the Amazon DocumentDB console interface. On the left is a navigation sidebar with options like Dashboard, Clusters, Snapshots, Subnet groups, Parameter groups, Events, What's New (16), Tutorials, and Blogs. The main content area is titled 'DocumentDB > Clusters' and displays a table of clusters. The table has columns for 'Cluster identifier' and 'Role'. The cluster 'docdb-cloud9-getstarted' is highlighted with a red circle, and its role is 'Primary'. Other clusters shown include 'robo3t' with roles 'Cluster' and 'Primary'.

<input type="checkbox"/>	<input type="checkbox"/>	Cluster identifier	Role
<input type="checkbox"/>	<input type="checkbox"/>	docdb-cloud9-getstarted	Cluster
<input type="checkbox"/>	<input type="checkbox"/>	docdb-cloud9-getstarted	Primary
<input type="checkbox"/>	<input type="checkbox"/>	robo3t	Cluster
<input type="checkbox"/>	<input type="checkbox"/>	robo3t	Primary

4. Seleziona la casella a sinistra dell'istanza che ti interessa.

5. Scorri la sezione Details (Dettagli) per individuare l'endpoint dell'istanza.



6. Per connetterti a questa istanza, scorri fino alla sezione Connect (Connetti). Individua la stringa di connessione per la shell mongo e una stringa di connessione che può essere utilizzata nel codice dell'applicazione per connetterti all'istanza.



Using the AWS CLI

Per trovare l'endpoint dell'istanza utilizzando l'AWS CLI, esegui il comando seguente con questi argomenti.

Argomenti

- **--db-instance-identifier**—Facoltativo. Specifica l'istanza per la quale restituire l'endpoint. Se omesso, restituisce l'endpoint per un massimo di 100 istanze.
- **--query**—Facoltativo. Specifica i campi da visualizzare. È utile per ridurre la quantità di dati da visualizzare per trovare gli endpoint. Se omesso, vengono restituite tutte le informazioni su un'istanza. Il campo Endpoint ha tre membri, quindi la sua inclusione nella query, come nell'esempio seguente, restituisce tutti e tre i membri. Se sei interessato solo ad alcuni dei membri Endpoint, sostituisci Endpoint nella query con i membri desiderati, come nel secondo esempio.

- **--region**—Facoltativo. Il parametro `--region` consente di specificare la regione a cui applicare il comando. Se omissso, viene usata la regione predefinita.

Example

Per Linux, macOS o Unix:

```
aws docdb describe-db-instances \
  --region us-east-1 \
  --db-instance-identifier sample-cluster-instance \
  --query 'DBInstances[*].[DBInstanceIdentifier,Endpoint]'
```

Per Windows:

```
aws docdb describe-db-instances ^
  --region us-east-1 ^
  --db-instance-identifier sample-cluster-instance ^
  --query 'DBInstances[*].[DBInstanceIdentifier,Endpoint]'
```

L'aspetto dell'output di questa operazione è simile al seguente (formato JSON).

```
[
  [
    "sample-cluster-instance",
    {
      "Port": 27017,
      "Address": "sample-cluster-instance.corcjozrlsfc.us-
east-1.docdb.amazonaws.com",
      "HostedZoneId": "Z2R2ITUGPM61AM"
    }
  ]
]
```

Riducendo l'output per eliminare `HostedZoneId` del codice puoi modificare la query specificando `Endpoint.Port` e `Endpoint.Address`.

Per Linux, macOS o Unix:

```
aws docdb describe-db-instances \
  --region us-east-1 \
  --db-instance-identifier sample-cluster-instance \
```

```
--query 'DBInstances[*].[DBInstanceIdentifier,Endpoint.Port,Endpoint.Address]'
```

Per Windows:

```
aws docdb describe-db-instances ^  
  --region us-east-1 ^  
  --db-instance-identifier sample-cluster-instance ^  
  --query 'DBInstances[*].[DBInstanceIdentifier,Endpoint.Port,Endpoint.Address]'
```

L'aspetto dell'output di questa operazione è simile al seguente (formato JSON).

```
[  
  [  
    "sample-cluster-instance",  
    27017,  
    "sample-cluster-instance.corcjzrlsfc.us-east-1.docdb.amazonaws.com"  
  ]  
]
```

Dopo aver installato l'endpoint dell'istanza, puoi connetterti all'istanza con mongo o mongod. Per ulteriori informazioni, consulta [Connessione agli endpoint](#).

Connessione agli endpoint

Quando hai l'endpoint del cluster o dell'istanza, puoi connetterti a esso utilizzando la shell mongo o una stringa di connessione.

Connessione con la shell Mongo

Utilizza la struttura seguente per costruire la stringa necessaria per connetterti al cluster o all'istanza utilizzando la shell mongo:

```
mongo \  
  --ssl \  
  --host Endpoint:Port \  
  --sslCAFile global-bundle.pem \  
  --username UserName \  
  --password Password
```

Esempi della shell mongo

Connessione a un cluster.

```
mongo \  
  --ssl \  
  --host sample-cluster.corcjozrlsfc.us-east-1.docdb.amazonaws.com:27017 \  
  --sslCAFile global-bundle.pem \  
  --username UserName \  
  --password Password
```

Connessione a un'istanza:

```
mongo \  
  --ssl \  
  --host sample-cluster-instance.corcjozrlsfc.us-east-1.docdb.amazonaws.com:27017 \  
  --sslCAFile global-bundle.pem \  
  --username UserName \  
  --password Password
```

Connessione con una stringa di connessione

Utilizza la struttura seguente per costruire la stringa di connessione necessaria per connetterti al cluster o all'istanza.

```
mongodb://UserName:Password@endpoint:port?replicaSet=rs0&ssl_ca_certs=global-  
bundle.pem
```

Esempi di stringa di connessione

Connessione a un cluster.

```
mongodb://UserName:Password@sample-cluster.cluster-corlsfccjozr.us-  
east-1.docdb.amazonaws.com:27017?replicaSet=rs0&ssl_ca_certs=global-bundle.pem
```

Connessione a un'istanza:

```
mongodb://UserName:Password@sample-cluster-instance.cluster-corlsfccjozr.us-  
east-1.docdb.amazonaws.com:27017?replicaSet=rs0&ssl_ca_certs=global-bundle.pem
```

Informazioni su Amazon DocumentDB Amazon Resource Names (ARN)

Le risorse che AWS crei sono identificate in modo univoco con un Amazon Resource Name (ARN). Per alcune operazioni con Amazon DocumentDB (con compatibilità con MongoDB), devi identificare in modo univoco una risorsa Amazon DocumentDB specificandone l'ARN. Ad esempio, quando aggiungi un tag a una risorsa, devi fornire l'ARN della risorsa.

Argomenti

- [Creazione di un ARN per una risorsa Amazon DocumentDB](#)
- [Ricerca dell'ARN di una risorsa Amazon DocumentDB](#)

Creazione di un ARN per una risorsa Amazon DocumentDB

Puoi creare un ARN per una risorsa Amazon DocumentDB utilizzando la seguente sintassi. Amazon DocumentDB condivide il formato di Amazon Relational Database Service (Amazon RDS) ARNS. Gli ARN di Amazon DocumentDB contengono e non contengono `rds.docdb`

`arn:aws:rds:region:account_number:resource_type:resource_id`

Nome della regione	Regione	Zone di disponibilità (elaborazione)
Stati Uniti orientali (Ohio)	<code>us-east-2</code>	3
Stati Uniti orientali (Virginia settentrionale)	<code>us-east-1</code>	6
US West (Oregon)	<code>us-west-2</code>	4
Sud America (São Paulo)	<code>sa-east-1</code>	3
Asia Pacifico (Hong Kong)	<code>ap-east-1</code>	3

Nome della regione	Regione	Zone di disponibilità (elaborazione)
Asia Pacific (Hyderabad)	ap-south-2	3
Asia Pacifico (Mumbai)	ap-south-1	3
Asia Pacifico (Seul)	ap-northeast-2	4
Asia Pacifico (Singapore)	ap-southeast-1	3
Asia Pacifico (Sydney)	ap-southeast-2	3
Asia Pacifico (Tokyo)	ap-northeast-1	3
Canada (Centrale)	ca-central-1	3
Regione Cina (Pechino)	cn-north-1	3
Cina (Ningxia)	cn-northwest-1	3
Europa (Francoforte)	eu-central-1	3
Europa (Irlanda)	eu-west-1	3
Europa (Londra)	eu-west-2	3
Europa (Milano)	eu-south-1	3
Europa (Parigi)	eu-west-3	3
Medio Oriente (Emirati Arabi Uniti)	me-central-1	3
AWS GovCloud (Stati Uniti occidentali)	us-gov-west-1	3

Nome della regione	Regione	Zone di disponibilità (elaborazione)
AWS GovCloud (Stati Uniti orientali)	us-gov-east-1	3

Note

L'architettura Amazon DocumentDB separa storage ed elaborazione. Per il livello di storage, Amazon DocumentDB replica sei copie dei dati su tre zone di AWS disponibilità (AZ). Le zone di disponibilità elencate nella tabella riportata sopra rappresentano il numero di zone di disponibilità che è possibile utilizzare in una determinata regione per effettuare il provisioning delle istanze di calcolo. Ad esempio, se stai lanciando un cluster Amazon DocumentDB in ap-northeast-1, lo storage verrà replicato in sei modi su tre AZ, ma le tue istanze di calcolo saranno disponibili solo in due AZ.

La tabella seguente mostra il formato da utilizzare per la creazione di un ARN per una particolare risorsa Amazon DocumentDB. Amazon DocumentDB condivide il formato di Amazon RDS ARNS. Gli ARN di Amazon DocumentDB contengono e non contengono `rds.docdb`

Tipo di risorsa	Formato ARN/Esempio
Istanza (db)	<code>arn:aws:rds: <i>region</i>:<i>account_number</i> :db:<i>resource_id</i></code> <div style="border: 1px solid #ccc; border-radius: 10px; padding: 10px; margin-top: 10px;"> <code>arn:aws:rds:us-east-1: 1234567890 :db:sample-db-instance</code> </div>
Cluster (cluster)	<code>arn:aws:rds: <i>region</i>:<i>account_number</i> :cluster:<i>resource_id</i></code> <div style="border: 1px solid #ccc; border-radius: 10px; padding: 10px; margin-top: 10px;"> <code>arn:aws:rds:us-east-1: 1234567890 :cluster: sample-db-cluster</code> </div>
Gruppo di parametri del cluster (cluster-pg)	<code>arn:aws:rds: <i>region</i>:<i>account_number</i> :cluster-pg: <i>resource_id</i></code>

Tipo di risorsa	Formato ARN/Esempio
	<pre>arn:aws:rds:us-east-1: 1234567890 :cluster- pg: sample-db-cluster-parameter-group</pre>
Gruppo di sicurezza (secgrp)	<pre>arn:aws:rds: region:account_n umber :secgrp:resource_id</pre> <pre>arn:aws:rds:us-east-1: 1234567890 :secgrp:sample-pu blic-secgrp</pre>
Snapshot del cluster (cluster-snapshot)	<pre>arn:aws:rds: region:account_number :cluster- snapshot: resource_id</pre> <pre>arn:aws:rds:us-east-1: 1234567890 :cluster-snapshot: sample-db-cluster-snapshot</pre>
Gruppo di sottoreti (subgrp)	<pre>arn:aws:rds: region:account_n umber :subgrp:resource_id</pre> <pre>arn:aws:rds:us-east-1: 1234567890 :subgrp:sample-su bnet-10</pre>

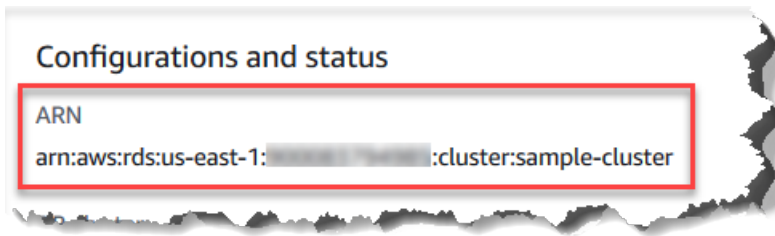
Ricerca dell'ARN di una risorsa Amazon DocumentDB

Puoi trovare l'ARN di una risorsa Amazon DocumentDB utilizzando AWS Management Console o il AWS CLI

Using the AWS Management Console

Per trovare un ARN utilizzando la console, accedi alla risorsa di cui desideri l'ARN e visualizzane i relativi dettagli.

Ad esempio, puoi ottenere l'ARN per un cluster nel riquadro Details (Dettagli) del cluster, come illustrato nella screenshot seguente.



Using the AWS CLI

Per ottenere un ARN utilizzando il AWS CLI per una particolare risorsa Amazon DocumentDB, usa `describe` l'operazione per quella risorsa. La tabella seguente mostra ogni AWS CLI operazione e la proprietà ARN utilizzata con l'operazione per ottenere un ARN.

AWS CLI Comando	Proprietà ARN
<code>describe-db-instances</code>	<code>DBInstanceArn</code>
<code>describe-db-clusters</code>	<code>DBClusterArn</code>
<code>describe-db-parameter-groups</code>	<code>DBParameterGroupArn</code>
<code>describe-db-cluster-parameter-groups</code>	<code>DBClusterParameterGroupArn</code>
<code>describe-db-security-groups</code>	<code>DBSecurityGroupArn</code>
<code>describe-db-snapshots</code>	<code>DBSnapshotArn</code>
<code>describe-db-cluster-snapshots</code>	<code>DBClusterSnapshotArn</code>
<code>describe-db-subnet-groups</code>	<code>DBSubnetGroupArn</code>

Example - Ricerca dell'ARN per un cluster

L' AWS CLI operazione seguente trova l'ARN per il cluster. `sample-cluster`

Per Linux, macOS o Unix:

```
aws docdb describe-db-clusters \
  --db-cluster-identifier sample-cluster \
  --query 'DBClusters[*].DBClusterArn'
```


Per Windows:

```
aws docdb describe-db-clusters ^
  --db-cluster-identifier sample-cluster \
  --query 'DBClusters[*].DBClusterArn'
```

L'aspetto dell'output di questa operazione è simile al seguente (formato JSON).

```
[
  "arn:aws:rds:us-east-1:123456789012:cluster:sample-cluster"
]
```

Example - Ricerca degli ARN per più gruppi di parametri

Per Linux, macOS o Unix:

```
aws docdb describe-db-cluster-parameter-groups \
  --query 'DBClusterParameterGroups[*].DBClusterParameterGroupArn'
```

Per Windows:

```
aws docdb describe-db-cluster-parameter-groups ^
  --query 'DBClusterParameterGroups[*].DBClusterParameterGroupArn'
```

L'aspetto dell'output di questa operazione è simile al seguente (formato JSON).

```
[
  "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"
]
```

Etichettatura delle risorse Amazon DocumentDB

Puoi utilizzare i tag Amazon DocumentDB (con compatibilità MongoDB) per aggiungere metadati alle tue risorse Amazon DocumentDB. Questi tag possono essere usati con AWS Identity and Access Management (IAM) politiche per gestire l'accesso alle risorse di Amazon DocumentDB e controllare quali azioni possono essere applicate alle risorse. Puoi utilizzare questi tag anche per tenere traccia dei costi raggruppando le spese per risorse con tag simili.

Puoi taggare le seguenti risorse Amazon DocumentDB:

- Cluster
- Istanze
- Snapshot
- Snapshot cluster
- Gruppi di parametri
- Gruppi di parametri di cluster
- Gruppi di sicurezza
- Gruppi di sottoreti

Panoramica dei tag delle risorse di Amazon DocumentDB

Un tag Amazon DocumentDB è una coppia nome-valore che definisci e associ a una risorsa Amazon DocumentDB. Il nome viene definito chiave. L'indicazione di un valore per la chiave è un'operazione facoltativa. Puoi utilizzare i tag per assegnare informazioni arbitrarie a una risorsa Amazon DocumentDB. Una chiave tag potrebbe essere impiegata, ad esempio, per definire una categoria e il valore di tag potrebbe essere un elemento di tale categoria. Ad esempio, puoi definire una chiave di tag di `project` un valore di tag di `Salix`, indicando che la risorsa Amazon DocumentDB è assegnata al progetto Salix. Puoi anche utilizzare i tag per designare le risorse di Amazon DocumentDB da utilizzare per test o produzione utilizzando una chiave come `environment=test` o `environment=production`. Ti consigliamo di utilizzare un set coerente di chiavi di tag per semplificare il monitoraggio dei metadati associati alle risorse di Amazon DocumentDB.

È possibile utilizzare i tag anche per organizzare le fatture AWS al fine di riflettere la struttura dei costi. Per eseguire questa operazione, registrarsi per far sì che la fattura dell'Account AWS includa i valori di chiave di tag. Per visualizzare il costo delle risorse combinate, puoi organizzare le informazioni di fatturazione in base alle risorse con gli stessi valori di chiave di tag. Puoi ad esempio applicare tag a numerose risorse con un nome di applicazione specifico, quindi organizzare le informazioni di fatturazione per visualizzare il costo totale dell'applicazione in più servizi. Per ulteriori informazioni, consulta [Utilizzo dei tag di allocazione dei costi](#) nell'AWS Guida per l'utente alla fatturazione e alla gestione dei costi.

Ogni risorsa Amazon DocumentDB ha un set di tag che contiene tutti i tag assegnati a quella risorsa. Un set di tag può contenere fino a 10 tag ma può anche essere vuoto. Se aggiungi un tag a una

risorsa Amazon DocumentDB che ha la stessa chiave di un tag esistente sulla risorsa, il nuovo valore sovrascrive il vecchio valore.

AWS non applica alcun significato semantico ai tag, che vengono interpretati rigorosamente come stringhe di caratteri. Amazon DocumentDB può impostare tag su un'istanza o altre risorse Amazon DocumentDB, a seconda delle impostazioni utilizzate al momento della creazione della risorsa. Ad esempio, Amazon DocumentDB potrebbe aggiungere un tag che indica che un'istanza è destinata alla produzione o ai test.

Puoi aggiungere un tag a una snapshot, tuttavia questo raggruppamento non sarà indicato riportato nella fattura.

Puoi usare ilAWS Management Consoleo ilAWS CLIper aggiungere, elencare ed eliminare tag sulle risorse Amazon DocumentDB. Quando utilizzi l'AWS CLI, devi fornire l'Amazon Resource Name (ARN) della risorsa che desideri utilizzare. Per ulteriori informazioni sugli ARN di Amazon DocumentDB, consulta[Informazioni su Amazon DocumentDB Amazon Resource Names \(ARN\)](#).

Vincoli per i tag

I seguenti vincoli si applicano ai tag Amazon DocumentDB:

- Numero massimo di tag per risorsa: 10
- Lunghezza massima della chiave: 128 caratteri Unicode
- Lunghezza massima del valore: 256 caratteri Unicode
- Caratteri validi per la chiave e il valore: lettere maiuscole e minuscole nel set di caratteri UTF-8, numeri, spazio e i seguenti caratteri: `_ . : / = + - e @` (espressioni regolari Java: `"^([\p{L}\p{Z}\p{N}_ . : / = + \ -]*)$"`)
- i valori e le chiavi dei tag rispettano la distinzione tra maiuscole e minuscole;
- Il prefisso `aws:` non può essere utilizzato per chiavi o valori dei tag, ma è riservato per AWS.

Aggiungere e aggiornare tag su una risorsa Amazon DocumentDB

È possibile aggiungere fino a 10 tag a una risorsa utilizzandoAWS Management Consoleo ilAWS CLI.

Using the AWS Management Console

Il processo di aggiunta di un tag a una risorsa è quasi identico, indipendentemente dal tipo di risorsa. In questo esempio, il tag viene aggiunto a un cluster.

Per aggiungere o aggiornare i tag in un cluster con la console

1. Accedi all'AWS Management Console e apri la console Amazon DocumentDB all'indirizzo <https://console.aws.amazon.com/docdb>.
2. Nel riquadro di navigazione scegli clusters (cluster).
3. Seleziona il nome del cluster a cui aggiungere i tag.
4. Scorri verso il basso fino alla sezione Tags (Tag) e scegli Edit (Modifica).
5. Per ogni tag da aggiungere alla risorsa, procedi nel seguente modo:
 - a. Per aggiungere un nuovo tag, immetti il nome del tag nella casella Key (Chiave). Per modificare il valore di un tag, individua il nome del tag nella colonna Key (Chiave).
 - b. Per assegnare al tag un valore nuovo o aggiornato, inserisci un valore per il tag nella casella Value (Valore).
 - c. Se desideri aggiungere altri tag, scegli Add (Aggiungi). Altrimenti, al termine, scegli Save (Salva).

Using the AWS CLI

Il processo di aggiunta di un tag a una risorsa è quasi identico, indipendentemente dal tipo di risorsa. In questo esempio, vengono aggiunti tre tag a un cluster. Il secondo tag key2 non contiene valori.

Utilizza l'operazione dell'AWS CLI, `add-tags-to-resource` con questi parametri.

Parametri

- **--resource-name**—L'ARN della risorsa Amazon DocumentDB a cui desideri aggiungere i tag.
- **--tags**—Un elenco dei tag (coppia chiave-valore) che si desidera aggiungere a questa risorsa nel formato `Key=key-name, Value=tag-value`.

Example

Per Linux, macOS o Unix:

```
aws docdb add-tags-to-resource \  
  --resource-name arn:aws:rds:us-east-1:1234567890:cluster:sample-cluster \  
  --tags key1=value1, key2=value2, key3=value3
```

```
--tags Key=key1,Value=value1 Key=key2 Key=key3,Value=value3
```

Per 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
```

L'operazione `add-tags-to-resource` non produce alcun output. Per visualizzare i risultati, utilizza l'operazione `list-tags-for-resource`.

Elencare i tag su una risorsa Amazon DocumentDB

Puoi usare ilAWS Management Consoleo ilAWS CLIper ottenere un elenco dei tag per una risorsa Amazon DocumentDB.

Using the AWS Management Console

Il processo per elencare i tag in una risorsa è quasi identico, indipendentemente dal tipo di risorsa a cui si aggiunge il tag. In questo esempio, vengono elencati i tag per un cluster.

Per elencare i tag in un cluster con la console

1. Apri la console Amazon DocumentDB all'indirizzo<https://console.aws.amazon.com/docdb>.
2. Nel riquadro di navigazione scegli clusters (cluster).
3. Seleziona il nome del cluster di cui desideri elencare i tag.
4. Per visualizzare un elenco dei tag in questa risorsa, scorri la sezione Tags (Tag).

Using the AWS CLI

Il processo per elencare i tag in una risorsa è quasi identico, indipendentemente dal tipo di risorsa di cui si elencano i tag. In questo esempio, vengono elencati i tag in un cluster.

Utilizza l'operazione dell'AWS CLI, `list-tags-for-resource` con questi parametri.

Parametri

- **--resource-name:** obbligatorio. L'ARN della risorsa Amazon DocumentDB per cui desideri elencare i tag.

Example

Per Linux, macOS o Unix:

```
aws docdb list-tags-for-resource \  
  --resource-name arn:aws:rds:us-east-1:1234567890:cluster:sample-cluster
```

Per Windows:

```
aws docdb list-tags-for-resource ^  
  --resource-name arn:aws:rds:us-east-1:1234567890:cluster:sample-cluster
```

L'aspetto dell'output di questa operazione è simile al seguente (formato JSON).

```
{  
  "TagList": [  
    {  
      "Key": "key1",  
      "Value": "value1"  
    },  
    {  
      "Key": "key2",  
      "Value": ""  
    },  
    {  
      "Key": "key3",  
      "Value": "value3"  
    }  
  ]  
}
```

Rimozione di tag da una risorsa Amazon DocumentDB

Puoi usare ilAWS Management Consoleo ilAWS CLIper rimuovere tag dalle risorse Amazon DocumentDB.

Using the AWS Management Console

Il processo di rimozione dei tag da una risorsa è quasi identico, indipendentemente dal tipo di risorsa. In questo esempio, vengono rimossi i tag da un cluster.

Per rimuovere tag da un cluster mediante la console

1. Apri la console Amazon DocumentDB all'indirizzo <https://console.aws.amazon.com/docdb>.
2. Nel riquadro di navigazione scegli clusters (cluster).
3. Seleziona il nome del cluster da cui desideri rimuovere i tag.
4. Scorri verso il basso fino alla sezione Tags (Tag) e scegli Edit (Modifica).
5. Se desideri rimuovere tutti i tag da questa risorsa, scegli Remove all (Rimuovi tutti). Altrimenti, per ogni tag da rimuovere dalla risorsa, procedi nel seguente modo:
 - a. Individua il nome del tag nella colonna Key (Chiave).
 - b. Scegli Remove (Rimuovi) sulla stessa riga della chiave del tag.
 - c. Al termine, scegli Save (Salva).

Using the AWS CLI

Il processo di rimozione di un tag da una risorsa è quasi identico, indipendentemente dal tipo di risorsa da cui viene rimosso il tag. In questo esempio, viene rimosso un tag da un cluster.

Utilizza l'operazione dell'AWS CLI, `remove-tags-from-resource` con questi parametri.

- **--resource-name**: obbligatorio. L'ARN della risorsa Amazon DocumentDB da cui desideri rimuovere i tag.
- **--tag-keys**: obbligatorio. Un elenco di chiavi dei tag che desideri rimuovere da questa risorsa.

Example

Per Linux, macOS o Unix:

```
aws docdb remove-tags-from-resource \  
  --resource-name arn:aws:rds:us-east-1:1234567890:cluster:sample-cluster \  
  --tag-keys key1 key3
```

Per Windows:

```
aws docdb remove-tags-from-resource ^  
  --resource-name arn:aws:rds:us-east-1:1234567890:cluster:sample-cluster \  
  --tag-keys key1 key3
```

```
--tag-keys key1 key3
```

L'operazione `removed-tags-from-resource` non produce alcun output. Per visualizzare i risultati, utilizza l'operazione `list-tags-for-resource`.

Manutenzione di Amazon DocumentDB

Periodicamente, Amazon DocumentDB esegue la manutenzione sulle risorse Amazon DocumentDB. La manutenzione spesso richiede aggiornamenti del motore di database (manutenzione del cluster) o del sistema operativo sottostante dell'istanza (manutenzione dell'istanza). Gli aggiornamenti del motore di database sono patch necessarie e includono correzioni di sicurezza, correzioni di bug e miglioramenti al motore di database. Gli aggiornamenti del sistema operativo spesso includono correzioni di sicurezza. Sebbene le patch del sistema operativo siano opzionali, consigliamo di applicarle alle istanze di Amazon DocumentDB non appena sono disponibili.

Le patch del motore di database richiedono che i cluster Amazon DocumentDB vengano messi offline per un breve periodo. Una volta disponibili, queste patch vengono automaticamente programmate per essere applicate durante una prossima finestra di manutenzione programmata del cluster Amazon DocumentDB.

Le operazioni di manutenzione su cluster e istanze hanno le loro rispettive finestre di manutenzione. Le modifiche a cluster e istanze che hai scelto di non applicare immediatamente vengono applicate anche durante la finestra di manutenzione. Per impostazione predefinita, quando crei un cluster, Amazon DocumentDB assegna una finestra di manutenzione sia per un cluster che per ogni singola istanza. Durante la creazione di un cluster o di un'istanza è possibile scegliere la finestra di manutenzione, che può anche essere modificata in qualsiasi momento per adeguarsi alla pianificazione o alle prassi del business. In genere è consigliabile scegliere finestre di manutenzione con impatto minimo sull'applicazione (per esempio, in serata o nel week end). Questa indicazione dipende tuttavia molto dal tipo di applicazione e dagli schemi di utilizzo riscontrati.

Argomenti

- [Notifiche per le patch del motore Amazon DocumentDB](#)
- [Visualizzazione delle azioni di manutenzione in sospeso di Amazon DocumentDB](#)
- [Applicazione degli aggiornamenti del motore Amazon DocumentDB](#)
- [Aggiornamenti avviati dall'utente](#)
- [Gestione delle finestre di manutenzione di Amazon DocumentDB](#)

- [Utilizzo degli aggiornamenti del sistema operativo](#)

Notifiche per le patch del motore Amazon DocumentDB

Riceverai notifiche di manutenzione per le patch richieste al motore di database tramite eventi sanitari in AWS Health Dashboard (AHD) nella AWS console e tramite e-mail. Quando una patch di manutenzione del motore Amazon DocumentDB diventa disponibile in una particolare AWS regione, tutti gli account utente di Amazon DocumentDB interessati nella regione riceveranno una notifica AHD e via e-mail per ogni versione di Amazon DocumentDB interessata dalla patch. Puoi visualizzare queste notifiche nella sezione Modifiche pianificate dell'AHD nella console. AWS La notifica conterrà dettagli sulla tempistica della disponibilità delle patch, sulla pianificazione dell'applicazione automatica, sull'elenco dei cluster interessati e sulle note di rilascio. Questa notifica verrà inviata anche via e-mail all'indirizzo e-mail dell'utente root dell' AWS account.

Open and recent issues (0)	Scheduled changes (1)	Other notifications (10)	Event log												
<p>Scheduled changes (1) Table Calendar</p> <p>View upcoming events and ongoing events from the past seven days that might affect your AWS infrastructure, such as scheduled maintenance activities. View scheduled changes that occurred more than 7 days ago.</p> <p>Q Add filter < 1 ></p> <table border="1"> <thead> <tr> <th>Event</th> <th>Status</th> <th>Region / Zone Info</th> <th>Start time</th> <th>End time</th> <th>Affected resources</th> </tr> </thead> <tbody> <tr> <td>Docdb DB patch upgrade maintenance scheduled</td> <td>Ongoing</td> <td>ap-south-1</td> <td>January 2, 2024 at 10:15:46 PM UTC-8</td> <td></td> <td>1 entity</td> </tr> </tbody> </table>				Event	Status	Region / Zone Info	Start time	End time	Affected resources	Docdb DB patch upgrade maintenance scheduled	Ongoing	ap-south-1	January 2, 2024 at 10:15:46 PM UTC-8		1 entity
Event	Status	Region / Zone Info	Start time	End time	Affected resources										
Docdb DB patch upgrade maintenance scheduled	Ongoing	ap-south-1	January 2, 2024 at 10:15:46 PM UTC-8		1 entity										

Una volta ricevuta questa notifica, puoi scegliere di applicare automaticamente queste patch del motore ai tuoi cluster Amazon DocumentDB prima della data di applicazione automatica pianificata. Oppure puoi attendere che le patch del motore vengano applicate automaticamente durante una finestra di manutenzione imminente (opzione predefinita).

Note

Lo stato della notifica nell'AHD sarà impostato su «In corso» fino al rilascio di una nuova patch del motore Amazon DocumentDB con una nuova versione della patch del motore. Una volta applicata la patch del motore al cluster Amazon DocumentDB, la versione della patch del motore del cluster verrà aggiornata in modo da riflettere la versione nella notifica. Puoi eseguire il `db.runCommand({getEngineVersion: 1})` comando per verificare questo aggiornamento.

AWS Health si integra anche con Amazon EventBridge , che utilizza gli eventi per creare applicazioni scalabili basate sugli eventi e si integra con oltre 20 destinazioni AWS Lambda, tra cui Amazon Simple Queue Service (SQS) e altre. Puoi utilizzare il codice `AWS_DOCDB_DB_PATCH_UPGRADE_MAINTENANCE_SCHEDULED` evento per configurare Amazon EventBridge prima che le patch del motore diventino disponibili. Puoi configurare la risposta EventBridge all'evento ed eseguire automaticamente azioni come l'acquisizione di informazioni sull'evento, l'avvio di eventi aggiuntivi, l'invio di notifiche tramite canali aggiuntivi come notifiche push e l'adozione di azioni correttive o di altro tipo AWS Console Mobile Application, quando una patch del motore Amazon DocumentDB diventa disponibile nella tua regione.

Nel raro scenario in cui Amazon DocumentDB annulli una patch del motore, riceverai una notifica AHD e un'e-mail che ti informa dell'annullamento. Di conseguenza, puoi utilizzare il codice `AWS_DOCDB_DB_PATCH_UPGRADE_MAINTENANCE_CANCELLED` evento per configurare Amazon in modo EventBridge che risponda a questo evento. Consulta la Amazon EventBridge User Guide per ulteriori informazioni sull'uso [EventBridge delle regole di Amazon](#).

Visualizzazione delle azioni di manutenzione in sospenso di Amazon DocumentDB

È possibile verificare se è disponibile un aggiornamento di manutenzione per il cluster utilizzando AWS Management Console o il AWS CLI.

Se è disponibile un aggiornamento, puoi scegliere una di queste operazioni:

- Rimanda un'azione di manutenzione attualmente pianificata per la prossima finestra di manutenzione (solo per le patch del sistema operativo).
- Applicare immediatamente le operazioni di manutenzione.
- Pianificare le operazioni di manutenzione perché vengano avviate durante la successiva finestra di manutenzione.

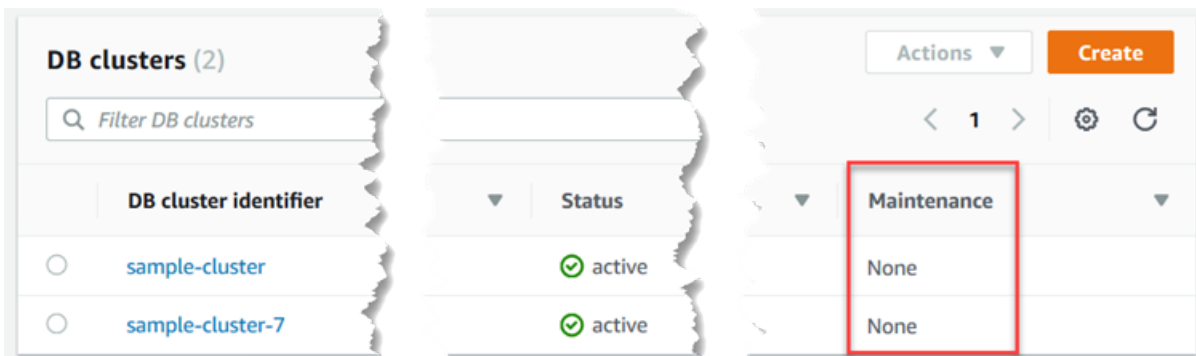
Note

Se non intraprendi alcuna azione, le azioni di manutenzione richieste, come le patch del motore, verranno applicate automaticamente in una finestra di manutenzione programmata imminente.

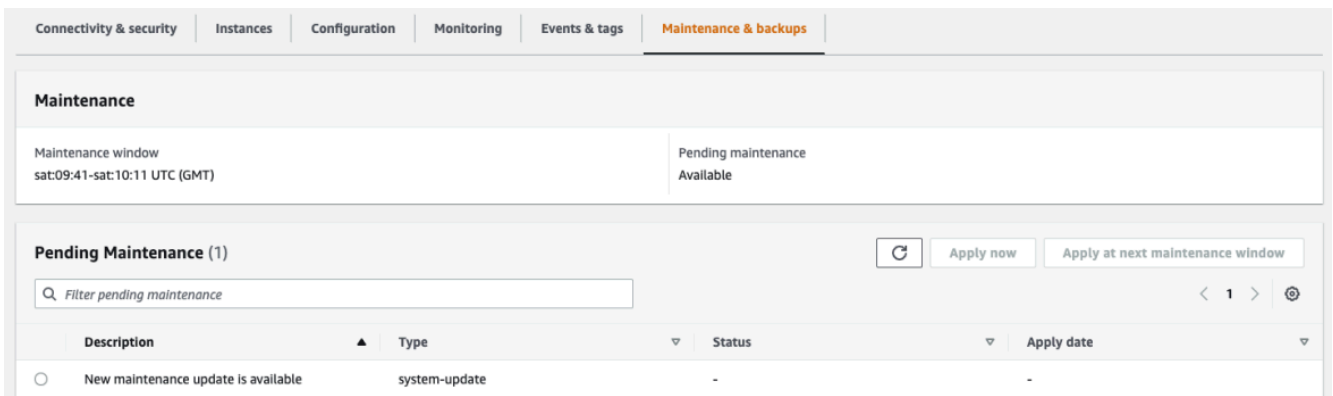
La finestra di manutenzione determina l'avvio delle operazioni in sospeso, ma non limita il tempo di esecuzione totale di tali operazioni.

Using the AWS Management Console

1. [Accedi a e apri AWS Management Console la console Amazon DocumentDB all'indirizzo `https://console.aws.amazon.com/docdb`.](https://console.aws.amazon.com/docdb)
2. Nel pannello di navigazione scegliere Clusters (Cluster).
3. Se è disponibile un aggiornamento, è indicato dalla parola Available, Required o Next Window nella colonna Maintenance per il cluster sulla console Amazon DocumentDB, come illustrato di seguito:



4. Per intraprendere un'azione, scegli il cluster per visualizzarne i dettagli, quindi scegli Manutenzione e backup. Vengono visualizzati gli elementi di manutenzione in sospeso.



Using the AWS CLI

Utilizza la seguente AWS CLI operazione per determinare quali azioni di manutenzione sono in sospeso. L'output di seguito mostra che non ci sono operazioni di manutenzione in attesa.

```
aws docdb describe-pending-maintenance-actions
```

L'aspetto dell'output di questa operazione è simile al seguente (formato JSON).

```
{
  "PendingMaintenanceActions": []
}
```

Applicazione degli aggiornamenti del motore Amazon DocumentDB

Con Amazon DocumentDB, puoi scegliere quando applicare le operazioni di manutenzione. Puoi decidere quando Amazon DocumentDB applicare gli aggiornamenti utilizzando o. AWS Management Console AWS CLI

Utilizza le procedure descritte in questo argomento per aggiornare immediatamente o pianificare un aggiornamento per il tuo cluster.

Using the AWS Management Console

Puoi utilizzare la console per gestire gli aggiornamenti per i tuoi cluster Amazon DocumentDB.

Per gestire un aggiornamento per un cluster

1. [Accedi a e apri AWS Management Console la console Amazon DocumentDB all'indirizzo https://console.aws.amazon.com/docdb.](https://console.aws.amazon.com/docdb)
2. Nel pannello di navigazione scegliere Clusters (Cluster).
3. Nell'elenco dei cluster, scegliere il pulsante accanto al nome del cluster a cui applicare l'operazione di manutenzione.
4. Nel menu Actions (Operazioni) scegliere una di queste opzioni:
 - Upgrade Now (Esegui l'aggiornamento ora) per eseguire subito le attività di manutenzione in sospeso.
 - Upgrade at next window (Aggiorna alla prossima finestra) per eseguire le attività di manutenzione in sospeso durante la finestra di manutenzione successiva del cluster.

In alternativa, puoi fare clic su Applica ora o Applica alla prossima finestra di manutenzione nella sezione Manutenzione in sospeso della scheda Manutenzione e backup del cluster (vedi Utilizzo della AWS Management Console sezione precedente).

Note

Se non ci sono attività di manutenzione in sospeso, tutte le opzioni precedenti sono inattive.

Using the AWS CLI

Per applicare un aggiornamento in sospeso a un cluster, utilizzare l'operazione `apply-pending-maintenance-action` AWS CLI

Parametri

- **--resource-identifier**—Amazon DocumentDB Amazon Resource Name (ARN) della risorsa a cui si applica l'azione di manutenzione in sospeso.
- **--apply-action**—L'azione di manutenzione in sospeso da applicare a questa risorsa.

Valori validi: `system-update` e `db-upgrade`.

- **--opt-in-type**—Un valore che specifica il tipo di richiesta di opt-in o annulla una richiesta di opt-in. Una richiesta di consenso esplicito di tipo `immediate` non può essere annullata.

Valori validi:

- `immediate`—Applica immediatamente l'azione di manutenzione.
- `next-maintenance`—Applica l'azione di manutenzione durante la finestra di manutenzione successiva per la risorsa.
- `undo-opt-in`—Annulla tutte le richieste di `next-maintenance opt-in` esistenti.

Example

Per Linux, macOS o Unix:

```
aws docdb apply-pending-maintenance-action \  
  --resource-identifier arn:aws:rds:us-east-1:123456789012:db:docdb \  
  --apply-action system-update \  
  --opt-in-type immediate
```

Per Windows:

```
aws docdb apply-pending-maintenance-action ^
  --resource-identifier arn:aws:rds:us-east-1:123456789012:db:docdb ^
  --apply-action system-update ^
  --opt-in-type immediate
```

Per restituire un elenco di risorse con almeno un aggiornamento in sospeso, usa l'operazione `describe-pending-maintenance-actions` AWS CLI

Example

Per Linux, macOS o Unix:

```
aws docdb describe-pending-maintenance-actions \
  --resource-identifier arn:aws:rds:us-east-1:001234567890:db:docdb
```

Per Windows:

```
aws docdb describe-pending-maintenance-actions ^
  --resource-identifier arn:aws:rds:us-east-1:001234567890:db:docdb
```

L'aspetto dell'output di questa operazione è simile al seguente (formato JSON).

```
{
  "PendingMaintenanceActions": [
    {
      "ResourceIdentifier": "arn:aws:rds:us-east-1:001234567890:cluster:sample-cluster",
      "PendingMaintenanceActionDetails": [
        {
          "Action": "system-update",
          "CurrentApplyDate": "2019-01-11T03:01:00Z",
          "Description": "db-version-upgrade",
          "ForcedApplyDate": "2019-01-18T03:01:00Z",
          "AutoAppliedAfterDate": "2019-01-11T03:01:00Z"
        }
      ]
    }
  ]
}
```

È inoltre possibile restituire un elenco di risorse per un cluster specificando il `--filters` parametro dell'`describe-pending-maintenance-actions` AWS CLI operazione. Il formato dell'operazione `--filters` è `Name=filter-name,Values=resource-id,...`

`db-cluster-id` è il valore accettabile per il `Name` parametro del filtro. Questo valore accetta un elenco di identificatori di cluster o ARN. L'elenco restituito include solo le operazioni di manutenzione in sospeso per i cluster specificati da questi identificatori o ARN.

L'esempio seguente restituisce le operazioni di manutenzione in sospeso per i cluster `sample-cluster1` e `sample-cluster2`.

Example

Per Linux, macOS o Unix:

```
aws docdb describe-pending-maintenance-actions \  
  --filters Name=db-cluster-id,Values=sample-cluster1,sample-cluster2
```

Per Windows:

```
aws docdb describe-pending-maintenance-actions ^  
  --filters Name=db-cluster-id,Values=sample-cluster1,sample-cluster2
```

Applica le date

Ogni operazione di manutenzione ha una rispettiva data di applicazione che è possibile trovare nella descrizione delle operazioni di manutenzione in attesa. Quando leggi l'output delle azioni di manutenzione in sospeso di AWS CLI, vengono elencate tre date:

- **CurrentApplyDate**—La data in cui l'azione di manutenzione verrà applicata immediatamente o durante la finestra di manutenzione successiva. Se la manutenzione è facoltativa, questo valore può essere `null`.
- **ForcedApplyDate**—La data in cui la manutenzione verrà applicata automaticamente, indipendentemente dalla finestra di manutenzione.
- **AutoAppliedAfterDate**—La data dopo la quale la manutenzione verrà applicata durante la finestra di manutenzione del cluster.

Aggiornamenti avviati dall'utente

In qualità di utente di Amazon DocumentDB, puoi avviare aggiornamenti ai tuoi cluster o istanze. Ad esempio, puoi modificare la classe di un'istanza con una con più o meno memoria oppure puoi modificare il gruppo di parametri di un cluster. Amazon DocumentDB visualizza queste modifiche in modo diverso dagli aggiornamenti avviati da Amazon DocumentDB. Per ulteriori informazioni sulla modifica di un cluster o di un'istanza, consulta:

- [Modifica di un cluster Amazon DocumentDB](#)
- [Modifica di un'istanza Amazon DocumentDB](#)

Per vedere un elenco delle modifiche in attesa avviate manualmente dall'utente, esegui il comando seguente.

Example

Per visualizzare le modifiche in attesa avviate dall'utente per le tue istanze

Per Linux, macOS o Unix:

```
aws docdb describe-db-instances \  
  --query 'DBInstances[*].  
[DBClusterIdentifier,DBInstanceIdentifier,PendingModifiedValues]'
```

Per Windows:

```
aws docdb describe-db-instances ^  
  --query 'DBInstances[*].  
[DBClusterIdentifier,DBInstanceIdentifier,PendingModifiedValues]'
```

L'aspetto dell'output di questa operazione è simile al seguente (formato JSON).

In questo caso, per `sample-cluster-instance` è in attesa il passaggio a una classe di istanza `db.r5.xlarge`, mentre per `sample-cluster-instance-2` non ci sono modifiche in attesa.

```
[  
  [  
    "sample-cluster",  
    "sample-cluster-instance",  
    {
```



```

        "DBInstanceClass": "db.r5.xlarge"
    }
],
[
    "sample-cluster",
    "sample-cluster-instance-2",
    {}
]
]

```

Gestione delle finestre di manutenzione di Amazon DocumentDB

Ogni istanza e ogni cluster hanno una finestra di manutenzione settimanale durante la quale vengono applicate le eventuali modifiche in attesa. La finestra di manutenzione è un'opportunità per controllare quando vengono applicate le modifiche e le patch software, nel caso in cui siano richieste o obbligatorie. Se un evento di manutenzione è pianificato per una settimana specifica, viene avviato durante la finestra di manutenzione di 30 minuti specificata dall'utente. La maggior parte degli eventi di manutenzione viene completata durante la finestra di manutenzione di 30 minuti, tuttavia l'esecuzione degli eventi di manutenzione di dimensioni maggiori può richiedere più di 30 minuti per il completamento.

La finestra di manutenzione di 30 minuti viene selezionata casualmente da un blocco di tempo di 8 ore per ogni regione. Se non specifichi una finestra di manutenzione preferita quando crei l'istanza o il cluster, Amazon DocumentDB assegna una finestra di manutenzione di 30 minuti in un giorno della settimana selezionato casualmente.

La seguente tabella elenca i blocchi temporali per ciascuna regione da cui sono assegnate le finestre di manutenzione predefinite.

Nome della regione	Regione	Blocco di tempo UTC
Stati Uniti orientali (Ohio)	us-east-2	03:00-11:00
US East (N. Virginia)	us-east-1	03:00-11:00
US West (Oregon)	us-west-2	06:00-14:00
Asia Pacifico (Hong Kong)	ap-east-1	06:00-14:00
Asia Pacific (Hyderabad)	ap-south-2	06:30 — 14:30

Nome della regione	Regione	Blocco di tempo UTC
Asia Pacific (Mumbai)	ap-south-1	06:00-14:00
Asia Pacifico (Seoul)	ap-northeast-2	13:00-21:00
Asia Pacific (Singapore)	ap-southeast-1	14:00-22:00
Asia Pacific (Sydney)	ap-southeast-2	12:00-20:00
Asia Pacifico (Tokyo)	ap-northeast-1	13:00-21:00
Canada (Central)	ca-central-1	03:00-11:00
China (Beijing)	cn-north-1	06:00-14:00
Cina (Ningxia)	cn-northwest-1	06:00-14:00
Europe (Frankfurt)	eu-central-1	21:00-05:00
Europa (Irlanda)	eu-west-1	22:00-06:00
Europe (London)	eu-west-2	22:00-06:00
Europa (Milano)	eu-south-1	02:00-10:00
Europe (Paris)	eu-west-3	23:59-07:29
Medio Oriente (Emirati Arabi Uniti)	me-central-1	05:00 — 13:00
Sud America (São Paulo)	sa-east-1	00:00-08:00
AWS GovCloud (Stati Uniti orientali)	us-gov-east-1	17:00-01:00
AWS GovCloud (Stati Uniti occidentali)	us-gov-west-1	06:00-14:00

Modifica delle finestre di manutenzione di Amazon DocumentDB

La finestra di manutenzione deve essere eseguita nel momento di utilizzo più basso e quindi potrebbe essere necessario cambiarla di tanto in tanto. In questo lasso di tempo, il cluster o l'istanza non è disponibile solo in caso vengano applicate modifiche al sistema (ad esempio per un'operazione di storage su larga scala o la modifica della classe di un'istanza) che richiedono un'interruzione. L'inattività dura solo per il tempo strettamente necessario all'esecuzione delle modifiche richieste.

Per gli aggiornamenti al motore di database, Amazon DocumentDB utilizza la finestra di manutenzione preferita del cluster e non la finestra di manutenzione per le singole istanze.

Per modificare la finestra di manutenzione

- Per un cluster: consulta [Modifica di un cluster Amazon DocumentDB](#)
- Per un'istanza: consulta [Modifica di un'istanza Amazon DocumentDB](#).

Utilizzo degli aggiornamenti del sistema operativo

Le istanze nei cluster Amazon DocumentDB richiedono occasionalmente aggiornamenti del sistema operativo. Amazon DocumentDB aggiorna il sistema operativo a una versione più recente per migliorare le prestazioni del database e il livello di sicurezza generale dei clienti. Gli aggiornamenti del sistema operativo non modificano la versione del motore del cluster o la classe di istanza di un'istanza Amazon DocumentDB.


Ti consigliamo di aggiornare prima le istanze reader in un cluster, poi l'istanza writer per massimizzare la disponibilità del cluster. Non è consigliabile aggiornare contemporaneamente le istanze Reader e Writer, poiché in caso di failover potrebbero verificarsi tempi di inattività più lunghi.

Gli aggiornamenti del sistema operativo non hanno una data di applicazione e possono essere applicati in qualsiasi momento. Ti consigliamo di applicarli periodicamente per mantenere aggiornati i database Amazon DocumentDB. Amazon DocumentDB non applica questi aggiornamenti automaticamente. Per ricevere una notifica quando diventa disponibile un nuovo aggiornamento facoltativo, è possibile iscriversi a RDS-EVENT-0230 nella categoria degli eventi di patch di sicurezza. Per informazioni sulla sottoscrizione agli eventi di Amazon DocumentDB, [consulta Abbonamento agli abbonamenti agli eventi di Amazon DocumentDB](#).


È possibile che si verifichi un failover durante la manutenzione del cluster o dell'istanza, se l'istanza è un'istanza primaria. Per migliorare la tua disponibilità, ti consigliamo di utilizzare più di un'istanza per i cluster Amazon DocumentDB. Per ulteriori informazioni, consulta [Failover di Amazon DocumentDB](#).

 Note

Per alcune funzionalità di gestione, Amazon DocumentDB utilizza la tecnologia operativa condivisa con Amazon Relational Database Service (Amazon RDS).

 Important

L'istanza di Amazon DocumentDB verrà messa offline durante l'aggiornamento del sistema operativo.

 Note

Potrebbe essere necessario rimanere aggiornati su tutti gli aggiornamenti facoltativi e obbligatori per soddisfare vari obblighi di conformità. Ti consigliamo di applicare regolarmente tutti gli aggiornamenti resi disponibili da Amazon DocumentDB durante le finestre di manutenzione.

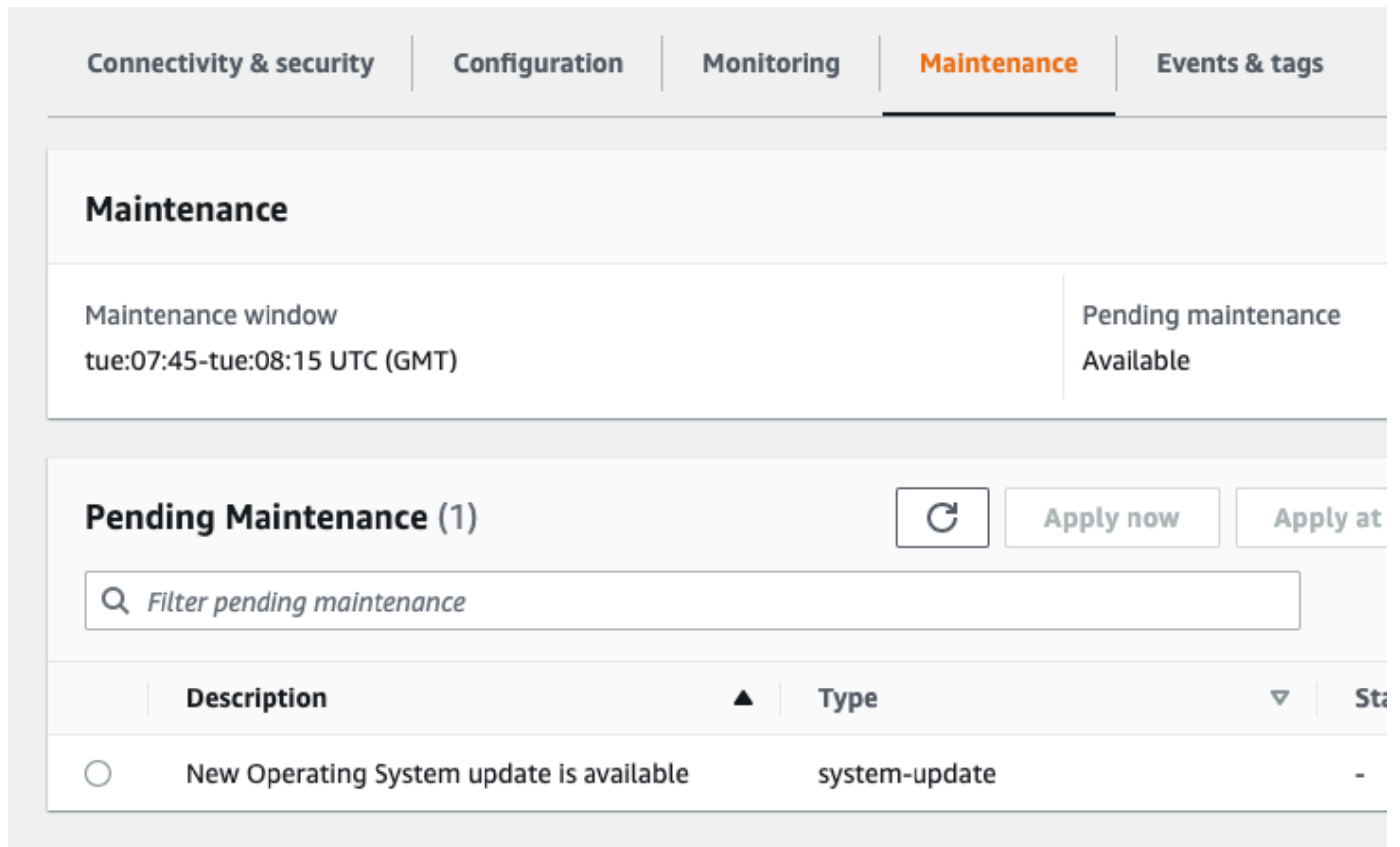
Puoi usare AWS Management Console o the AWS CLI per determinare se un aggiornamento è facoltativo o obbligatorio.

Using the AWS Management Console

Per determinare se un aggiornamento è facoltativo o obbligatorio, utilizzare AWS Management Console:

1. [Accedi a e apri AWS Management Console la console Amazon DocumentDB all'indirizzo https://console.aws.amazon.com/docdb.](https://console.aws.amazon.com/docdb)
2. Nel riquadro di navigazione, scegli Clusters, quindi seleziona l'istanza.
3. Scegli Manutenzione.
4. Nella sezione Manutenzione in sospenso, trova l'aggiornamento del sistema operativo e controlla il valore dello stato.

Nella AWS Management Console, lo stato di manutenzione di un aggiornamento del sistema operativo è impostato su Disponibile e non ha una data di applicazione, come mostrato nell'immagine seguente:



Puoi selezionare l'aggiornamento del sistema operativo e fare clic su Applica ora o Applica alla finestra di manutenzione successiva nella sezione Manutenzione in sospeso. Se il valore di manutenzione è nella finestra successiva, rimanda gli elementi di manutenzione scegliendo Rinvia aggiornamento. Non puoi rinviare un'azione di manutenzione se è già stata avviata.

In alternativa, puoi scegliere l'istanza da un elenco di cluster facendo clic su Cluster nel riquadro di navigazione e selezionando Applica ora o Applica alla finestra di manutenzione successiva dal menu Azioni.

Using the AWS CLI

Per determinare se un aggiornamento è facoltativo o obbligatorio utilizzando il, chiamate il AWS CLI comando: `describe-pending-maintenance-actions`

```
aws docdb describe-pending-maintenance-actions
```

Un aggiornamento obbligatorio del sistema operativo include un valore `AutoAppliedAfterDate` e un valore `CurrentApplyDate`. Un aggiornamento facoltativo del sistema operativo non include questi valori.

L'output seguente mostra un aggiornamento obbligatorio del sistema operativo:

```
{
  "ResourceIdentifier": "arn:aws:docdb:us-east-1:123456789012:db:mydb1",
  "PendingMaintenanceActionDetails": [
    {
      "Action": "system-update",
      "AutoAppliedAfterDate": "2022-08-31T00:00:00+00:00",
      "CurrentApplyDate": "2022-08-31T00:00:00+00:00",
      "Description": "New Operating System update is available"
    }
  ]
}
```

The following output shows an optional operating system update.

```
{
  "ResourceIdentifier": "arn:aws:docdb:us-east-1:123456789012:db:mydb2",
  "PendingMaintenanceActionDetails": [
    {
      "Action": "system-update",
      "Description": "New Operating System update is available"
    }
  ]
}
```

Disponibilità di aggiornamenti del sistema operativo

Gli aggiornamenti del sistema operativo sono specifici per le versioni del motore e le classi di istanze di Amazon DocumentDB. Pertanto, le istanze di Amazon DocumentDB ricevono o richiedono aggiornamenti in momenti diversi. Quando è disponibile un aggiornamento del sistema operativo per l'istanza in base alla versione del motore e alla classe di istanza, l'aggiornamento viene visualizzato nella console. Può essere visualizzato anche eseguendo il AWS CLI `describe-pending-maintenance-actions` comando o chiamando l'operazione `DescribePendingMaintenanceActions` API. Se è disponibile un aggiornamento per la tua istanza, puoi aggiornare il sistema operativo seguendo le istruzioni in [Applicazione degli aggiornamenti di Amazon DocumentDB](#).

Comprendere i ruoli collegati ai servizi

Amazon DocumentDB (con compatibilità con MongoDB) utilizza ruoli collegati ai servizi AWS Identity and Access Management (IAM). Un [ruolo collegato ai servizi](#) è un tipo unico di ruolo IAM collegato direttamente ad Amazon DocumentDB. I ruoli collegati ai servizi sono predefiniti da Amazon DocumentDB e includono tutte le autorizzazioni richieste dal servizio per chiamare altri AWS servizi per tuo conto.

Un ruolo collegato ai servizi semplifica l'utilizzo di Amazon DocumentDB perché non è necessario aggiungere manualmente le autorizzazioni necessarie. Amazon DocumentDB definisce le autorizzazioni dei suoi ruoli collegati ai servizi e, se non diversamente definito, solo Amazon DocumentDB può assumerne i ruoli. Le autorizzazioni definite includono la policy di trust e la policy delle autorizzazioni. Una policy delle autorizzazioni specifica non può essere collegata a un'altra entità IAM.

È possibile eliminare i ruoli solo dopo aver eliminato le risorse correlate. Questo protegge le tue risorse di Amazon DocumentDB perché non puoi rimuovere inavvertitamente l'autorizzazione di accesso alle risorse.

Per informazioni sugli altri servizi che supportano i ruoli collegati ai servizi, consulta [Servizi AWS che funzionano con IAM](#) e cerca i servizi che riportano Sì nella colonna Ruolo associato ai servizi. Scegli Yes (Sì) in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Autorizzazioni di ruolo collegate al servizio Amazon DocumentDB

Amazon DocumentDB (compatibile con MongoDB) utilizza il ruolo collegato ai servizi denominato `AWSServiceRoleForRDS` per consentire ad Amazon DocumentDB di chiamare AWS i servizi per conto dei tuoi cluster.

Ai fini dell'assunzione del ruolo, il ruolo collegato ai servizi `AWSServiceRoleForRDS` considera attendibili i seguenti servizi:

- `docdb.amazonaws.com`

La politica sulle autorizzazioni dei ruoli consente ad Amazon DocumentDB di completare le seguenti azioni sulle risorse specificate:

- Operazioni su `ec2`:

- `AssignPrivateIpAddresses`
- `AuthorizeSecurityGroupIngress`
- `CreateNetworkInterface`
- `CreateSecurityGroup`
- `DeleteNetworkInterface`
- `DeleteSecurityGroup`
- `DescribeAvailabilityZones`
- `DescribeInternetGateways`
- `DescribeSecurityGroups`
- `DescribeSubnets`
- `DescribeVpcAttribute`
- `DescribeVpcs`
- `ModifyNetworkInterfaceAttribute`
- `RevokeSecurityGroupIngress`
- `UnassignPrivateIpAddresses`
- Operazioni su sns:
 - `ListTopic`
 - `Publish`
- Operazioni su cloudwatch:
 - `PutMetricData`
 - `GetMetricData`
 - `CreateLogStream`
 - `PullLogEvents`
 - `DescribeLogStreams`
 - `CreateLogGroup`

Note

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. Potrebbe essere visualizzato il messaggio di errore seguente:

Unable to create the resource. (Impossibile creare la risorsa. Verify that you have permission to create service linked role. (Verifica di possedere le autorizzazioni necessarie per creare un ruolo collegato ai servizi.) Otherwise wait and try again later. (In caso contrario, attendi e riprova più tardi.

Se viene visualizzato questo errore, verifica che le autorizzazioni seguenti siano abilitate:

```
{
  "Action": "iam:CreateServiceLinkedRole",
  "Effect": "Allow",
  "Resource": "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
  "Condition": {
    "StringLike": {
      "iam:AWSServiceName": "rds.amazonaws.com"
    }
  }
}
```

Per ulteriori informazioni, consulta [Autorizzazioni del ruolo collegato ai servizi](#) nella Guida per l'utente di IAM.

Creazione di un ruolo collegato ai servizi Amazon DocumentDB

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando crei un cluster, Amazon DocumentDB crea automaticamente il ruolo collegato ai servizi.

Se devi ricreare un ruolo collegato ai servizi che hai precedentemente eliminato, puoi utilizzare lo stesso processo per ricreare il ruolo nel tuo account. Quando crei un cluster, Amazon DocumentDB crea nuovamente il ruolo collegato ai servizi per te.

Modifica di un ruolo collegato ai servizi di Amazon DocumentDB

Amazon DocumentDB non consente di modificare il ruolo collegato ai `AWSServiceRoleForRDS` servizi. Dopo aver creato un ruolo collegato al servizio, non potrai modificarne il nome perché potrebbero farvi riferimento varie entità. Tuttavia, puoi modificare la descrizione del ruolo utilizzando IAM. Per ulteriori informazioni, consulta [Modifica di un ruolo collegato al servizio](#) nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato al servizio Amazon DocumentDB

Se non è più necessario utilizzare una caratteristica o un servizio che richiede un ruolo collegato ai servizi, ti consigliamo di eliminare il ruolo. In questo modo non sarà più presente un'entità non utilizzata che non viene monitorata e gestita attivamente. Tuttavia, prima di poter eliminare il ruolo collegato ai servizi, dovrai eliminare tutti i cluster .

Ripulire un ruolo collegato al servizio Amazon DocumentDB

Prima di utilizzare IAM per eliminare un ruolo collegato ai servizi, devi innanzitutto verificare che il ruolo non abbia sessioni attive ed eliminare tutte le risorse utilizzate dal ruolo.

Per verificare la presenza di una sessione attiva del ruolo collegato ai servizi utilizzando la console

1. Accedi AWS Management Console e apri la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel riquadro di navigazione della console IAM, scegli Ruoli, quindi scegli il nome (non la casella di controllo) del AWSServiceRoleForRDSruolo.
3. Nella pagina Summary (Riepilogo) per il ruolo selezionato, scegliere la scheda Access Advisor (Consulente accessi).
4. Nella scheda Access Advisor (Consulente accessi) esaminare l'attività recente per il ruolo collegato ai servizi.

Note

Se non sei sicuro che Amazon DocumentDB stia utilizzando il AWSServiceRoleForRDS ruolo, puoi provare a eliminarlo. Se il servizio sta utilizzando il ruolo, l'eliminazione non andrà a buon fine e potrai visualizzare le regioni in cui il ruolo viene utilizzato. Se il ruolo è in uso, prima di poterlo eliminare dovrai attendere il termine della sessione. Non puoi revocare la sessione per un ruolo collegato ai servizi.

Per rimuovere il ruolo AWSServiceRoleForRDS, devi prima eliminare tutti i cluster e le istanze. Per informazioni sull'eliminazione delle istanze e dei cluster, consulta i seguenti argomenti:

- [Eliminazione di un'istanza Amazon DocumentDB](#)
- [Eliminazione di un cluster Amazon DocumentDB](#)

Regioni supportate per i ruoli collegati ai servizi di Amazon DocumentDB

Amazon DocumentDB supporta l'utilizzo di ruoli collegati ai servizi in tutte le regioni in cui il servizio è disponibile. Per ulteriori informazioni, consulta <https://docs.aws.amazon.com/documentdb/latest/developerguide/regions-and-azs.html#regions-and-azs-availability>.

Utilizzo dei cluster elastici di Amazon DocumentDB

I cluster elastici di Amazon DocumentDB supportano carichi di lavoro con milioni di letture/scritture al secondo e petabyte di capacità di storage. I cluster elastici semplificano anche il modo in cui gli sviluppatori interagiscono con Amazon DocumentDB eliminando la necessità di scegliere, gestire o aggiornare le istanze.

I cluster elastici di Amazon DocumentDB sono stati creati per:

- Fornisci una soluzione per i clienti che cercano un database che offra una scalabilità praticamente illimitata con funzionalità di query avanzate e compatibilità con le API MongoDB.
- Offri ai clienti limiti di connessione più elevati e riduci i tempi di inattività dovuti all'applicazione di patch.
- Continua a investire in un'architettura nativa del cloud, elastica e all'avanguardia per i carichi di lavoro JSON.

Argomenti

- [Casi d'uso del cluster elastico](#)
- [Vantaggi dei cluster elastici](#)
- [Disponibilità della regione e della versione del cluster elastico](#)
- [Limitazioni](#)
- [Cluster elastici Amazon DocumentDB: come funzionano](#)
- [Inizia a usare i cluster elastici di Amazon DocumentDB](#)
- [Best practice](#)
- [Gestione dei cluster elastici](#)
- [Critografia dei dati inattivi per i cluster elastici Amazon DocumentDB](#)
- [Ruoli collegati ai servizi nei cluster elastici](#)

Casi d'uso del cluster elastico

I database di documenti sono utili per i carichi di lavoro che richiedono uno schema flessibile per uno sviluppo rapido e iterativo. Ad esempio, i casi d'uso di Amazon DocumentDB, vedi. [Casi d'uso del database di documenti](#)

Di seguito sono riportati alcuni esempi di casi d'uso per i quali i cluster elastici possono offrire vantaggi significativi:

Profili utente

Poiché i database di documenti hanno uno schema flessibile, possono archiviare documenti con attributi e valori di dati diversi su larga scala. I cluster elastici sono una soluzione pratica per i profili online in cui utenti diversi forniscono diversi tipi di informazioni. Supponete che le vostre applicazioni supportino centinaia di milioni di profili utente. È possibile utilizzare i cluster elastici per supportare tali applicazioni, poiché possono essere scalati verso l'alto e verso l'esterno per supportare milioni di scritture e letture su questi profili utente. È inoltre possibile ridurre i costi per le ore non di punta.

Gestione dei contenuti e record storici

Per gestire in modo efficiente i contenuti, devi poterli raccogliere e aggregare da diverse origini e quindi inviarli al cliente. Grazie al loro schema flessibile, i database di documenti sono perfetti per raccogliere e archiviare qualsiasi tipo di dati. Puoi usarli per creare e incorporare nuovi tipi di contenuti, inclusi contenuti generati dagli utenti come immagini, commenti e video. Nel tempo, il database potrebbe richiedere più spazio di archiviazione. Con i cluster elastici, puoi distribuire i dati su più volumi di storage, consentendoti di archiviare petabyte di dati in un singolo cluster.

Vantaggi dei cluster elastici

AWS integrazione dei servizi

I cluster elastici di Amazon DocumentDB si integrano con altri AWS servizi nello stesso modo in cui Amazon DocumentDB:

- **Migrazione:** puoi utilizzare AWS Database Migration Service (DMS) per migrare da MongoDB e altri database relazionali ai cluster elastici di Amazon DocumentDB.
- **Monitoraggio:** puoi monitorare lo stato e le prestazioni del tuo cluster elastico utilizzando Amazon CloudWatch.
- **Sicurezza:** puoi configurare l'autenticazione e l'autorizzazione tramite AWS Identity and Access Management (IAM) per gestire i cluster elastici e utilizzare Amazon VPC per connessioni sicure solo VPC.
- **Gestione dei dati:** puoi utilizzarla AWS Glue per importare ed esportare dati da/verso altri AWS servizi come Amazon S3, Amazon Redshift e Amazon Service. OpenSearch

Disponibilità della regione e della versione del cluster elastico

Disponibilità nelle regioni

La tabella seguente mostra le AWS regioni in cui i cluster elastici di Amazon DocumentDB sono attualmente disponibili e gli endpoint per ciascuna regione.

Nome regione	Regione	Zone di disponibilità
Stati Uniti orientali (Virginia settentrionale)	us-east-1	5
Stati Uniti orientali (Ohio)	us-east-2	3
US West (Oregon)	us-west-2	3
Asia Pacifico (Mumbai)	ap-south-1	3
Asia Pacifico (Seul)	ap-northeast-2	3
Asia Pacifico (Singapore)	ap-southeast-1	3
Asia Pacifico (Sydney)	ap-southeast-2	3
Asia Pacifico (Tokyo)	ap-northeast-1	3
Sud America (San Paolo)	sa-east-1	3
Europa (Francoforte)	eu-central-1	3
Europa (Irlanda)	eu-west-1	3
Europa (Londra)	eu-west-2	3

Disponibilità della versione

I cluster elastici supportano il protocollo cablato compatibile con MongoDB 5.0. Per le differenze tra i cluster basati su istanze di DocumentDB 4.0 e i cluster elastici, vedere. [Differenze funzionali tra Amazon DocumentDB 4.0 e cluster elastici](#)

Limitazioni

Gestione elastica dei cluster

Le seguenti funzionalità e funzionalità di gestione dei cluster non sono supportate in questa versione:

- Capacità di creare cluster globali
- Eventi Amazon DocumentDB esistenti e sottoscrizione agli eventi
- Ripartizione dell'intervallo
- Condividi la collezione esistente
- Chiave shard multicampo
- Cambia chiave shard
- Ripristino Point-in-time
- Clonazione
- Approfondimenti sulle prestazioni

Note

Per informazioni sui limiti dei cluster elastici, vedere [Quote e limiti di Amazon DocumentDB](#).

Operazioni di interrogazione e scrittura

I seguenti comandi e funzionalità delle operazioni di interrogazione e scrittura non sono supportati in questa versione:

- Comandi DDL durante le operazioni di ridimensionamento
- Profiler
- Gruppi di parametri
- AWS Config
- AWS Backup

Gestione della raccolta e dell'indice

Le seguenti funzionalità di raccolta e gestione degli indici non sono supportate in questa versione:

- Indici di tipo sparse
- Indici geospaziali
- Creazione dell'indice di sfondo

Amministrazione e diagnostica

I seguenti comandi e funzionalità di amministrazione e diagnostica non sono supportati in questa versione:

- AWS Secrets Manager
- Ruoli personalizzati Role-based-access-control (RBAC).
- Durante la connessione, la priorità di scrittura pari a 0 non è supportata.
- Modifica delle sottoreti appartenenti a un VPC che non è attualmente assegnato a un cluster elastico esistente.

Funzionalità di attivazione

Le seguenti funzionalità di attivazione di Amazon DocumentDB non sono supportate in questa versione:

- Transazioni ACID
- Controllo DDL/DML
- Change streams
- Comandi di sessione

Cluster elastici Amazon DocumentDB: come funzionano

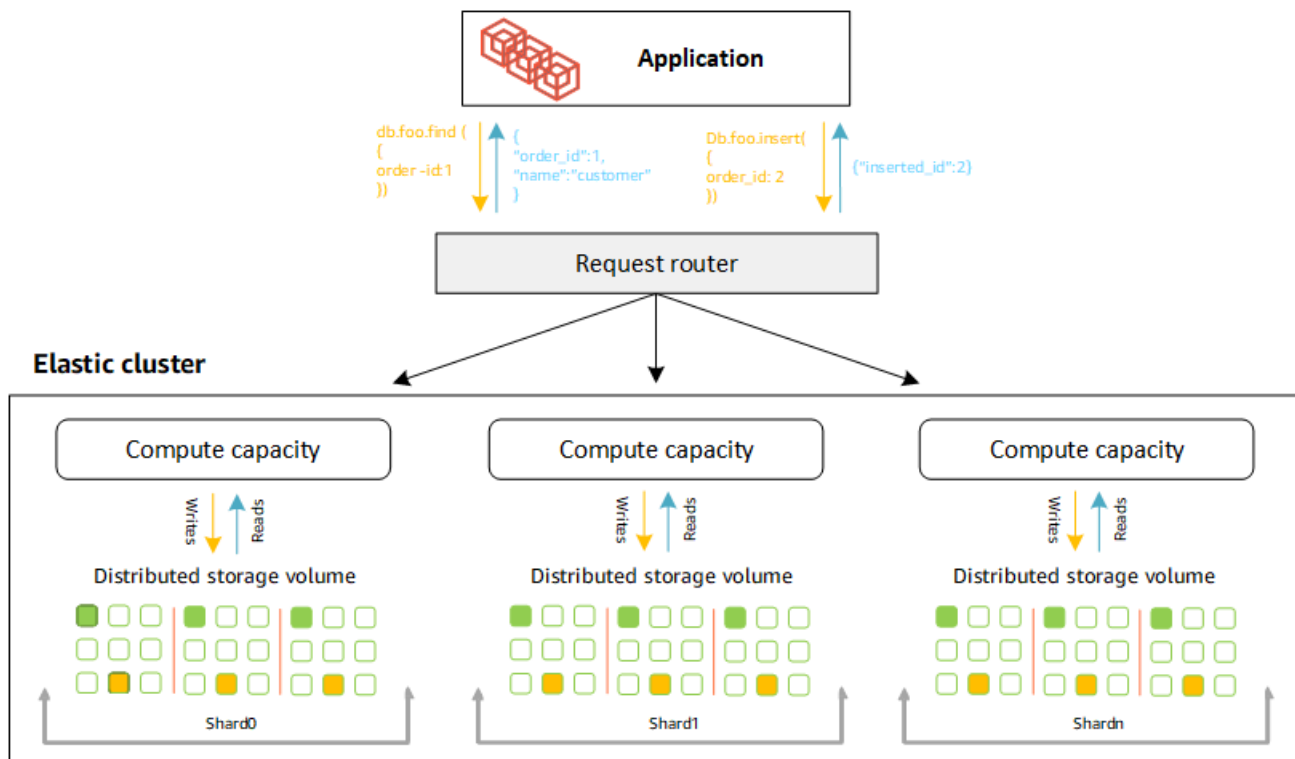
Gli argomenti di questa sezione forniscono informazioni sui meccanismi e le funzioni alla base dei cluster elastici di Amazon DocumentDB.

Argomenti

- [Sharding elastico dei cluster di Amazon DocumentDB](#)
- [Migrazione elastica dei cluster](#)
- [Scalabilità elastica dei cluster](#)
- [Affidabilità elastica del cluster](#)
- [Archiviazione e disponibilità di cluster elastici](#)
- [Differenze funzionali tra Amazon DocumentDB 4.0 e cluster elastici](#)

Sharding elastico dei cluster di Amazon DocumentDB

I cluster elastici di Amazon DocumentDB utilizzano lo sharding basato su hash per partizionare i dati su un sistema di storage distribuito. Lo sharding, noto anche come partizionamento, divide set di dati di grandi dimensioni in piccoli set di dati su più nodi, consentendoti di scalare il database oltre i limiti di scalabilità verticale. I cluster elastici utilizzano la separazione, o «disaccoppiamento», di elaborazione e storage in Amazon DocumentDB, consentendoti di scalare indipendentemente l'uno dall'altro. Anziché ripartizionare le raccolte spostando piccoli blocchi di dati tra i nodi di elaborazione, i cluster elastici copiano i dati in modo efficiente all'interno del sistema di storage distribuito.



Definizioni condivise

Definizioni della nomenclatura degli shard:

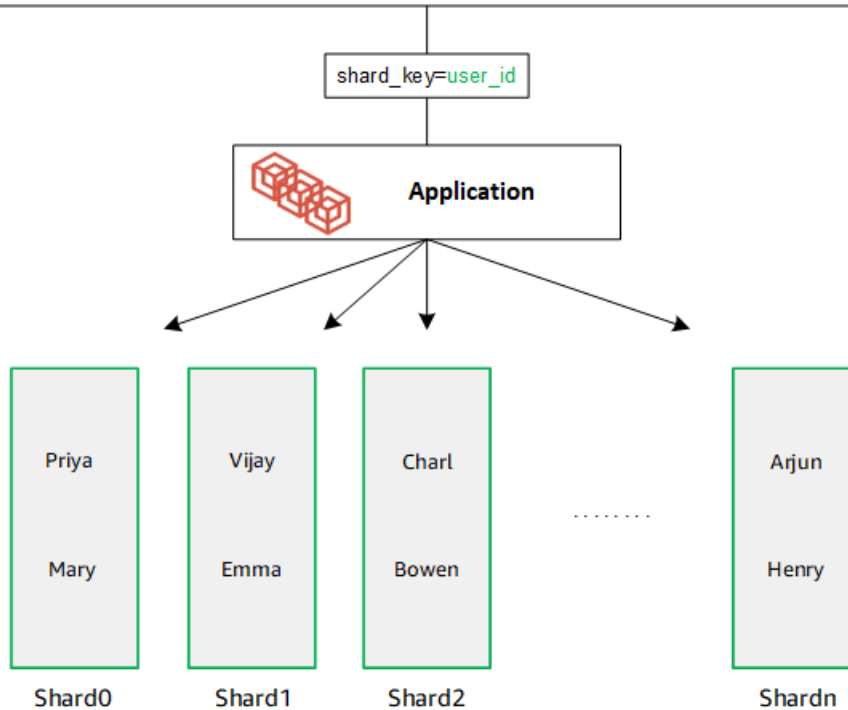
- **Shard:** uno shard fornisce il calcolo per un cluster elastico. Per impostazione predefinita, uno shard avrà due nodi. È possibile configurare un massimo di 32 shard e ogni shard può avere un massimo di 64 vCPU.
- **Chiave shard:** una chiave shard è un campo obbligatorio nei documenti JSON in raccolte condivise utilizzate dai cluster elastici per distribuire il traffico di lettura e scrittura sullo shard corrispondente.
- **Raccolta di shard:** una raccolta di shard è una raccolta i cui dati sono distribuiti su un cluster elastico in partizioni di dati.
- **Partizione:** una partizione è una parte logica di dati suddivisi. Quando si crea una raccolta condivisa, i dati vengono organizzati automaticamente in partizioni all'interno di ogni frammento in base alla chiave dello shard. Ogni shard ha più partizioni.

Distribuzione dei dati tra shard configurati

Crea una chiave shard con molti valori univoci. Una buona shard key partiziona i dati in modo uniforme tra gli shard sottostanti, offrendo al carico di lavoro la velocità di trasmissione e le prestazioni migliori. L'esempio seguente sono i dati relativi ai nomi dei dipendenti che utilizzano una chiave shard denominata «user_id»:

Employee Dataset

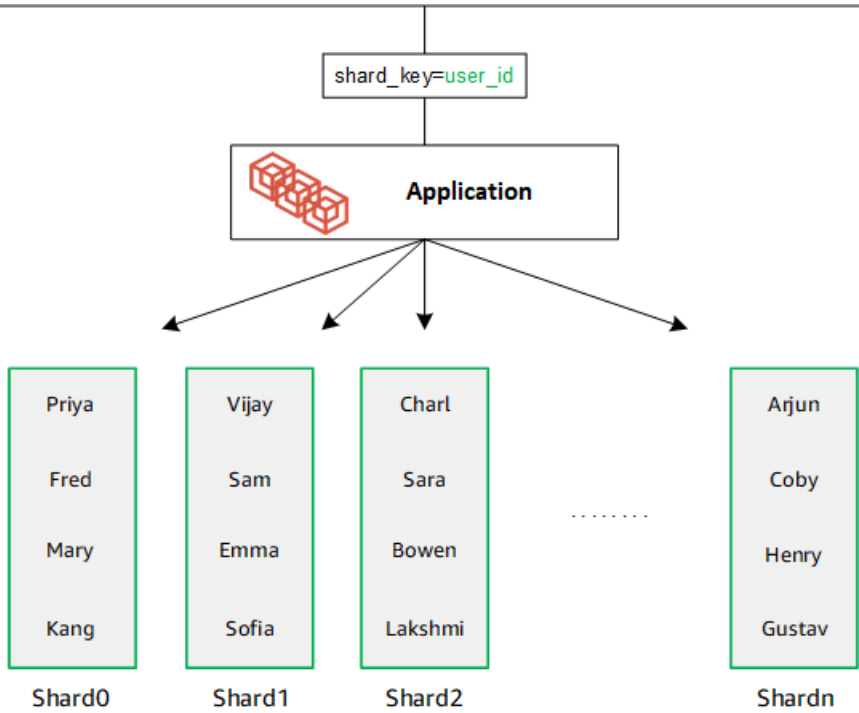
```
{ "name": "Priya", "lastname": "Kumar", "role": "Manager", "user_id": 1, "phone": "2223333" }
{ "name": "Mary", "lastname": "Johnson", "role": "Manager", "user_id": 2, "phone": "3334444" }
{ "name": "Vijay", "lastname": "Agarwal", "role": "Manager", "user_id": 3, "phone": "4445555" }
{ "name": "Emma", "lastname": "Wu", "role": "SW Architect", "user_id": 4, "phone": "6667777" }
{ "name": "Charl", "lastname": "Van rooyen", "role": "SW Architect", "user_id": 5, "phone": "7778888" }
{ "name": "Bowen", "lastname": "Chen", "role": "SW Developer", "user_id": 6, "phone": "8889999" }
{ "name": "Arjun", "lastname": "Reddy", "role": "SW Developer", "user_id": 7, "phone": "9991111" }
{ "name": "Henry", "lastname": "Carlson", "role": "Marketing", "user_id": 8, "phone": "1112222" }
```



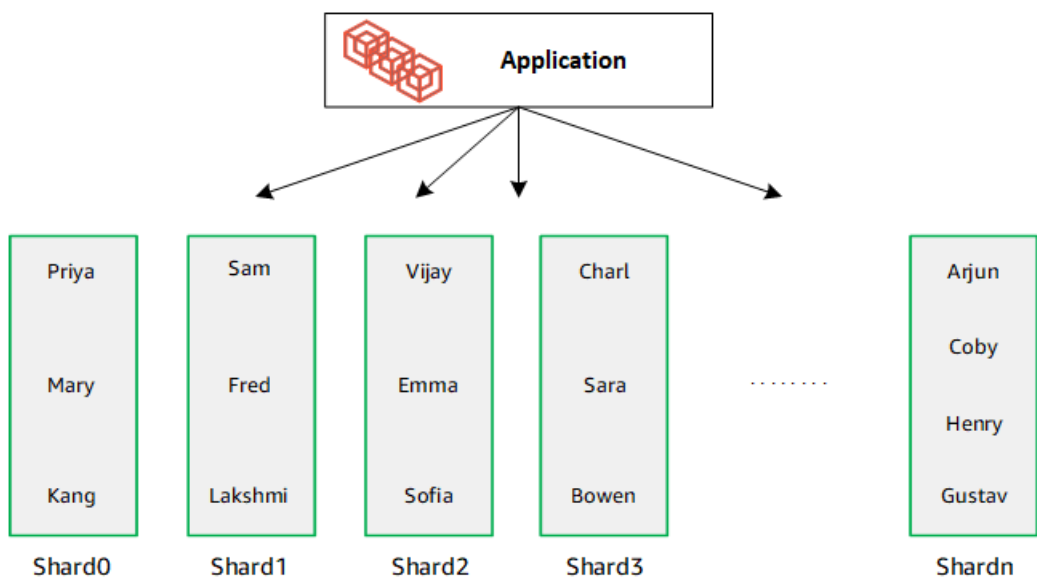
DocumentDB utilizza l'hash sharding per partizionare i dati tra gli shard sottostanti. I dati aggiuntivi vengono inseriti e distribuiti nello stesso modo:

Employee Dataset

```
{
  "name": "Sam", "lastname": "Fender", "role": "Manager", "user_id": 9, "phone": "2223333"
}, {
  "name": "Gustav", "lastname": "Friedrich", "role": "Manager", "user_id": 10, "phone": "3334444"
}, {
  "name": "Sara", "lastname": "Goldstien", "role": "Manager", "user_id": 11, "phone": "4445555"
}, {
  "name": "Fred", "lastname": "Williams", "role": "SW Architect", "user_id": 12, "phone": "6667777"
}, {
  "name": "Sofia", "lastname": "Velez", "role": "SW Architect", "user_id": 13, "phone": "7778888"
}, {
  "name": "Lakshmi", "lastname": "Ghosh", "role": "SW Developer", "user_id": 14, "phone": "8889999"
}, {
  "name": "Coby", "lastname": "Jones", "role": "SW Developer", "user_id": 15, "phone": "9991111"
}, {
  "name": "Kang", "lastname": "Zhu", "role": "Marketing", "user_id": 16, "phone": "1112222"
}
```



Quando ridimensioni il database aggiungendo shard aggiuntivi, Amazon DocumentDB ridistribuisce automaticamente i dati:



Migrazione elastica dei cluster

Amazon DocumentDB supporta la migrazione di dati condivisi MongoDB in cluster elastici. Sono supportati metodi di migrazione offline, online e ibridi. Per ulteriori informazioni, consulta [Migrazione ad Amazon DocumentDB](#).

Scalabilità elastica dei cluster

Amazon DocumentDB Elastic Clusters offre la possibilità di aumentare il numero di shard (scalabilità orizzontale) nel cluster elastico e il numero di vCPU applicate a ogni shard (scalabilità verticale). È inoltre possibile ridurre il numero di shard e la capacità di elaborazione (vCPU) in base alle esigenze.

Per le migliori pratiche di scalabilità, consulta [Dimdelle](#)

Note

È disponibile anche la scalabilità a livello di cluster. Per ulteriori informazioni, consulta [Scalabilità dei cluster Amazon DocumentDB](#).

Affidabilità elastica del cluster

Amazon DocumentDB è progettato per essere affidabile, durevole e tollerante ai guasti. Per migliorare la disponibilità, i cluster elastici distribuiscono due nodi per shard posizionati in diverse zone di disponibilità. Amazon DocumentDB include diverse funzionalità automatiche che lo rendono una soluzione di database affidabile. Per ulteriori informazioni, consulta [Affidabilità di Amazon DocumentDB](#).

Archiviazione e disponibilità di cluster elastici

I dati di Amazon DocumentDB sono archiviati in un volume cluster, che è un singolo volume virtuale che utilizza unità a stato solido (SSD). Un volume cluster è composto da sei copie dei dati, che vengono replicate automaticamente su più zone di disponibilità in una singola regione. AWS Questa replica contribuisce a garantire l'estrema durata dei tuoi dati e a ridurre il rischio di perdita dei dati. Consente inoltre di assicurare che il cluster non sia più disponibile durante un failover perché le copie dei dati sono già presenti in altre zone di disponibilità. Per ulteriori dettagli sullo storage, l'alta disponibilità e la replica, vedere [Amazon DocumentDB: come funziona](#)

Differenze funzionali tra Amazon DocumentDB 4.0 e cluster elastici

Esistono le seguenti differenze funzionali tra Amazon DocumentDB 4.0 e i cluster elastici.

- I risultati provengono da top e collStats sono partizionati per frammenti. Per le raccolte suddivise, i dati vengono distribuiti tra più partizioni e i collStats report vengono aggregati dalle partizioni. collScans
- Le statistiche di raccolta da top e collStats per le raccolte suddivise vengono reimpostate quando viene modificato il numero di frammenti del cluster.
- Il ruolo integrato di backup ora supporta. serverStatus Azione: gli sviluppatori e le applicazioni con ruolo di backup possono raccogliere statistiche sullo stato del cluster Amazon DocumentDB.
- Il SecondaryDelaySecs campo viene sostituito slaveDelay in replSetGetConfig output.
- Il hello comando sostituisce isMaster: hello restituisce un documento che descrive il ruolo del cluster elastico.
- L'\$elemMatch operatore nei cluster elastici corrisponde solo ai documenti nel primo livello di nidificazione di un array. In Amazon DocumentDB 4.0, l'operatore attraversa tutti i livelli prima di restituire i documenti corrispondenti. Per esempio:

```
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 ] } ] ] }
```

- La proiezione «\$» in Amazon DocumentDB 4.0 restituisce tutti i documenti con tutti i campi. Con i cluster elastici, il `find` comando con una proiezione «\$» restituisce documenti che corrispondono al parametro di query contenente solo il campo corrispondente alla proiezione «\$».
- Nei cluster elastici, i `find` comandi con `$regex` parametri di `$options` query restituiscono un errore: «Impossibile impostare opzioni sia in `$regex` che in `$options`».
- Con i cluster elastici, `$indexOfCP` ora restituisce «-1» quando:
 - la sottostringa non si trova in, o `string expression`
 - `start` è un numero maggiore di `end`, o
 - `start` è un numero maggiore della lunghezza in byte della stringa.

In Amazon DocumentDB 4.0, `$indexOfCP` restituisce «0» quando la `start` posizione è un numero maggiore `end` o la lunghezza in byte della stringa.

- Con i cluster elastici, le operazioni di proiezione in `_id fields`, ad esempio: `{"_id.nestedField" : 1}`, restituiscono documenti che includono solo il campo proiettato. In Amazon DocumentDB 4.0, invece, i comandi di proiezione di campo annidati non filtrano alcun documento.

Inizia a usare i cluster elastici di Amazon DocumentDB

Questa sezione introduttiva illustra come creare e interrogare il primo cluster elastico. Esistono molti modi per connettersi e iniziare a utilizzare i cluster elastici. Questa guida utilizza [AWS Cloud9](#) un terminale basato sul Web per connettersi e interrogare il cluster elastico utilizzando la shell mongo direttamente da AWS Management Console

Argomenti

- [Configurazione](#)
- [Fase 1: Creare un cluster elastico](#)
- [Fase 2: Creare un ambiente AWS Cloud9](#)
- [Passaggio 3: installa la shell mongo](#)
- [Fase 4: Connect al nuovo cluster elastico](#)

- [Fase 5: Condividi la tua raccolta; inserisci e interroga i dati](#)

Configurazione

[Se preferisci connetterti ad Amazon DocumentDB dal tuo computer locale creando una connessione SSH a un'istanza Amazon EC2, consulta Connecting with Amazon EC2.](#)

Prerequisiti

Prima di creare il tuo primo cluster Amazon DocumentDB, devi effettuare le seguenti operazioni:

Crea un account Amazon Web Services (AWS)

Prima di iniziare a utilizzare Amazon DocumentDB, devi disporre di un account Amazon Web Services (AWS). L' AWS account è gratuito. Paghi solo per i servizi e le risorse che utilizzi.

Se non ne possiedi uno Account AWS, completa i seguenti passaggi per crearne uno.

Per iscriverti a un Account AWS

1. Apri la pagina all'indirizzo <https://portal.aws.amazon.com/billing/signup>.
2. Segui le istruzioni online.

Nel corso della procedura di registrazione riceverai una telefonata, durante la quale sarà necessario inserire un codice di verifica attraverso la tastiera del telefono.

Quando ti iscrivi a un Account AWS, Utente root dell'account AWS viene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come best practice di sicurezza, [assegna l'accesso amministrativo a un utente amministrativo](#) e utilizza solo l'utente root per eseguire [attività che richiedono l'accesso di un utente root](#).

Imposta le autorizzazioni necessarie AWS Identity and Access Management (IAM).

L'accesso alla gestione delle risorse di Amazon DocumentDB come cluster, istanze e gruppi di parametri del cluster richiede credenziali che AWS possono essere utilizzate per autenticare le richieste. Per ulteriori informazioni, consulta [Identity and Access Management per Amazon DocumentDB](#).

1. Nella barra di ricerca di AWS Management Console, digita IAM e seleziona IAM nel menu a discesa.

2. Una volta che sei nella console IAM, seleziona Utenti dal pannello di navigazione.
3. Seleziona il tuo nome utente.
4. Fai clic sul pulsante Aggiungi autorizzazioni.
5. Seleziona Attach existing policies directly (Collega direttamente le policy esistenti).
6. Digita AmazonDocDBFullAccess nella barra di ricerca e selezionala quando appare nei risultati della ricerca.
7. Fai clic sul pulsante blu in basso che dice Avanti: revisione.
8. Fai clic sul pulsante blu in basso che dice Aggiungi autorizzazioni.

Crea un Amazon Virtual Private Cloud (Amazon VPC)

Questo passaggio è necessario solo se non disponi già di un Amazon VPC predefinito. In caso contrario, completa il passaggio 1 della [Guida introduttiva ad Amazon VPC nella Amazon VPC User Guide](#). Questa operazione richiederà meno di cinque minuti.

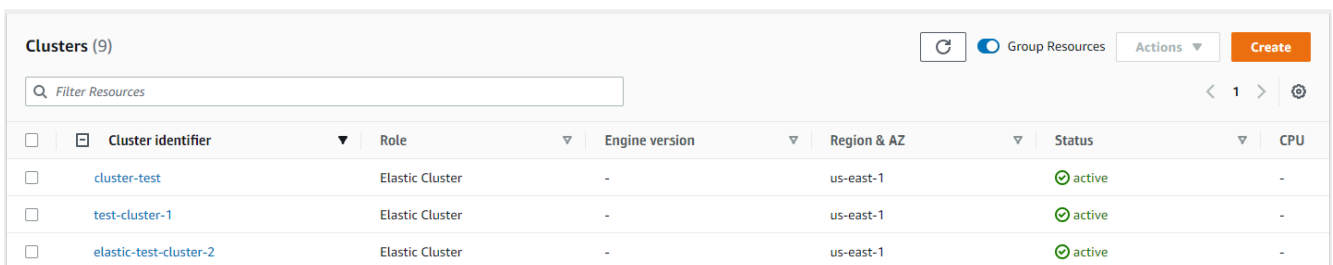
Fase 1: Creare un cluster elastico

In questa sezione spieghiamo come creare un cluster elastico nuovo di zecca, utilizzando AWS Management Console o AWS CLI con le seguenti istruzioni.

Using the AWS Management Console

Per creare una configurazione di cluster elastico utilizzando AWS Management Console:

1. Accedi [AWS Management Console](#) e apri la console Amazon DocumentDB.
2. Nella Console di gestione Amazon DocumentDB, in Clusters, scegli Crea.



The screenshot shows the 'Clusters (9)' page in the AWS Management Console. It features a search bar, a 'Group Resources' toggle, and an 'Actions' dropdown menu. Below these is a table with columns for Cluster identifier, Role, Engine version, Region & AZ, Status, and CPU. Three clusters are listed: 'cluster-test', 'test-cluster-1', and 'elastic-test-cluster-2', all with 'Elastic Cluster' roles, 'us-east-1' regions, and 'active' statuses.

<input type="checkbox"/>	Cluster identifier	Role	Engine version	Region & AZ	Status	CPU
<input type="checkbox"/>	cluster-test	Elastic Cluster	-	us-east-1	active	-
<input type="checkbox"/>	test-cluster-1	Elastic Cluster	-	us-east-1	active	-
<input type="checkbox"/>	elastic-test-cluster-2	Elastic Cluster	-	us-east-1	active	-

3. Nella pagina Crea cluster Amazon DocumentDB, nella sezione Tipo di cluster, scegli Elastic Cluster.

Cluster type

Instance Based Cluster
Instance based cluster can scale your database to millions of reads per second and upto 64TB of storage capacity. With instance based clusters you can choose your instance type based on your requirements.

Elastic Cluster
Elastic clusters can scale your database to millions of reads and writes per second, with petabytes of storage capacity. Elastic clusters support MongoDB compatible sharding APIs. With Elastic Clusters, you do not need to choose, manage or upgrade instances.


4. Nella pagina Crea cluster Amazon DocumentDB, nella sezione Configurazione, inserisci un identificatore univoco del cluster (seguendo i requisiti di denominazione sotto il campo).

Configuration

Cluster identifier
Specify a unique cluster identifier.


The cluster identifier is required, can have up to 50 characters, and must begin with a letter. It should not end with a hyphen or contain two consecutive hyphens. Valid characters: A-Z, a-z, 0-9, and -(hyphen)

5. Per i campi di configurazione dello shard:
- Nel campo Shard count, inserisci il numero di shard che desideri inserire nel cluster. Il numero massimo di shard per cluster è 32.

 **Note**

Verranno distribuiti due nodi per ogni shard. Entrambi i nodi avranno la stessa capacità di shard.

- Nel campo Shard instance count, scegli il numero di istanze di replica che desideri associare a ogni shard. Il numero massimo di istanze shard è 16, in incrementi di 1. Tutte le istanze di replica hanno la stessa capacità di shard definita nel campo seguente.

 **Note**

Il numero di istanze di replica si applica a tutti gli shard del cluster elastico. Un valore di conteggio delle istanze shard pari a 1 indica che esiste un'istanza di writer e tutte le istanze aggiuntive sono repliche che possono essere utilizzate per le letture e per migliorare la disponibilità.

- c. Nel campo Capacità dello shard, scegli il numero di CPU virtuali (vCPU) che desideri associare a ciascuna istanza dello shard. Il numero massimo di vCPU per istanza shard è 64. I valori consentiti sono 2, 4, 8, 16, 32, 64.

Configuration

Cluster Name
Specify a unique cluster identifier.

The cluster identifier is required, can have up to 50 characters, and must begin with a letter. It should not end with a hyphen or contain two consecutive hyphens. Valid characters: A-Z, a-z, 0-9, and -(hyphen)

Shard count
Number of shards the Elastic Cluster will use.

Shard instance count
Number of instances for each shard. All instances will have the same shard capacity.

Shard capacity
vCPU capacity of each shard.

6. Nel campo Virtual Private Cloud (VPC), scegli un VPC dall'elenco a discesa.

Per le sottoreti e i gruppi di sicurezza VPC, puoi utilizzare le impostazioni predefinite o selezionare tre sottoreti a tua scelta e fino a tre gruppi di sicurezza VPC (almeno uno).

Virtual Private Cloud (VPC)
VPC defines the virtual networking environment for this cluster.

vpc-5368fa2e ▼

Subnets

Select either 0 or 2-6 subnets ▼

VPC security groups
A security group acts as a virtual firewall for your instance to control inbound and outbound traffic.

Select VPC security groups ▼

default (VPC) ✕

7. Nella sezione Autenticazione, inserisci una stringa che identifica il nome di accesso dell'utente principale nel campo Nome utente.

Nel campo Password, inserisci una password univoca conforme alle istruzioni.

Authentication


Username
Specify an alphanumeric string that defines the login ID for the master user.

Password

Master password must be at least eight characters long and cannot contain a / (slash), " (double quote) or @ (at symbol).

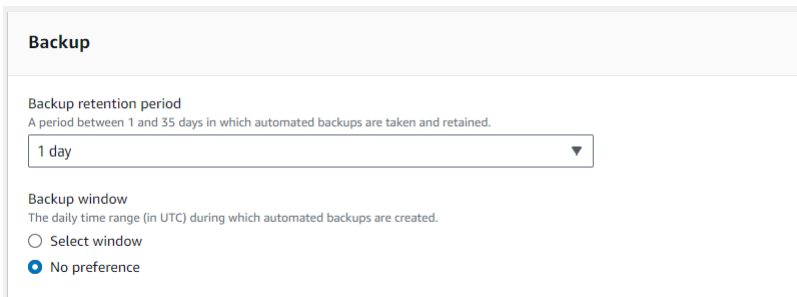
8. Nella sezione Crittografia, mantieni le impostazioni predefinite.

Facoltativamente, puoi inserire un AWS KMS key ARN che hai creato. Per ulteriori informazioni, consulta [Crittografia dei dati inattivi per i cluster elastici Amazon DocumentDB](#).

 **Important**

La crittografia deve essere abilitata per i cluster elastici.

9. Nella sezione Backup, modifica i campi in base ai requisiti di backup.



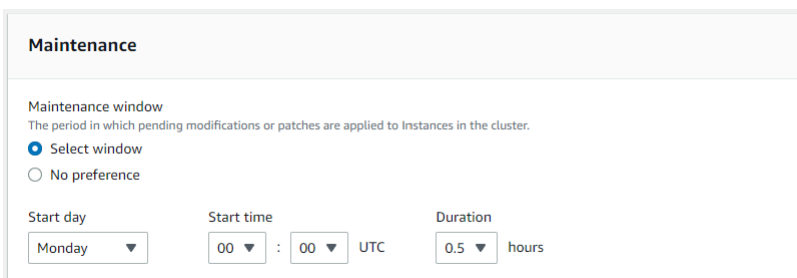
- a. Periodo di conservazione dei backup: nell'elenco, scegli il numero di giorni in cui conservare i backup automatici di questo cluster prima di eliminarli.
- b. Finestra di backup: imposta l'ora e la durata giornaliere durante le quali Amazon DocumentDB deve effettuare i backup di questo cluster.
 - i. Scegli Seleziona finestra se desideri configurare l'ora e la durata di creazione dei backup.

Ora di inizio: nel primo elenco, scegli l'ora di inizio (UTC) per avviare i backup automatici. Dal secondo elenco scegli il minuto dell'ora in cui desideri inizino i backup automatici.

Durata: nell'elenco, scegli il numero di ore da assegnare alla creazione di backup automatici.

- ii. Scegli Nessuna preferenza se desideri che Amazon DocumentDB scelga l'ora e la durata di creazione dei backup.

10. Nella sezione Manutenzione, scegli il giorno, l'ora e la durata in cui le modifiche o le patch vengono applicate al cluster.



11. Scegli Create cluster (Crea cluster).

Il cluster elastico è ora in fase di provisioning. Il completamento di questa operazione può richiedere fino a qualche minuto. È possibile connettersi al cluster quando lo stato del cluster elastico viene visualizzato, come **active** nell'elenco Cluster.

Using the AWS CLI

Per creare un cluster elastico utilizzando il AWS CLI, utilizza l'`create-cluster` operazione con i seguenti parametri:

- `--cluster-name`: obbligatorio. Il nome corrente del cluster in scala elastica immesso durante la creazione o l'ultima modifica.
- `--shard-capacity`: obbligatorio. Il numero di vCPU assegnate a ogni shard. Il massimo è 64. I valori consentiti sono 2, 4, 8, 16, 32, 64.
- `--shard-count`: obbligatorio. Il numero di shard assegnati al cluster. Il massimo è 32.
- `--shard-instance-count`—Facoltativo. Il numero di istanze di replica applicabili a tutti gli shard di questo cluster. Il massimo è 16.
- `--admin-user-name`: obbligatorio. Il nome utente associato all'utente amministratore.
- `--admin-user-password`: obbligatorio. La password associata all'utente amministratore.
- `--auth-type`: obbligatorio. Il tipo di autenticazione utilizzato per determinare dove recuperare la password utilizzata per accedere al cluster elastico. I tipi validi sono `PLAIN_TEXT` o `SECRET_ARN`.
- `--vpc-security-group-ids`—Facoltativo. Configura un elenco di gruppi di sicurezza VPC EC2 da associare a questo cluster.
- `--preferred-maintenance-window`—Facoltativo. Configura l'intervallo di tempo settimanale durante il quale può avvenire la manutenzione del sistema, in UTC (Universal Coordinated Time).

Il formato è: `ddd:hh24:mi-ddd:hh24:mi`. Giorni validi (gdd): lun, mar, mer, gio, ven, sab, dom

L'impostazione predefinita è una finestra di 30 minuti selezionata a caso da un periodo di 8 ore per ogni regione di Amazon Web Services, che si verifica in un giorno casuale della settimana.

Finestra minima di 30 minuti.

- `--kms-key-id`—Facoltativo. Configurare l'identificatore della chiave KMS per un cluster crittografato.

L'identificatore della chiave KMS è l'Amazon Resource Name (ARN) per la chiave di crittografia. AWS KMS Se stai creando un cluster utilizzando lo stesso account Amazon Web Services che possiede la chiave di crittografia KMS utilizzata per crittografare il nuovo cluster, puoi utilizzare l'alias della chiave KMS anziché l'ARN per la chiave di crittografia KMS.

Se non è specificata una chiave di crittografia `KmsKeyId` e se il `StorageEncrypted` parametro è vero, Amazon DocumentDB utilizza la chiave di crittografia predefinita.

- `--preferred-backup-window`—Facoltativo. L'intervallo di tempo giornaliero preferito durante il quale vengono creati i backup automatici. L'impostazione predefinita è una finestra di 30 minuti selezionata a caso da un periodo di 8 ore per ciascuna. Regione AWS
- `--backup-retention-period`—Facoltativo. Il numero di giorni durante i quali vengono conservati i backup automatici. Il valore predefinito è 1.
- `--storage-encrypted`—Facoltativo. Configura se il cluster è crittografato o meno.
 - `--no-storage-encrypted` specifica che il cluster non è crittografato.
- `--subnet-ids`—Facoltativo. Configura gli ID delle sottoreti di rete.

Nell'esempio seguente, sostituisci ogni *segnaposto dell'input utente* con le tue informazioni.

Note

Gli esempi seguenti includono la creazione di una chiave KMS specifica. Per utilizzare la chiave KMS predefinita, non includere il `--kms-key-id` parametro.

Per Linux, macOS o 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
```

Per 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
```

Fase 2: Creare un ambiente AWS Cloud9

AWS Cloud9 fornisce un terminale basato sul Web che puoi utilizzare per connetterti e interrogare i cluster elastici di Amazon DocumentDB utilizzando la shell mongo.

Note

Nota: l' AWS Cloud9 ambiente deve appartenere allo stesso gruppo di sicurezza dell'istanza. Puoi modificare il gruppo di sicurezza nella console [Amazon EC2](#).

1. Usa il tuo AWS account e accedi a AWS Management Console
2. Vai alla AWS Cloud9 console. Puoi digitare «Cloud9» nel campo di ricerca per individuarlo.
3. Nella home page dell'AWS Cloud9ambiente, scegli Crea ambiente.
4. Nella pagina Ambiente del nome, nel campo Nome, inserisci un nome a tua scelta.

Seleziona Fase successiva.

Name environment

Environment name and description

Name
The name needs to be unique per user. You can update it at any time in your environment settings.

Limit: 60 characters

Description - *Optional*
This will appear on your environment's card in your dashboard. You can update it at any time in your environment settings.

Write a short description for your environment

Limit: 200 characters

[Cancel](#) [Next step](#)

5. Nelle impostazioni dell'ambiente, nella sezione Tipo di ambiente, seleziona Crea una nuova istanza EC2 per l'ambiente (accesso diretto).

Nella sezione Tipo di istanza, seleziona il tipo di istanza appropriato per la tua rete.

Nella sezione Piattaforma, seleziona Amazon Linux 2 (consigliato).

Configure settings

Environment settings

Environment type [Info](#)

Run your environment in a new EC2 instance or an existing server. With EC2 instances, you can connect directly through Secure Shell (SSH) or connect via AWS Systems Manager (without opening inbound ports).

- Create a new EC2 instance for environment (direct access)**
Launch a new instance in this region that your environment can access directly via SSH.
- Create a new no-ingress EC2 instance for environment (access via Systems Manager)**
Launch a new instance in this region that your environment can access through Systems Manager.
- Create and run in remote server (SSH connection)**
Configure the secure connection to the remote server for your environment.

Instance type

- t2.micro (1 GiB RAM + 1 vCPU)**
Free-tier eligible. Ideal for educational users and exploration.
- t3.small (2 GiB RAM + 2 vCPU)**
Recommended for small-sized web projects.
- m5.large (8 GiB RAM + 2 vCPU)**
Recommended for production and general-purpose development.
- Other instance type**
Select an instance type.

t3.nano

Platform

- Amazon Linux 2 (recommended)**
- Amazon Linux AMI
- Ubuntu Server 18.04 LTS

6. Espandere Network settings (advanced) (Impostazioni di rete (avanzate)).

Scegli il VPC e una delle sottoreti che hai usato per creare il tuo cluster elastico.

Seleziona Fase successiva.

▼ Network settings (advanced)

Network (VPC)
 Launch your EC2 instance into an existing Amazon Virtual Private Cloud (VPC) or create a new one. To allow the AWS Cloud9 environment to connect to its EC2 instance, attach an internet gateway (IGW) to your new VPC.

vpc-5368fa2e (default) ↻ ↗ Create new VPC

Subnet
 Select a public subnet in which the EC2 instance is created. (For a private subnet, you must create an environment that connects to its instance via Systems Manager.)

subnet-21a7eb00 | Default in us-east-1c ↻ ↗ Create new subnet

No tags associated with the resource.

Add new tag

You can add 50 more tags.

Cancel
Previous step
Next step

7. Rivedi la tua configurazione. AWS Cloud9

Se la configurazione è corretta, scegli Crea ambiente.

Passaggio 3: installa la shell mongo

Una volta che AWS Cloud9 l'ambiente è pronto, sei pronto per connetterti al tuo cluster. Quindi, installa la shell mongo nell' AWS Cloud9 ambiente che hai creato nel passaggio 3. La mongo shell è un'utilità a riga di comando che usi per connettere e interrogare il tuo cluster elastico.

Se l' AWS Cloud9 ambiente è ancora aperto dalla Fase 3, tornate a quell'ambiente e passate all'istruzione 3. Se ti sei allontanato dal tuo AWS Cloud9 ambiente, nella AWS Cloud9 console, nella sezione I tuoi ambienti, trova l'ambiente etichettato con il nome impostato nel passaggio precedente. Scegli Open IDE.

1. Al prompt dei comandi, create il file del repository con il seguente comando:

Example

```
echo -e "[mongodb-org-4.0] \nname=MongoDB Repository\nbaseurl=https://
repo.mongodb.org/yum/amazon/2013.03/mongodb-org/4.0/x86_64/\ngpgcheck=1 \nenabled=1
```

```
\ngpgkey=https://www.mongodb.org/static/pgp/server-4.0.asc" | sudo tee /etc/
yum.repos.d/mongodb-org-4.0.repo
```

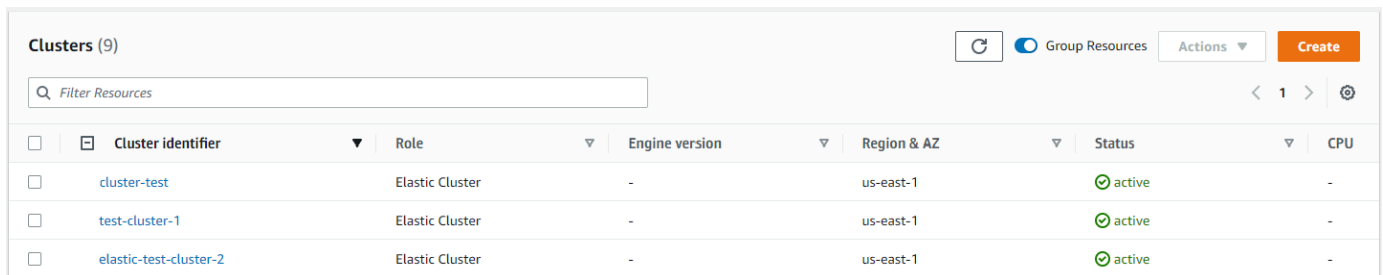
- Quando è completo, installa la shell mongo con il seguente comando:

```
sudo yum install -y mongodb-org-shell
```

Fase 4: Connect al nuovo cluster elastico

Connect al cluster utilizzando la shell mongo installata nello Step 4.

- Nella Console di gestione Amazon DocumentDB, in Clusters, individua il cluster. Ordina per ruolo per visualizzare tutti i cluster con il ruolo Elastic Cluster.



The screenshot shows the 'Clusters (9)' page in the Amazon DocumentDB console. It features a search bar, a 'Filter Resources' input, and a table with columns for Cluster identifier, Role, Engine version, Region & AZ, Status, and CPU. Three clusters are listed, all with the role 'Elastic Cluster' and status 'active'.

Cluster identifier	Role	Engine version	Region & AZ	Status	CPU
cluster-test	Elastic Cluster	-	us-east-1	active	-
test-cluster-1	Elastic Cluster	-	us-east-1	active	-
elastic-test-cluster-2	Elastic Cluster	-	us-east-1	active	-

- Scegli il cluster che hai creato selezionando l'identificatore del cluster. Da Connettività e sicurezza, copia l'endpoint e incollalo nel tuo AWS Cloud9 ambiente.

Connect

Connect to this cluster with the mongo shell [Copy](#)

```
mongo mongodb://vin:<insertPassword>@dec-feats-477568677630.us-west-
2.docdb-elastic.amazonaws.com:27017 -ssl
```

- Una volta connesso, dovresti vedere il seguente output:

```
Admin:~/environment $ mongo mongodb://vin:mytestpw@dec-feats-477568254530.us-west-2.docdb-elastic.amazonaws.com:27017 -ssl
MongoDB shell version v4.0.28
connecting to: mongodb://dec-feats-477568254530.us-west-2.docdb-elastic.amazonaws.com:27017/?gssapiServiceName=mongodb
Implicit session: session { "id" : UUID("7413d0ae-43d4-426e-bbe8-c2dabb0b257b") }
MongoDB server version: 5.0.0
WARNING: shell and server versions do not match
mongos>
```

Fase 5: Condividi la tua raccolta; inserisci e interroga i dati

I cluster elastici aggiungono il supporto per lo sharding in Amazon DocumentDB. Ora che sei connesso al cluster, puoi suddividere il cluster, inserire dati ed eseguire alcune query.

1. Per condividere una raccolta, inserisci quanto segue:

```
sh.shardCollection("db.Employee1" , { "Employeeid" : "hashed" })
```

2. Per inserire un singolo documento, inserisci quanto segue:

```
db.Employee1.insert({"Employeeid":1, "Name":"Joe", "LastName": "Bruin",  
"level": 1 })
```

Viene visualizzato il seguente output:

```
WriteResult({ "nInserted" : 1 })
```

3. Per leggere il documento che hai scritto, inserisci il `findOne()` comando (restituisce un singolo documento):

```
db.Employee1.findOne()
```

Viene visualizzato il seguente output:

Example

```
{  
  "_id" : ObjectId("61f344e0594fe1a1685a8151"),  
  "EmployeeID" : 1,  
  "Name" : "Joe",  
  "LastName" : "Bruin",  
  "level" : 1  
}
```

4. Per eseguire qualche altra domanda, considera un caso d'uso di un profilo di gioco. Innanzitutto, inserisci alcune voci in una raccolta intitolata «Employee». Inserisci i seguenti dati:

Example

```
db.Employee1.insertMany([  
  { "Employeeid" : 1, "name" : "Matt", "lastname": "Winkle", "level": 12},  
  { "Employeeid" : 2, "name" : "Frank", "lastname": "Chen", "level": 2},
```

```
{ "Employeeid" : 3, "name" : "Karen", "lastname": "William", "level": 7},  
  { "Employeeid" : 4, "name" : "Katie", "lastname": "Schaper", "level": 3}  
])
```

Viene visualizzato il seguente output:

```
{ "acknowledged" : true, "insertedIds" : [ 1, 2, 3, 4 ] }
```

5. Per restituire tutti i documenti della raccolta di profili, immettete il comando `find ()`:

```
db.Employee1.find()
```

Vengono visualizzati i dati inseriti nel passaggio 4.

6. Per interrogare un singolo documento, includi un filtro (ad esempio: «Katie»). Inserisci i seguenti dati:

```
db.Employee1.find({name: "Katie"})
```

Viene visualizzato il seguente output:

```
{ "_id" : 4, "name" : "Katie", "lastname": "Schaper", "level": 3 }
```

7. Per trovare un profilo e modificarlo, inserisci il `findAndModify` comando. In questo esempio, al dipendente «Matt» viene assegnato un livello superiore di «14»:

Example

```
db.Employee1.findAndModify(  
  query: { "Employeeid" : 1, "name" : "Matt"},  
  update: { "Employeeid" : 1, "name" : "Matt", "lastname" : "Winkle", "level" :  
    14 }  
)
```

Viene visualizzato il seguente output (si noti che il livello non è ancora cambiato):

Example

```
{  
  "_id" : 1,  
  "name" : "Matt",  
  "lastname" : "Winkle",  
  "level" : 12,
```

```
}
```

8. Per verificare l'aumento del livello, inserisci la seguente query:

```
db.Employee1.find({name: "Matt"})
```

Viene visualizzato il seguente output:

```
{ "_id" : 1, "name" : "Matt", "lastname" : "winkle", "level" : 14 }
```

Best practice

Scopri le best practice per Amazon DocumentDB utilizzo di Tutte le [best practice per i cluster Amazon DocumentDB basati su istanze](#) si applicano anche ai cluster elastici. Questa sezione viene continuamente aggiornata man mano che vengono identificate nuove best practice.

Argomenti

- [Scelta delle chiavi di](#)
- [Gestione delle connessioni](#)
- [Raccolte non condivise](#)
- [Dimdelle](#)
- [Mon](#)

Scelta delle chiavi di

L'elenco seguente descrive le linee guida per la creazione di chiavi shard.

- Usa una chiave hash distribuita in modo uniforme per distribuire i tuoi dati su tutti gli shard del cluster (evita i tasti di scelta rapida).
- Usa la tua chiave shard in tutte le richieste di lettura/aggiornamento/eliminazione per evitare le query di raccolta dispersione.
- Evita le chiavi condivise annidate durante le operazioni di lettura/aggiornamento/eliminazione.
- Quando si eseguono operazioni in batch, `ordered` impostate su `false` in modo che tutti gli shard possano essere eseguiti in parallel e migliorare le latenze.

Gestione delle connessioni

L'elenco seguente descrive le linee guida per la gestione delle connessioni al database.

- Monitora il numero di connessioni e la frequenza con cui le nuove connessioni vengono aperte e chiuse.
- Distribuisci le connessioni su tutte le sottoreti nella configurazione dell'applicazione. Se il cluster è configurato in più sottoreti ma si utilizza solo un sottoinsieme delle sottoreti, è possibile che si verifichi un collo di bottiglia sul numero massimo di connessioni.

Raccolte non condivise

Di seguito vengono descritte le linee guida per le raccolte non condivise.

- Quando lavori con raccolte non condivise, per distribuire il carico, prova a conservare le raccolte non condivise altamente utilizzate su database diversi. I cluster elastici di Amazon DocumentDB collocano i database su diversi shard e collocano contemporaneamente le raccolte non condivise per lo stesso database sullo stesso shard.

Dimdelle

L'elenco seguente descrive le linee guida per scalare i cluster elastici.

- Le operazioni di scalabilità possono causare un breve periodo di errori intermittenti del database e della rete. Quando possibile, evita la scalabilità nelle ore di punta. Di seguito sono illustrate le best practice per l'utilizzo di manutenzione.
- È preferibile scalare la capacità dello shard verso l'alto e verso il basso (modificando il numero di vCPU per shard) per aumentare l'elaborazione piuttosto che aumentare o diminuire il numero di shard in quanto è più veloce e comporta una durata più breve degli errori intermittenti del database e della rete.
- Quando prevedi una crescita, preferisci aumentare il numero di frammenti invece di aumentare la capacità dei frammenti. Ciò consente di scalare il cluster aumentando la capacità dello shard per gli scenari in cui è necessario scalare rapidamente.
- Monitora le policy relative ai tentativi sul lato client e riprova con backoff e jitter esponenziali per evitare di sovraccaricare il database quando si verificano errori durante il ridimensionamento.

Mon

L'elenco seguente descrive le linee guida per il monitoraggio dei cluster elastici.

- Tieni traccia del peak-to-average rapporto tra le metriche per frammento per determinare se stai generando traffico irregolare (hai un hot-key/hot-spot). Le metriche chiave per tracciare i peak-to-average rapporti sono:
 - `PrimaryInstanceCPUUtilization`
 - Questo può essere monitorato a livello di ogni frammento.
 - A livello di cluster è possibile monitorare lo skew medio fino a p99.
 - `PrimaryInstanceFreeableMemory`
 - Questo può essere monitorato a livello di ogni frammento.
 - A livello di cluster è possibile monitorare lo skew medio fino a p99.
 - `DatabaseCursorsMax`
 - Questo deve essere monitorato a livello di ogni frammento per determinare l'inclinazione.
 - `Documents-Inserted/Updated/Returned/Deleted`
 - Questo deve essere monitorato a livello di ogni frammento per determinare l'inclinazione.

Gestione dei cluster elastici

Per gestire un cluster elastico di Amazon DocumentDB, è necessario disporre di una policy IAM con le autorizzazioni appropriate del piano di controllo di Amazon DocumentDB. Queste autorizzazioni consentono di creare, modificare ed eliminare i cluster. La `FullAccess` policy di Amazon DocumentDB fornisce tutte le autorizzazioni necessarie per amministrare un cluster elastico Amazon DocumentDB.

I seguenti argomenti mostrano come eseguire varie attività quando si lavora con i cluster elastici di Amazon DocumentDB.

Argomenti

- [Modifica delle configurazioni dei cluster elastici](#)
- [Monitoraggio di un cluster elastico](#)
- [Eliminazione di un cluster elastico](#)
- [Gestione delle istantanee dei cluster elastici](#)
- [Arresto e avvio di un cluster elastico Amazon DocumentDB](#)

Modifica delle configurazioni dei cluster elastici

In questa sezione spieghiamo come modificare il cluster elastico, utilizzando AWS Management Console o AWS CLI con le seguenti istruzioni.

Uno degli usi principali della modifica del cluster consiste nel ridimensionare gli shard aumentando o diminuendo il numero di shard e/o la capacità di calcolo degli shard.

Using the AWS Management Console

Per modificare una configurazione elastica del cluster utilizzando: AWS Management Console

1. Accedi [AWS Management Console](#) e apri la console Amazon DocumentDB.
2. Nel pannello di navigazione scegliere Clusters (Cluster).

Tip

Se non vedi il riquadro di navigazione sul lato sinistro dello schermo, scegli l'icona del menu nell'angolo in alto a sinistra del pannello di navigazione.

3. Scegli il nome del cluster che desideri modificare nella colonna Identificatore del cluster.
4. Scegli Modifica.
5. Modifica i campi che desideri modificare, quindi seleziona Modifica cluster.

Configuration

Cluster identifier

SampleCluster

Shard count

Number of shards the Elastic Cluster will use.

Shard instance count

Number of instances for each shard. All instances will have the same shard capacity.

Shard capacity

vCPU capacity of each shard.

Maintenance

Maintenance window

The period in which pending modifications or patches are applied to your Elastic cluster.

- Select window
- No preference

Authentication

Username

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

- subnet-0b2962f92a0f5a8fb X
- subnet-08c6d849efd4dfe96 X

VPC security groups

Note

In alternativa, puoi accedere alla finestra di dialogo Modifica cluster accedendo alla pagina Cluster, selezionando la casella accanto al cluster, scegliendo Azioni, quindi Modifica.

Using the AWS CLI

Per modificare una configurazione di cluster elastico utilizzando il AWS CLI, utilizza l'`update-cluster` operazione con i seguenti parametri:

- **--cluster-arn**: obbligatorio. L'identificatore ARN del cluster che si desidera modificare.
- **--shard-capacity**—Facoltativo. Il numero di vCPU assegnate a ogni shard. Il massimo è 64. I valori consentiti sono 2, 4, 8, 16, 32, 64.
- **--shard-count**—Facoltativo. Il numero di shard assegnati al cluster. Il massimo è 32.
- **--shard-instance-Count**: facoltativo. Il numero di istanze di replica che si applicano a tutti gli shard di questo cluster. Il massimo è 16.
- **--auth-type**—Facoltativo. Il tipo di autenticazione utilizzato per determinare dove recuperare la password utilizzata per accedere al cluster elastico. I tipi validi sono PLAIN_TEXT o SECRET_ARN.
- **--admin-user-password**—Facoltativo. La password associata all'utente amministratore.
- **--vpc-security-group-ids**—Facoltativo. Configura un elenco di gruppi di sicurezza Amazon EC2 e Amazon Virtual Private Cloud (VPC) da associare a questo cluster.
- **--preferred-maintenance-window**—Facoltativo. Configura l'intervallo di tempo settimanale durante il quale può avvenire la manutenzione del sistema, in UTC (Universal Coordinated Time)

Il formato è: `ddd:hh24:mi-ddd:hh24:mi`. Giorni validi (gdd): lun, mar, mer, gio, ven, sab, dom

L'impostazione predefinita è una finestra di 30 minuti selezionata a caso da un periodo di 8 ore per ogni regione di Amazon Web Services, che si verifica in un giorno casuale della settimana.

Finestra minima di 30 minuti.

- **--subnet-ids**—Facoltativo. Configura gli ID delle sottoreti di rete.

Nell'esempio seguente, sostituisci ogni *segnaposto dell'input utente* con le tue informazioni.

Per Linux, macOS o 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
```

Per 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
```

Per monitorare lo stato del cluster elastico dopo la modifica, vedi Monitoraggio di un cluster elastico.

Monitoraggio di un cluster elastico

In questa sezione, spieghiamo come monitorare il cluster elastico, utilizzando AWS Management Console o AWS CLI con le seguenti istruzioni.

Using the AWS Management Console

Per monitorare una configurazione di cluster elastico utilizzando AWS Management Console:

1. Accedi [AWS Management Console](#) e apri la console Amazon DocumentDB.
2. Nel pannello di navigazione scegliere Clusters (Cluster).

Tip

Se non vedi il riquadro di navigazione sul lato sinistro dello schermo, scegli l'icona del menu nell'angolo in alto a sinistra del pannello di navigazione.

3. Scegli il nome del cluster che desideri monitorare nella colonna Identificatore del cluster.
4. Scegliere la scheda Monitoring (Monitoraggio).

▼ Summary			
Cluster Name SampleCluster	Cluster identifier cc05c8f6-e529-4f10-87d5-7ee3b5b4c7b9	Shard count 2	Shard capacity 2 vCPUs
Instances per shard 2	Cluster status 🟢 active		

Connectivity & security | Configuration | Tags | **Monitoring**

CloudWatch Vengono visualizzati alcuni grafici di Amazon per le seguenti categorie di monitoraggio:

- Utilizzo delle risorse
- Prestazioni
- Latenza
- Operazioni
- System (Sistema)

Puoi anche accedere ad Amazon CloudWatch tramite il AWS Management Console per configurare il tuo ambiente di monitoraggio per i tuoi cluster elastici.

Using the AWS CLI

Per monitorare una configurazione specifica di un cluster elastico utilizzando il AWS CLI, utilizza l'`get-cluster` operazione con i seguenti parametri:

- **--cluster-arn**: obbligatorio. L'identificatore ARN del cluster per il quale desideri informazioni.

Nell'esempio seguente, sostituisci ogni *segnaposto dell'input utente* con le tue informazioni.

Per Linux, macOS o Unix:

```
aws docdb-elastic get-cluster \  
  --cluster-arn arn:aws:docdb-elastic:us-west-2:123456789012:cluster:/68ffcdf8-  
e3af-40a3-91e4-24736f2dacc9
```

Per Windows:

```
aws docdb-elastic get-cluster ^  
  --cluster-arn arn:aws:docdb:-elastic:us-west-2:123456789012:cluster:/68ffcdf8-  
e3af-40a3-91e4-24736f2dacc9
```

L'output di questa operazione è simile al seguente:

```
"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",  
  ...  
}
```

Per ulteriori informazioni, consulta `DescribeClusterSnapshot` Amazon DocumentDB Resource Management API Reference.

Per visualizzare i dettagli di tutti i cluster elastici che utilizzano il AWS CLI, utilizza l'`list-clusters` operazione con i seguenti parametri:

- **--next-token**—Facoltativo. Se l'output del numero di elementi (`--max-results`) è inferiore rispetto al numero totale di elementi restituito dalle chiamate API sottostanti, l'output include

NextToken, che può essere trasferito a un comando successivo per recuperare il set di elementi successivo.

- **--max-results**—Facoltativo. Il numero totale di elementi da restituire nell'output del comando. Se esistono più risultati rispetto al `max-results` valore specificato, nella risposta viene incluso un token di paginazione (`next-token`) in modo da poter recuperare i risultati rimanenti.
 - Impostazione predefinita: 100
 - Minimo 20, massimo 100

Nell'esempio seguente, sostituisci ogni *segnaposto dell'input utente* con le tue informazioni.

Per Linux, macOS o Unix:

```
aws docdb-elastic list-clusters \  
  --next-token eyJNYXJrZXIiOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQiOiAxfQ== \  
  --max-results 2
```

Per Windows:

```
aws docdb-elastic list-clusters ^  
  --next-token eyJNYXJrZXIiOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQiOiAxfQ== ^  
  --max-results 2
```

L'output di questa operazione è simile al seguente:

```
{  
  "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"
  }
]
}
```

Eliminazione di un cluster elastico

In questa sezione spieghiamo come eliminare un cluster elastico, utilizzando AWS Management Console o AWS CLI con le seguenti istruzioni.

Using the AWS Management Console

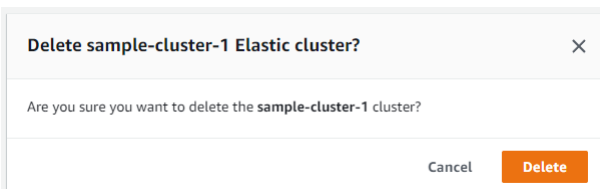
Per eliminare una configurazione di cluster elastico utilizzando AWS Management Console:

1. Accedi [AWS Management Console](#) e apri la console Amazon DocumentDB.
2. Nel pannello di navigazione scegliere Clusters (Cluster).

Tip

Se non vedi il riquadro di navigazione sul lato sinistro dello schermo, scegli l'icona del menu nell'angolo in alto a sinistra del pannello di navigazione.

3. Nella tabella con l'elenco dei cluster, seleziona la casella di controllo a sinistra del nome del cluster che desideri eliminare, quindi scegli Azioni. Dal menu a discesa, scegli Delete (Elimina).
4. Nel cluster elastico Elimina «nome-cluster»? nella finestra di dialogo, scegli Elimina.



Sono necessari alcuni minuti per l'eliminazione del cluster. Per monitorare lo stato del cluster, consulta [Monitoraggio dello stato di un cluster Amazon DocumentDB](#).

Using the AWS CLI

Per eliminare un cluster elastico utilizzando il AWS CLI, utilizza l'`delete-cluster` operazione con i seguenti parametri:

- **--cluster-arn**: obbligatorio. L'identificatore ARN del cluster che si desidera eliminare.
- **--no-skip-final-backup**—Facoltativo. Se si desidera un backup finale, è necessario includere questo parametro con un nome per il backup finale. È necessario includere `--final-backup-identifier` o `--skip-final-backup`.
- **--skip-final-backup**—Facoltativo. Utilizzate questo parametro solo se non desiderate eseguire un backup finale prima di eliminare il cluster. L'impostazione predefinita prevede l'acquisizione di uno snapshot finale

I seguenti esempi di AWS CLI codice eliminano un cluster con un ARN di `arn:aws:docdb:us-west-2:123456789012:sharded-cluster:sample-cluster` con un backup finale.

Nell'esempio seguente, *sostituisci ogni segnaposto di input dell'utente con le tue informazioni*.

Per Linux, macOS o 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
```

Per 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
```

I seguenti esempi di AWS CLI codice eliminano un cluster con un ARN di `arn:aws:docdb:us-west-2:123456789012:sharded-cluster:sample-cluster` senza eseguire un backup finale.

Nell'esempio seguente, sostituisci ogni *segnaposto dell'input utente* con le tue informazioni.

Per Linux, macOS o Unix:

```
aws docdb-elastic delete-cluster \  
  --cluster-arn arn:aws:docdb:us-west-2:123456789012:sharded-cluster:sample-cluster \  
  --skip-final-backup \  
  
```

Per Windows:

```
aws docdb-elastic delete-cluster ^  
  --cluster-arn arn:aws:docdb:us-west-2:123456789012:sharded-cluster:sample-cluster ^  
  --skip-final-backup ^  
  
```

L'output dell'operazione è una visualizzazione del cluster che si sta `delete-cluster` eliminando.

Sono necessari alcuni minuti per l'eliminazione del cluster. Per monitorare lo stato del cluster, consulta [Monitoraggio dello stato di un cluster Amazon DocumentDB](#).

Gestione delle istantanee dei cluster elastici

Le istantanee manuali possono essere scattate dopo la creazione di un cluster elastico. I backup automatici vengono creati nel momento in cui viene creata l'istanza del cluster elastico.

Note

Il cluster elastico deve essere nello `Available` stato in cui è possibile scattare un'istanza manuale.

Questa sezione spiega come creare, visualizzare, ripristinare ed eliminare istantanee di cluster elastici.

I seguenti argomenti mostrano come eseguire varie attività quando si lavora con istantanee di cluster elastici di Amazon DocumentDB.

Argomenti

- [Creazione manuale di uno snapshot del cluster elastico](#)
- [Visualizzazione di un'istantanea del cluster elastico](#)
- [Ripristino di un cluster elastico da un'istantanea](#)
- [Copia di un'istantanea del cluster elastico](#)
- [Eliminazione di un'istantanea del cluster elastico](#)
- [Gestione di un backup automatico di snapshot del cluster elastico](#)

Creazione manuale di uno snapshot del cluster elastico

In questa sezione viene spiegato come creare uno snapshot manuale di un cluster elastico, utilizzando AWS Management Console o AWS CLI con le seguenti istruzioni.

Using the AWS Management Console

Per creare un'istantanea manuale del cluster elastico utilizzando: AWS Management Console

1. Accedi [AWS Management Console](#) e apri la console Amazon DocumentDB.
2. Nel pannello di navigazione, selezionare Snapshots (Snapshot).

Tip

Se non vedi il riquadro di navigazione sul lato sinistro dello schermo, scegli l'icona del menu nell'angolo in alto a sinistra del pannello di navigazione.

3. Nella pagina Snapshots (Snapshot) scegli Create (Crea).
4. Nella pagina Crea un'istantanea del cluster, nel campo Identificatore del cluster, scegli il tuo cluster elastico dall'elenco a discesa.

Nel campo Identificatore Snapshot, inserisci un identificatore univoco per il tuo cluster elastico.

Scegli Crea.

Create cluster snapshot

Settings
To create a snapshot, select a cluster and specify a snapshot identifier.

Cluster identifier
Cluster identifier. This is the unique key that identifies a cluster.

elastic-test-cluster-2

Snapshot identifier [Info](#)
Identifier for the cluster snapshot.

elastic-snapshot-2

Cancel Create

Note

In alternativa, puoi accedere alla finestra di dialogo Crea istantanea del cluster andando alla pagina Cluster, selezionando la casella accanto al cluster, quindi scegliendo Azioni, quindi Scatta istantanea.

Lo snapshot del cluster elastico è ora in fase di provisioning. Il completamento di questa operazione può richiedere fino a qualche minuto. È possibile visualizzare e ripristinare dall'istantanea quando lo stato è visualizzato, come `Available` nell'elenco Istantanee.

Using the AWS CLI

Per creare un'istantanea manuale del cluster elastico utilizzando il AWS CLI, utilizzate l'`create-cluster-snapshot` operazione con i seguenti parametri:

- **--snapshot-name**: obbligatorio. Il nome dello snapshot del cluster che si desidera creare.
- **--cluster-arn**: obbligatorio. L'identificatore ARN del cluster di cui si desidera creare un'istantanea.

Nell'esempio seguente, sostituisci ogni *segnaposto dell'input utente* con le tue informazioni.

Per Linux, macOS o 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
```

Per 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
```

Visualizzazione di un'istantanea del cluster elastico

In questa sezione spieghiamo come visualizzare le informazioni sugli snapshot del cluster elastico, utilizzando AWS Management Console o AWS CLI con le seguenti istruzioni.

Using the AWS Management Console

Per visualizzare le informazioni su uno specifico snapshot del cluster elastico, utilizzare: AWS Management Console

1. Accedi [AWS Management Console](#) e apri la console Amazon DocumentDB.
2. Nel pannello di navigazione, selezionare Snapshots (Snapshot).

Tip

Se non vedi il riquadro di navigazione sul lato sinistro dello schermo, scegli l'icona del menu nell'angolo in alto a sinistra del pannello di navigazione.

3. Nella pagina Istantanee, scegli la tua istantanea dall'elenco facendo clic sul nome nella colonna dell'identificatore dell'istantanea.
4. Visualizza le informazioni sull'istantanea in Dettagli.

test-snapshot-id-1

▼ Details	
ARN arn:aws:rds:us-east-1:477568257630:cluster-snapshot:test-snapshot-id-1	Snapshot identifier test-snapshot-id-1
Cluster Name docdb-2022-07-18-22-22-13	VPC vpc-5368fa2e
Snapshot type manual	Engine docdb
Engine version 4.0.0	Master username vin
Status 🟢 available	Storage 6 GiB
Storage type manual	Snapshot creation time 10/25/2022, 4:02:04 PM UTC-5
KMS key ID arn:aws:kms:us-east-1:477568257630:key/93644e8d-77ea-484c-80a6-8fb24c901385	Cluster creation time 7/18/2022, 5:22:59 PM UTC-5

Using the AWS CLI

Per visualizzare informazioni su uno specifico snapshot del cluster elastico utilizzando il AWS CLI, utilizzate l'`get-cluster-snapshot` operazione con i seguenti parametri:

- **--snapshot-arn**: obbligatorio. L'identificatore ARN dell'istantanea per la quale desideri informazioni.

Nell'esempio seguente, sostituisci ogni *segnaposto dell'input utente* con le tue informazioni.

Per Linux, macOS o Unix:

```
aws docdb-elastic get-cluster-snapshot \
  --snapshot-arn sampleResourceName
```

Per Windows:

```
aws docdb-elastic get-cluster-snapshot ^
  --snapshot-arn sampleResourceName
```

Per visualizzare informazioni su uno specifico snapshot del cluster elastico utilizzando il AWS CLI, utilizzate l'`get-cluster-snapshot` operazione con i seguenti parametri:

- **--snapshot-arn**: obbligatorio. L'identificatore ARN dell'istantanea per la quale desideri informazioni.

Nell'esempio seguente, sostituisci ogni *segnaposto dell'input utente* con le tue informazioni.

Per Linux, macOS o Unix:

```
aws docdb-elastic get-cluster-snapshot \  
  --snapshot-arn sampleResourceName
```

Per Windows:

```
aws docdb-elastic get-cluster-snapshot ^  
  --snapshot-arn sampleResourceName
```

Per visualizzare le informazioni su tutte le istantanee del cluster elastico che utilizzano il AWS CLI, utilizzate l'`list-cluster-snapshots` operazione con i seguenti parametri:

- **--snapshot-type**—Facoltativo. Il tipo di istantanee del cluster da restituire. È possibile specificare uno dei seguenti valori:
 - `automated`- Restituisci tutte le istantanee del cluster che Amazon DocumentDB ha creato automaticamente per AWS il tuo account.
 - `manual`- Restituisci tutte le istantanee del cluster che hai creato manualmente per il tuo account. AWS
 - `shared`- Restituisci tutte le istantanee manuali del cluster che sono state condivise con il tuo AWS account.
 - `public`- Restituisce tutte le istantanee del cluster che sono state contrassegnate come pubbliche.
- **--next-token**—Facoltativo. Token di paginazione opzionale fornito da una richiesta precedente. Se viene specificato questo parametro, la risposta include solo i record oltre a questo token, fino al valore specificato da `max-results`.
- **--max-results**—Facoltativo. Il numero massimo di risultati da includere nella risposta. Se esistono più risultati rispetto al `max-results` valore specificato, nella risposta viene incluso un token di paginazione (`next-token`) in modo da poter recuperare i risultati rimanenti.

- Impostazione predefinita: 100
- Minimo 20, massimo 100

Nell'esempio seguente, sostituisci ogni *segnaposto dell'input utente* con le tue informazioni.

Per Linux, macOS o Unix:

```
aws docdb-elastic list-cluster-snapshots \  
  --snapshot-type value \  
  --next-token value \  
  --max-results 50
```

Per Windows:

```
aws docdb-elastic list-cluster-snapshots ^  
  --snapshot-type value ^  
  --next-token value ^  
  --max-results 50
```

Ripristino di un cluster elastico da un'istantanea

In questa sezione viene spiegato come ripristinare un cluster elastico da un'istantanea, utilizzando AWS Management Console o AWS CLI con le seguenti istruzioni.

Using the AWS Management Console

Per ripristinare un cluster elastico da un'istantanea utilizzando: AWS Management Console

1. Accedi [AWS Management Console](#) e apri la console Amazon DocumentDB.
2. Nel pannello di navigazione, selezionare Snapshots (Snapshot).

Tip

Se non vedi il riquadro di navigazione sul lato sinistro dello schermo, scegli l'icona del menu nell'angolo in alto a sinistra del pannello di navigazione.

3. Scegli il pulsante a sinistra dell'istantanea, che desideri utilizzare per ripristinare un cluster, nella colonna Identificatore dell'istantanea.

4. Scegli Azioni, quindi Ripristina.

Restore snapshot

You are creating a new cluster from a source instance from a cluster snapshot. This new cluster will have the default cluster parameter group.

Configuration

Snapshot Name
The name for the snapshot.
test-snapshot-id-1

Cluster identifier [Info](#)
Specify a unique cluster identifier.

Instance class [Info](#)

2 vCPUs 16GiB RAM

Number of instances [Info](#)

5. Nella pagina Ripristina istantanea, inserisci un nome per il nuovo cluster nel campo Identificatore del cluster.

Note

Per qualsiasi ripristino manuale delle istantanee, è necessario creare un nuovo cluster.

6. Nel campo Virtual Private Cloud (VPC), scegli un VPC dall'elenco a discesa.
7. Per le sottoreti e i gruppi di sicurezza VPC, puoi utilizzare le impostazioni predefinite o selezionare tre sottoreti a tua scelta e fino a tre gruppi di sicurezza VPC (almeno uno).
8. Se si è soddisfatti della configurazione del cluster, scegliere Restore cluster (Ripristina cluster) e attendere il ripristino del cluster.

Using the AWS CLI

Per ripristinare un cluster elastico da un'istantanea utilizzando il, utilizzate l'operazione con i seguenti parametri: AWS CLI `restore-cluster-from-snapshot`

- **--cluster-name**: obbligatorio. Il nome corrente del cluster elastico immesso durante la creazione o l'ultima modifica.
- **--snapshot-arn**: obbligatorio. L'identificatore ARN dello snapshot utilizzato per ripristinare il cluster.

- **--vpc-security-group-ids**—Facoltativo. Uno o più gruppi di sicurezza Amazon EC2 e Amazon Virtual Private Cloud (VPC) da associare al cluster.
- **--kms-key-id**—Facoltativo. Configurare l'identificatore della chiave KMS per un cluster crittografato.

L'identificatore della chiave KMS è l'Amazon Resource Name (ARN) per la chiave di crittografia. AWS KMS Se stai creando un cluster utilizzando lo stesso account Amazon Web Services che possiede la chiave di crittografia KMS utilizzata per crittografare il nuovo cluster, puoi utilizzare l'alias della chiave KMS anziché l'ARN per la chiave di crittografia KMS.

Se non è specificata una chiave di crittografia `KmsKeyId` e se il `StorageEncrypted` parametro è vero, Amazon DocumentDB utilizza la chiave di crittografia predefinita.

- **--subnet-ids**—Facoltativo. ID di sottorete di rete.

Nell'esempio seguente, sostituisci ogni *segnaposto di input dell'utente* con le tue informazioni.

Per Linux, macOS o 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
```

Per 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
```

Copia di un'istantanea del cluster elastico

In Amazon DocumentDB, puoi copiare istantanee di cluster elastici manuali e automatici all'interno della stessa regione e all'interno dello stesso account. In questa sezione spieghiamo come copiare uno snapshot di un cluster elastico, utilizzando o. AWS Management Console AWS CLI

Using the AWS Management Console

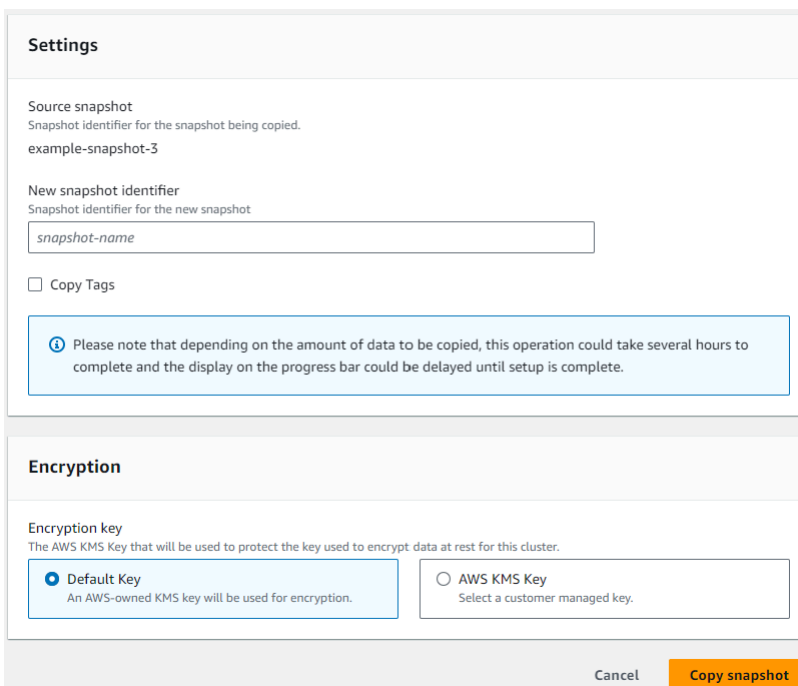
Per copiare un'istantanea del cluster elastico utilizzando: AWS Management Console

1. Accedi [AWS Management Console](#) e apri la console Amazon DocumentDB.
2. Nel pannello di navigazione, selezionare Snapshots (Snapshot).

Tip

Se non vedi il riquadro di navigazione sul lato sinistro dello schermo, scegli l'icona del menu nell'angolo in alto a sinistra del pannello di navigazione.

3. Scegli il pulsante a sinistra dell'istantanea che desideri copiare nella colonna dell'identificatore dell'istantanea.
4. Scegli Azioni, quindi Copia.



The screenshot shows the 'Copy snapshot' dialog box in the AWS Management Console. It is divided into two main sections: 'Settings' and 'Encryption'. In the 'Settings' section, there is a 'Source snapshot' field with the value 'example-snapshot-3' and a 'New snapshot identifier' text input field containing 'snapshot-name'. There is a checkbox for 'Copy Tags' which is currently unchecked. A blue information box contains a warning: 'Please note that depending on the amount of data to be copied, this operation could take several hours to complete and the display on the progress bar could be delayed until setup is complete.' The 'Encryption' section has two radio button options: 'Default Key' (selected) and 'AWS KMS Key'. At the bottom, there are 'Cancel' and 'Copy snapshot' buttons.

5. Per New snapshot identifier, inserisci il nome della nuova istantanea.

6. Per Copia tag, seleziona la casella se desideri copiare tutti i tag dallo snapshot del cluster elastico di origine allo snapshot del cluster elastico di destinazione.
7. Per la crittografia, scegli una chiave AWS KMS predefinita o una chiave KMS a tua scelta. La seconda opzione ti consente di selezionare una chiave KMS esistente che hai già creato o di crearne una nuova.
8. Scegli Copia istantanea al termine.

Using the AWS CLI

Per copiare un'istantanea del cluster elastico utilizzando il AWS CLI, utilizzate l'`copy-cluster-snapshot` operazione con i seguenti parametri:

- **--source-db-cluster-snapshot-identifier**: obbligatorio. L'identificatore dello snapshot del cluster elastico esistente che viene copiato. L'istantanea del cluster elastico deve esistere ed essere nello stato disponibile. Se si copia l'istantanea su un'altra Regione AWS, questo identificatore deve essere nel formato ARN dell'origine. Regione AWS Questo parametro non distingue tra maiuscole e minuscole.
- **--target-db-cluster-snapshot-identifier**: obbligatorio. L'identificatore della nuova istantanea del cluster elastico da creare a partire dall'istantanea del cluster esistente. Questo parametro non distingue tra maiuscole e minuscole.

Vincoli relativi al nome dello snapshot di destinazione:

- Non può essere il nome di uno snapshot esistente.
- La lunghezza è di [1—63] lettere, numeri o trattini.
- Il primo carattere deve essere una lettera.
- Non può terminare con un trattino o contenere due trattini consecutivi.

Nell'esempio seguente, sostituisci ogni *segnaposto dell'input utente* con le tue informazioni.

Per Linux, macOS o Unix:

```
aws docdb-elastic copy-cluster-snapshot \  
  --source-cluster-snapshot-arn <sample ARN> \  
  --target-cluster-snapshot-name my-target-copied-snapshot
```

Per Windows:

```
aws docdb-elastic copy-cluster-snapshot ^
  --source-cluster-snapshot-arn <sample ARN> ^
  --target-cluster-snapshot-name my-target-copied-snapshot
```

Eliminazione di un'istantanea del cluster elastico

In questa sezione viene spiegato come eliminare un'istantanea di un cluster elastico, utilizzando o. AWS Management Console AWS CLI

Using the AWS Management Console

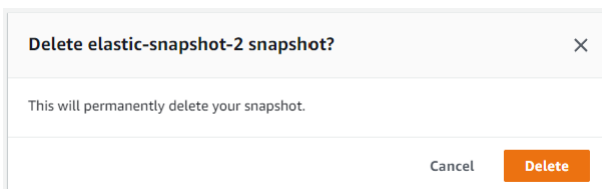
Per ripristinare un cluster elastico da un'istantanea utilizzando: AWS Management Console

1. Accedi [AWS Management Console](#) e apri la console Amazon DocumentDB.
2. Nel pannello di navigazione, selezionare Snapshots (Snapshot).

Tip

Se non vedi il riquadro di navigazione sul lato sinistro dello schermo, scegli l'icona del menu nell'angolo in alto a sinistra del pannello di navigazione.

3. Scegli il pulsante a sinistra dell'istantanea, che desideri utilizzare per ripristinare un cluster, nella colonna Identificatore dell'istantanea.
4. Scegli Operazioni, quindi Elimina.



5. Nella finestra di dialogo Elimina istantanea «snapshot-name», scegli Elimina.

Using the AWS CLI

Per eliminare un'istantanea del cluster elastico utilizzando il AWS CLI, utilizzate l'operazione con i seguenti parametri: `delete-cluster-snapshot`

- **--snapshot-arn**: obbligatorio. L'identificatore ARN dello snapshot utilizzato per ripristinare il cluster.

Nell'esempio seguente, sostituisci ogni *segnaposto di input dell'utente* con le tue informazioni.

Per Linux, macOS o Unix:

```
aws docdb-elastic delete-cluster-snapshot \  
  --snapshot-arn sampleResourceName
```

Per Windows:

```
aws docdb-elastic delete-cluster-snapshot ^  
  --snapshot-arn sampleResourceName
```

Gestione di un backup automatico di snapshot del cluster elastico

Amazon DocumentDB acquisisce istantanee giornaliere dei tuoi cluster elastici. Puoi specificare la finestra di backup preferita e il periodo di conservazione del backup in una configurazione di snapshot del cluster elastico nuova o esistente. In questa sezione viene spiegato come impostare i parametri di backup automatico in un'istanza del cluster elastico, utilizzando o. AWS Management Console AWS CLI

Using the AWS Management Console

Per impostare un backup automatico per una nuova istanza del cluster elastico utilizzando: AWS Management Console

1. Accedi [AWS Management Console](#) e apri la console Amazon DocumentDB.
2. Nel pannello di navigazione scegliere Clusters (Cluster).

Tip

Se non vedi il riquadro di navigazione sul lato sinistro dello schermo, scegli l'icona del menu nell'angolo in alto a sinistra del pannello di navigazione.

3. Scegli il pulsante a sinistra del cluster per il quale desideri modificare le impostazioni di backup nella colonna Identificatore del cluster.
4. Scegli Azioni, quindi Modifica.
5. Nella sezione Backup, modifica i campi in base ai requisiti di backup.

Backup

Backup retention period
A period between 1 and 35 days in which automated backups are taken and retained.

1 day ▼

Backup window
The daily time range (in UTC) during which automated backups are created.

Select window

No preference

- a. Periodo di conservazione dei backup: nell'elenco, scegli il numero di giorni in cui conservare i backup automatici di questo cluster prima di eliminarli.
- b. Finestra di backup: imposta l'ora e la durata giornaliere durante le quali Amazon DocumentDB deve effettuare i backup di questo cluster.
 - i. Scegli Seleziona finestra se desideri configurare l'ora e la durata di creazione dei backup.

Ora di inizio: nel primo elenco, scegli l'ora di inizio (UTC) per avviare i backup automatici. Dal secondo elenco scegli il minuto dell'ora in cui desideri inizino i backup automatici.

Durata: nell'elenco, scegli il numero di ore da assegnare alla creazione di backup automatici.

- ii. Scegli Nessuna preferenza se desideri che Amazon DocumentDB scelga l'ora e la durata di creazione dei backup.

6. Al termine, scegli Modifica cluster.

Using the AWS CLI

Per impostare un backup automatico per una nuova istantanea del cluster elastico utilizzando il AWS CLI, utilizzate l'`create-cluster-snapshot` operazione con i seguenti parametri:

- **--preferred-backup-window**—Facoltativo. L'intervallo di tempo giornaliero preferito durante il quale vengono creati i backup automatici. L'impostazione predefinita è una finestra di 30 minuti selezionata a caso da un intervallo di tempo di 8 ore per ciascuna. Regione AWS

Vincoli:

- Il valore deve essere nel formato `hh24:mi-hh24:mi`.
- Il valore deve essere nel fuso orario UTC (Universal Coordinated Time).

- Il valore non deve essere in conflitto con la finestra di manutenzione preferita.
- Il valore deve essere almeno di 30 minuti.
- **--backup-retention-period**—Facoltativo. Il numero di giorni durante i quali vengono conservati i backup automatici. Il valore predefinito è 1.

Vincoli:

- È necessario specificare un valore minimo di 1.
- L'intervallo è compreso tra 1 e 35.

i Note

I backup automatici vengono eseguiti solo quando il cluster è in uno stato «attivo».

i Note

È inoltre possibile modificare i `backup-retention-period` parametri `preferred-backup-window` e di un cluster elastico esistente utilizzando il `aws docdb-elastic update-cluster` comando.

Nell'esempio seguente, sostituisci ogni *segnaposto dell'input utente* con le tue informazioni.

L'create-clusteresempio seguente crea il cluster elastico Amazon DocumentDB sample-cluster con un periodo di conservazione per i backup automatici di 7 giorni e una finestra di backup preferita di 18:00-18:30 UTC.

Per Linux, macOS o Unix:

```
aws docdb-elastic create-cluster \  
  --cluster-name sample-cluster \  
  --shard-capacity 2 \  
  --shard-count 2 \  
  --admin-user-name SampleAdmin \  
  --auth-type PLAIN_TEXT \  
  --backup-retention-period 7 \  
  --preferred-backup-window 18:00-18:30
```

```
--admin-user-password SamplePass123! \  
--preferred-backup-window 18:00-18:30 \  
--backup-retention-period 7
```

Per 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
```

Arresto e avvio di un cluster elastico Amazon DocumentDB

L'arresto e l'avvio dei cluster elastici di Amazon DocumentDB può aiutarti a gestire i costi per gli ambienti di sviluppo e test. Invece di creare ed eliminare cluster elastici ogni volta che usi Amazon DocumentDB, puoi interrompere temporaneamente il cluster quando non è necessario. Potrai quindi riavviarlo quando riprenderai i test.

Argomenti

- [Panoramica dell'arresto e dell'avvio di un cluster elastico](#)
- [Operazioni che è possibile eseguire su un cluster elastico interrotto](#)

Panoramica dell'arresto e dell'avvio di un cluster elastico

Nei periodi in cui non è necessario un cluster elastico Amazon DocumentDB, è possibile interrompere il cluster. È possibile avviare nuovamente il cluster ogni volta che è necessario utilizzarlo. L'avvio e l'arresto semplificano i processi di configurazione e smontaggio dei cluster elastici utilizzati per lo sviluppo, il test o attività simili che non richiedono una disponibilità continua. È possibile arrestare e avviare un cluster elastico utilizzando AWS Management Console o il AWS CLI con una singola azione.

Mentre il cluster elastico è fermo, il volume di archiviazione del cluster rimane invariato. Vengono addebitati solo i costi per lo storage, gli snapshot manuali e lo storage di backup automatici

all'interno della finestra di retention specificata. Amazon DocumentDB avvia automaticamente il tuo cluster elastico dopo sette giorni in modo da non rimanere indietro rispetto agli aggiornamenti di manutenzione richiesti. Quando il cluster si avvia dopo sette giorni, inizieranno nuovamente a essere addebitati i costi per l'utilizzo del cluster elastico. Mentre il cluster è fermo, non è possibile interrogare il volume di archiviazione perché l'interrogazione richiede che il cluster sia nello stato disponibile.

Quando un cluster elastico Amazon DocumentDB viene interrotto, il cluster non può essere modificato in alcun modo. Ciò include l'eliminazione del cluster.

Using the AWS Management Console

La procedura seguente mostra come arrestare un cluster elastico nello stato disponibile o avviare un cluster elastico interrotto.


Per arrestare o avviare un cluster elastico Amazon DocumentDB

1. [Accedi a e apri AWS Management Console la console Amazon DocumentDB all'indirizzo https://console.aws.amazon.com/docdb](https://console.aws.amazon.com/docdb).
2. Nel pannello di navigazione scegliere Clusters (Cluster).

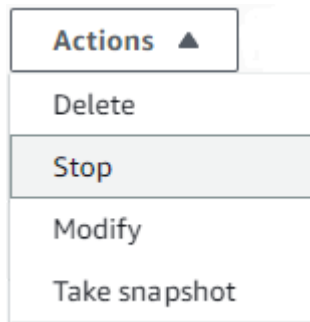
Tip

Se il riquadro di navigazione non viene visualizzato sul lato sinistro della schermata, scegliere l'icona del menu (☰) nell'angolo in alto a sinistra della pagina.

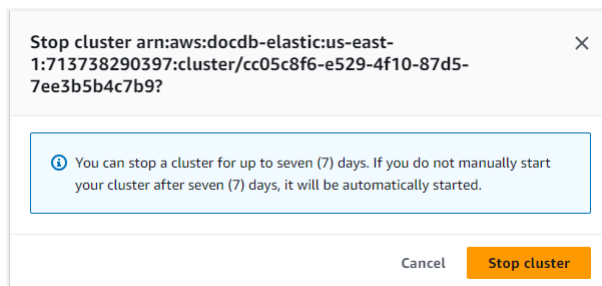
3. Quindi, nell'elenco dei cluster, scegliere il pulsante a sinistra del nome del cluster che si desidera arrestare o avviare.

<input checked="" type="checkbox"/>	SampleCluster	Elastic Cluster	-	us-east-1	
-------------------------------------	---------------	-----------------	---	-----------	---

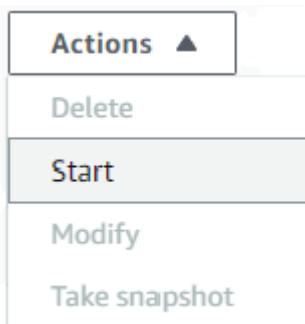
4. Scegliere Actions (Operazioni) e quindi scegliere l'operazione che si desidera eseguire sul cluster.
 - Se si desidera arrestare il cluster e il cluster è disponibile:
 - a. Scegli Stop (Arresta).



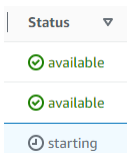
- b. Nella finestra di dialogo di conferma, conferma che desideri interrompere il cluster elastico scegliendo **Arresta cluster** oppure, per mantenere il cluster in esecuzione, scegli **Annulla**.



- Se si desidera avviare il cluster e il cluster è arrestato, scegliere **Start (Avvia)**.



5. Monitora lo stato del cluster elastico. Se hai avviato il cluster, puoi riprendere a utilizzarlo quando il cluster sarà disponibile. Per ulteriori informazioni, consulta [Determinazione dello stato di un cluster](#).



Using the AWS CLI

I seguenti esempi di codice mostrano come arrestare un cluster elastico nello stato attivo o disponibile o avviare un cluster elastico interrotto.

Per interrompere un cluster elastico utilizzando il AWS CLI, utilizzare l'operazione `stop-cluster`. Per avviare un cluster arrestato, utilizzare l'operazione `start-cluster`. Entrambe le operazioni consentono di utilizzare il parametro `--cluster-arn`.

Parametro:

- **`--cluster-arn`**: obbligatorio. L'identificatore ARN del cluster elastico che si desidera interrompere o avviare.

Example — Per arrestare un cluster elastico utilizzando AWS CLI

Nell'esempio seguente, sostituisci ogni *segnaposto dell'input utente* con le tue informazioni.

Il codice seguente arresta il cluster elastico con un ARN di `arn:aws:docdb-elastic:us-east-1:477568257630:cluster/b9f1d489-6c3e-4764-bb42-da62ceb7bda2`

Note

Il cluster elastico deve essere nello stato attivo o disponibile.

Per Linux, macOS o Unix:

```
aws docdb-elastic stop-cluster \  
  --cluster-arn arn:aws:docdb-elastic:us-east-1:477568257630:cluster/  
b9f1d489-6c3e-4764-bb42-da62ceb7bda2
```


Per Windows:

```
aws docdb-elastic stop-cluster ^  
  --cluster-arn arn:aws:docdb-elastic:us-east-1:477568257630:cluster/  
b9f1d489-6c3e-4764-bb42-da62ceb7bda2
```

Example — Per avviare un cluster elastico utilizzando AWS CLI

Nell'esempio seguente, sostituisci ogni *segnaposto dell'input utente* con le tue informazioni.

Il codice seguente avvia il cluster elastico con un ARN di. `arn:aws:docdb-elastic:us-east-1:477568257630:cluster/b9f1d489-6c3e-4764-bb42-da62ceb7bda2`

 Note

Il cluster elastico deve essere attualmente interrotto.

Per Linux, macOS o Unix:

```
aws docdb-elastic start-cluster \  
  --cluster-arn arn:aws:docdb-elastic:us-east-1:477568257630:cluster/  
b9f1d489-6c3e-4764-bb42-da62ceb7bda2
```

Per Windows:

```
aws docdb-elastic start-cluster ^  
  --cluster-arn arn:aws:docdb-elastic:us-east-1:477568257630:cluster/  
b9f1d489-6c3e-4764-bb42-da62ceb7bda2
```

Operazioni che è possibile eseguire su un cluster elastico interrotto

Non è possibile modificare la configurazione di un cluster elastico Amazon DocumentDB mentre il cluster è fermo. Devi avviare il cluster prima di eseguire questo tipo di operazioni amministrative.

Amazon DocumentDB applica qualsiasi manutenzione programmata al cluster elastico interrotto solo dopo che è stato riavviato. Dopo sette giorni, Amazon DocumentDB avvia automaticamente un cluster elastico interrotto in modo che non rimanga troppo indietro nello stato di manutenzione. Al riavvio del cluster elastico, ricomincerai a farti pagare per gli shard presenti nel cluster.

Mentre un cluster elastico viene interrotto, Amazon DocumentDB non esegue backup automatici né prolunga il periodo di conservazione dei backup.

Crittografia dei dati inattivi per i cluster elastici Amazon DocumentDB

I seguenti argomenti ti aiutano a conoscere, creare e monitorare le chiavi di AWS Key Management Service crittografia per i cluster elastici di Amazon DocumentDB:

Argomenti

- [In che modo i cluster elastici di Amazon DocumentDB utilizzano le sovvenzioni in AWS KMS](#)
- [Creazione di una chiave gestita dal cliente](#)
- [Monitoraggio delle chiavi di crittografia per i cluster elastici Amazon DocumentDB](#)
- [Ulteriori informazioni](#)

I cluster elastici di Amazon DocumentDB si integrano automaticamente con AWS Key Management Service (AWS KMS) per la gestione delle chiavi e utilizzano un metodo noto come crittografia a busta per proteggere i tuoi dati. Per ulteriori informazioni sulla crittografia envelope, consulta [Crittografia envelope](#) nella Guida per sviluppatori di AWS Key Management Service.

Una AWS KMS key è la rappresentazione logica di una chiave. La chiave KMS include metadati, ad esempio l'ID della chiave, la data di creazione, la descrizione e lo stato della chiave. La chiave KMS contiene anche il materiale della chiave utilizzato per crittografare e decrittare i dati. Per ulteriori informazioni sulle chiavi KMS, consulta [AWS KMS keys](#) nella Guida per gli sviluppatori di AWS Key Management Service.

I cluster elastici di Amazon DocumentDB supportano la crittografia con due tipi di chiavi:

- **Chiavi di proprietà:** i cluster elastici di Amazon DocumentDB utilizzano queste chiavi di default per crittografare automaticamente i dati di identificazione personale. Non puoi visualizzare, gestire o utilizzare chiavi di proprietà o utilizzare chiavi o utilizzare chiavi o utilizzare chiavi o utilizzare chiavi AWS di proprietà o utilizzare chiavi o utilizzare chiavi di proprietà o utilizzare chiavi. Tuttavia, non devi intervenire o modificare alcun programma per proteggere le chiavi che eseguono la crittografia dei dati. Per ulteriori informazioni, consulta [le chiavi AWS possedute](#) nella Guida per gli sviluppatori di AWS Key Management Service.
- **Chiavi gestite dal cliente:** simmetriche da creare, AWS KMS keys possedute e gestite dal cliente. Poiché hai il pieno controllo di questo livello di crittografia, puoi eseguire attività come:
 - Stabilire e mantenere politiche chiave
 - Definizione e gestione delle politiche e delle sovvenzioni IAM

- Abilitazione e disabilitazione delle policy chiave
- Rotazione del materiale crittografico
- Aggiunta di tag
- Creazione di alias chiave
- Pianificazione delle chiavi per la cancellazione

Per ulteriori informazioni, consulta [Chiavi gestite dai clienti](#) nella Guida per gli AWS Key Management Service sviluppatori.

Important

Per crittografare il cluster è necessario utilizzare una chiave KMS per crittografare il cluster poiché Amazon DocumentDB supporta solo chiavi KMS. Non utilizzare una chiave KMS per tentare di crittografare i dati nei cluster elastici Amazon DocumentDB. Per ulteriori informazioni, consulta [Chiavi asimmetriche AWS KMS nella Guida](#) per gli AWS Key Management Service sviluppatori.

Se Amazon DocumentDB non riesce più ad accedere alla chiave di crittografia per un cluster, ad esempio quando viene revocato l'accesso a una chiave, il cluster crittografato passa a uno stato terminale. In questo caso, puoi solo ripristinare il cluster da un backup. Per Amazon DocumentDB, i backup sono sempre abilitati per 1 giorno. Inoltre, se disabiliti la chiave per un cluster Amazon DocumentDB crittografato, alla fine perderai l'accesso di lettura e scrittura a quel cluster. Quando Amazon DocumentDB trova un cluster crittografato da una chiave alla quale non ha accesso, imposta il cluster in uno stato terminale. In questo stato, il cluster non è più disponibile e lo stato attuale del database non può essere ripristinato. Per ripristinare il cluster, devi riabilitare l'accesso alla chiave di crittografia per Amazon DocumentDB e ripristinare il cluster da un backup.

Important

Non puoi modificare la chiave KMS per un cluster crittografato dopo averlo già creato. Assicurati di determinare i requisiti della chiave di crittografia prima di creare il cluster elastico crittografato.

In che modo i cluster elastici di Amazon DocumentDB utilizzano le sovvenzioni in AWS KMS

I cluster elastici Amazon DocumentDB richiedono una [concessione](#) per utilizzare la chiave gestita dal cliente.

Quando crei un cluster crittografato con una chiave gestita dal cliente, i cluster elastici Amazon DocumentDB creano una concessione per tuo conto inviando una `CreateGrant` richiesta a AWS KMS. Le concessioni in AWS KMS vengono utilizzate per consentire ai cluster elastici Amazon DocumentDB a una chiave KMS in un account cliente.

I cluster elastici Amazon DocumentDB richiedono la concessione per utilizzare la chiave gestita dal cliente per le seguenti operazioni interne:

- Invia `DescribeKey` richieste AWS KMS a per verificare che l'ID chiave KMS simmetrico gestito dal cliente, inserito durante la creazione di un tracker o di una collezione di geofence, sia valido.
- Invia `GenerateDataKey` richieste AWS KMS a per generare chiavi dati crittografate dalla chiave gestita dal cliente.
- Invia `Decrypt` richieste AWS KMS a per decrittografare le chiavi di dati crittografate in modo che possano essere utilizzate per crittografare i dati.
- Puoi revocare l'accesso alla concessione o rimuovere l'accesso del servizio alla chiave gestita dal cliente in qualsiasi momento. In tal caso, i cluster elastici Amazon DocumentDB non saranno in grado di accedere a nessuno dei dati crittografati dalla chiave gestita dal cliente; ciò influisce sulle operazioni che dipendono da tali dati.

Creazione di una chiave gestita dal cliente

Puoi creare una chiave simmetrica gestita dal cliente utilizzando la AWS Management Console o le AWS KMS API.

Creazione simmetrica di chiavi gestita dal cliente

Segui i passaggi per la [creazione di una chiave simmetrica gestita dal cliente nella Guida per gli AWS Key Management Services](#) sviluppatori.

Policy delle chiavi

Le policy chiave controllano l'accesso alla chiave gestita dal cliente. Ogni chiave gestita dal cliente deve avere esattamente una policy delle chiavi, che contiene istruzioni che determinano

chi può usare la chiave e come la possono usare. Quando crei la chiave gestita dal cliente, puoi specificare una policy chiave. Per ulteriori informazioni, consulta le informazioni di accesso alle chiavi KMS disponibili nella [AWS Key Management Service panoramica](#) della Guida per gli AWS Key Management Service sviluppatori.

Per utilizzare la chiave gestita dal cliente con le risorse elastiche Amazon DocumentDB, è necessario che le seguenti operazioni API siano consentite nella policy chiave:

- [kms:CreateGrant](#)— Aggiunge una concessione a una chiave gestita dal cliente. Concede l'accesso di controllo a una chiave KMS specificata, che consente l'accesso alle operazioni di concessione richieste da Amazon Location Service. Per ulteriori informazioni sull'utilizzo delle sovvenzioni, consulta [Grants AWS KMS in](#) the AWS Key Management Service Developer Guide.
- [kms:DescribeKey](#)— Fornisce i dettagli chiave gestiti dal cliente per consentire a Docdb Elastic di convalidare la chiave.
- [kms:Decrypt](#)— Consente a Docdb Elastic di utilizzare la chiave dati crittografata archiviata per accedere ai dati crittografati.
- [kms:GenerateDataKey](#)— Consente a Docdb Elastic di generare una chiave di dati crittografata e di archivarla perché la chiave dati non viene utilizzata immediatamente per la crittografia.

Per ulteriori informazioni, consulta [Autorizzazioni per AWS i servizi nelle politiche chiave](#) e [Risoluzione dei problemi di accesso tramite chiave](#) nella Guida per gli AWS Key Management Service sviluppatori.

Limitazione dell'accesso alle chiavi gestite dai clienti tramite policy IAM

Oltre alle politiche chiave KMS, puoi anche limitare le autorizzazioni delle chiavi KMS in una politica IAM.

Esistono diversi modi per rendere la policy IAM più efficace. Ad esempio, per consentire alla chiave gestita dal cliente di essere utilizzata solo per le richieste che provengono da cluster elastici Amazon DocumentDB, puoi utilizzare la [chiave di kms:ViaService condizione](#) con il `docdb-elastic.<region-name>.amazonaws.com` valore.

Per ulteriori informazioni, consultare [Consentire agli utenti in altri account di utilizzare una chiave KMS](#) nella Guida per gli sviluppatori di AWS Key Management Service.

Monitoraggio delle chiavi di crittografia per i cluster elastici Amazon DocumentDB

Quando utilizzi una chiave gestita AWS KMS key dal cliente con le tue risorse Docdb Elastic, puoi utilizzare AWS CloudTrail Amazon CloudWatch Logs per tenere traccia delle richieste inviate da Docdb Elastic. AWS KMS

I seguenti esempi sono AWS CloudTrail eventi per `CreateGrant` `GenerateDataKeyWithoutPlainTextDecrypt`, e `DescribeKey` monitorare AWS KMS key le operazioni richiamate dai cluster elastici di Amazon DocumentDB per accedere ai dati crittografati dalla chiave gestita dal cliente:

CreateGrant

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAI0SF0DNN7EXAMPLE:Sampleuser01",
    "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSF0DNN7EXAMPLE3",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAI0SF0DNN7EXAMPLE",
        "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":
"0ab0acd0b000f00ea00cc0a0e00fc00bce000c000f0000000c0bc0a0000aaafSAMPLE",
  "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": "AROAIQDTESTANDEXAMPLE:Sampleuser01",
    "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAIQDTESTANDEXAMPLE",
        "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": "AROAIQDTESTANDEXAMPLE:Sampleuser01",
    "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAIQDTESTANDEXAMPLE",
        "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": "AROAIQDTESTANDEXAMPLE:Sampleuser01",
    "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAIQDTESTANDEXAMPLE",
        "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"
}

```

Ulteriori informazioni

Le seguenti risorse forniscono ulteriori informazioni sulla crittografia dei dati inattivi:

- Per ulteriori informazioni sui AWS KMS concetti, consulta i [concetti AWS Key Management Service di base](#) nella Guida per gli AWS Key Management Service sviluppatori.
- Per ulteriori informazioni sulla AWS KMS sicurezza, consulta [le migliori pratiche di sicurezza AWS Key Management Service nella Guida per](#) gli AWS Key Management Service sviluppatori.

Ruoli collegati ai servizi nei cluster elastici

[I cluster elastici di Amazon DocumentDB utilizzano ruoli collegati ai servizi AWS Identity and Access Management \(IAM\)](#). Un ruolo collegato ai servizi è un tipo unico di ruolo IAM collegato direttamente ai cluster elastici di Amazon DocumentDB. I ruoli collegati ai servizi sono predefiniti dai cluster elastici di Amazon DocumentDB e includono tutte le autorizzazioni richieste dal servizio per chiamare altri servizi per tuo conto. AWS

Un ruolo collegato ai servizi semplifica l'utilizzo dei cluster elastici di Amazon DocumentDB perché non è necessario aggiungere manualmente le autorizzazioni necessarie. I cluster elastici di Amazon DocumentDB definiscono le autorizzazioni dei ruoli collegati ai servizi e, salvo diversa definizione, solo i cluster elastici di Amazon DocumentDB possono assumerne i ruoli. Le autorizzazioni definite includono la policy di trust e la policy delle autorizzazioni. Una policy delle autorizzazioni specifica non può essere collegata a un'altra entità IAM. È possibile eliminare i ruoli solo dopo aver eliminato le risorse correlate. Ciò protegge le risorse dei cluster elastici di Amazon DocumentDB perché non è possibile rimuovere inavvertitamente l'autorizzazione ad accedere alle risorse.

Per informazioni su altri servizi che supportano ruoli collegati ai servizi, consulta i [AWSservizi che funzionano con IAM e cerca i servizi contrassegnati con](#) Sì nella colonna Service-Linked Role. Scegli Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Autorizzazioni di ruolo collegate ai servizi per i cluster elastici

I cluster elastici di Amazon DocumentDB utilizzano il ruolo collegato ai servizi denominato per consentire ai cluster elastici di `AWSServiceRoleForDocDB-Elastic` Amazon DocumentDB di chiamare i servizi per conto dei tuoi cluster. AWS

A questo ruolo collegato ai servizi è collegata un policy di autorizzazione denominata `AmazonDocDB-ElasticServiceRolePolicy` che concede le autorizzazioni per operare nell'account. La policy di autorizzazione dei ruoli consente ai cluster elastici di Amazon DocumentDB di completare le seguenti azioni sulle risorse specificate:

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

```

        "cloudwatch:PutMetricData"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "cloudwatch:namespace": [
                "AWS/DocDB-Elastic"
            ]
        }
    }
}
]
}

```

Note

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. Se viene visualizzato il seguente messaggio di errore: «Impossibile creare la risorsa. Verify that you have permission to create service linked role. (Verifica di possedere le autorizzazioni necessarie per creare un ruolo collegato ai servizi.) Altrimenti attendi e riprova più tardi». , assicurati di avere le seguenti autorizzazioni abilitate:

```

{
  "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"
    }
  }
}

```

Per ulteriori informazioni, vedere [Autorizzazioni dei ruoli collegati ai servizi](#) nella Guida per l'utente di AWS Identity and Access Management.

Creazione di un ruolo collegato ai servizi per i cluster elastici di Amazon DocumentDB

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando crei un'istanza DB, i cluster elastici di Amazon DocumentDB creano automaticamente il ruolo collegato al servizio.

Modifica di un ruolo collegato ai servizi per i cluster elastici di Amazon DocumentDB

I cluster elastici di Amazon DocumentDB non consentono di modificare il `AWSServiceRoleForDocDB-Elastic` ruolo collegato al servizio. Dopo aver creato un ruolo collegato al servizio, non potrai modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, vedere [Modifica di un ruolo collegato al servizio](#) nella Guida per l'utente di AWS Identity and Access Management.

Eliminazione di un ruolo collegato ai servizi per i cluster elastici di Amazon DocumentDB

Se non è più necessario utilizzare una caratteristica o un servizio che richiede un ruolo collegato ai servizi, ti consigliamo di eliminare quel ruolo. In questo modo non sarà più presente un'entità non utilizzata che non viene monitorata e gestita attivamente. Tuttavia, prima di poter eliminare il ruolo collegato ai servizi, dovrai eliminare tutti i cluster .

Pulizia di un ruolo collegato ai servizi

Prima di utilizzare IAM per eliminare un ruolo collegato ai servizi, devi innanzitutto verificare che il ruolo non abbia sessioni attive ed eliminare tutte le risorse utilizzate dal ruolo.

Per verificare se il ruolo collegato al servizio ha una sessione attiva nella console IAM:

1. Accedi alla [AWS Management Console](#) e apri la console IAM.
2. Nel pannello di navigazione della console IAM seleziona Ruoli. Quindi, scegli il nome (non la casella di controllo) del ruolo `AWSServiceRoleForDocDB-Elastic`.
3. Nella pagina Summary (Riepilogo) per il ruolo selezionato, scegli la scheda Access Advisor (Consulente accessi).

Note

Se non sei sicuro che i cluster elastici di Amazon DocumentDB stiano utilizzando `AWSServiceRoleForDocDB-Elastic` il ruolo, puoi provare a eliminarlo. Se il servizio utilizza il ruolo, l'eliminazione non riesce e puoi visualizzare Regioni AWS dove viene

utilizzato il ruolo. Se il ruolo è in uso, prima di poterlo eliminare dovrai attendere il termine della sessione. Non puoi revocare la sessione per un ruolo collegato al servizio. Se desideri rimuovere il `AWSServiceRoleForDocDB-Elastic` ruolo, devi prima eliminare tutti i cluster.

Eliminazione di tutti i cluster

Per eliminare un cluster nella console Amazon DocumentDB:

1. Accedi [AWS Management Console](#) e apri la console Amazon DocumentDB.
2. Nel pannello di navigazione scegliere Clusters (Cluster).
3. Scegli il cluster che desideri eliminare.
4. In Actions (Azioni), scegliere Delete (Elimina).
5. Se ti viene richiesto di creare un'istantanea finale? , scegli Sì o No.
6. Se si sceglie Yes (Sì) nella fase precedente, in Final snapshot name (Nome snapshot finale) immettere il nome dell'ultimo snapshot.
7. Scegliere Delete (Elimina).

Note

Per eliminare il ruolo collegato ai servizi `AWSServiceRoleForDocDB-Elastic`, puoi utilizzare la console IAM, l'interfaccia a riga di comando IAM o l'API IAM. Per ulteriori informazioni, vedere [Eliminazione di un ruolo collegato al servizio nella Guida](#) per l'utente di AWS Identity and Access Management.

Monitoraggio Amazon DocumentDB

Il monitoraggio AWS dei servizi è una parte importante per mantenere i sistemi sani e funzionanti in modo ottimale. È consigliabile raccogliere i dati sul monitoraggio da tutte le parti della AWS soluzione per consentire un debug e la correzione più facile di eventuali guasti o degradazioni. Prima di iniziare a monitorare le AWS soluzioni, ti consigliamo di prendere in considerazione e formulare le risposte alle seguenti domande:

- Quali sono gli obiettivi del monitoraggio?
- Quali risorse verranno monitorate?
- Con quale frequenza eseguirai il monitoraggio di queste risorse?
- Quali strumenti di monitoraggio verranno utilizzati?
- Chi è il responsabile del monitoraggio?
- In caso di errore, a chi vanno inviate le notifiche e con quale modalità?

Per comprendere i tuoi modelli attuali relativi alle prestazioni, identificare le anomalie e formulare metodi per risolvere i problemi, è opportuno stabilire dei parametri di base per le prestazioni da applicare in momenti diversi e con diverse condizioni di carico. Durante il monitoraggio della AWS soluzione, si consiglia di archiviare i dati di monitoraggio storici per riferimenti future e per stabilire le linee di base.

In generale, i valori accettabili per i parametri di prestazione dipendono dalla baseline e da cosa sta facendo l'applicazione. Indagare le variazioni della baseline coerenti o che rappresentano dei trend. Di seguito sono riportati alcuni suggerimenti su tipi di parametri specifici:

- Consumo elevato di CPU o RAM: valori elevati per l'utilizzo di CPU o RAM potrebbero essere appropriati, purché tengano conto degli obiettivi previsti dell'applicazione (come throughput o simultaneità) che e siano previsti.
- Consumo del volume di storage: esamina il consumo dello storage (`VolumeBytesUsed`) se lo spazio usato supera costantemente l'85% dello spazio del volume di storage totale. Verifica se puoi eliminare dati dal volume di archiviazione o archiviare dati su un sistema diverso per liberare spazio. Per ulteriori informazioni, consultare [Archiviazione Amazon DocumentDB](#) e [Quote e limiti di Amazon DocumentDB](#).

- **Traffico di rete:** per il traffico di rete, rivolgiti al tuo amministratore di sistema per identificare il throughput previsto per la rete del dominio e la connessione Internet. Indaga il traffico di rete se il throughput è costantemente al di sotto del valore previsto.
- **Connessioni al database:** valuta se limitare le connessioni al database se noti un numero elevato di connessioni utente e contemporaneamente un peggioramento delle prestazioni e del tempo di risposta delle istanze. Il numero ideale di connessioni utente per l'istanza dipende dalla classe di istanza e dalla complessità delle operazioni eseguite.
- **Parametri di IOPS:** poiché i valori previsti per i parametri di IOPS dipendono dalle specifiche del disco e dalla configurazione del server, usa i valori di riferimento per identificare i comportamenti tipici. Verifica se i valori effettivi sono costantemente diversi rispetto a quelli di riferimento. Per prestazioni IOPS ottimali, verifica che il working set tipico possa essere caricato nella memoria per ridurre al minimo le operazioni di lettura e scrittura.

Amazon DocumentDB (con compatibilità MongoDB) fornisce una varietà di CloudWatch parametri Amazon che puoi monitorare per determinare lo stato e le prestazioni dei cluster e delle istanze Amazon DocumentDB. Puoi visualizzare le metriche di Amazon DocumentDB utilizzando vari strumenti, tra cui la console Amazon DocumentDBAWS CLI, l'CloudWatchAPI e Performance Insights.

Argomenti

- [Monitoraggio dello stato di un cluster Amazon DocumentDB](#)
- [Monitoraggio dello stato di un'istanza Amazon DocumentDB](#)
- [Visualizzazione dei suggerimenti Amazon DocumentDB](#)
- [Utilizzo delle sottoscrizioni agli eventi Amazon DocumentDB](#)
- [Monitoraggio di Amazon DocumentDB con CloudWatch](#)
- [Registrazione delle chiamate API di AmazonAWS CloudTrail](#)
- [Profilazione delle operazioni di Amazon DocumentDB](#)
- [Monitoraggio con Performance Insights](#)

Monitoraggio dello stato di un cluster Amazon DocumentDB

Lo stato di un cluster ne indica l'integrità. Puoi visualizzare lo stato di un cluster utilizzando la console Amazon DocumentDB o il `AWS CLI describe-db-clusters` comando.

Argomenti

- [Valori dello stato del cluster](#)
- [Monitoraggio dello stato di un cluster](#)

Valori dello stato del cluster

Nella tabella seguente sono elencati i valori validi per lo stato di un cluster.

Stato del cluster	Descrizione
<code>active</code>	Il cluster è attivo. Questo stato si applica solo ai cluster elastici.
<code>available</code>	Il cluster è integro e disponibile. Questo stato si applica solo ai cluster basati su istanze.
<code>backing-up</code>	Il cluster è attualmente sottoposto a backup.
<code>creating</code>	Il cluster è in fase di creazione. L'accesso durante la creazione non è consentito.
<code>deleting</code>	Il cluster è in fase di eliminazione. L'accesso durante l'eliminazione non è consentito.
<code>failing-over</code>	È in fase di esecuzione un failover da parte dell'istanza primaria in una replica Amazon DocumentDB.
<code>inaccessible-encryption-credentials</code>	La chiave AWS KMS utilizzata per crittografare o decrittografare il cluster non è accessibile.

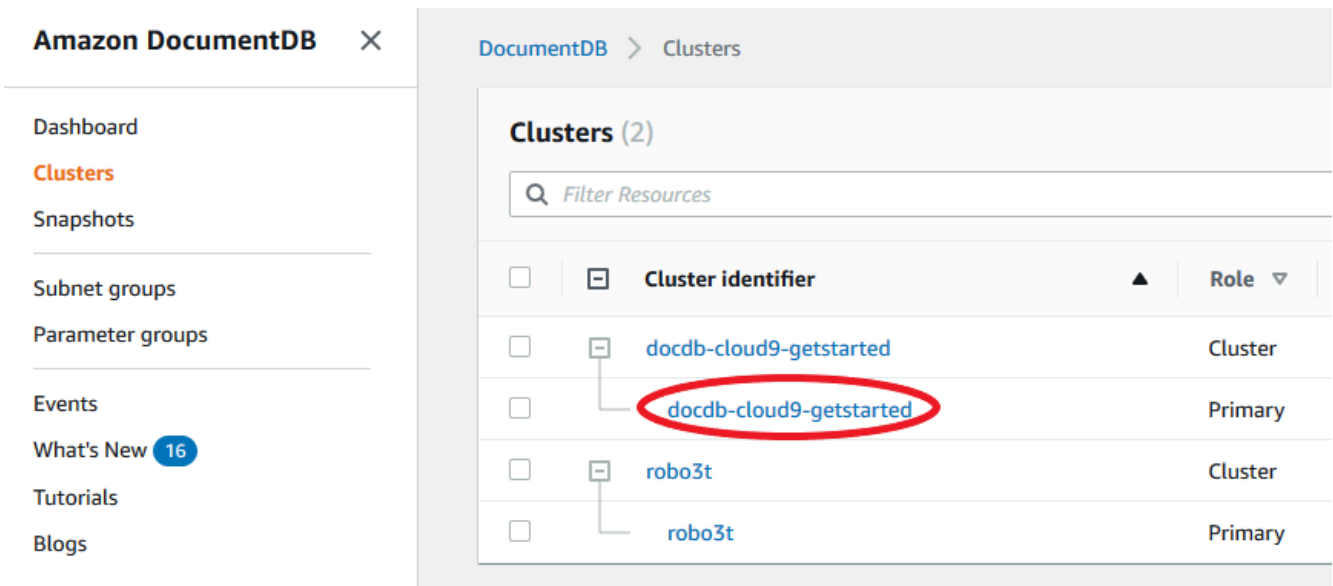
Stato del cluster	Descrizione
<code>maintenance</code>	È in corso l'applicazione di un aggiornamento di manutenzione al cluster. Questo stato viene utilizzato per la manutenzione a livello di cluster pianificata in anticipo da Amazon DocumentDB.
<code>migrating</code>	Una snapshot del cluster è stata ripristinata in un cluster.
<code>migration-failed</code>	Una migrazione non è riuscita.
<code>modifying</code>	È in corso la modifica del cluster in seguito alla richiesta da parte di un cliente.
<code>renaming</code>	È in corso la ridenominazione del cluster in seguito alla richiesta da parte di un cliente.
<code>resetting-master-credentials</code>	È in corso il ripristino delle credenziali master del cluster in seguito alla richiesta da parte di un cliente.
<code>upgrading</code>	La versione del motore del cluster è in fase di aggiornamento.

Monitoraggio dello stato di un cluster

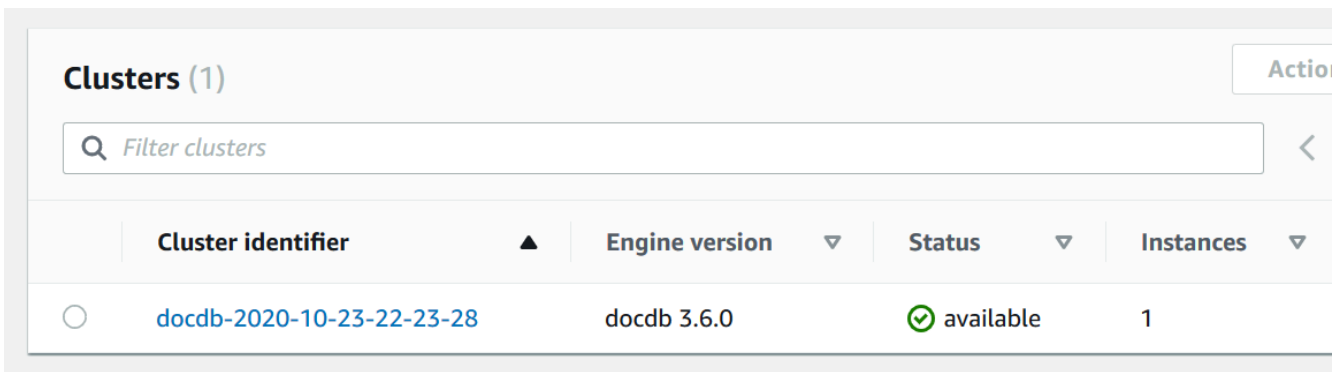
Using the AWS Management Console

Quando utilizzi l'AWS Management Console per determinare lo stato di un cluster, utilizza la seguente procedura.

1. Accedere alla AWS Management Console e aprire la console Amazon DocumentDB all'indirizzo <https://console.aws.amazon.com/docdb>.
2. Nel pannello di navigazione scegliere Clusters (Cluster).
3. Nella casella di navigazione Cluster, vedrai la colonna Identificatore del cluster. Le tue istanze sono elencate in cluster, in modo simile alla schermata seguente.



4. Nella colonna dell'identificatore del cluster, trova il nome dell'istanza che ti interessa. Quindi, per trovare lo stato dell'istanza, leggi attraverso quella riga fino alla colonna Stato, come mostrato di seguito.



Using the AWS CLI

Quando utilizzi l'AWS CLI per determinare lo stato di un cluster, utilizza l'operazione `describe-db-clusters`. Il codice seguente individua lo stato del cluster `sample-cluster`.

Per Linux, macOS o Unix:

```
aws docdb describe-db-clusters \  
  --db-cluster-identifier sample-cluster \  
  --query 'DBClusters[*].[DBClusterIdentifier,Status]'
```

Per Windows:

```
aws docdb describe-db-clusters ^  
  --db-cluster-identifier sample-cluster ^  
  --query 'DBClusters[*].[DBClusterIdentifier,Status]'
```

L'aspetto dell'output di questa operazione è simile al seguente.

```
[  
  [  
    "sample-cluster",  
    "available"  
  ]  
]
```

Monitoraggio dello stato di un'istanza Amazon DocumentDB

Amazon DocumentDB fornisce informazioni sulla condizione corrente di ogni istanza configurata nel database.

Esistono tre tipi di stato che puoi visualizzare per un'istanza Amazon DocumentDB:

- **Stato dell'istanza:** questo stato è mostrato nella colonna Stato della tabella del cluster nellaAWS Management Console e mostra la condizione corrente del ciclo di vita dell'istanza. I valori mostrati nella colonna Stato derivano dalStatus campo della rispostaDescribeDBCluster API.
- **Stato di integrità dell'istanza:** questo stato viene visualizzato nella colonna Stato dell'istanza della tabella del cluster nellaAWS Management Console e indica se il motore del database, il componente responsabile della gestione e del recupero dei dati, è in esecuzione. I valori mostrati nella colonna Stato dell'istanza si basano sulla metricaCloudWatchEngineUptime del sistema Amazon.
- **Stato di manutenzione:** questo stato è mostrato nella colonna Manutenzione della tabella del cluster nellaAWS Management Console e indica lo stato di qualsiasi evento di manutenzione che deve essere applicato a un'istanza. Lo stato di manutenzione è indipendente dallo stato dell'altra

istanza e deriva dall'`PendingMaintenanceActionAPI`. Per ulteriori informazioni sullo stato di manutenzione, consulta [Manutenzione di Amazon DocumentDB](#).

Argomenti

- [Valori di stato delle istanze](#)
- [Monitoraggio dello stato dell'istanza utilizzando AWS Management Console o AWS CLI](#)
- [Valori dello stato di integrità dell'istanza](#)
- [Monitoraggio dello stato di integrità dell'istanza utilizzando il AWS Management Console](#)

Valori di stato delle istanze

Nella tabella seguente sono elencati i possibili valori di stato per le istanze e la modalità di fatturazione per ogni stato. Viene inoltre indicato se è prevista la fatturazione per l'istanza e lo storage, solo per lo storage oppure se la fatturazione non è prevista. Per tutti gli stati delle istanze, l'utilizzo del backup viene inserito in fattura.

Stato dell'istanza	Fatturata	Descrizione
<code>available</code>	Fatturata	L'istanza è integra e disponibile.
<code>backing-up</code>	Fatturata	L'istanza è attualmente sottoposta a backup.
<code>configuring-log-exports</code>	Fatturata	La pubblicazione dei file di log in Amazon CloudWatch Logs per questa istanza è in fase di abilitazione o disabilitazione.
<code>creating</code>	Non fatturata	L'istanza è in fase di creazione. Non è possibile accedere all'istanza mentre è in fase di creazione.
<code>deleting</code>	Non fatturata	L'istanza è in fase di eliminazione.
<code>failed</code>	Non fatturata	L'istanza ha restituito un errore e Amazon DocumentDB non è stato in grado di recuperarla. Per ripristinare i dati, esegui

Stato dell'istanza	Fatturata	Descrizione
		unpoint-in-time ripristino all'ultimo orario di ripristino dell'istanza.
inaccessible-encryption-credentials	Non fatturata	La chiave AWS KMS utilizzata per crittografare o decrittografare l'istanza non è accessibile.
incompatible-network	Non fatturata	Il tentativo di Amazon DocumentDB di eseguire un'operazione di ripristino su un'istanza ha esito negativo perché il VPC si trova in uno stato che impedisce il completamento dell'operazione. Questo stato si verifica ad esempio se tutti gli indirizzi IP di una sottorete erano in uso e Amazon DocumentDB non è stato in grado di ottenere un indirizzo IP per l'istanza.
maintenance	Fatturata	È in fase di applicazione da parte di Amazon DocumentDB di un aggiornamento di manutenzione all'istanza. Questo stato viene utilizzato per la manutenzione a livello di istanza pianificata in anticipo da Amazon DocumentDB. Stiamo valutando nuovi modi per fornire altre operazioni di manutenzione ai clienti attraverso questo stato.
modifying	Fatturata	È in corso la modifica dell'istanza in seguito a una richiesta di eseguire tale operazione.
rebooting	Fatturata	È in fase di riavvio dell'istanza a causa della richiesta o perché è necessario per un processo Amazon DocumentDB.
renaming	Fatturata	È in corso la ridenominazione dell'istanza in seguito a una richiesta di eseguire tale operazione.

Stato dell'istanza	Fatturata	Descrizione
<code>resetting-master-credentials</code>	Fatturata	È in corso il ripristino delle credenziali master dell'istanza in seguito a una richiesta di eseguire tale operazione.
<code>restore-error</code>	Fatturata	L'istanza ha riscontrato un errore durante il tentativo di esecuzione di un ripristino da point-in-time o da una snapshot.
<code>starting</code>	Fatturato per storage	L'istanza è in fase di avvio.
<code>stopped</code>	Fatturato per storage	L'istanza è stata arrestata.
<code>stopping</code>	Fatturato per storage	L'istanza è in fase di arresto.
<code>storage-full</code>	Fatturata	L'istanza ha raggiunto la capacità di storage allocata. Si tratta di uno stato critico che richiede l'immediata risoluzione del problema; dimensionare la capacità di storage modificando l'istanza. Imposta gli CloudWatch allarmi Amazon per emettere un avviso quando lo spazio di storage diminuisce per evitare questa situazione.

Monitoraggio dello stato dell'istanza utilizzando AWS Management Console o AWS CLI

Usa AWS Management Console o AWS CLI per monitorare lo stato della tua istanza.

Using the AWS Management Console

Quando utilizzi l'AWS Management Console per determinare lo stato di un cluster, utilizza la seguente procedura.

1. Accedere alla AWS Management Console e aprire la console Amazon DocumentDB all'indirizzo <https://console.aws.amazon.com/docdb>.
2. Nel pannello di navigazione scegliere Clusters (Cluster).

Note

Nota che nella casella di navigazione Cluster, la colonna Identificatore cluster mostra sia i cluster che le istanze. Le istanze sono elencate sotto i cluster, in modo simile all'immagine seguente.

Cluster identifier	Role	Engine version	Region & AZ
docdb-cloud9-getstarted	Cluster	3.6.0	us-east-1
docdb-cloud9-getstarted	Primary	3.6.0	us-east-1f
robo3t	Cluster	3.6.0	us-east-1
robo3t	Primary	3.6.0	us-east-1d

3. Trova il nome dell'istanza che ti interessa. Quindi, per trovare lo stato dell'istanza, leggi la riga in corrispondenza della colonna Status (Stato), come illustrato di seguito.

Cluster identifier	Role	Engine version	Region & AZ	Status
docdb-cloud9-getstarted	Cluster	3.6.0	us-east-1	available
docdb-cloud9-getstarted	Primary	3.6.0	us-east-1f	available
robo3t	Cluster	3.6.0	us-east-1	available
robo3t	Primary	3.6.0	us-east-1d	available

Using the AWS CLI

Quando utilizzi l'AWS CLI per determinare lo stato di un cluster, utilizza l'operazione `describe-db-instances`. Il codice seguente individua lo stato dell'istanza `sample-cluster-instance-01`.

Per Linux, macOS o Unix:

```
aws docdb describe-db-instances \
  --db-instance-identifier sample-cluster-instance-01 \
  --query 'DBInstances[*].[DBInstanceIdentifier,DBInstanceStatus]'
```

Per Windows:

```
aws docdb describe-db-instances ^
  --db-instance-identifier sample-cluster-instance-01 ^
  --query 'DBInstances[*].[DBInstanceIdentifier,DBInstanceStatus]'
```

L'aspetto dell'output di questa operazione è simile al seguente.

```
[
  [
    "sample-cluster-instance-01",
    "available"
  ]
]
```

Valori dello stato di integrità dell'istanza

La tabella seguente elenca i possibili valori dello stato di integrità per le istanze. La colonna Stato dell'istanza, situata nella tabella Cluster dellaAWS Management Console, mostra se il motore del database, il componente responsabile dell'archiviazione, della gestione e del recupero dei dati, funziona normalmente. Questa colonna indica anche se la metrica diEngineUptime sistema, disponibile inCloudWatch, mostra lo stato di integrità di ogni istanza.

Stato di integrità dell'istanza	Descrizione
integro	Il motore di database è in esecuzione nell'istanza Amazon DocumentDB.
malsano	Il motore del database non è in esecuzione o è stato riavviato meno di un minuto fa.

Monitoraggio dello stato di integrità dell'istanza utilizzando ilAWS Management Console

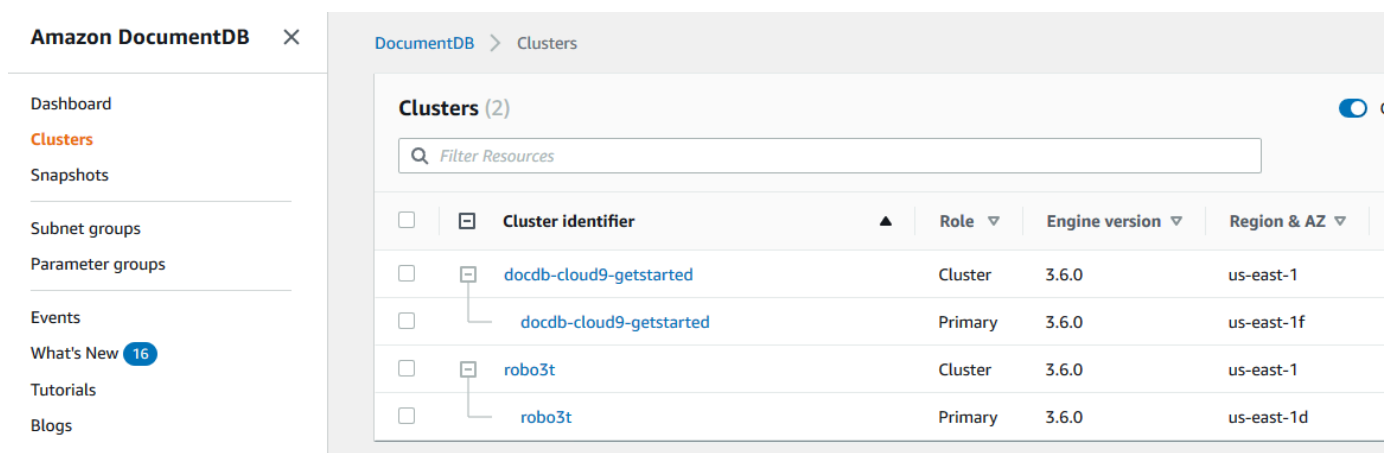
UtilizzaloAWS Management Console per monitorare lo stato di integrità della tua istanza.

Durante l'utilizzoAWS Management Console, utilizza i seguenti passaggi per comprendere lo stato di integrità dell'istanza.

1. Accedere allaAWS Management Console e aprire la console Amazon DocumentDB all'[indirizzo https://console.aws.amazon.com/docdb](https://console.aws.amazon.com/docdb).
2. Nel pannello di navigazione scegliere Clusters (Cluster).

Note

Nella casella di navigazione Cluster, la colonna Identificatore cluster mostra sia i cluster che le istanze. Le istanze sono elencate sotto i cluster, in modo simile all'immagine seguente.



3. Trova il nome dell'istanza che ti interessa. Quindi, per trovare lo stato dell'istanza, leggi attraverso quella riga fino alla colonna Stato dell'istanza, come mostrato nell'immagine seguente:

Clusters (4) 🔄

🔍 Filter Resources

<input type="checkbox"/>	Cluster identifier ▲	Role ▼	Engine version ▼	Region & AZ ▼	Status ▼	Instance health	CPU
<input type="checkbox"/>	iad-fra-global-cluster	Global cluster	4.0.0	2 regions	🟢 available	-	-
<input type="checkbox"/>	docdb-2023-03-27-11-56-04	Primary cluster	4.0.0	us-east-1	🟢 available	-	-
<input type="checkbox"/>	docdb-2023-03-27-11-56-04	Primary instance	4.0.0	us-east-1a	🟢 available	🟢 healthy	📊 5.58%
<input type="checkbox"/>	docdb-2023-03-27-11-56-042	Replica instance	4.0.0	us-east-1d	🟢 available	🟢 healthy	📊 5.79%
<input type="checkbox"/>	docdb-2023-03-27-11-56-043	Replica instance	4.0.0	us-east-1b	🟢 available	🟢 healthy	📊 5.68%
<input type="checkbox"/>	docdb-2023-03-27-12-02-55	Secondary cluster	4.0.0	eu-central-1	🟢 available	-	-
<input type="checkbox"/>	docdb-2023-03-27-12-02-55	Replica instance	4.0.0	eu-central-1c	🟢 available	🟢 healthy	📊 5.88%
<input type="checkbox"/>	docdb-2023-03-27-12-02-552	Replica instance	4.0.0	eu-central-1a	🟢 available	🟢 healthy	📊 5.97%
<input type="checkbox"/>	docdb-2023-03-28-09-45-05	Regional cluster	5.0.0	us-east-1	⏸ stopped	-	-
<input type="checkbox"/>	docdb-2023-03-28-09-45-05	Replica instance	5.0.0	us-east-1d	⏸ stopped	🔴 unhealthy	-
<input type="checkbox"/>	docdb-2023-03-28-09-45-052	Replica instance	5.0.0	us-east-1a	⏸ stopped	🔴 unhealthy	-
<input type="checkbox"/>	docdb-2023-03-28-09-45-053	Primary instance	5.0.0	us-east-1b	⏸ stopped	🔴 unhealthy	-

📘 Note

Il sondaggio sullo stato di integrità dell'istanza viene eseguito ogni 60 secondi e si basa sulla metrica `CloudWatchEngineUptime` del sistema. I valori nella colonna Stato dell'istanza vengono aggiornati automaticamente.

Visualizzazione dei suggerimenti Amazon DocumentDB

Amazon DocumentDB fornisce un elenco di raccomandazioni automatiche per le risorse del database, come le istanze e i cluster. Queste raccomandazioni forniscono consigli sulle best practice analizzando le configurazioni di cluster e istanza.

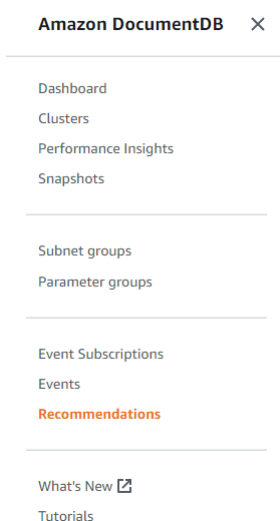
Come esempio di questi suggerimenti, consulta i seguenti argomenti:

Type (Tipo)	Descrizione	Raccomandazione	Informazioni aggiuntive
Una istanza	Il cluster contiene solo un'istanza	Prestazioni e disponibilità: ti consigliamo di aggiungere un'altra istanza con la stessa classe di istanza in una zona di disponibilità diversa.	Amazon DocumentDB Alta disponibilità e replica

Amazon DocumentDB genera raccomandazioni per una risorsa quando questa viene creata o modificata. Amazon DocumentDB periodicamente esegue anche la scansione delle risorse e genera suggerimenti.

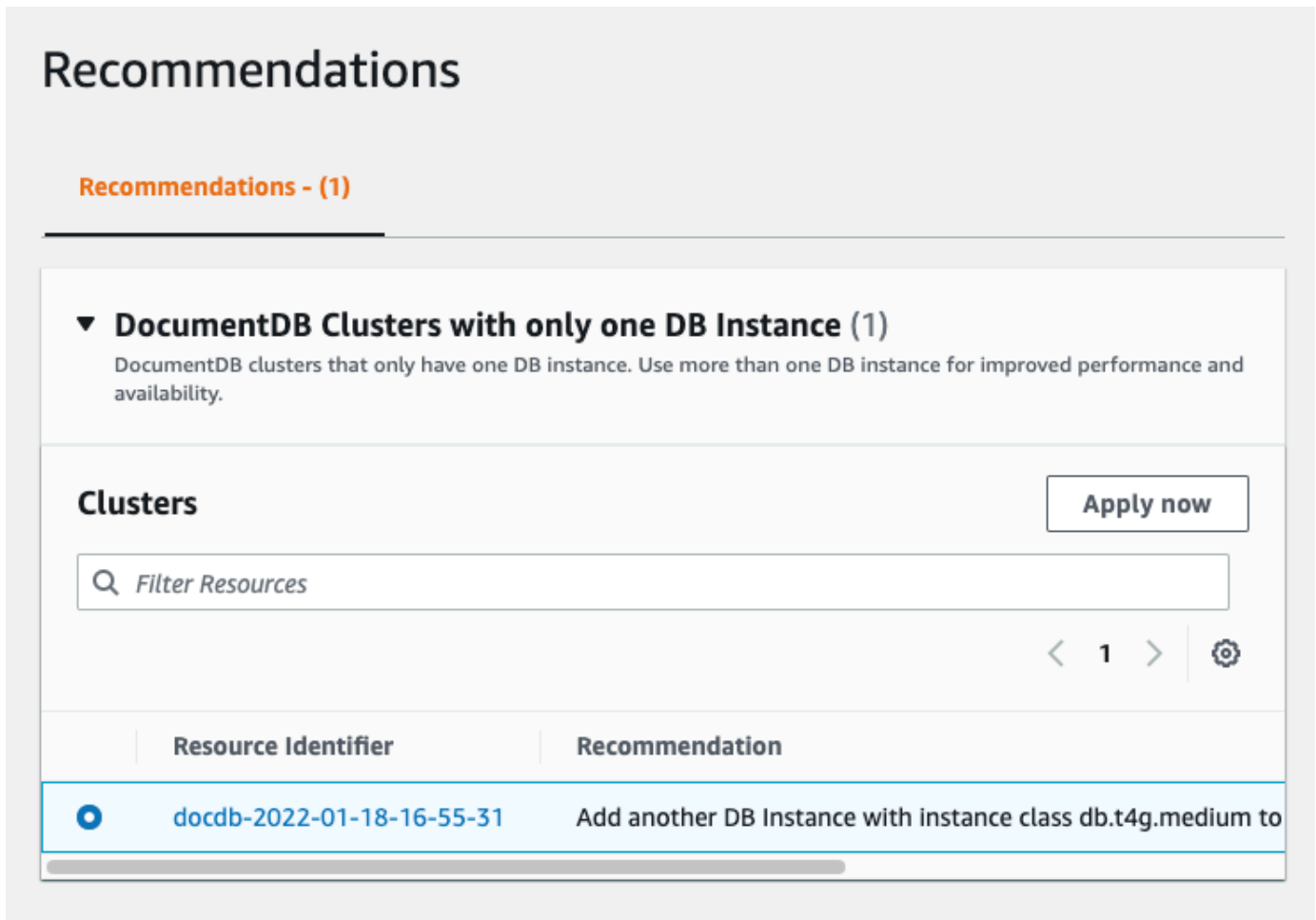
Per visualizzare e adottare misure in base ai consigli di Amazon DocumentDB

1. Accedere allaAWS Management Console e aprire la console Amazon DocumentDB all'[indirizzo https://console.aws.amazon.com/docdb](https://console.aws.amazon.com/docdb).
2. Nel riquadro di navigazione scegli Consigli:



3. Nella finestra di dialogo Consigli, espandi la sezione di interesse e seleziona l'attività consigliata.

Nell'esempio seguente, l'attività consigliata si applica a un cluster Amazon DocumentDB con una sola istanza. Si consiglia di aggiungere un'altra istanza per migliorare le prestazioni e la disponibilità.



The screenshot shows the 'Recommendations' section in the Amazon DocumentDB console. It features a heading 'Recommendations - (1)' and a section titled 'DocumentDB Clusters with only one DB Instance (1)'. Below this, there is a 'Clusters' section with a search bar labeled 'Filter Resources' and an 'Apply now' button. A table lists the recommendation details:

Resource Identifier	Recommendation
docdb-2022-01-18-16-55-31	Add another DB Instance with instance class db.t4g.medium to

4. Fai clic su Applica ora.

Per questo esempio, viene visualizzata la finestra di dialogo Aggiungi istanze:

DocumentDB > Clusters > Add Instances

Add instances to: docdb-2022-01-18-16-55-31

Instance settings

You can create up to 16 instances for a cluster (one primary and 15 replicas).
'docdb-2022-01-18-16-55-31' cluster currently has 1/16 instances.

Instance identifier Info	Instance class Info	Promotion tier Info	
<input type="text" value="docdb-2022-01-18-16-5"/>	<input type="text" value="db.t3.medium (fre..."/>	<input type="text" value="No preference"/>	<input type="button" value="Remove"/>

Specify a unique instance identifier.

You can create 14 more instances.

5. Modifica le impostazioni della nuova istanza e fai clic su Crea.

Utilizzo delle sottoscrizioni agli eventi Amazon DocumentDB

Amazon DocumentDB usa Amazon Simple Notification Service (Amazon SNS) per fornire le notifiche quando si verifica un evento Amazon DocumentDB. Queste notifiche possono essere in qualsiasi forma supportata da Amazon SNS per un'Regione AWSe-mail, un SMS o una chiamata a un endpoint HTTP.

Amazon DocumentDB raggruppa gli eventi in categorie che puoi sottoscrivere, per ricevere una notifica quando si verifica un evento di tale categoria. Puoi sottoscrivere una categoria di eventi per un'istanza, un cluster, uno snapshot, uno snapshot cluster, uno snapshot cluster, uno snapshot cluster, uno snapshot cluster, uno snapshot cluster, uno snapshot Ad esempio, sottoscrivendo la categoria Backup per una determinata istanza, riceverai una notifica ogni volta che si verifica un evento relativo al backup che interessa l'istanza. Riceverai una notifica anche quando viene modificata la sottoscrizione a un evento.

Gli eventi si verificano sia a livello di cluster che di istanza, quindi puoi ricevere gli eventi se esegui la sottoscrizione a un cluster o a un'istanza.

Le sottoscrizioni agli eventi vengono inviate all'indirizzo fornito al momento della creazione della sottoscrizione. È possibile creare più sottoscrizioni diverse, ad esempio una che riceve notifiche per tutti gli eventi e un'altra che include solo gli eventi critici per le istanze di produzione. Puoi disattivare facilmente le notifiche senza eliminare un abbonamento. A tale scopo, imposta il pulsante di opzione Abilitato su No nella console Amazon DocumentDB.

Important

Amazon DocumentDB non garantisce l'ordine degli eventi inviato in un flusso di eventi. Tale ordine è soggetto a modifiche.

Amazon DocumentDB usa l'Amazon Resource Name (ARN) di un argomento Amazon SNS per identificare ogni sottoscrizione. La console Amazon DocumentDB crea automaticamente l'ARN quando crei la sottoscrizione.

Fatturazione per gli abbonamenti agli eventi Amazon DocumentDB avviene tramite Amazon SNS. L'uso della notifica degli eventi è soggetta alle tariffe di Amazon SNS. Per ulteriori informazioni, consulta Prezzi di Amazon Simple Notification Service. Oltre ai costi di Amazon SNS, Amazon DocumentDB non fattura gli abbonamenti agli eventi.

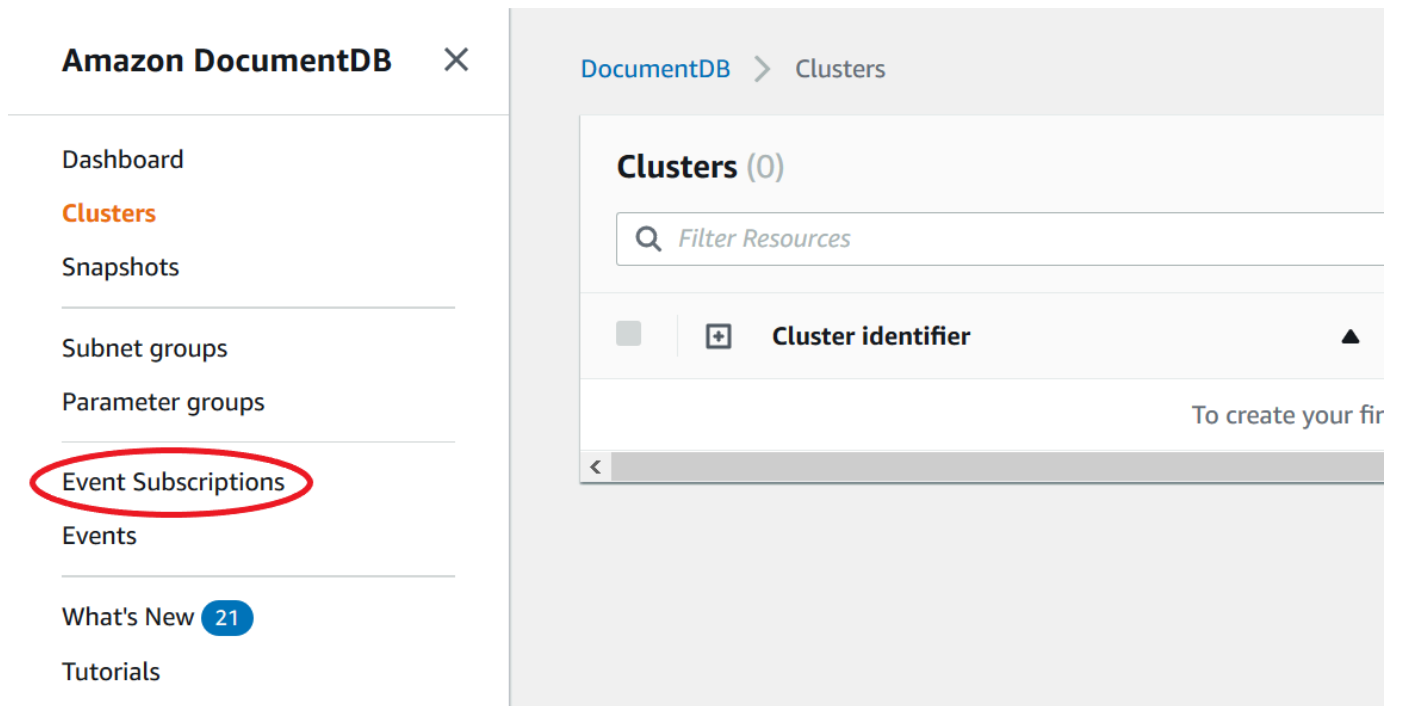
Argomenti

- [Sottoscrizione alle sottoscrizioni agli eventi Amazon DocumentDB](#)
- [Gestione delle sottoscrizioni per le notifiche di eventi Amazon DocumentDB](#)
- [Categorie di eventi e messaggi di Amazon DocumentDB](#)

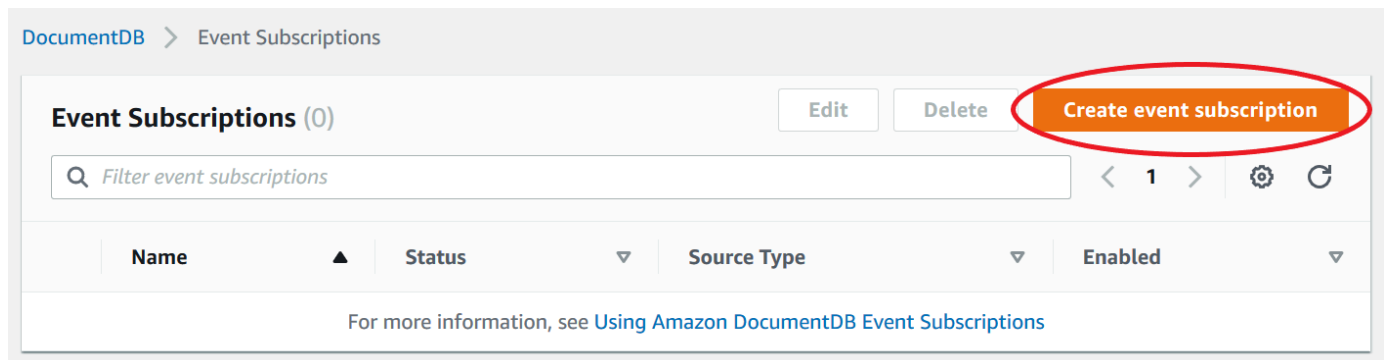
Sottoscrizione alle sottoscrizioni agli eventi Amazon DocumentDB

Puoi utilizzare la console Amazon DocumentDB per sottoscrivere gli abbonamenti agli eventi, come segue:

1. Accedi alla AWS Management Console all'indirizzo <https://console.aws.amazon.com/docdb>.
2. Nel pannello di navigazione selezionare Event subscriptions (Sottoscrizioni di eventi).



3. Nel riquadro Event subscriptions (Sottoscrizioni di eventi) scegliere Create event subscription (Crea sottoscrizione di eventi).



4. Nella finestra di dialogo Create event subscription (Crea sottoscrizione di eventi), seguire questa procedura:
 - Per Name (Nome), immettere un nome per la sottoscrizione alle notifiche eventi.

DocumentDB > Event Subscriptions > Create event subscription

Create event subscription

Details

Name

Name of the subscription

Test

- Per Target, scegli dove vuoi inviare le notifiche. Puoi scegliere un ARN esistente o scegliere Nuovo argomento e-mail per inserire il nome di un argomento e un elenco di destinatari.

Target

Send notifications to

ARN

New Email Topic

ARN

ARN to send notifications to

Choose ARN

- Per Origine, scegliere un tipo di origine. A seconda del tipo di origine selezionato, scegliere le categorie di eventi e le origini da cui ricevere le notifiche eventi.

Source

Source Type

Source type of resource this subscription will consume events from

Choose source type

- Seleziona Create (Crea).

Source

Source Type
Source type of resource this subscription will consume events from

Instances ▼

Instances to include
Instances that this subscription will consume events from

All instances
 Select specific instances

Event Categories to include
Event Categories that this subscription will consume events from

All event categories
 Select specific event categories

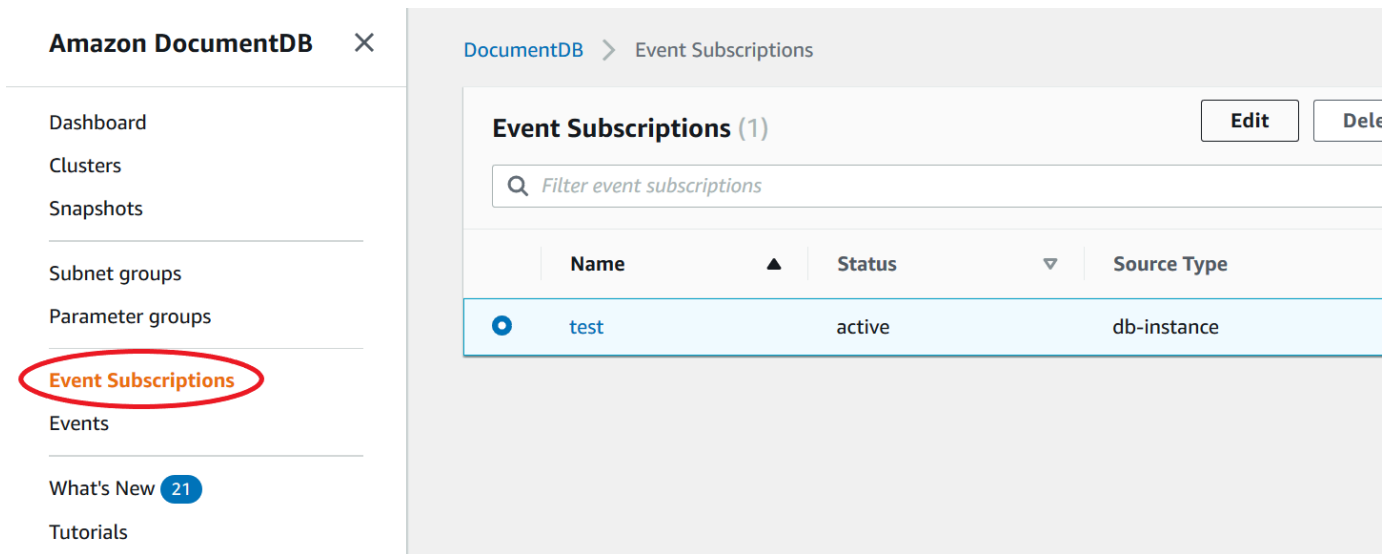
Cancel **Create**

Gestione delle sottoscrizioni per le notifiche di eventi Amazon DocumentDB

Se scegli Abbonamenti per eventi nel pannello di navigazione della console Amazon DocumentDB, puoi visualizzare le categorie di sottoscrizioni e un elenco degli abbonamenti correnti. Puoi anche modificare o eliminare un abbonamento specifico.

Per modificare le sottoscrizioni correnti alle notifiche di eventi Amazon DocumentDB

1. Accedi alla AWS Management Console all'indirizzo <https://console.aws.amazon.com/docdb>.
2. Nel pannello di navigazione selezionare Event subscriptions (Sottoscrizioni di eventi). Il riquadro Event subscriptions (Sottoscrizioni di eventi) mostra tutte le sottoscrizioni delle notifiche degli eventi.



Amazon DocumentDB

- Dashboard
- Clusters
- Snapshots
- Subnet groups
- Parameter groups
- Event Subscriptions**
- Events
- What's New **21**
- Tutorials

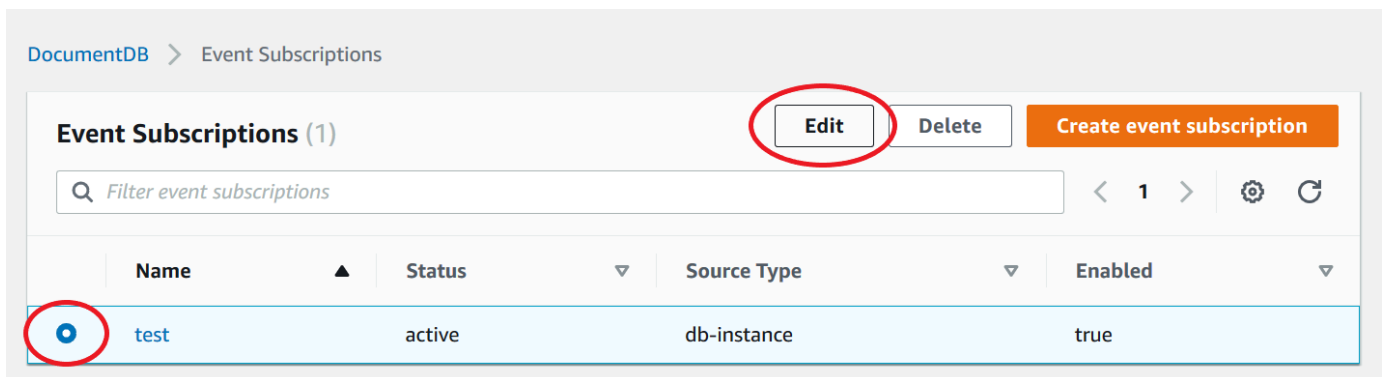
DocumentDB > Event Subscriptions

Event Subscriptions (1) Edit Delete

Filter event subscriptions

Name	Status	Source Type
test	active	db-instance

3. Nel riquadro Event subscriptions (Sottoscrizioni di eventi) scegliere la sottoscrizione da modificare e selezionare Edit (Modifica).



DocumentDB > Event Subscriptions

Event Subscriptions (1) Edit Delete Create event subscription

Filter event subscriptions

Name	Status	Source Type	Enabled
test	active	db-instance	true

4. Apportare le modifiche alla sottoscrizione nella sezione Target (Destinazione) o Source (Origine). Puoi aggiungere o rimuovere gli identificatori di origine selezionandoli o deselegionandoli nella sezione Origine.

Modify event subscription

Details

Enabled

- Enabled
 Disabled

Target

Send notifications to

- ARN
 New Email Topic

ARN

ARN to send notifications to

Test

5. Scegli Modifica. La console Amazon DocumentDB indica che è in corso la modifica della sottoscrizione.

Event Categories to include

Event Categories that this subscription will consume events from

- All event categories
 Select specific event categories

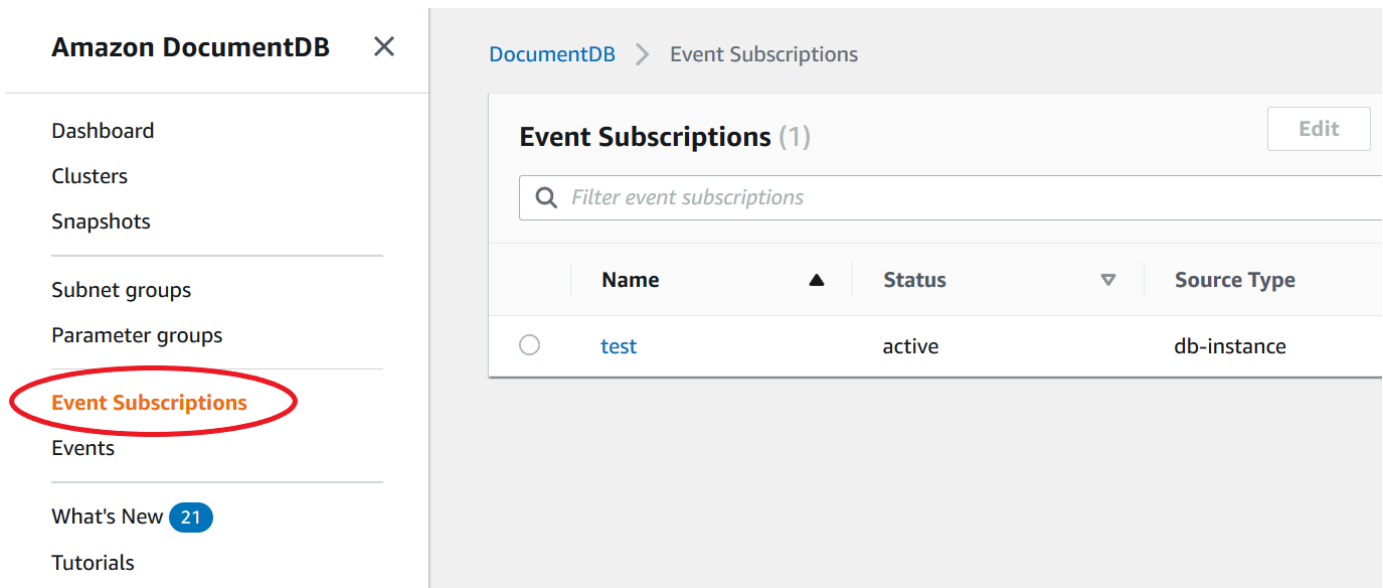
Cancel

Modify

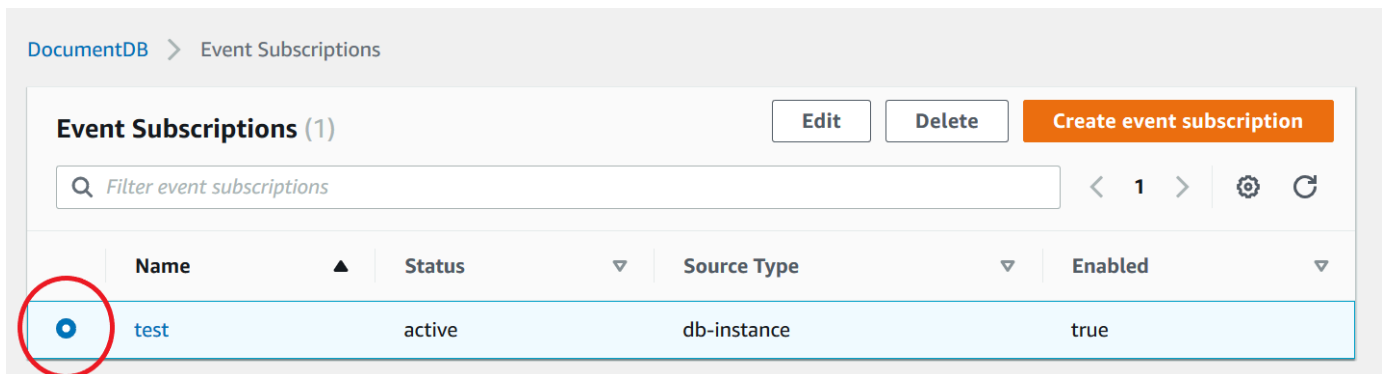
Eliminazione di una sottoscrizione alle notifiche di eventi Amazon DocumentDB

Puoi eliminare un abbonamento quando questo non è più necessario. Tutti gli abbonati all'argomento non riceveranno più le notifiche di eventi specificate dall'abbonamento.

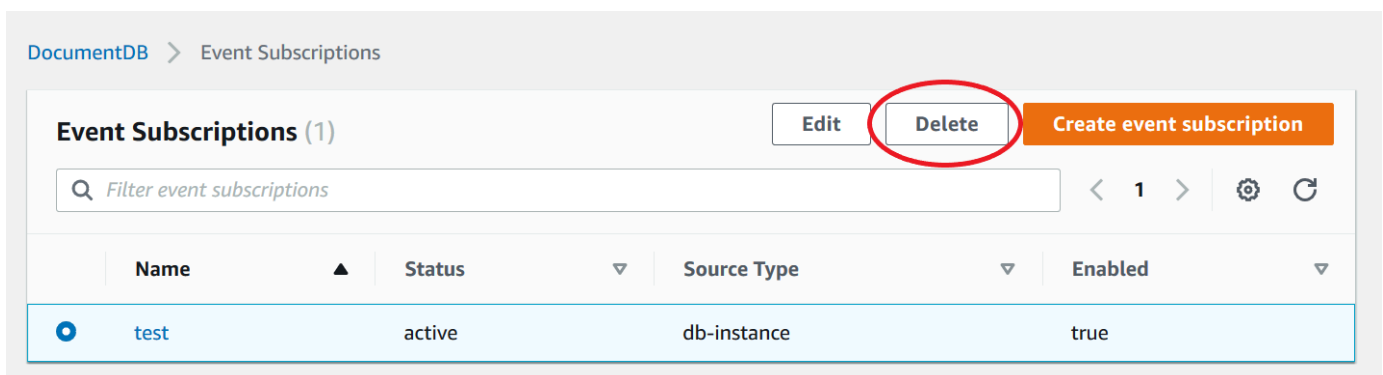
1. Accedi alla AWS Management Console all'indirizzo <https://console.aws.amazon.com/docdb>.
2. Nel pannello di navigazione selezionare Event subscriptions (Sottoscrizioni di eventi).



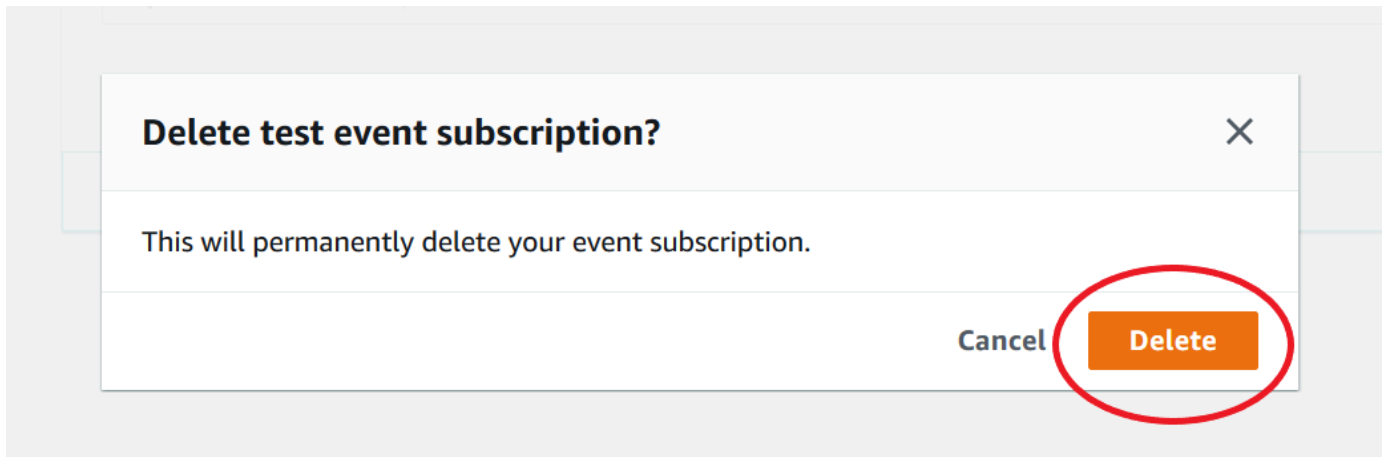
3. Nel riquadro Sottoscrizioni eventi, scegli la sottoscrizione che desideri eliminare.



4. Scegliere Elimina.



5. Apparirà una finestra pop-up che ti chiederà se desideri eliminare definitivamente questa notifica. Scegliere Elimina.



Categorie di eventi e messaggi di Amazon DocumentDB

Amazon DocumentDB genera un numero significativo di eventi in categorie che puoi sottoscrivere tramite la console. Ogni categoria si applica a un tipo di origine, ad esempio un'istanza, uno snapshot o un gruppo di parametri.

Note

Amazon DocumentDB utilizza le definizioni e gli ID di eventi Amazon RDS esistenti.

Eventi Amazon DocumentDB provenienti da istanze

Categoria	Descrizione
availability	L'istanza è stata riavviata.
disponibilità	L'istanza è stata arrestata.
modifica della configurazione	Vengono applicate le modifiche a una classe di istanza.
modifica della configurazione	È stata completata l'applicazione della modifica a una classe di istanza.
modifica della configurazione	Reimposta le credenziali master.

Categoria	Descrizione
creazione	Viene creata l'istanza.
eliminazione	Istanza eliminata
errore	L'istanza ha avuto esito negativo a causa di una configurazione non compatibile o di un problema di storage sottostante. Inizia a point-in-time-restore per l'istanza.
notifica	Viene arrestata l'istanza.
notifica	Istanza avviata.
notifica	L'istanza è in fase di avvio poiché supera il tempo massimo concesso per l'arresto.
recupero	È stato avviato il recupero dell'istanza. La durata del recupero varia in funzione della quantità di dati da recuperare.
recupero	È stato completato il recupero dell'istanza.
applicazione di patch di sicurezza	L'aggiornamento del sistema operativo è disponibile per la tua istanza. Per informazioni sull'applicazione degli aggiornamenti, consulta Gestione di Amazon DocumentDB .

Eventi Amazon DocumentDB provenienti da un cluster

Categoria	Descrizione
creazione	Cluster creato
eliminazione	Cluster eliminato.

Categoria	Descrizione
failover	Promuovere nuovamente le primarie precedenti.
failover	Failover sull'istanza completato.
failover	Failover avviato su istanza DB: %s
failover	È stato avviato lo stesso failover AZ sull'istanza DB: %s
failover	Failover su istanza DB avviato tra AZ: %s
manutenzione	Il cluster è stato corretto.
manutenzione	Il cluster di database è in uno stato che non può essere aggiornato: %s
notifica	Il cluster è stato arrestato.
notifica	Il cluster è stato avviato.
notifica	Impossibile interrompere il cluster.
notifica	Il cluster è in fase di avvio poiché supera il tempo massimo concesso per l'arresto.
notifica	Cluster rinominato da %s a %s.

Eventi Amazon DocumentDB provenienti da un'istantanea del cluster

La tabella seguente riporta la categoria di eventi e un elenco di eventi applicabili quando il tipo di origine è uno snapshot del cluster Amazon DocumentDB.

Categoria	Descrizione
backup	Creazione snapshot cluster manuale.
backup	Snapshot di cluster creato manualmente.

Categoria	Descrizione
backup	Creazione snapshot cluster automatizzato.
backup	Snapshot di cluster automatizzato creato.

Eventi Amazon DocumentDB provenienti da un gruppo di parametri

Nella tabella seguente sono indicati la categoria di evento e un elenco di eventi quando il tipo di origine è un gruppo di parametri.

Categoria	Descrizione
modifica della configurazione	Parametro %s aggiornato a %s con il metodo di applicazione %s

Monitoraggio di Amazon DocumentDB con CloudWatch

Amazon DocumentDB (con compatibilità MongoDB) si integra con Amazon CloudWatch in modo da poter raccogliere e analizzare i parametri operativi per i cluster. È possibile monitorare queste metriche utilizzando il CloudWatch console, la console Amazon DocumentDB, ilAWS Command Line Interface(AWS CLI), oppure CloudWatchAPI.

CloudWatch consente inoltre di impostare allarmi in modo da poter essere avvisati se un valore metrico supera una soglia specificata. Puoi persino configurare Amazon CloudWatch Eventi per intraprendere azioni correttive in caso di violazione. Per ulteriori informazioni sull'utilizzo CloudWatch e allarmi, vedi [Amazon CloudWatch documentazione](#).

Argomenti

- [Parametri di Amazon DocumentDB](#)
- [Visualizzazione CloudWatch Dati](#)
- [Dimensioni Amazon DocumentDB](#)
- [Monitoraggio degli opcounter](#)
- [Monitoraggio delle connessioni al database](#)

Parametri di Amazon DocumentDB

Per monitorare lo stato e le prestazioni del cluster e delle istanze Amazon DocumentDB, puoi visualizzare le seguenti metriche nella console Amazon DocumentDB.

Note

Le metriche nelle tabelle seguenti si applicano sia ai cluster basati su istanze che ai cluster elastici.

Utilizzo delle risorse

Parametro	Descrizione	
BackupRetentionPeriodStorageUsed	La quantità totale di storage di backup in GiB utilizzata per supportare point-in-time funzionalità di ripristino all'interno della finestra di conservazione di Amazon DocumentDB. Incluso nel totale riportato dal parametro TotalBackupStorageBilled . Calcolato separatamente per ogni cluster Amazon DocumentDB.	
ChangeStreamLogSize	La quantità di storage utilizzata dal cluster per archiviare il log del flusso di modifiche in megabyte. Questo valore è un sottoinsieme dello storage totale per il cluster (VolumeBytesUsed) e influisce sul costo del cluster. Per informazioni sui prezzi dello storage, consulta	

Parametro	Descrizione
	<p>il Pagina del prodotto Amazon DocumentDB. La dimensione del log del flusso di modifiche è una funzione della quantità di modifiche applicata nel cluster e della durata di conservazione prolungata del flusso di modifiche. Per ulteriori informazioni sui flussi di modifiche, consulta Utilizzo di Change Streams con Amazon DocumentDB.</p>
CPUUtilization	La percentuale di CPU utilizzata da un'istanza.
DatabaseConnections	Il numero di connessioni aperte su un'istanza acquisita con una frequenza di un minuto.
DatabaseConnectionsMax	Il numero massimo di connessioni al database aperte su un'istanza in un periodo di un minuto.
DatabaseCursors	Il numero di cursori aperti su un'istanza acquisita con una frequenza di un minuto.
DatabaseCursorsMax	Il numero massimo di cursori aperti su un'istanza in un periodo di un minuto.
DatabaseCursorsTimedOut	Il numero di cursori scaduti in un periodo di un minuto.

Parametro	Descrizione	
<code>FreeableMemory</code>	La quantità di memoria RAM disponibile, in byte.	
<code>FreeLocalStorage</code>	Questo parametro indica la quantità di storage disponibile in ogni istanza per le tabelle e i log temporanei. Questo valore dipende dalla classe di istanza. Puoi aumentare la quantità di storage gratuito per un'istanza scegliendo una classe di istanza più ampia per l'istanza.	
<code>LowMemThrottleQueueDepth</code>	La profondità della coda per le richieste che vengono limitate a causa della scarsa memoria disponibile occupata con una frequenza di un minuto.	
<code>LowMemThrottleMaxQueueDepth</code>	La profondità massima di coda per le richieste che vengono limitate a causa della scarsa memoria disponibile in un periodo di un minuto.	
<code>LowMemNumOperationsThrottled</code>	Il numero di richieste che vengono limitate a causa della scarsa memoria disponibile in un periodo di un minuto.	

Parametro	Descrizione	
SnapshotStorageUsed	La quantità totale di storage di backup in GiB utilizzata da tutte le istantanee di un determinato cluster Amazon DocumentDB al di fuori della relativa finestra di conservazione del backup. Incluso nel totale riportato dal parametro TotalBackupStorageBilled . Calcolato separatamente per ogni cluster Amazon DocumentDB.	
SwapUsage	La quantità di spazio di swapping utilizzato sull'istanza.	
TotalBackupStorageBilled	La quantità totale di storage di backup in GiB che ti viene fatturata per un determinato cluster Amazon DocumentDB. Include lo storage di backup misurato dai parametri BackupRetentionPeriodStorageUsed e SnapshotStorageUsed . Calcolato separatamente per ogni cluster Amazon DocumentDB.	
TransactionsOpen	Il numero di transazioni aperte su un'istanza eseguite con una frequenza di un minuto.	

Parametro	Descrizione
TransactionsOpenMax	Il numero massimo di transazioni aperte su un'istanza in un periodo di un minuto.
VolumeBytesUsed	La quantità di storage in byte utilizzata dal cluster. Questo valore influisce sul costo del cluster. Per informazioni sui prezzi, consulta il Pagina del prodotto Amazon DocumentDB .

Latenza

Parametro	Descrizione
DBClusterReplicaLagMaximum	Il ritardo massimo, in millisecondi, tra l'istanza principale e ogni istanza di Amazon DocumentDB nel cluster.
DBClusterReplicaLagMinimum	Il ritardo minimo, in millisecondi, tra l'istanza primaria e ogni istanza di replica nel cluster.
DBInstanceReplicaLag	Il ritardo, in millisecondi, durante la replica degli aggiornamenti dall'istanza primaria a un'istanza di replica.
ReadLatency	La quantità di tempo media che occorre per ciascuna operazione I/O su disco.

Parametro	Descrizione	
WriteLatency	La quantità di tempo media, in millisecondi, che occorre per ciascuna operazione I/O su disco.	

Operazioni

Parametro	Descrizione	
DocumentsDeleted	Il numero di documenti eliminati in un periodo di un minuto.	
DocumentsInserted	Il numero di documenti inseriti in un periodo di un minuto.	
DocumentsReturned	Il numero di documenti restituiti in un periodo di un minuto.	
DocumentsUpdated	Il numero di documenti aggiornati in un periodo di un minuto.	
OpcountersCommand	Il numero di comandi emessi in un periodo di un minuto.	
OpcountersDelete	Il numero di operazioni di eliminazione eseguite in un periodo di un minuto.	
OpcountersGetmore	Il numero di getmore emessi in un periodo di un minuto.	
OpcountersInsert	Il numero di operazioni di inserimento emesse in un periodo di un minuto.	

Parametro	Descrizione	
OpcountersQuery	Il numero di interrogazioni emesse in un periodo di un minuto.	
OpcountersUpdate	Il numero di operazioni di aggiornamento eseguite in un periodo di un minuto.	
TransactionsStarted	Il numero di transazioni avviate su un'istanza in un periodo di un minuto.	
TransactionsCommitted	Il numero di transazioni eseguite su un'istanza in un periodo di un minuto.	
TransactionsAborted	Il numero di transazioni interrotte su un'istanza in un periodo di un minuto.	
TTLDeletedDocuments	Il numero di documenti eliminati da un TTLMonitor in un periodo di un minuto.	

Prestazioni

Parametro	Descrizione	
NetworkReceiveThroughput	La quantità di throughput della rete, in byte al secondo, ricevuta dai clienti per ogni istanza nel cluster. Questo throughput non include il traffico di rete tra le istanze nel cluster e il volume cluster.	

Parametro	Descrizione	
NetworkThroughput	La quantità di throughput di rete, in byte al secondo, ricevuta e trasmessa ai client da ciascuna istanza del cluster Amazon DocumentDB. Questo throughput non include il traffico di rete tra le istanze nel cluster e il volume cluster.	
NetworkTransmitThroughput	La quantità di throughput della rete, in byte al secondo, inviata ai clienti per ogni istanza nel cluster. Questo throughput non include il traffico di rete tra le istanze nel cluster e il volume cluster.	
ReadIOPS	Il numero medio di operazioni di I/O di lettura del disco al secondo. Amazon DocumentDB riporta gli IOPS di lettura e scrittura separatamente e a intervalli di un minuto.	
ReadThroughput	Il numero medio di byte letti dal disco al secondo.	

Parametro	Descrizione	
VolumeReadIOPs	<p>Numero medio delle operazioni I/O di lettura fatturate da un volume di cluster, indicato a intervalli di 5 minuti. Le operazioni di lettura fatturate sono calcolate a livello del volume del cluster, aggregate da tutte le istanze nel cluster e quindi indicate a intervalli di 5 minuti. Il valore viene calcolato prendendo il valore del parametro per le operazioni di lettura in un periodo di 5 minuti. Puoi determinare la quantità delle operazioni di lettura fatturate al secondo prendendo il valore del parametro per le operazioni di lettura fatturate e dividendolo per 300 secondi.</p> <p>Ad esempio, se <code>VolumeReadIOPs</code> restituisce 13.686, quindi le operazioni di lettura fatturate al secondo sono 45 ($13.686 / 300 = 45,62$).</p> <p>Le operazioni di lettura fatturate si accumulano per le query che richiedono o pagine del database che non si trovano nella cache del buffer e, per questo, devono essere caricate dallo storage. Potresti vedere dei picchi nelle</p>	

Parametro	Descrizione	
	operazioni di lettura fatturate poiché i risultati della query vengono letti dallo storage e, in seguito, caricati nella cache del buffer.	

Parametro	Descrizione	
<code>VolumeWriteIOPs</code>	<p>Numero medio delle operazioni I/O di scrittura fatturate da un volume di cluster, indicato a intervalli di 5 minuti. Le operazioni di scrittura fatturate sono calcolate a livello del volume del cluster, aggregate da tutte le istanze nel cluster e quindi indicate a intervalli di 5 minuti. Il valore è calcolato prendendo il valore del parametro delle operazioni di scrittura per un periodo che supera i 5 minuti. Puoi determinare la quantità delle operazioni di scrittura fatturate al secondo prendendo il valore del parametro delle operazioni di scrittura fatturate e dividendo per 300 secondi.</p> <p>Ad esempio, se <code>VolumeWriteIOPs</code> restituisce 13.686, quindi le operazioni di scrittura fatturate al secondo sono 45 ($13.686 / 300 = 45,62$).</p> <p>Nota che <code>VolumeReadIOPs</code> e <code>VolumeWriteIOPs</code> le metriche sono calcolate dal livello di archiviazione DocumentDB e includono gli IO eseguiti dalle istanze primarie e di replica. I dati vengono aggregati ogni</p>	

Parametro	Descrizione	
	20-30 minuti e quindi riportati a intervalli di 5 minuti, emettendo così lo stesso punto dati per la metrica nel periodo di tempo. Se stai cercando una metrica da correlare alle operazioni di inserimento su un intervallo di 1 minuto, puoi utilizzare la metrica <code>WriteIOPS</code> a livello di istanza. La metrica è disponibile nella scheda di monitoraggio dell'istanza principale di Amazon DocumentDB.	
<code>WriteIOPS</code>	Il numero medio di operazioni di I/O di scrittura su disco al secondo. Se utilizzato a livello di cluster, <code>WriteIOPS</code> vengono valutate in tutte le istanze del cluster. Gli IOPS di lettura e scrittura vengono riportati separatamente, a intervalli di 1 minuto.	
<code>WriteThroughput</code>	Il numero medio di byte scritti sul disco al secondo.	

System (Sistema)

Parametro	Descrizione	
<code>BufferCacheHitRatio</code>	La percentuale di richieste gestite dalla cache del buffer.	

Parametro	Descrizione	
DiskQueueDepth	il numero di richieste di scrittura simultanee sul volume di storage distribuito.	
EngineUptime	Il periodo di esecuzione dell'istanza, in secondi.	
IndexBufferCacheHitRatio	La percentuale di richieste di indice servite dalla buffer cache. Potresti vedere un picco superiore al 100% per la metrica subito dopo aver eliminato un indice, una raccolta o un database. Questo errore verrà corretto automaticamente dopo 60 secondi. Questa limitazione verrà corretta in un futuro aggiornamento della patch.	

Metriche delle istanze T3

Parametro	Descrizione	
CPUCreditUsage	Il numero di crediti CPU spesi durante il periodo di misurazione.	
CPUCreditBalance	Il numero di crediti CPU accumulati da un'istanza. Questo saldo è esaurito quando la CPU ottimizza le prestazioni e i crediti CPU vengono spesi più rapidamente di quanto guadagnati.	

Parametro	Descrizione	
CPUSurplusCreditBalance	Il numero di crediti CPU in eccesso spesi per sostenere le prestazioni della CPU quando la CPU è attivaCreditBalance il valore è zero.	
CPUSurplusCreditsCharged	Il numero di crediti CPU in eccesso che supera il numero massimo di crediti CPU ottenibili in un periodo di 24 ore, con conseguente addebito di un costo aggiuntivo. Per ulteriori informazioni, vedere Monitoraggio dei crediti della CPU .	

Visualizzazione CloudWatch Dati

Puoi visualizzare Amazon CloudWatch dati utilizzando il CloudWatch console, la console Amazon DocumentDB, AWS Command Line Interface (AWS CLI), oppure CloudWatch API.

Using the AWS Management Console

Da visualizzare CloudWatch i parametri che utilizzano la console di gestione Amazon DocumentDB, completa i seguenti passaggi.

1. Accedi a AWS Management Console e apri la console Amazon DocumentDB all'indirizzo <https://console.aws.amazon.com/docdb>.
2. Nel pannello di navigazione scegliere Clusters (Cluster).

Tip

Se il riquadro di navigazione non viene visualizzato sul lato sinistro della schermata, scegliere l'icona del menu

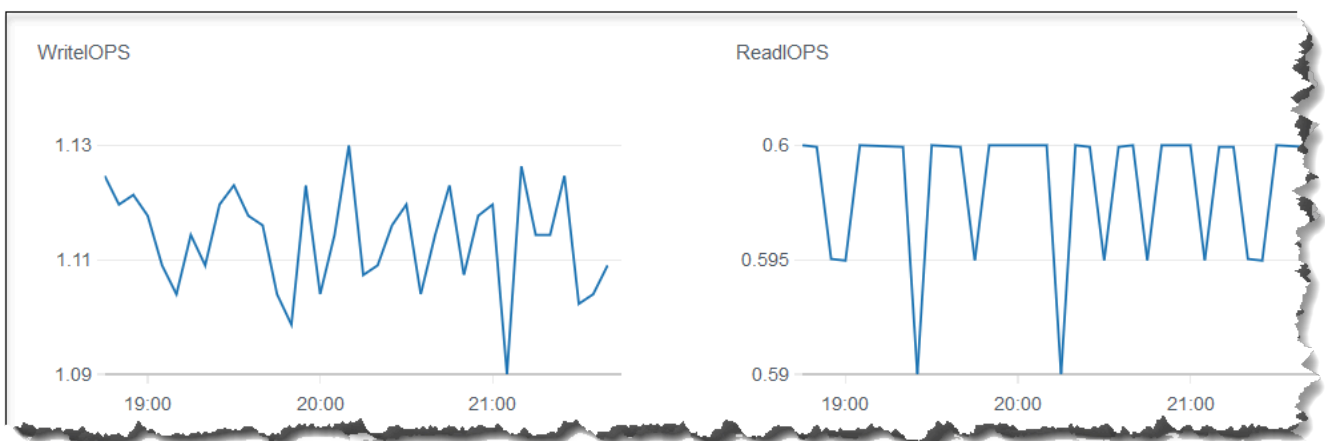
(☰) nell'angolo in alto a sinistra della pagina.

- Nella casella di navigazione Clusters, vedrai la colonna identificatore del cluster. Le tue istanze sono elencate in cluster, in modo simile alla schermata seguente.

<input type="checkbox"/>	<input type="checkbox"/>	Cluster identifier	Role
<input type="checkbox"/>	<input type="checkbox"/>	docdb-cloud9-getstarted	Cluster
<input type="checkbox"/>	<input type="checkbox"/>	docdb-cloud9-getstarted	Primary
<input type="checkbox"/>	<input type="checkbox"/>	robo3t	Cluster
<input type="checkbox"/>	<input type="checkbox"/>	robo3t	Primary

- Dall'elenco delle istanze, scegli il nome dell'istanza per cui desideri le metriche.
- Nella pagina di riepilogo dell'istanza risultante, scegli Monitoraggio scheda per visualizzare le rappresentazioni grafiche dei parametri dell'istanza Amazon DocumentDB. Poiché è necessario generare un grafico per ogni metrica, potrebbero essere necessari alcuni minuti per CloudWatch grafici da compilare.

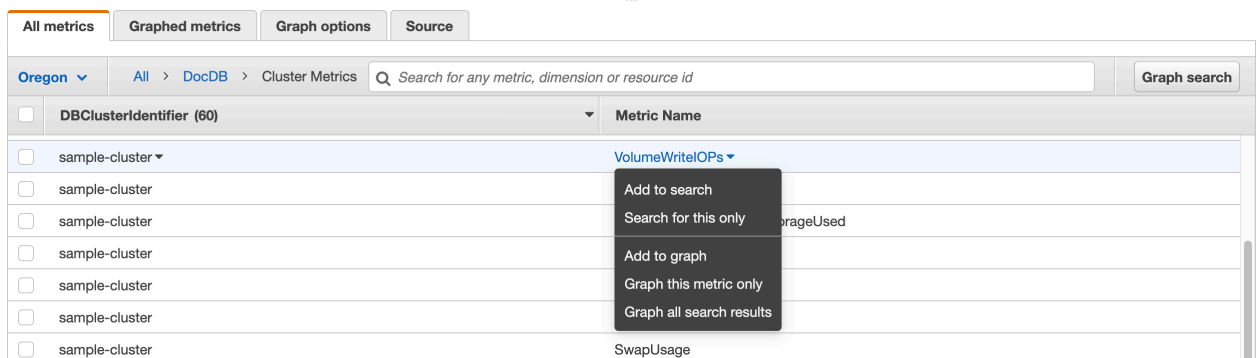
L'immagine seguente mostra le rappresentazioni grafiche di due CloudWatch metriche nella console Amazon DocumentDB, WriteIOPS e ReadIOPS.



Using the CloudWatch Management Console

Per visualizzare CloudWatch metriche che utilizzano il CloudWatch Console di gestione, completa i seguenti passaggi.

1. Accedere aAWS Management Consolee apri la console Amazon DocumentDB all'indirizzo<https://console.aws.amazon.com/cloudwatch>.
2. Nel riquadro di navigazione, selezionare Parametri. Quindi, dall'elenco dei nomi dei servizi, scegliDocDB.
3. Scegli una dimensione metrica (ad esempioMetriche del cluster).
4. LaTutte le metricheLa scheda mostra tutte le metriche per quella dimensione inDocDB.
 - a. Per ordinare la tabella, utilizza l'intestazione della colonna.
 - b. Per creare il grafico di un parametro, seleziona la casella di controllo accanto al parametro. Per selezionare tutte i parametri, seleziona la casella di controllo nella riga dell'intestazione della tabella.
 - c. Per filtrare in base alla metrica, passa il mouse sul nome della metrica e seleziona la freccia a discesa accanto al nome della metrica. Quindi, scegliAggiungi alla ricerca, come mostrato nell'immagine qui sotto.



Using the AWS CLI

Per visualizzare CloudWatch dati per Amazon DocumentDB, usa CloudWatch `get-metric-statistics` funzionamento con i seguenti parametri.

Parametri

- **--namespace**: obbligatorio. Lo spazio dei nomi del servizio di cui desideri visualizzare i parametri CloudWatch . Per Amazon DocumentDB, deve essere `AWS/DocDB`.

- **--metric-name**: obbligatorio. Il nome della metrica per la quale desideri i dati.
- **--start-time**: obbligatorio. Il timestamp che determina il primo punto dati da restituire.

Il valore specificato è inclusivo. I risultati comprendono i punti dati con il timestamp specificato. Il timestamp deve essere in formato UTC ISO 8601, ad esempio 2016-10-03T23:00:00Z.

- **--end-time**: obbligatorio. Il timestamp che determina l'ultimo punto dati da restituire.

Il valore specificato è inclusivo. I risultati comprendono i punti dati con il timestamp specificato. Il timestamp deve essere in formato UTC ISO 8601, ad esempio 2016-10-03T23:00:00Z.

- **--period**: obbligatorio. La granularità, in secondi, per i punti dati restituiti. Per i parametri con una risoluzione regolare, un periodo può avere un valore minimo di un minuto (60 secondi) e deve essere un multiplo di 60. Per i parametri ad alta risoluzione raccolti a intervalli inferiori al minuto, il periodo può essere 1, 5, 10, 30, 60 o qualsiasi multiplo di 60.
- **--dimensions**— Facoltativo. Se la metrica contiene più dimensioni, è necessario includere un valore per ogni dimensione. CloudWatch considera ogni combinazione unica di dimensioni come una metrica separata. Se una specifica combinazione di dimensioni non è stata pubblicata, non puoi recuperare le statistiche associate. Occorre specificare le stesse dimensioni utilizzate al momento della creazione dei parametri.
- **--statistics**— Facoltativo. Le statistiche dei parametri diverse dai percentili. Per le statistiche dei percentili, utilizzare `ExtendedStatistics`. Quando chiami `GetMetricStatistics`, devi specificare `Statistics` o `ExtendedStatistics`, ma non entrambi.

Valori consentiti:

- `SampleCount`
- `Average`
- `Sum`
- `Minimum`
- `Maximum`
- **--extended-statistics**— Facoltativo Le statistiche percentile. Specifica valori compresi tra p0.0 e p100. Quando chiami `GetMetricStatistics`, devi specificare `Statistics` o `ExtendedStatistics`, ma non entrambi.
- **--unit**— Facoltativo L'unità per un determinato parametro. I parametri possono essere riportati con più unità. Se non specifichi un'unità, vengono restituite tutte le unità. Se specifichi solo un'unità che il parametro non supporta, i risultati della chiamata sono nulli.

Valori possibili:

- 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

L'esempio seguente rileva il valore massimo di `CPUUtilization` per un periodo di 2 ore, durante il quale viene estratto un campione ogni 60 secondi.

Per Linux, macOS o 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
```

Per 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
```

L'aspetto dell'output di questa operazione è simile al seguente.

```
{  
  "Label": "CPUUtilization",  
  "Datapoints": [  
    {  
      "Unit": "Percent",  
      "Maximum": 4.49152542374361,  
      "Timestamp": "2019-02-11T05:51:00Z"  
    },  
    {  
      "Unit": "Percent",  
      "Maximum": 4.250000000000485,  
      "Timestamp": "2019-02-11T06:44:00Z"  
    }  
  ]  
}
```

```

    },
    ***** some output omitted for brevity *****
    {
      "Unit": "Percent",
      "Maximum": 4.33333333331878,
      "Timestamp": "2019-02-11T06:07:00Z"
    }
  ]
}

```

Dimensioni Amazon DocumentDB

Le metriche per Amazon DocumentDB sono qualificate in base ai valori dell'account o dell'operazione. Puoi usare il CloudWatch console per recuperare i dati di Amazon DocumentDB filtrati in base a una qualsiasi delle dimensioni nella tabella seguente.

Dimensione	Descrizione
<code>DBClusterIdentifier</code>	Filtra i dati richiesti per uno specifico cluster Amazon DocumentDB.
<code>DBClusterIdentifier, Role</code>	Filtra i dati richiesti per uno specifico cluster Amazon DocumentDB, aggregando la metrica per ruolo di istanza (WRITER/READER). Ad esempio, puoi aggregare i parametri per tutte le istanze READER che appartengono a un cluster.
<code>DBInstanceIdentifier</code>	Filtra i dati richiesti per un'istanza database specifica.

Monitoraggio degli opcounter

Le metriche di Opcounter hanno un valore diverso da zero (di solito ~50) per i cluster inattivi. Questo perché Amazon DocumentDB esegue controlli periodici dello stato, operazioni interne e attività di raccolta dei parametri.

Monitoraggio delle connessioni al database

Quando si visualizza il numero di connessioni utilizzando comandi del motore di database `comedb.runCommand({ serverStatus: 1 })`, potresti visualizzare fino a 10 connessioni in più rispetto a quelle visualizzate in `DatabaseConnections` attraverso CloudWatch. Ciò si verifica perché Amazon DocumentDB esegue controlli periodici dello stato di salute e attività di raccolta delle metriche che non vengono prese in considerazione in `DatabaseConnections`. `DatabaseConnections` rappresenta solo le connessioni avviate dal cliente.

Registrazione delle chiamate API di AmazonAWS CloudTrail

Amazon DocumentDB (compatibile con MongoDB) è integrato con AWS CloudTrail, un servizio che offre un record delle operazioni eseguite da utenti, da un ruolo o da un AWS servizio in Amazon DocumentDB (compatibile con MongoDB). CloudTrail acquisisce tutte le chiamate AWS CLI API per Amazon DocumentDB come eventi, incluse le chiamate dalla console Amazon DocumentDB e dal codice ad Amazon DocumentDB. Se crei un percorso, puoi abilitare la distribuzione continua di CloudTrail eventi in un bucket Amazon S3, inclusi gli eventi per Amazon DocumentDB. Se non si configura un percorso, è comunque possibile visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi. Le informazioni raccolte da consentono CloudTrail di determinare la richiesta effettuata ad Amazon DocumentDB (compatibile con MongoDB), l'indirizzo IP da cui è partita la richiesta, l'autore della richiesta, il momento in cui è stata eseguita e altri dettagli.

Important

Per alcune funzionalità di gestione, Amazon DocumentDB utilizza la tecnologia operativa condivisa con Amazon Relational Database Service (Amazon RDS). Le chiamate alla console Amazon DocumentDB e alle API vengono registrate come chiamate effettuate all'API Amazon RDS.AWS CLI

Per ulteriori informazioni su AWS CloudTrail, consulta la [Guida per l'utente di AWS CloudTrail](#).

Informazioni su Amazon DocumentDB in CloudTrail

CloudTrail è abilitato sul tuo account AWS momento della sua creazione. Quando si verifica un'attività in Amazon DocumentDB, questa viene registrata in un CloudTrail evento insieme ad altri

eventi di AWS servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare gli eventi recenti nell'Account AWS. Per ulteriori informazioni, consulta [Visualizzazione di eventi mediante la cronologia CloudTrail eventi](#) di.

Per una registrazione continua degli eventi nell'che includa eventi per Amazon DocumentDB (compatibile con MongoDB), crea un percorso.Account AWS Un percorso consente di CloudTrail distribuire i file di log in un bucket Amazon S3. Per impostazione predefinita, quando si crea un percorso nella console, questo sarà valido in tutte le Regioni AWS. Il percorso registra gli eventi di tutte le Regioni nella partizione AWS e distribuisce i file di log nel bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare con maggiore dettaglio e usare i dati raccolti nei CloudTrail log. Per ulteriori informazioni, consulta gli argomenti seguenti nella Guida per l'utente di AWS CloudTrail:

- [Panoramica della creazione di un percorso](#)
- [CloudTrail Servizi e integrazioni supportati](#)
- [Configurazione delle notifiche Amazon SNS per CloudTrail](#)
- [Ricezione di file di CloudTrail log da più regioni](#)
- [Ricezione di file di CloudTrail log da più account](#)

Ogni evento o voce di log include informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali utente o root.
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro servizio AWS.

Per ulteriori informazioni, consulta [Elemento CloudTrail userIdentity](#).

Profilazione delle operazioni di Amazon DocumentDB

Puoi utilizzare il profiler in Amazon DocumentDB (compatibile con MongoDB) per registrare il tempo di esecuzione e i dettagli delle operazioni eseguite sul tuo cluster. Il profiler è utile per monitorare le operazioni più lente sul cluster per aiutare a migliorare le prestazioni delle singole query e le prestazioni complessive del cluster.

Per impostazione predefinita, la funzionalità profiler è disabilitata. Se abilitato, il profiler registra le operazioni che richiedono più tempo di un valore di soglia definito dal cliente (ad esempio, 100 ms) su Amazon CloudWatch Registri. I dettagli registrati includono il comando profilato, l'ora, il riepilogo del piano e i metadati del client. Dopo aver effettuato l'accesso alle operazioni CloudWatch Registri, puoi usare CloudWatch Logs Insights per analizzare, monitorare e archiviare i dati di profilazione di Amazon DocumentDB. Le query comuni vengono fornite nella sezione [Query comuni](#).

Se abilitato, il profiler utilizza risorse aggiuntive nel cluster. Ti consigliamo di iniziare con un valore di soglia elevato (ad esempio, 500 ms) e di ridurre gradualmente il valore per identificare le operazioni lente. Iniziare con un valore di soglia di 50 ms può causare problemi di prestazioni sul cluster per applicazioni a throughput elevato. Il profiler è abilitato a livello di cluster e funziona su tutte le istanze e i database di un cluster. Amazon DocumentDB registra le operazioni su Amazon CloudWatch Effettua i log con la massima diligenza possibile.

Sebbene Amazon DocumentDB non imponga alcun costo aggiuntivo per abilitare il profiler, ti vengono addebitate le tariffe standard per l'utilizzo di CloudWatch Registri. Per informazioni su CloudWatch Registra i prezzi, vedi [Amazon CloudWatch prezzi](#).

Argomenti

- [Operazioni supportate](#)
- [Restrizioni](#)
- [Abilitazione di Amazon DocumentDB Profiler](#)
- [Disattivazione di Amazon DocumentDB Profiler](#)
- [Disabilitazione dell'esportazione dei log del profiler](#)
- [Accesso ai log di Amazon DocumentDB Profiler](#)
- [Query comuni](#)

Operazioni supportate

Amazon DocumentDB profiler supporta le seguenti operazioni:

- aggregate
- count
- delete
- distinct
- find (OP_QUERY e comando)

- `findAndModify`
- `insert`
- `update`

Restrizioni

Lo slow query profiler è in grado di emettere i log del profiler solo se l'intero set di risultati della query può essere contenuto in un batch e se il set di risultati è inferiore a 16 MB (dimensione massima BSON). I set di risultati superiori a 16 MB vengono automaticamente suddivisi in più batch.

La maggior parte dei driver o delle shell può impostare una dimensione del batch predefinita piccola. È possibile specificare la dimensione del batch come parte della query. Per acquisire log di query lenti, si consiglia di utilizzare un batch di dimensioni superiori a quelle del set di risultati previsto. Se non siete sicuri della dimensione del set di risultati o se questa varia, potete anche impostare la dimensione del batch su un numero elevato (ad esempio 100k).

Tuttavia, l'utilizzo di un batch di dimensioni maggiori significa che sarà necessario recuperare più risultati dal database prima di inviare una risposta al client. Per alcune domande, ciò potrebbe creare ritardi più lunghi prima di ottenere risultati. Se non si prevede di utilizzare l'intero set di risultati, è possibile che si impieghino più operazioni di I/O per elaborare la query e buttare via il risultato.

Abilitazione di Amazon DocumentDB Profiler

L'abilitazione del profiler su un cluster è un processo in tre fasi. Assicurati che tutti i passaggi siano stati completati, altrimenti i registri di profilazione non verranno inviati a CloudWatch Registri. Il profiler è impostato a livello di cluster e viene eseguito su tutti i database e le istanze del cluster.

Per abilitare il profiler su un cluster

1. Poiché non puoi modificare un gruppo predefinito di parametri del cluster, assicurati di disporre di un gruppo personalizzato di parametri del cluster. Per ulteriori informazioni, consulta [Creazione di gruppi di parametri del cluster Amazon DocumentDB](#).
2. Utilizzando un gruppo di parametri personalizzato del cluster disponibile, modifica i seguenti parametri: `profiler`, `profiler_threshold_ms`, e `profiler_sampling_rate`. Per ulteriori informazioni, consulta [Modifica dei gruppi di parametri del cluster Amazon DocumentDB](#).
3. Crea o modifica il cluster per utilizzare il gruppo di parametri del cluster personalizzato e abilitare l'esportazione del profiler a CloudWatch Registri.

Le sezioni seguenti mostrano come implementare queste fasi utilizzando la AWS Management Console e AWS Command Line Interface (AWS CLI).

Using the AWS Management Console

1. Prima di iniziare, crea un cluster Amazon DocumentDB e un gruppo di parametri di cluster personalizzato se non ne hai già uno. Per ulteriori informazioni, consultare [Creazione di gruppi di parametri del cluster Amazon DocumentDB](#) e [Creazione di un cluster Amazon DocumentDB](#).
2. Utilizzando un gruppo personalizzato di parametri del cluster disponibile, modifica i parametri seguenti. Per ulteriori informazioni, consulta [Modifica dei gruppi di parametri del cluster Amazon DocumentDB](#).
 - `profiler`— Abilita o disabilita la profilazione delle query. I valori consentiti sono `enabled` e `disabled`. Il valore di default è `disabled`. Per abilitare il profiling, impostare il valore su `enabled`.
 - `profiler_threshold_ms`— Quando `profiler` è impostato su `enabled`, tutti i comandi che richiedono più tempo di `profiler-threshold-ms` sono connessi a CloudWatch. I valori consentiti sono `[50-INT_MAX]`. Il valore di default è `100`.
 - `profiler_sampling_rate`— La frazione di operazioni lente che deve essere profilata o registrata. I valori consentiti sono `[0.0-1.0]`. Il valore di default è `1.0`.
3. Modifica il cluster per utilizzare il gruppo di parametri del cluster personalizzato e imposta le esportazioni dei log del profiler per la pubblicazione su Amazon CloudWatch.
 - a. Nel riquadro di navigazione scegliere Clusters (Cluster) per aggiungere il nuovo gruppo di parametri personalizzato a un cluster.
 - b. Scegliere il pulsante a sinistra del nome del cluster a cui si desidera associare il gruppo di parametri. Selezionare Actions (Operazioni), quindi Modify (Modifica) per modificare il cluster.
 - c. In Cluster options (Opzioni cluster), scegliere il gruppo di parametri personalizzato dal passaggio precedente per aggiungerlo al cluster.
 - d. Sotto Esportazioni di log, selezionare registri Profiler da pubblicare su Amazon CloudWatch.
 - e. Scegliere Continue (Continua) per visualizzare un riepilogo delle modifiche.
 - f. Dopo aver verificato le modifiche, è possibile applicarle immediatamente o durante la successiva finestra di manutenzione in Scheduling of modifications (Pianificazione delle modifiche).

- g. Scegliere **Modify cluster** (Modifica cluster) per aggiornare il cluster con il nuovo gruppo di parametri.

Using the AWS CLI

La procedura seguente abilita il profiler su tutte le operazioni supportate per il cluster `sample-cluster`.

1. Prima di iniziare, assicurati di avere un gruppo di parametri del cluster personalizzati disponibile eseguendo il comando seguente e verificando che l'output di un gruppo di parametri del cluster non abbia `default` nel nome e che abbia `docdb3.6` come famiglia del gruppi di parametri. Se non disponi di un gruppo di parametri cluster non predefinito, consulta [Creazione di gruppi di parametri del cluster Amazon DocumentDB](#).

```
aws docdb describe-db-cluster-parameter-groups \  
  --query 'DBClusterParameterGroups[*].  
  [DBClusterParameterGroupName,DBParameterGroupFamily]'
```

Nel seguente output, solo `sample-parameter-group` soddisfa entrambi i criteri.

```
[  
  [  
    "default.docdb3.6",  
    "docdb3.6"  
  ],  
  [  
    "sample-parameter-group",  
    "docdb3.6"  
  ]  
]
```

2. Utilizzando il gruppo personalizzato di parametri del cluster, modifica i parametri seguenti:
 - `profiler`— Abilita o disabilita la profilazione delle query. I valori consentiti sono `enabled` e `disabled`. Il valore di default è `disabled`. Per abilitare il profiling, impostare il valore su `enabled`.
 - `profiler_threshold_ms`— Quando `profiler` è impostato su `enabled`, tutti i comandi richiedono più tempo di `profiler -threshold-ms` sono connessi a CloudWatch. I valori

consentiti sono `[0-INT_MAX]`. L'impostazione di questo valore su `0` esegue il profiling di tutte le operazioni supportate. Il valore di default è `100`.

- `profiler_sampling_rate`— La frazione di operazioni lente che deve essere profilata o registrata. I valori consentiti sono `[0.0-1.0]`. Il valore di default è `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. Modifica il tuo cluster Amazon DocumentDB in modo che utilizzi il `sample-parameter-group` gruppo di parametri del cluster personalizzato del passaggio precedente e impostazione del parametro `--enable-cloudwatch-logs-exports` `profiler`.

Il codice seguente modifica il cluster `sample-cluster` usare il `sample-parameter-group` dal passaggio precedente e aggiunge `profiler` agli abilitati CloudWatch Registra le esportazioni.

```
aws docdb modify-db-cluster \
  --db-cluster-identifier sample-cluster \
  --db-cluster-parameter-group-name sample-parameter-group \
  --cloudwatch-logs-export-configuration '{"EnableLogTypes":["profiler"]}'
```

L'aspetto dell'output di questa operazione è simile al seguente.

```
{
  "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": "ABCDEFGHJKLMN",
"StorageEncrypted": true,
"KmsKeyId": "arn:aws:kms:us-east-1:<accountID>:key/sample-key",
"DbClusterResourceId": "cluster-ABCDEFGHIJKLMNQRSTUWXYZ",
"DBClusterArn": "arn:aws:rds:us-east-1:<accountID>:cluster:sample-
cluster",
"AssociatedRoles": [],
"ClusterCreateTime": "2020-01-10T22:13:38.261Z",
"EnabledCloudwatchLogsExports": [
  "profiler"
],
```

```
    "DeletionProtection": true
  }
}
```

Disattivazione di Amazon DocumentDB Profiler

Per disabilitare il profiler, si disattivano entrambi i parametri `profiler` e l'esportazione di `profiler` accedendo a CloudWatch Registri.

Disabilitazione del profiler

Puoi disabilitare il parametro `profiler` utilizzando la AWS Management Console o l'AWS CLI, come segue.

Using the AWS Management Console

La procedura seguente utilizza l'AWS Management Console per disabilitare Amazon DocumentDB `profiler`.

1. Accedi all'AWS Management Console e apri la console Amazon DocumentDB all'indirizzo <https://console.aws.amazon.com/docdb>.
2. Nel riquadro di navigazione scegliere **Parameter groups (Gruppi di parametri)**. Scegliere quindi il nome del gruppo di parametri del cluster su cui si desidera disabilitare il profiler.
3. Nella pagina **Cluster parameters (Parametri cluster)** risultante, selezionare il pulsante a sinistra del parametro `profiler` e scegliere **Edit (Modifica)**.
4. Nella finestra di dialogo **Modify profiler (Modifica profiler)**, scegliere `disabled` nell'elenco.
5. Scegliere **Modify cluster parameter (Modifica parametro cluster)**.

Using the AWS CLI

Per disabilitare `profiler` su un cluster utilizzando l'AWS CLI, modificare il cluster come segue.

```
aws docdb modify-db-cluster-parameter-group \
  --db-cluster-parameter-group-name sample-parameter-group \
  --parameters
ParameterName=profiler,ParameterValue=disabled,ApplyMethod=immediate
```

Disabilitazione dell'esportazione dei log del profiler

Puoi disabilitare l'esportazione dei log del profiler accedendo a CloudWatch Esegue i log utilizzando uno dei AWS Management Console o AWS CLI, come segue.

Using the AWS Management Console

La procedura seguente utilizza AWS Management Console per disabilitare l'esportazione dei log di Amazon DocumentDB in CloudWatch.

1. Apri la console Amazon DocumentDB all'indirizzo <https://console.aws.amazon.com/docdb>.
2. Nel pannello di navigazione scegliere Clusters (Cluster). Scegliere il pulsante a sinistra del nome del cluster per il quale si desidera disabilitare l'esportazione dei log.
3. Nel menu Actions (Operazioni) selezionare Modify (Modifica).
4. Scorrere verso il basso fino alla sezione Log exports (Esportazioni log) e deselezionare Profiler logs (Log del profiler).
5. Scegli Continue (Continua).
6. Esaminare le modifiche, quindi scegliere quando applicare la modifica al cluster.
 - Apply during the next scheduled maintenance window (Applica durante la prossima finestra di manutenzione pianificata)
 - Apply immediately (Applica immediatamente)
7. Scegliere Modify cluster (Modifica cluster).

Using the AWS CLI

Il codice seguente modifica il cluster `sample-cluster` e disabilita CloudWatch registri del profiler.

Example

Per Linux, macOS o Unix:

```
aws docdb modify-db-cluster \
  --db-cluster-identifier sample-cluster \
  --cloudwatch-logs-export-configuration '{"DisableLogTypes":["profiler"]}'
```

Per Windows:

```
aws docdb modify-db-cluster ^
  --db-cluster-identifier sample-cluster ^
  --cloudwatch-logs-export-configuration '{"DisableLogTypes":["profiler"]}'
```

L'aspetto dell'output di questa operazione è simile al seguente.

```
{
  "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
}
```

Accesso ai log di Amazon DocumentDB Profiler

Segui questi passaggi per accedere ai log del tuo profilo su Amazon CloudWatch.

1. Aprire il CloudWatch console in <https://console.aws.amazon.com/cloudwatch/>.
2. Assicurati di trovarti nella stessa regione del cluster Amazon DocumentDB.
3. Nel riquadro di navigazione scegli Logs (Log).
4. Per trovare i log del profiler per il cluster, nell'elenco scegliere `/aws/docdb/yourClusterName/profiler`.

I log del profiler per ogni istanza sono disponibili nei rispettivi nomi di istanza.

Query comuni

Di seguito sono riportate alcune query comuni che è possibile utilizzare per analizzare i comandi profilati. Per ulteriori informazioni su CloudWatch Logs Insights, vedi [Analisi dei dati di registro con CloudWatch Logs InsightseDomande di esempio](#).

Ottenere le 10 operazioni più lente su una raccolta specificata

```
filter ns="test.foo" | sort millis desc | limit 10
```

Ottenere tutte le operazioni di aggiornamento su una raccolta che hanno richiesto più di 60 ms

```
filter millis > 60 and op = "update"
```

Ottenere le 10 operazioni più lente nell'ultimo mese

```
sort millis desc | limit 10
```

Ottenere tutte le query con un riepilogo del piano COLLSCAN

```
filter planSummary="COLLSCAN"
```

Monitoraggio con Performance Insights

Performance Insights si aggiunge alle funzionalità di monitoraggio esistenti di Amazon DocumentDB per illustrare le prestazioni del cluster e aiutarti ad analizzare eventuali problemi che lo riguardano. Con la dashboard Performance Insights, puoi visualizzare il carico del database e filtrarlo per attese, istruzioni di query, host o applicazioni.

Note

Performance Insights è disponibile solo per i cluster basati su istanze Amazon DocumentDB 3.6, 4.0 e 5.0.

In che modo è utile?

- Visualizza le prestazioni del database: visualizza il carico per determinare quando e dove si trova il carico sul database
- Determina la causa del carico sul database: determina quali query, host e applicazioni stanno contribuendo al carico sull'istanza
- Determina quando c'è carico sul tuo database: ingrandisci la dashboard di Performance Insights per concentrarti su eventi specifici o rimpicciolisci per esaminare le tendenze in un arco di tempo più ampio

- Avviso sul caricamento del database: accedi automaticamente alle nuove metriche di carico del database da CloudWatch dove puoi monitorare le metriche di carico del DB insieme ad altre metriche di DocumentDB e impostare avvisi su di esse

Quali sono i limiti di Amazon DocumentDB Performance Insights?

- Performance Insights nella regione AWS GovCloud (Stati Uniti occidentali) non sono ancora disponibili
- Performance Insights for DocumentDB conserva fino a 7 giorni di dati sulle prestazioni
- Le query più lunghe di 1024 kb non vengono aggregate in Performance Insights

Argomenti

- [Concetti di Performance Insights](#)
- [Abilitazione e disattivazione di Performance Insights](#)
- [Configurazione delle policy di accesso per Performance Insights](#)
- [Per analizzare il parametro utilizzando il pannello di controllo di Performance Insights](#)
- [Recupero dei parametri con l'API Performance Insights](#)
- [CloudWatch Metriche Amazon per Performance Insights](#)
- [Performance Insights per le contrometriche](#)

Concetti di Performance Insights

Argomenti

- [Media delle sessioni attive](#)
- [Dimensioni](#)
- [Numero massimo di vCPU](#)

Media delle sessioni attive

Il carico del database (carico DB) misura il livello di attività nel database. Il parametro chiave in Performance Insights è DB Load, che viene raccolto ogni secondo. L'unità per la DBLoad metrica è l'Average Active Sessions (AAS) per un'istanza DocumentDB.

Una sessione attiva è una connessione che ha inviato lavoro all'istanza DocumentDB ed è in attesa di una risposta. Ad esempio, se si invia una query a un'istanza DocumentDB, la sessione del database è attiva mentre l'istanza elabora la query.

Per ottenere le sessioni attive medie (AAS), Performance Insights esegue il campionamento del numero di sessioni che eseguono contemporaneamente una query. L'AAS è il numero totale di sessioni diviso per il numero totale di campioni. La tabella seguente mostra cinque esempi consecutivi di una query in esecuzione.

Project N.E.M.O.	Numero di sessioni che eseguono query	AAS	Calcolo
1	2	2	2 sessioni/1 campione
2	0	1	2 sessioni/2 campioni
3	4	2	6 sessioni/3 campioni
4	0	1.5	6 sessioni/4 campioni
5	4	2	10 sessioni/5 campioni

Nell'esempio precedente, il DB Load per l'intervallo di tempo compreso tra 1 e 5 è 2 AAS. Un aumento del carico database significa che, in media, più sessioni sono in esecuzione sul database.

Dimensioni

Il parametro DB Load è diverso dagli altri parametri di serie temporali in quanto può essere suddiviso in sottocomponenti detti dimensioni. Le dimensioni possono essere considerate come categorie per le diverse caratteristiche della metrica DB Load. Quando si diagnosticano problemi di prestazioni, le dimensioni più utili sono gli stati di attesa e la top query.

stati di attesa

Uno stato di attesa fa sì che un'istruzione di query attenda il verificarsi di un evento specifico prima di poter continuare a essere eseguita. Ad esempio, un'istruzione di query potrebbe attendere lo sblocco di una risorsa bloccata. DB Load Combinando gli stati di attesa, è possibile ottenere un quadro completo dello stato della sessione. Ecco vari stati di attesa di DocumentDB:

Stato di attesa di DocumentDB	Descrizione dello stato di attesa
Chiavistello	Lo stato di attesa Latch si verifica quando la sessione è in attesa di impaginare il pool di buffer. Il paging frequente in entrata e in uscita dal buffer pool può avvenire più spesso quando il sistema elabora frequentemente query di grandi dimensioni, scansioni di raccolta o quando il pool di buffer è troppo piccolo per gestire il set di lavoro.
CPU	Lo stato di attesa della CPU si verifica quando la sessione è in attesa della CPU.
CollectionLock	Lo stato di CollectionLock attesa si verifica quando la sessione è in attesa di acquisire un blocco sulla raccolta. Questi eventi si verificano o quando sono presenti operazioni DDL sulla raccolta.
DocumentLock	Lo stato di DocumentLock attesa si verifica quando la sessione è in attesa di acquisire un blocco su un documento. Un numero elevato di scritture simultanee sullo stesso documento contribuirà a aumentare gli stati di DocumentLock attesa su quel documento.
SystemLock	Lo stato di SystemLock attesa si verifica quando la sessione è in attesa sul sistema. Ciò può verificarsi in presenza di frequenti interrogazioni di lunga durata, transazioni di lunga durata o elevata concorrenza nel sistema.
IO	Lo stato di attesa IO si verifica quando la sessione è in attesa del completamento dell'IO.
BufferLock	Lo stato di BufferLock attesa si verifica quando la sessione è in attesa di acquisire un blocco

Stato di attesa di DocumentDB	Descrizione dello stato di attesa
	<p>su una pagina condivisa nel buffer. BufferLock gli stati di attesa possono essere prolungati se altri processi mantengono i cursori aperti sulle pagine richieste.</p>
LowMemThrottle	<p>Lo stato di LowMemThrottle attesa si verifica quando la sessione è in attesa a causa della forte pressione della memoria sull'istanza di Amazon DocumentDB. Se questo stato persiste a lungo, valuta la possibilità di scalare l'istanza per fornire memoria aggiuntiva. Per ulteriori informazioni, consulta Resource Governor.</p>
BackgroundActivity	<p>Lo stato di BackgroundActivity attesa si verifica quando la sessione è in attesa di processi interni del sistema.</p>
Altro	<p>L'altro stato di attesa è uno stato di attesa interno. Se questo stato persiste a lungo, valuta la possibilità di terminare questa interrogazione. Per ulteriori informazioni, vedi Come posso trovare e terminare le interrogazioni di lunga durata o bloccate?</p>

Domande principali

Mentre gli stati di attesa mostrano dei punti deboli, le query principali mostrano quali sono le query che contribuiscono maggiormente al carico del database. Ad esempio, molte query potrebbero essere attualmente in esecuzione nel database, ma una singola query potrebbe consumare il 99% del carico DB. In questo caso, il carico elevato potrebbe indicare un problema con la query.

Numero massimo di vCPU

Nel dashboard, il grafico di caricamento del database raccoglie, aggrega e visualizza le informazioni sulla sessione. Per verificare se le sessioni attive superano la CPU massima, esaminare la loro

relazione con la linea vCPU massima. Il valore Max vCPU è determinato dal numero di core vCPU (CPU virtuale) per l'istanza DocumentDB.

Se il carico è spesso sopra la linea vCPU massima e lo stato di attesa primario è CPU, la CPU è sovraccarica. In questo caso, potresti voler limitare le connessioni all'istanza, ottimizzare le query con un carico di CPU elevato o prendere in considerazione una classe di istanza più grande. Istanze elevate e costanti di qualsiasi stato di attesa indicano che possono verificarsi colli di bottiglia o problemi di conflitto delle risorse da risolvere. Questo può valere anche se il carico database non supera il valore della riga CPU massima.

Abilitazione e disattivazione di Performance Insights

Per utilizzare Performance Insights, è necessario attivarlo nell'istanza database. Puoi disabilitarlo in un secondo momento, se necessario. L'attivazione e la disattivazione di Performance Insights non determina tempi di inattività, riavvio o failover.

L'agente Performance Insights consuma CPU e memoria limitate sull'host DB. Quando il carico del DB è elevato, l'agente limita l'impatto sulle prestazioni raccogliendo i dati meno frequentemente.

Abilitazione di Performance Insights durante la creazione di un cluster

Nella console è possibile attivare o disattivare Performance Insights quando si crea o si modifica una nuova istanza DB.

Utilizzo di AWS Management Console

Nella console, è possibile abilitare Performance Insights quando si crea un cluster DocumentDB. Quando crei un nuovo cluster DocumentDB, abilita Performance Insights scegliendo Enable Performance Insights nella sezione Performance Insights.

Istruzioni per la console

1. Per creare un cluster, segui le istruzioni per la [creazione di un cluster Amazon DocumentDB](#).
2. Seleziona Abilita Performance Insights nella sezione Performance Insights.

Performance Insights [Info](#)

Enable Performance Insights

AWS KMS Key [Info](#)

(default) aws/rds

Account

KMS key ID

 You can't change the KMS key after enabling Performance Insights.

Note

Il periodo di conservazione dei dati di Performance Insights sarà di sette giorni.

AWS KMSChiave: specifica la tua chiave AWS KMS. Performance Insights crittografa tutti i dati potenzialmente sensibili con la chiave AWS KMS. I dati vengono crittografati mentre sono in transito o inattivi. Per ulteriori informazioni, vedere Configurazione di una AWS AWS KMS policy per Performance Insights.

Abilitazione e disabilitazione durante la modifica di un'istanza


È possibile modificare un'istanza DB per abilitare o disabilitare Performance Insights utilizzando la console o AWS CLI.

Using the AWS Management Console

Istruzioni della console

1. [Accedi a e apri AWS Management Console la console Amazon DocumentDB all'indirizzo https://console.aws.amazon.com/docdb.](https://console.aws.amazon.com/docdb)
2. Scegli Cluster.

3. Scegliere un'istanza DB e scegliere Modifica.
4. Nella sezione Performance Insights, scegli Abilita Performance Insights o Disabilita Performance Insights.

 Note

Se scegli Enable Performance Insights, puoi specificare la tua AWS KMS chiave. Performance Insights crittografa tutti i dati potenzialmente sensibili con la chiave AWS KMS. I dati vengono crittografati mentre sono in transito o inattivi. Per ulteriori informazioni, [consulta *Encrypting Amazon DocumentDB Data at Rest*](#).

5. Scegli Continue (Continua).
6. In Scheduling of Modifications (Pianificazione delle modifiche), scegliere Apply immediately (Applica immediatamente). Se scegli Applica durante la successiva finestra di manutenzione pianificata, l'istanza ignora questa impostazione e abilita immediatamente Performance Insights.
7. Scegli Modify instance (Modifica istanza).

Using the AWS CLI

Quando si utilizzano i `modify-db-instance` AWS CLI comandi `create-db-instance` o, è possibile abilitare Performance Insights `--enable-performance-insights` specificando o disabilitarlo `--no-enable-performance-insights` specificando.

La procedura seguente descrive come abilitare o disabilitare Performance Insights per un'istanza DB utilizzando AWS CLI.

AWS CLI istruzioni

Chiamate il `modify-db-instance` AWS CLI comando e fornite i seguenti valori:

- `--db-instance-identifier`— Il nome dell'istanza DB
- `--enable-performance-insights` per abilitare o `--no-enable-performance-insights` per disabilitare

Example

L'esempio seguente abilita Performance Insights per `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
```

Configurazione delle policy di accesso per Performance Insights

Per accedere a Performance Insights, devi avere le autorizzazioni appropriate da AWS Identity and Access Management (IAM). Per concedere l'accesso sono disponibili le seguenti opzioni:

- Collega la policy gestita `AmazonRDSPerformanceInsightsReadOnly` a un set di autorizzazioni o a un ruolo.
- Crea una policy IAM personalizzata e collegala a un set di autorizzazioni o un ruolo.

Inoltre, se è stata specificata una chiave gestita dal cliente durante l'attivazione di Performance Insights, è necessario assicurarsi che gli utenti dell'account dispongano delle autorizzazioni `kms:Decrypt` e `kms:GenerateDataKey` sulla chiave KMS.

Note

[Per quanto riguarda `encryption-at-rest` riguarda la gestione delle AWS KMS chiavi e dei gruppi di sicurezza, Amazon DocumentDB sfrutta la tecnologia operativa condivisa con Amazon RDS.](#)

Associare la policy di `PerformanceInsightsReadOnly` AmazonRDS a un principale IAM

`AmazonRDSPerformanceInsightsReadOnly` è una policy AWS gestita che garantisce l'accesso a tutte le operazioni di sola lettura dell'API Amazon DocumentDB Performance Insights. Al momento, tutte le operazioni in questa API sono di sola lettura. Se si collega `AmazonRDSPerformanceInsightsReadOnly` a un set di autorizzazioni o un ruolo, il destinatario può utilizzare Performance Insights insieme ad altre funzionalità della console.

Creazione di una policy IAM personalizzata per Performance Insights

Per gli utenti che non hanno accesso completo alla policy

AmazonRDSPerformanceInsightsReadOnly, si può concedere l'accesso a Performance Insights creando o modificando una policy IAM gestita dall'utente. Quando alleggi la policy a un set di autorizzazioni o a un ruolo, il destinatario può utilizzare Performance Insights.

Per creare una policy personalizzata

1. Aprire la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel pannello di navigazione, selezionare Policies (Policy).
3. Scegli Create Policy (Crea policy).
4. Nella pagina Create Policy (Crea policy), seleziona la scheda JSON.
5. Copia e incolla il testo seguente, sostituendo *us-east-1* con il nome della Regione AWS e *111122223333* con il numero di account del cliente.

```
{
  "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. Scegliere Review policy (Esamina policy).
7. Specifica un nome per la policy e, facoltativamente, una descrizione e quindi scegli Create policy (Crea policy).

Ora è possibile collegare la policy a un set di autorizzazioni o un ruolo. La seguente procedura presuppone che si disponga già di un utente disponibile allo scopo.

Per collegare la policy a un utente

1. Aprire la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel pannello di navigazione, seleziona Users (Utenti).
3. Seleziona un utente esistente dall'elenco.

Important

Per utilizzare Performance Insights, assicurati di avere accesso ad Amazon DocumentDB oltre alla policy personalizzata. [Ad esempio, la policy ReadOnlyAccess](#)

[predefinita del AmazonDocDB fornisce l'accesso in sola lettura ad Amazon DocDB. Per ulteriori informazioni, consulta \[Gestire l'accesso utilizzando le policy\]\(#\).](#)

- Nella pagina Summary (Riepilogo), scegli Add permissions (Aggiungi autorizzazioni).
- Scegli Attach existing policies directly (Collega direttamente le policy esistenti). Per Search (Ricerca) digita i primi caratteri del nome della policy, come mostrato di seguito.

The screenshot shows the 'Add permissions to test' interface in the AWS IAM console. It includes a 'Grant permissions' section with three main options: 'Add user to group', 'Copy permissions from existing user', and 'Attach existing policies directly' (which is highlighted with a blue border). Below these options is a 'Create policy' button and a search bar. The search bar contains the text 'Perf' and shows 'Showing 1 result'. The result is a table with the following data:

Policy name	Type	Used as
PerformanceInsightsCustomPolicy	Customer managed	None

- Scegli la policy e quindi seleziona Next: Review (Successivo: Rivedi).
- Scegli Add Permissions (Aggiungi autorizzazioni).

Configurazione di una policy AWS KMS per Performance Insights

Performance Insights utilizza una AWS KMS key per crittografare i dati sensibili. Quando si abilita Performance Insights mediante l'API o la console, sono disponibili le seguenti opzioni:

- Scegli il valore di default Chiave gestita da AWS.

Amazon DocumentDB utilizza la Chiave gestita da AWS per la tua nuova istanza DB. Amazon DocumentDB ne crea una Chiave gestita da AWS per il tuo AWS account. Il tuo AWS account ha un nome diverso Chiave gestita da AWS per Amazon DocumentDB per ogni AWS regione.

- Scegli una chiave gestita dal cliente.

Se si specifica una chiave gestita dal cliente, gli utenti dell'account che chiamano l'API Performance Insights necessitano delle autorizzazioni `kms:Decrypt` e `kms:GenerateDataKey`

per la chiave KMS. È possibile configurare queste autorizzazioni mediante le policy IAM. Tuttavia, è consigliabile gestire queste autorizzazioni mediante la policy della chiave KMS. Per ulteriori informazioni, consulta [Utilizzo di policy chiave in AWS KMS](#).

Example

La seguente policy chiave di esempio mostra come aggiungere istruzioni alla propria policy della chiave KMS. Queste istruzioni consentono l'accesso a Performance Insights. A seconda di come utilizzi ilAWS KMS, potresti voler modificare alcune restrizioni. Prima di aggiungere istruzioni alle policy, ai criteri, rimuovi tutti i commenti.

```
{
  "Version" : "2012-10-17",
  "Id" : "your-policy",
  "Statement" : [ {
    //This represents a statement that currently exists in your policy.
  }
  .....,
  //Starting here, add new statement to your policy for Performance Insights.
  //We recommend that you add one new statement for every RDS/DocumentDB instance
  {
    "Sid" : "Allow viewing RDS Performance Insights",
    "Effect": "Allow",
    "Principal": {
      "AWS": [
        //One or more principals allowed to access Performance Insights
        "arn:aws:iam::444455556666:role/Role1"
      ]
    },
    "Action": [
      "kms:Decrypt",
      "kms:GenerateDataKey"
    ],
    "Resource": "*",
    "Condition" :{
      "StringEquals" : {
        //Restrict access to only RDS APIs (including Performance Insights).
        //Replace *region* with your AWS Region.
        //For example, specify us-west-2.
        "kms:ViaService" : "rds.*region*.amazonaws.com"
      }
    },
    "ForAnyValue:StringEquals": {
```

```
//Restrict access to only data encrypted by Performance Insights.
"kms:EncryptionContext:aws:pi:service": "rds",
"kms:EncryptionContext:service": "pi",

//Restrict access to a specific DocDB instance.
//The value is a DbiResourceId.
"kms:EncryptionContext:aws:rds:db-id": "db-AAAAABBBBBCCCCDDDDDEEEEEE"
    }
}
}
```

Per analizzare il parametro utilizzando il pannello di controllo di Performance Insights

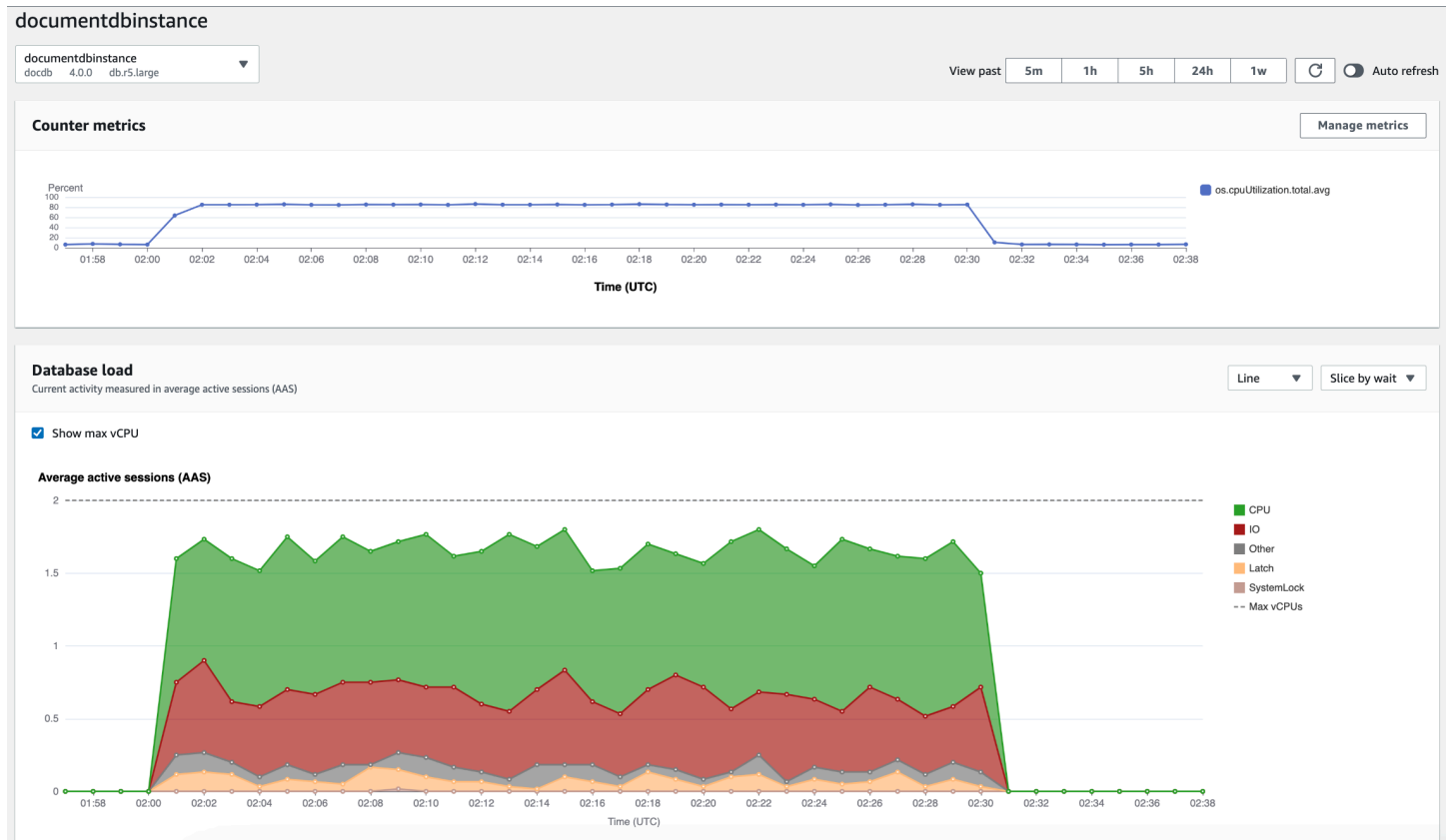
Il pannello di controllo di Performance Insights contiene informazioni sulle performance del database, per consentire di analizzare e risolvere i problemi di performance. Nella pagina principale della dashboard, puoi visualizzare le informazioni sul carico del database (caricamento del DB). È possibile «suddividere» il carico del DB in base a dimensioni quali stati di attesa o interrogazione.

Argomenti

- [Panoramica del pannello di controllo di Performance Insights](#)
- [Per aprire il pannello di controllo di Performance Insights](#)
- [Analisi del carico del database in base agli stati di attesa](#)
- [Panoramica della scheda Domande principali](#)
- [Ingrandimento del grafico di caricamento del database](#)

Panoramica del pannello di controllo di Performance Insights

Il pannello di controllo è il modo più semplice per interagire con Performance Insights. L'esempio seguente mostra la dashboard per un'istanza di Amazon DocumentDB. Per impostazione predefinita, il pannello di controllo di Performance Insights mostra i dati relativi agli ultimi 60 minuti.



Il pannello di controllo è diviso nelle seguenti parti:

1. Parametri dei contatori: mostra i dati relativi ai contatori delle prestazioni specifici.
2. Caricamento del database: mostra il confronto tra il carico del database e la capacità dell'istanza DB rappresentata dalla riga Max vCPU.
3. Dimensioni principali: mostra le dimensioni principali che contribuiscono al carico del DB. Queste dimensioni includono `waitsqueries`, `hosts`, `databases`, `applications`.

Argomenti

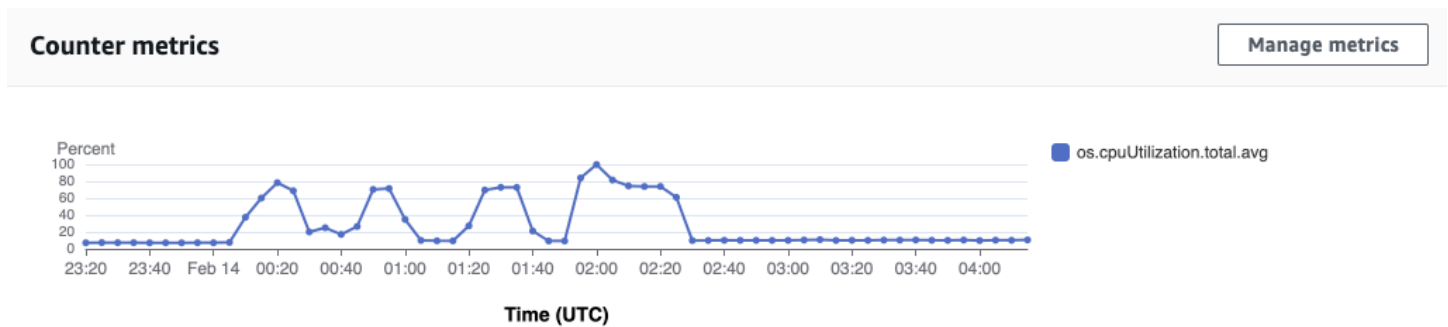
- [Grafico Parametri contatore](#)
- [Grafico di carico database](#)
- [Tabella dimensioni superiori](#)

Grafico Parametri contatore

Con i parametri contatore, puoi personalizzare il pannello di controllo di Performance Insights per includere fino a 10 grafici aggiuntivi. Questi grafici mostrano una selezione di dozzine di metriche

del sistema operativo. Queste informazioni possono essere correlate ai carichi dei database per agevolare l'individuazione e l'analisi di problemi legati alle prestazioni.

Il grafico Counter Metrics (Parametri contatore) visualizza i dati per i contatori delle prestazioni.



Per modificare i contatori delle prestazioni, scegli Gestisci metriche. Puoi selezionare più metriche del sistema operativo come mostrato nella schermata seguente. Per visualizzare i dettagli relativi a qualsiasi metrica, passare il mouse sul nome della metrica.

Select metrics shown on the graph ✕

Check the metrics that you want to see on the Performance Insights dashboard.

OS metrics (4) Clear all selections

▼ **general**

numVCPUs

▼ **cpuUtilization**

idle system total

user wait

▼ **loadAverageMinute**

fifteen five one

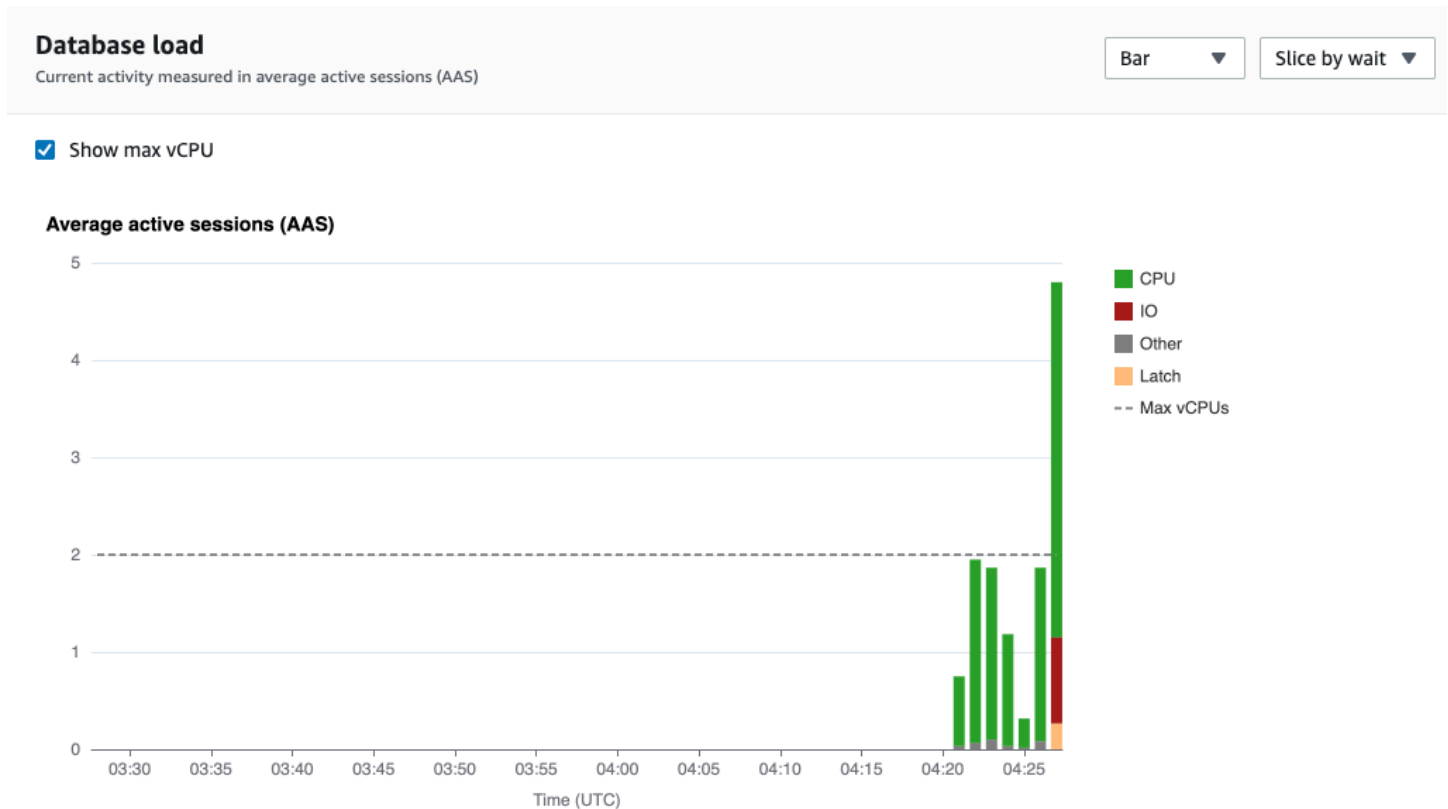
▼ **memory**

active buffers cached

dirty free inactive

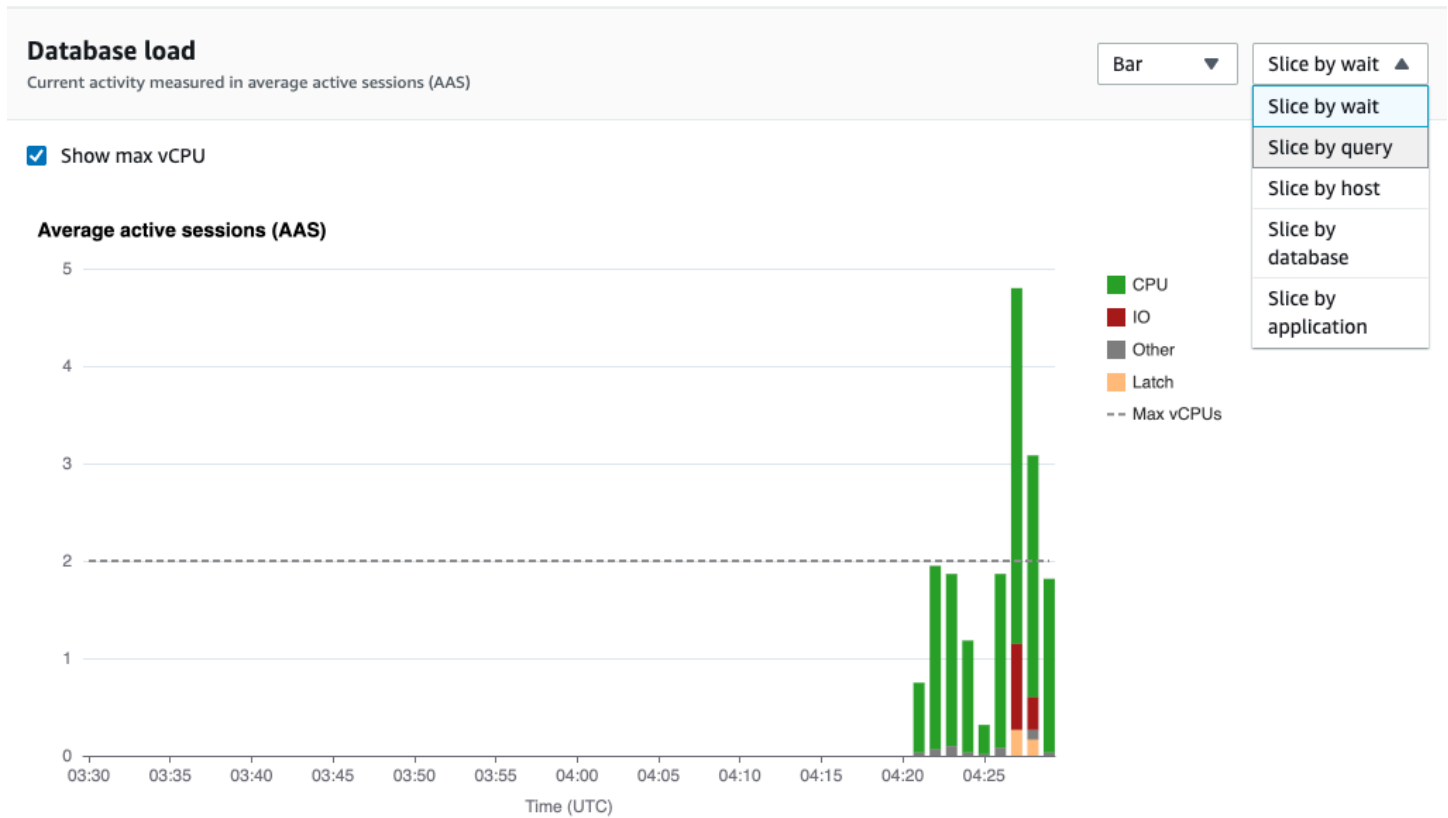
Grafico di carico database

Il grafico di carico del database mostra il confronto tra l'attività del database e la capacità dell'istanza rappresentata dalla riga Max vCPU. Per impostazione predefinita, il grafico a linee in pila rappresenta il carico DB come sessioni attive medie per unità di tempo. Il carico DB viene suddiviso (raggruppato) in base agli stati di attesa.



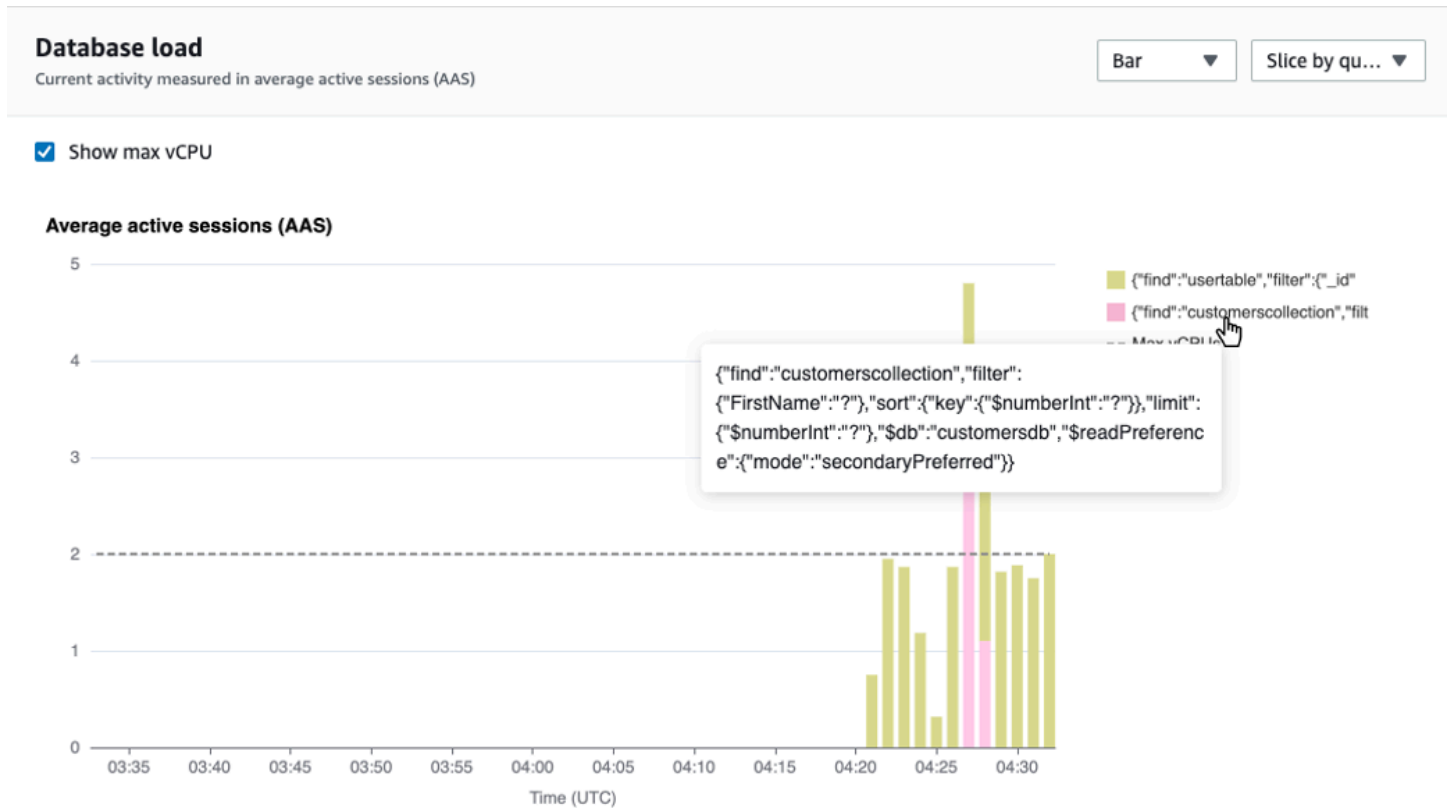
Carico del database suddiviso per dimensioni

È possibile scegliere di visualizzare il carico sotto forma di sessioni attive raggruppate in base alle dimensioni supportate. L'immagine seguente mostra le dimensioni dell'istanza Amazon DocumentDB.



Dettagli del carico DB per un elemento della dimensione

Per visualizzare i dettagli su un elemento del carico del database all'interno di una dimensione, passa il mouse sul nome dell'elemento. L'immagine seguente mostra i dettagli di un'istruzione di query.



Per visualizzare i dettagli relativi a qualsiasi elemento per il periodo di tempo selezionato nella legenda, passa il mouse su tale elemento.

Database load

Current activity measured in average active sessions (AAS)

Bar ▾ Slice by qu... ▾

Show max vCPU

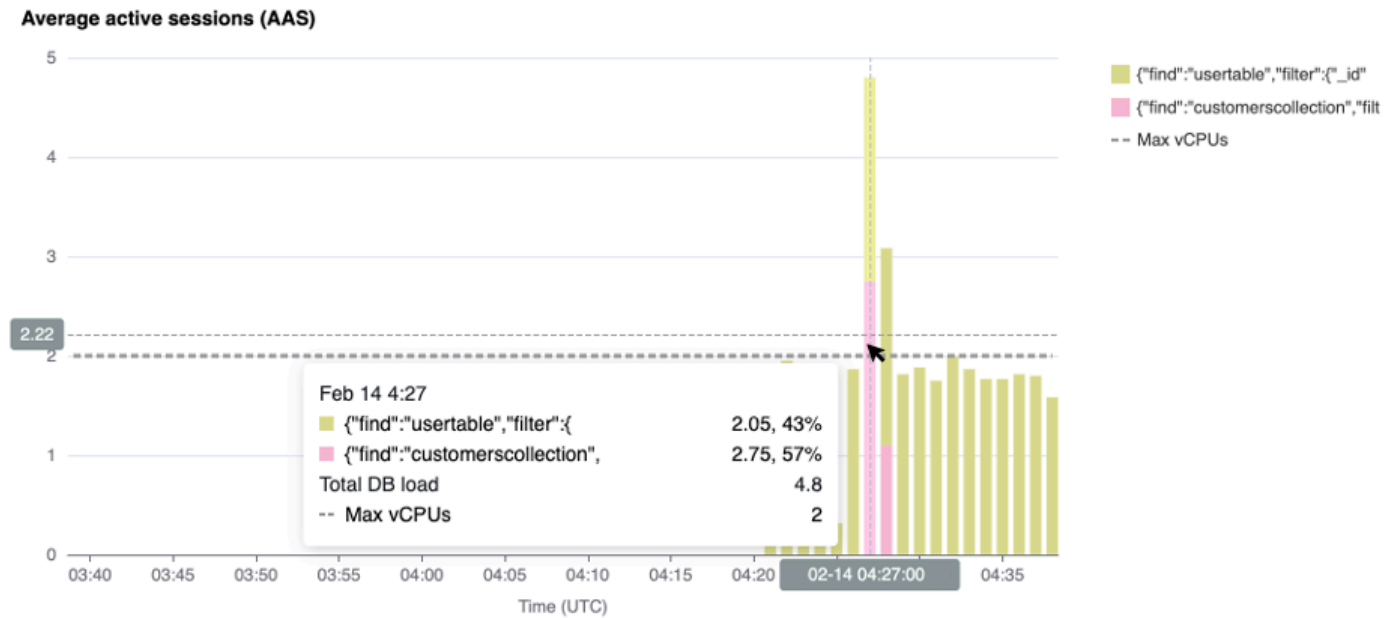


Tabella dimensioni superiori

La tabella delle dimensioni principali suddivide il carico del DB in base a dimensioni diverse.

Una dimensione è una categoria o una suddivisione per le diverse caratteristiche del carico del database. Se la dimensione è una query, Top queries mostra le istruzioni di query che contribuiscono maggiormente al carico del DB.

Scegli una delle seguenti schede di dimensione.

Top waits | **Top queries** | Top hosts | Top databases | Top applications

Top queries (2) [Learn more](#)

Find query statements

Load by query (AAS)	Query statements
0.85	{"find":"usertable","filter":{"_id":"?"},"limit":{"\$numberInt":"?"},"singleBatch...
0.06	{"find":"customerscollection","filter":{"FirstName":"?"},"sort":{"key":{"\$number...

La tabella seguente fornisce una breve descrizione di ogni scheda.

Selezio
ne

Principa
l
iper
stati
d'attesa
il
back-
end
del
database
è
in
attesa

Le
diminuzione
più
frequenti
interroga
zione
attualmen
te
in
esecuzione
e

Host
principal
ia
porta
dell'host
del
client
connesso

Selezio
ne

Database
principale
database
a
cui
è
connesso
il
client

Applicazi
one
principale
applicazione
connessa
al
database

Per informazioni su come analizzare le interrogazioni utilizzando la scheda Interrogazioni principali, consulta. [Panoramica della scheda Domande principali](#)

Per aprire il pannello di controllo di Performance Insights

Per visualizzare il dashboard di Performance Insights nella console di AWS gestione, attenersi alla seguente procedura:

1. Apri la console Performance Insights all'[indirizzo https://console.aws.amazon.com/docdb/](https://console.aws.amazon.com/docdb/).
2. Scegli un'istanza database. La dashboard Performance Insights viene mostrata per quell'istanza di Amazon DocumentDB.

Per le istanze Amazon DocumentDB con Performance Insights abilitata, puoi anche accedere alla dashboard selezionando la voce Sessions nell'elenco delle istanze. In Current activity (Attività corrente) la voce Sessions (Sessioni) mostra il carico del database in sessioni attive medie negli ultimi cinque minuti. Il grafico mostra graficamente il carico: Quando la barra è vuota,

l'istanza è inattiva. Con l'aumentare del carico, la barra si riempie ed è di colore blu. Quando il carico supera il numero di CPU virtuali (vCPU) sulla classe di istanza, la barra diventa rossa, indicando un potenziale collo di bottiglia.

Clusters (1) Group Resources Actions Create

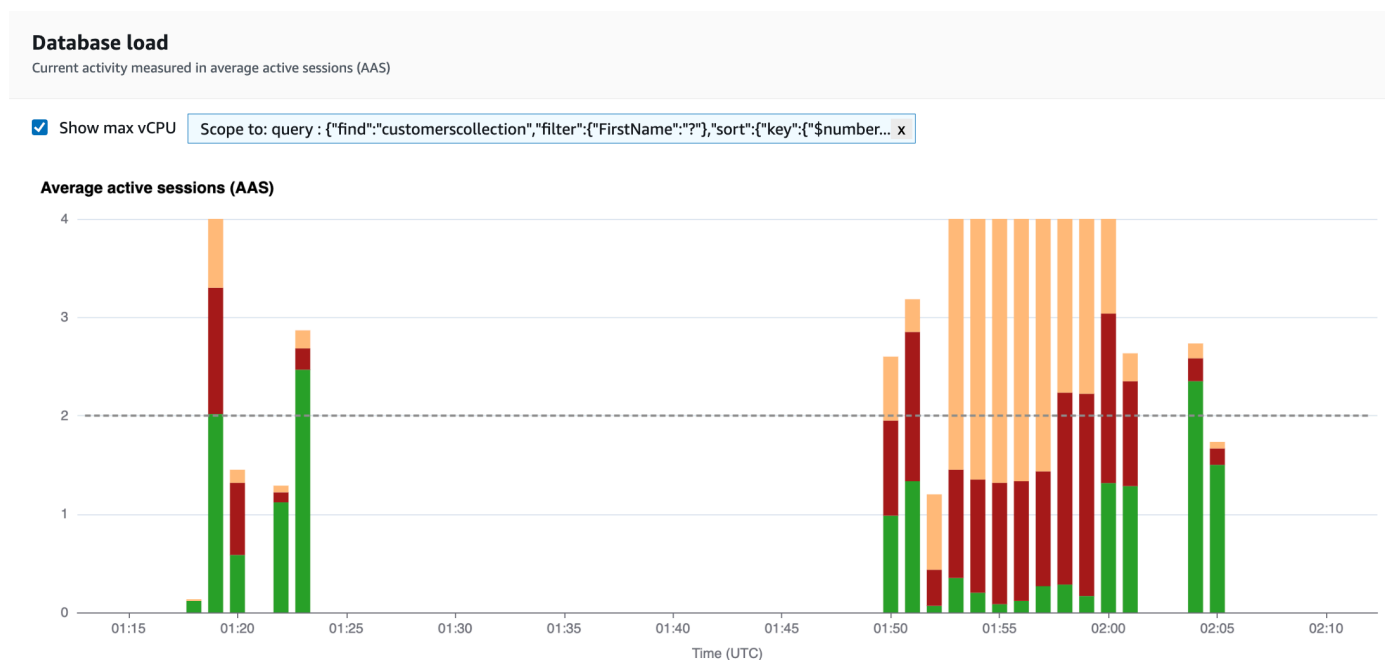
Filter Resources

Cluster identifier	Role	Engine version	Region & AZ	Status	CPU	Current activity
documentdbinstance	Regional cluster	4.0.0	ap-south-1	available	-	-
documentdbinstance	Primary instance	4.0.0	ap-south-1c	available	84.99%	5 Connections
documentdbinstance2	Replica instance	4.0.0	ap-south-1b	available	15.37%	2 Connections
documentdbinstance3	Replica instance	4.0.0	ap-south-1a	available	14.84%	2 Connections

3. (Facoltativo) Scegliere un intervallo di tempo diverso selezionando un pulsante in alto a destra. Ad esempio, per modificare l'intervallo a 1 ora, seleziona 1 ora.

View past 5m 1h 5h 24h 1w Refresh Auto refresh

Nella schermata seguente, l'intervallo di caricamento del DB è di 1 ora.



4. Per aggiornare automaticamente i dati, abilita l'aggiornamento automatico.

View past 5m 1h 5h 24h 1w Refresh Auto refresh

Il pannello di controllo di Performance Insights si aggiorna automaticamente con i nuovi dati. La frequenza di aggiornamento dipende dalla quantità di dati visualizzati:

- Se scegli 5 minuti, l'aggiornamento avviene ogni 5 secondi.
- 1 ora si aggiorna ogni minuto.
- 5 ore si aggiorna ogni minuto.
- Se scegli 24 ore, l'aggiornamento avviene ogni 5 minuti.
- Se scegli 1 settimana, l'aggiornamento avviene ogni ora.

Analisi del carico del database in base agli stati di attesa

Se il grafico di caricamento del database (carico del DB) mostra un punto debole, puoi scoprire da dove proviene il carico. A questo scopo, osserva la tabella Top Load Items (Elementi con carico) sotto la tabella Database load (Caricamento database). Scegli un elemento particolare, ad esempio una query o un'applicazione, per approfondire quell'elemento e visualizzarne i dettagli.

Il carico del database, raggruppato per attese e query principali, in genere fornisce le informazioni più dettagliate sui problemi di prestazioni. Il carico del database raggruppato in base alle attese mostra la presenza di eventuali colli di bottiglia nel database relativamente alle risorse o alla simultaneità. In questo caso, la scheda Interrogazioni principali della tabella degli elementi di caricamento principale mostra le query che generano tale carico.

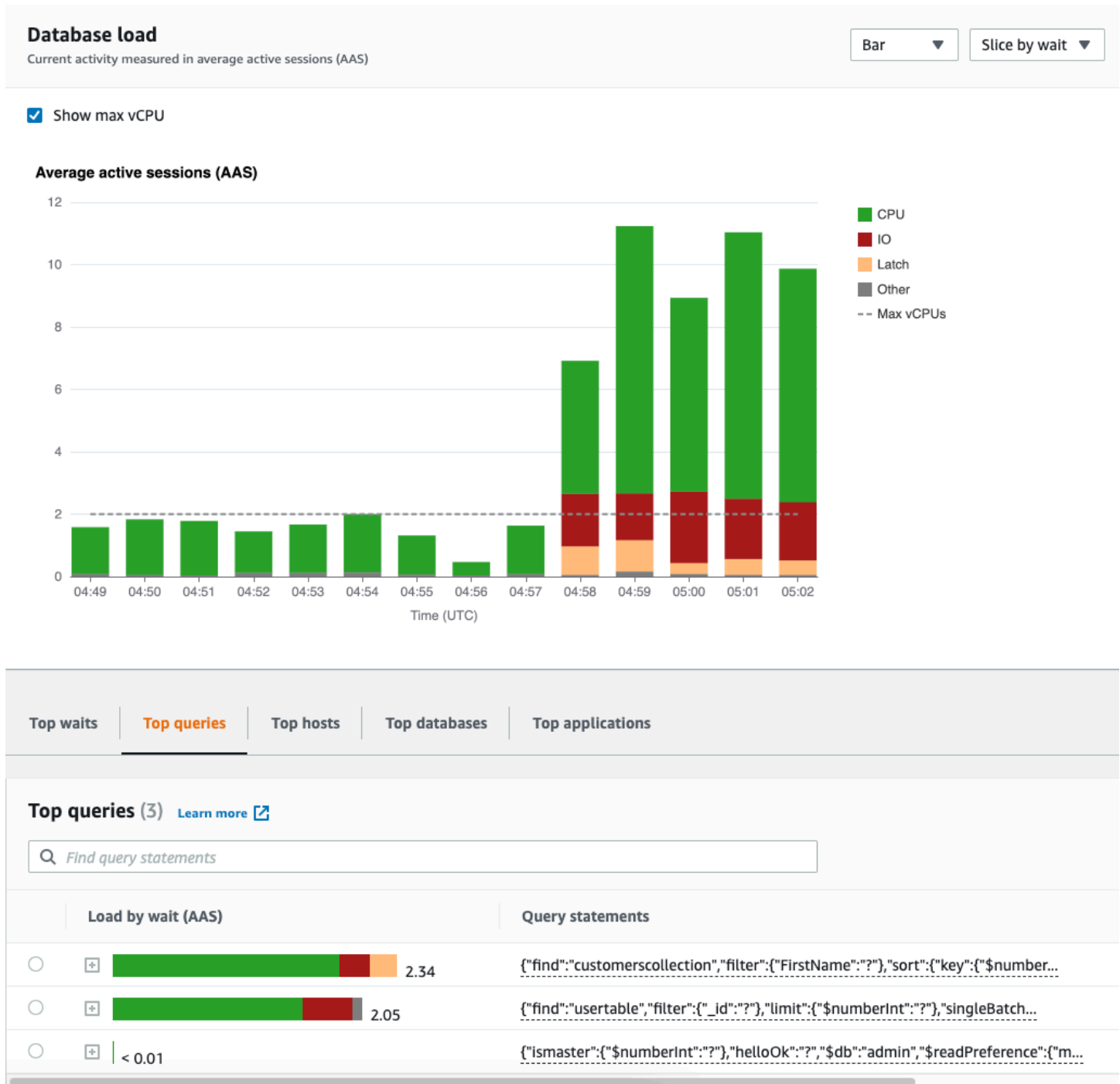
Il flusso di lavoro tipico per diagnosticare problemi di performance è il seguente:

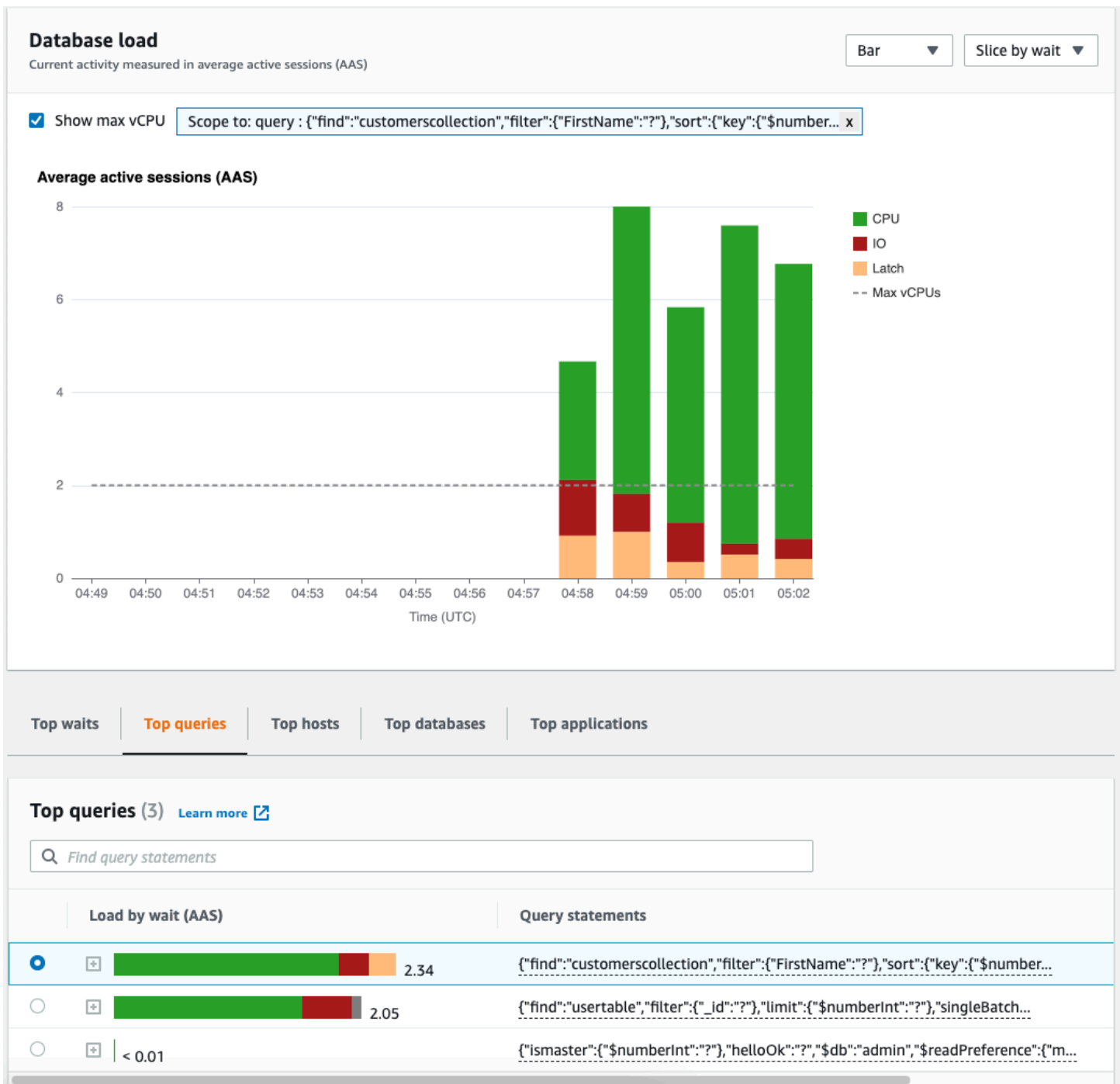
1. Esaminare il grafico Database load (Caricamento database) per determinare se sono presenti eventi imprevisti di superamento della riga Max CPU (CPU max) da parte del carico del database.
2. Se sono presenti, osservare il grafico Database load (Caricamento database) e individuare lo stato o gli stati di attesa che sono i principali responsabili.
3. Identifica le query di riepilogo che causano il caricamento visualizzando quali delle query presenti nella scheda Top queries nella tabella Top Load Items stanno contribuendo maggiormente a questi stati di attesa. È possibile identificarle tramite la colonna Load by Wait (AAS).
4. Scegliete una di queste query di riepilogo nella scheda Query principali per espanderla e visualizzare le query secondarie da cui è composta.

Puoi anche vedere quali host o applicazioni contribuiscono maggiormente al carico selezionando Top host o Top applications, rispettivamente. I nomi delle applicazioni sono specificati nella stringa di

connessione all'istanza Amazon DocumentDB. Unknown indica che il campo dell'applicazione non è stato specificato.

Ad esempio, nella dashboard seguente, la CPU attende la maggior parte del carico del DB. Selezionando la query principale in Prime query, verrà analizzato il grafico di caricamento del database in modo da concentrarsi sulla maggior parte del carico apportato dalla query di selezione.





Panoramica della scheda Domande principali

Per impostazione predefinita, la scheda Top query mostra le query che contribuiscono maggiormente al carico del DB. È possibile analizzare il testo della query per ottimizzare le query.

Argomenti

- [Digest delle query](#)

- [Caricamento per attesa \(AAS\)](#)
- [Visualizzazione di informazioni dettagliate sull'interrogazione](#)
- [Accesso al testo della richiesta di dichiarazione](#)
- [Visualizzazione e download del testo della richiesta di istruzione](#)

Digest delle query





Un Query Digest è un insieme di più query effettive strutturalmente simili ma che potrebbero avere valori letterali diversi. Il digest sostituisce i valori codificati con un punto interrogativo. Ad esempio, un Query Digest potrebbe avere il seguente aspetto:

```
{"find":"customerscollection","filter":{"FirstName":"?"},"sort":{"key":{"$numberInt":"?"}},"limit":{"$numberInt":"?"}}
```

Questo digest può includere le seguenti query figlio:

```
{"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"}}
```

Per visualizzare le istruzioni di query letterali in un digest, selezionate la query, quindi scegliete il simbolo più (). + Nella schermata seguente, la query selezionata è un digest.

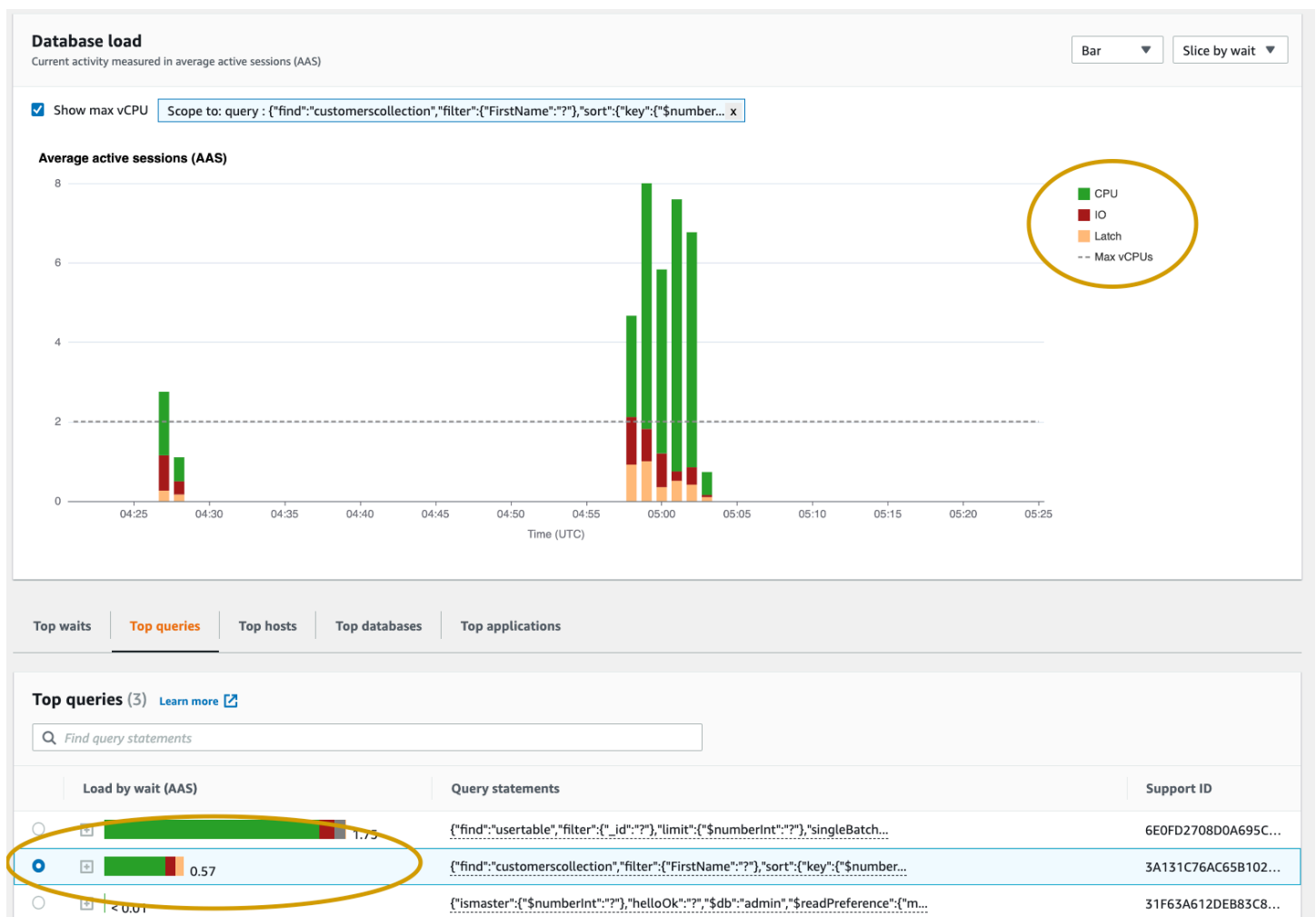
Top waits	Top queries	Top hosts	Top databases	Top applications
Top queries (3) Learn more				
<input type="text" value="Find query statements"/>				
Load by wait (AAS)	Query statements			
<input type="radio"/>  1.27	{"find":"usertable","filter":{"_id":"?"},"limit":{"\$numberInt":"?"},"singleBatch...			
<input type="radio"/>  0.41	{"find":"customerscollection","filter":{"FirstName":"?"},"sort":{"key":{"\$numberInt":"1"}},"limit":{"\$numberInt":"3"}}			
<input checked="" type="radio"/>  0.02	{"find":"customerscollection","filter":{"FirstName":"Jesse"},"sort":{"key":{"\$numberInt":"1"}},"limit":{"\$numberInt":"3"}}			
<input type="radio"/>  0.02	{"find":"customerscollection","filter":{"FirstName":"Jesse"},"sort":{"key":{"\$numberInt":"1"}},"limit":{"\$numberInt":"3"}}			

Note

Un Query Digest raggruppa istruzioni di query simili, ma non oscura le informazioni riservate.

Caricamento per attesa (AAS)

In Top queries, la colonna Load by waits (AAS) illustra la percentuale di carico del database associata a ciascun elemento di primo caricamento. Questa colonna riflette il carico di quell'elemento in base al raggruppamento attualmente selezionato nel grafico di caricamento del DB. Ad esempio, è possibile raggruppare il Carico DB in base agli stati di attesa. In questo caso, la barra DB Load by Waits (Carico del database in base alle attese) è dimensionata, segmentata e rappresentata da un colore per mostrare qual è il contributo della query a un dato stato di attesa. Mostra anche quali stati di attesa stanno influenzando la query selezionata.



Visualizzazione di informazioni dettagliate sull'interrogazione

Nella tabella Top query, è possibile aprire un'istruzione digest per visualizzarne le informazioni. Le informazioni vengono visualizzate nel riquadro inferiore.

Top waits
Top queries
Top hosts
Top databases
Top applications

Top queries (3) [Learn more](#)

	Load by wait (AAS)	Query statements	Support ID
<input type="radio"/>	<div style="width: 100%; height: 10px; background: linear-gradient(to right, green, red);"></div> 1.75	{ "find": "usertable", "filter": { "_id": "?" }, "limit": { "\$numberInt": "?" }, "singleBatch...	6E0FD2708D0A695C...
<input type="radio"/>	<div style="width: 100%; height: 10px; background: linear-gradient(to right, green, red);"></div> 0.57	{ "find": "customerscollection", "filter": { "FirstName": "?" }, "sort": { "key": { "\$number...	3A131C76AC65B102...
<input checked="" type="radio"/>	<div style="width: 100%; height: 10px; background: linear-gradient(to right, green, red);"></div> 0.03	{ "find": "customerscollection", "filter": { "FirstName": "Jesse" }, "sort": { "key": { "\$nu...	7C19C88DD78407E0...
<input type="radio"/>	<div style="width: 100%; height: 10px; background: linear-gradient(to right, green, red);"></div> 0.03	{ "find": "customerscollection", "filter": { "FirstName": "Jesse" }, "sort": { "key": { "\$nu...	FBF2993E2172FCFC6...
<input type="radio"/>	<div style="width: 100%; height: 10px; background: linear-gradient(to right, green, red);"></div> 0.03	{ "find": "customerscollection", "filter": { "FirstName": "Jesse" }, "sort": { "key": { "\$nu...	77449E3F829AC210...
<input type="radio"/>	<div style="width: 100%; height: 10px; background: linear-gradient(to right, green, red);"></div> 0.03	{ "find": "customerscollection", "filter": { "FirstName": "Jesse" }, "sort": { "key": { "\$nu...	01B0434C5D4F140D...
<input type="radio"/>	<div style="width: 100%; height: 10px; background: linear-gradient(to right, green, red);"></div> 0.03	{ "find": "customerscollection", "filter": { "FirstName": "Jesse" }, "sort": { "key": { "\$nu...	D995AB7F6C835AE7...
<input type="radio"/>	<div style="width: 100%; height: 10px; background: linear-gradient(to right, green, red);"></div> 0.03	{ "find": "customerscollection", "filter": { "FirstName": "Jesse" }, "sort": { "key": { "\$nu...	613864818FDD36E2...
<input type="radio"/>	<div style="width: 100%; height: 10px; background: linear-gradient(to right, green, red);"></div> 0.03	{ "find": "customerscollection", "filter": { "FirstName": "Jesse" }, "sort": { "key": { "\$nu...	49537B8EA748E915...
<input type="radio"/>	<div style="width: 100%; height: 10px; background: linear-gradient(to right, green, red);"></div> 0.03	{ "find": "customerscollection", "filter": { "FirstName": "Jesse" }, "sort": { "key": { "\$nu...	098E33A525332BBC...
<input type="radio"/>	<div style="width: 100%; height: 10px; background: linear-gradient(to right, green, red);"></div> 0.03	{ "find": "customerscollection", "filter": { "FirstName": "Jesse" }, "sort": { "key": { "\$nu...	792692547FD45F14...
<input type="radio"/>	<div style="width: 100%; height: 10px; background: linear-gradient(to right, green, red);"></div> 0.03	{ "find": "customerscollection", "filter": { "FirstName": "Jesse" }, "sort": { "key": { "\$nu...	367B900BA7E20C39...
<input type="radio"/>	<div style="width: 100%; height: 10px; background: linear-gradient(to right, green, red);"></div> < 0.01	{ "ismaster": { "\$numberInt": "?" }, "helloOk": "?", "\$db": "admin", "\$readPreference": { "m...	31F63A612DEB83C8...

Query information

```
{"find": "customerscollection", "filter": {"FirstName": "Jesse"}, "sort": {"key": {"$numberInt": "1"}}, "limit": {"$numberInt": "3"}, "lsid": {"id": {"$binary": {"base64": "DG/4c0FLRxywzmltINb+MA==", "subType": "04"}}}, "$db": "customersdb", "$readPreference": {"mode": "secondaryPreferred"}}
```

Query ID: pi-563169974 ([Support query ID](#)) Digest ID: pi-563169974 ([Support Digest ID](#))

Copy Download

I seguenti tipi di identificatori (ID) sono associati alle istruzioni di interrogazione:

1. Support query ID: un valore hash dell'ID della query. Questo valore serve solo per fare riferimento a un ID di query quando si lavora con AWS Support. AWS Support non ha accesso agli ID e al testo delle query effettivi.
2. Support digest ID: un valore hash dell'ID digest. Questo valore serve solo come riferimento a un ID Digest quando si utilizza AWS Support. AWS Support non ha accesso agli ID digest effettivi e al testo della query.

Accesso al testo della richiesta di dichiarazione

Per impostazione predefinita, ogni riga della tabella Top queries mostra 500 byte di testo di query per ogni istruzione di query. Quando un'istruzione digest supera i 500 byte, puoi visualizzare altro testo aprendo l'istruzione nella dashboard di Performance Insights. In questo caso, la lunghezza massima per la query visualizzata è 1 KB. Se visualizzi un'istruzione di interrogazione completa, puoi anche scegliere Scarica.

Visualizzazione e download del testo della richiesta di istruzione

Nella dashboard di Performance Insights, puoi visualizzare o scaricare il testo della query.

Per visualizzare altro testo della query nella dashboard di Performance Insights

1. [Apri la console Amazon DocumentDB all'indirizzo: https://console.aws.amazon.com/docdb/](https://console.aws.amazon.com/docdb/)
2. Nel pannello di navigazione scegli Approfondimenti sulle prestazioni.
3. Scegli istanza database. Viene visualizzato il pannello di controllo di Performance Insights per l'istanza database.

Le istruzioni di query con testo più grande di 500 byte appariranno come nell'immagine seguente:

	Load by wait (AAS)	Query statements	Support ID
○	1.75	{ "find": "usertable", "filter": { "_id": "?" }, "limit": { "\$numberInt": "?" }, "singleBatch..."	6E0FD2708D0A695C...
○	0.57	{ "find": "customerscollection", "filter": { "FirstName": "?" }, "sort": { "key": { "\$number..."	3A131C76AC65B102...
●	0.03	{ "find": "customerscollection", "filter": { "FirstName": "Jesse" }, "sort": { "key": { "\$nu...	7C19C88DD78407E0...
○	0.03	{ "find": "customerscollection", "filter": { "FirstName": "Jesse" }, "sort": { "key": { "\$nu...	FBF2993E2172CFC6...

4. Esamina la sezione delle informazioni sulla query per visualizzare una parte maggiore del testo della query.

Query information

```
{ "find": "customerscollection", "filter": { "FirstName": "Jesse" }, "sort": { "key": { "$numberInt": "1" }, "limit": { "$numberInt": "3" }, "lsid": { "id": { "$binary": { "base64": "DG/4c0FLRxywzmtINb+MA==", "subType": "04" } } }, "$db": "customersdb", "$readPreference": { "mode": "secondaryPreferred" } }
```

Query ID: pi-563169974 (Support query ID) Digest ID: pi-563169974 (Support Digest ID)

Copy Download

Il dashboard Performance Insights può visualizzare fino a 1 KB per ogni istruzione di query completa.

Note

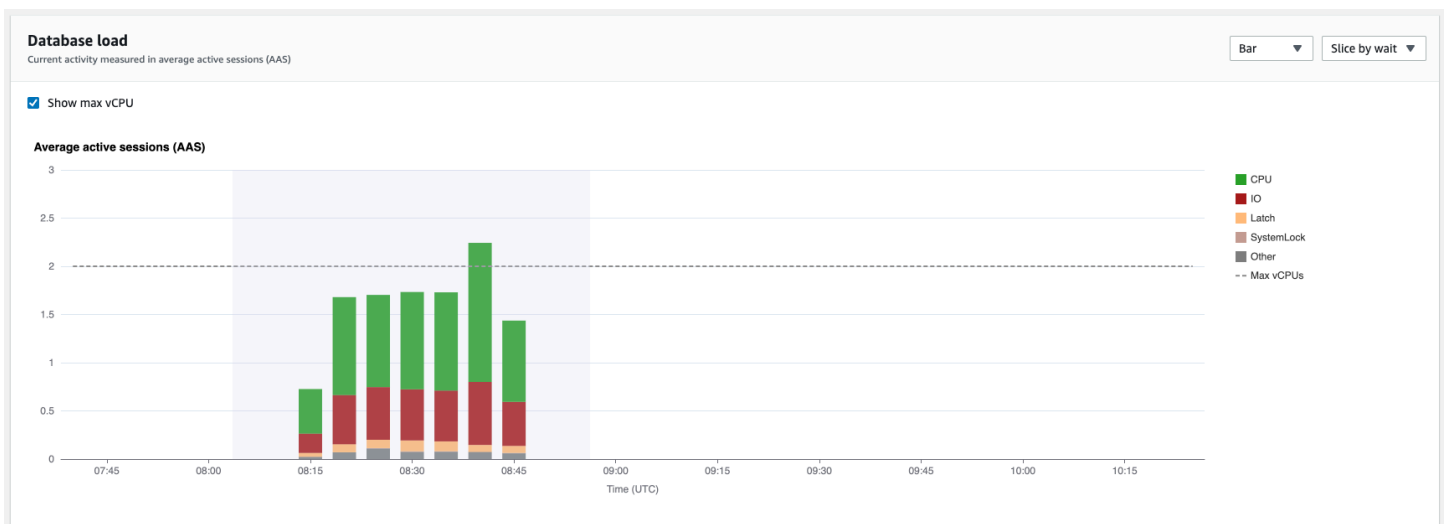
Per copiare o scaricare l'istruzione di interrogazione, disattiva tutti i blocchi popup.

Ingrandimento del grafico di caricamento del database

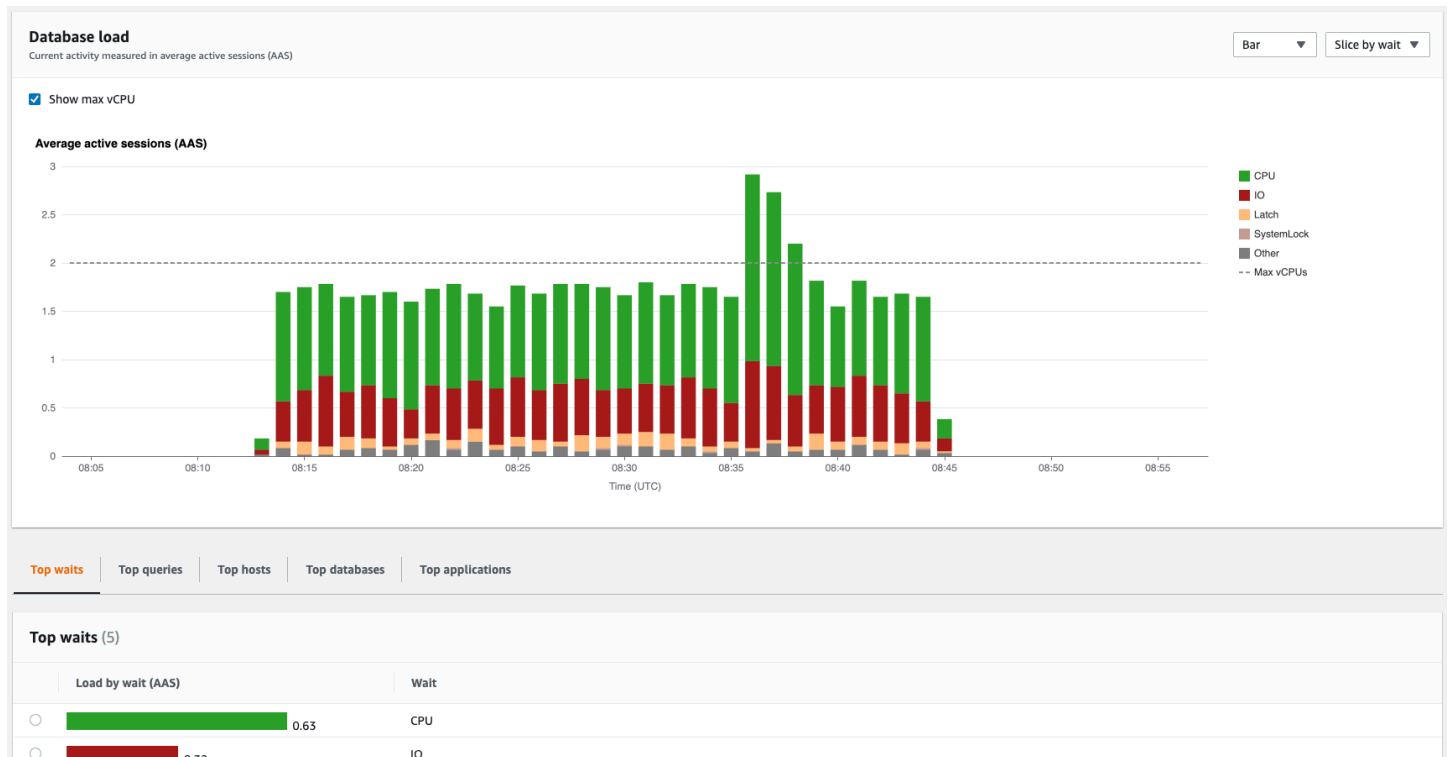
Si possono utilizzare altre funzionalità dell'interfaccia utente di Performance Insights per analizzare i dati sulle performance.

Clic e trascina e zoom avanti

Nell'interfaccia di Performance Insights, puoi scegliere una piccola parte del grafico di carico e ingrandire il dettaglio.



Per ingrandire una parte del grafico di carico, scegli l'ora di inizio e trascina fino alla fine del periodo di tempo che ti interessa. Una volta fatto, l'area selezionata è evidenziata. Quando rilasciate il mouse, il grafico di carico si ingrandisce sull'area selezionata e la tabella Primi elementi viene ricalcolata.



Recupero dei parametri con l'API Performance Insights

Quando Performance Insights è abilitato, l'API fornisce visibilità sulle prestazioni dell'istanza. Amazon CloudWatch Logs fornisce la fonte autorevole per i parametri di monitoraggio forniti per i servizi. AWS

Performance Insights offre una vista specifica del dominio del carico del database misurato come numero medio di sessioni attive (AAS). Questo parametro viene visualizzata dai consumer API come un set di dati temporali bidimensionali. La dimensione temporale dei dati fornisce i dati relativi al carico del database per ogni momento dell'intervallo di tempo in cui è stata eseguita la query. Ogni punto temporale scompone il carico complessivo in relazione alle dimensioni richieste, come Query, Wait-state, Application o Host, misurato in corrispondenza di quel punto temporale.

Amazon DocumentDB Performance Insights monitora l'istanza DB di Amazon DocumentDB per consentirti di analizzare e risolvere i problemi relativi alle prestazioni del database. Un modo per visualizzare i dati di Performance Insights è disponibile nella AWS Management Console. Performance Insights fornisce inoltre un'API pubblica per eseguire query sui dati. Puoi usare l'API per effettuare quanto segue:

- Scaricamento dei dati in un database
- Aggiungi dati Performance Insights ai pannelli di controllo di monitoraggio esistenti
- Crea strumenti di monitoraggio

Per utilizzare l'API Performance Insights, abilita Performance Insights su una delle tue istanze Amazon DocumentDB. Per informazioni sull'abilitazione di Performance Insights, consulta [Abilitazione e disattivazione di Performance Insights](#). Per ulteriori informazioni sull'API di Performance Insights, consulta la [Documentazione di riferimento dell'API di Performance Insights](#).

L'API di Performance Insights fornisce le seguenti operazioni.

Operazione di Performance Insights	AWS CLI command	Descrizione
DescribeDimensionKeys	aws pi describe-dimension-keys	Recupera le prime N chiavi di dimensione per un parametro per un determinato periodo di tempo.
GetDimensionKeyDetails	aws pi get-dimension-key-details	Recupera gli attributi del gruppo di dimensioni specificato per un'istanza database o un'origine dati. Ad esempio, se specifichi un ID di query e se i dettagli della dimensione sono disponibili, <code>GetDimensionKeyDetails</code> recupera il testo completo della dimensione <code>db.query.statement</code> associata a questo ID. Questa operazione è utile perché <code>DescribeDimensionKeys</code> non supporta <code>GetResourceMetrics</code> il recupero di testo di istruzioni di query di grandi dimensioni.
GetResourceMetadata	aws pi get-resource-metadata	Recupera i metadati per diverse caratteristiche. Ad esempio, i metadati potrebbero indicare che una caratteri

Operazione di Performance Insights	AWS CLI command	Descrizione
		stica è attivata o disattivata su un'istanza database specifica.
<u>GetResourceMetrics</u>	<u>aws pi get-resource-metrics</u>	Recupera parametri Performance Insights per un set di origini dati, su un periodo di tempo. Puoi fornire gruppi di dimensioni e dimensioni specifiche e fornire criteri di aggregazione e filtro per ogni gruppo.
<u>ListAvailableResourceDimensions</u>	<u>aws pi list-available-resource-dimensions</u>	Recupera le dimensioni su cui è possibile eseguire query per ogni tipo di parametro specificato su un'istanza specificata.
<u>ListAvailableResourceMetrics</u>	<u>aws pi list-available-resource-metrics</u>	Recupera tutti i parametri disponibili dei tipi di parametro specificati su cui è possibile eseguire query per un'istanza database specificata.

Argomenti

- [AWS CLI per Performance Insights](#)
- [Recupero dei parametri di serie temporali](#)
- [AWS CLIEsempi di utilizzo di per Performance Insights](#)

AWS CLI per Performance Insights

Puoi visualizzare i dati di Performance Insights utilizzando la AWS CLI. Puoi visualizzare la guida per i comandi AWS CLI per Performance Insights inserendo quanto segue nella riga di comando.

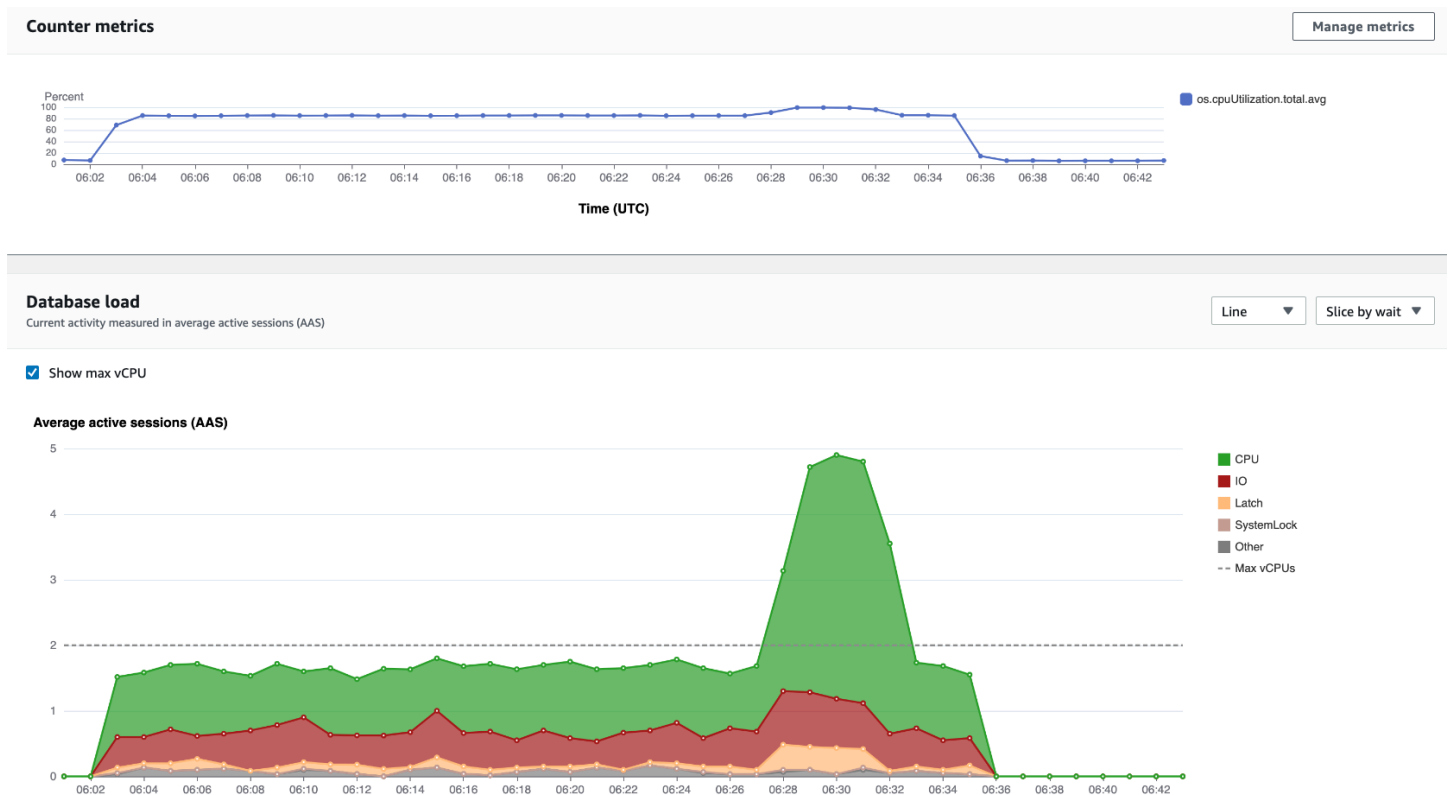
aws pi help

Se AWS CLI non è installato, consulta [Installazione dell'interfaccia a riga di comando di AWS](#) nella Guida per l'utente di AWS CLI per informazioni sull'installazione.

Recupero dei parametri di serie temporali

L'operazione `GetResourceMetrics` recupera uno o più parametri di serie temporali dai dati di Performance Insights. `GetResourceMetrics` richiede un parametro e un periodo di tempo e restituisce una risposta con un elenco di punti di dati.

Ad esempio, la AWS Management Console utilizza `GetResourceMetrics` per popolare il grafico Counter Metrics (Parametri contatore) e il grafico Database Load (Carico del database), come illustrato nell'immagine seguente.



Tutti i parametri restituiti da `GetResourceMetrics` sono parametri di serie temporali standard ad eccezione di `db.load`. Questo parametro è visualizzato nel grafico Database Load (Carico del database). Il parametro `db.load` è diverso dagli altri parametri di serie temporali in quanto può essere suddiviso in sottocomponenti detti dimensioni. Nell'immagine precedente, `db.load` è suddiviso e raggruppato in base agli stati delle attese che formano il `db.load`.

Note

GetResourceMetrics può anche restituire il parametro `db.sampleload`, ma il parametro `db.load` è appropriato nella maggior parte dei casi.

Per informazioni sui parametri contatore restituiti da GetResourceMetrics, consulta [Performance Insights per le contrometriche](#).

I seguenti calcoli sono supportati per i parametri:

- Media: il valore medio per il parametro su un periodo di tempo. Aggiungi `.avg` al nome parametro.
- Minimo: il valore minimo per il parametro su un periodo di tempo. Aggiungi `.min` al nome parametro.
- Massimo: il valore massimo per il parametro su un periodo di tempo. Aggiungi `.max` al nome parametro.
- Somma: la somma dei valori dei parametri su un periodo di tempo. Aggiungi `.sum` al nome parametro.
- Conteggio di esempio: il numero di volte che il parametro è stato raccolto su un periodo di tempo. Aggiungi `.sample_count` al nome parametro.

Ad esempio, supponiamo che un parametro venga raccolto per 300 secondi (5 minuti) e che il parametro venga raccolto una volta al minuto. I valori per ogni minuto sono 1, 2, 3, 4 e 5. In questo caso, vengono restituiti i seguenti calcoli:

- Media: 3
- Minimo: 1
- Massimo: 5
- Somma: 15
- Conteggio del campione: 5

Per ulteriori informazioni sull'utilizzo del comando `get-resource-metrics` della AWS CLI, consulta [get-resource-metrics](#).

Per l'opzione `--metric-queries`, specifica una o più query per cui ottenere risultati. Ciascuna query consiste di un parametro obbligatorio `Metric` e parametri facoltativi `GroupBy` e `Filter`. Di seguito è riportato un esempio della specifica di un'opzione `--metric-queries`.

```
{
  "Metric": "string",
  "GroupBy": {
    "Group": "string",
    "Dimensions": ["string", ...],
    "Limit": integer
  },
  "Filter": {"string": "string"
  ...}
```

AWS CLIEsempi di utilizzo di per Performance Insights

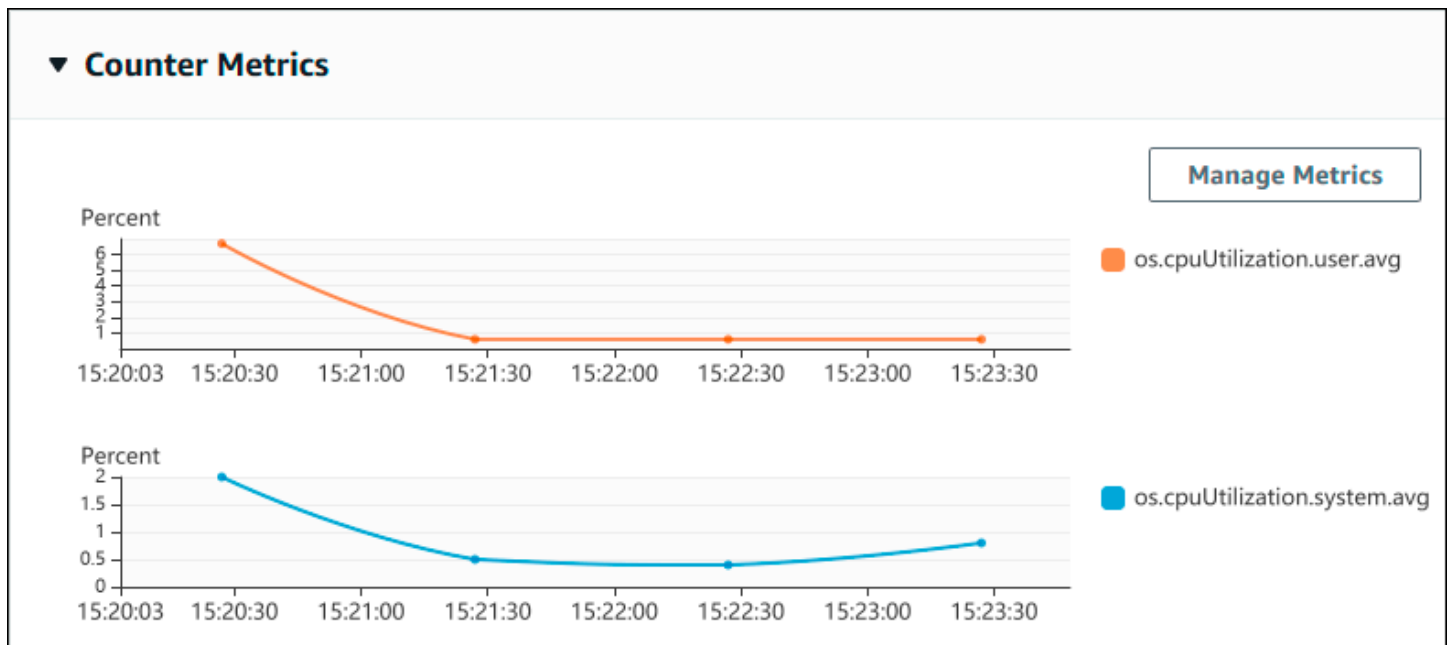
Negli esempi seguenti viene illustrato come utilizzare AWS CLI per Performance Insights.

Argomenti

- [Recupero dei parametri contatore](#)
- [Recupero della media di carico del DB per i principali stati di attesa](#)
- [Recupero della media di carico del DB per Top Query](#)
- [Recupero della media di carico del DB filtrata per Query](#)

Recupero dei parametri contatore

Lo screenshot seguente mostra due grafici dei parametri contatore nella AWS Management Console.



L'esempio seguente mostra come raccogliere gli stessi dati che utilizza la AWS Management Console per generare i due grafici dei parametri contatore.

Per Linux, macOS o 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"}]'
```

Per 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"}]'
```

Puoi agevolare la lettura del comando specificando un file per l'opzione `--metrics-query`. Il seguente esempio utilizza un file denominato `query.json` per l'opzione. Il file presenta i seguenti contenuti.

```
[
  {
    "Metric": "os.cpuUtilization.user.avg"
  },
  {
    "Metric": "os.cpuUtilization.idle.avg"
  }
]
```

Esegui il comando seguente per utilizzare il file.

Per Linux, macOS o 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
```

Per 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
```

L'esempio precedente specifica i seguenti valori per le opzioni:

- `--service-type`— DOCDB per Amazon DocumentDB
- `--identifier` – L'ID risorsa per l'istanza database
- `--start-time` e `--end-time` – I valori ISO 8601 DateTime per il periodo su cui eseguire le query, con supporto di più formati

Esegue query per un intervallo di tempo di un'ora:

- `--period-in-seconds` – 60 per una query al minuto
- `--metric-queries` – Una serie di due query, ognuna solo per un parametro

Il nome del parametro utilizza punti per classificare il parametro in una categoria utile, dove l'ultimo elemento è una funzione. Nell'esempio, la funzione è `avg` per ciascuna query. Come per Amazon CloudWatch, le funzioni supportate sono `min`, `max`, `total`, e `avg`.

La risposta è simile a quella riportata di seguito.

```
{
  "AlignedStartTime": "2022-03-13T08:00:00+00:00",
  "AlignedEndTime": "2022-03-13T09:00:00+00:00",
  "Identifier": "db-NQF3TTMFQ3GT0KIMJ0DMC3KQQ4",
  "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

```

La risposta presenta un Identifier, un AlignedStartTime e un AlignedEndTime. Poiché il valore `--period-in-seconds` era 60, l'ora di inizio e fine è stata allineata al minuto. Se `--period-in-seconds` fosse stato 3600, l'ora di inizio e fine sarebbe stata allineata all'ora.

MetricList nella risposta ha una serie di voci, ciascuna con una voce Key e una voce DataPoints. Ciascun DataPoint ha un Timestamp e un Value. Ciascun elenco Datapoints ha 60 punti di dati in quanto le query sono per dati al minuto nell'arco di un'ora, con Timestamp1/Minute1, Timestamp2/Minute2 e così via, fino a Timestamp60/Minute60.

Poiché la query è per due diversi parametri contatore, la risposta contiene due element MetricList.

Recupero della media di carico del DB per i principali stati di attesa

L'esempio seguente mostra la stessa query che utilizza la AWS Management Console per generare un grafico a linee ad area in pila. Questo esempio recupera l'`db.load.avg`ultima ora con carico diviso in base ai primi sette stati di attesa. Il comando è come quello in [Recupero dei parametri contatore](#). Tuttavia, il file `query.json` presenta i seguenti contenuti.

```

[
  {
    "Metric": "db.load.avg",
    "GroupBy": { "Group": "db.wait_state", "Limit": 7 }
  }
]

```

Eeguire il comando riportato qui di seguito.

Per Linux, macOS o 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
```

Per 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
```

L'esempio specifica la metrica `db.load.avg` e una dei primi sette GroupBy stati di attesa.

Per i dettagli sui valori validi per questo esempio, consulta il riferimento [DimensionGroup](#) all'API Performance Insights.

La risposta è simile a quella riportata di seguito.

```
{  
  "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 questa risposta, ci sono tre voci in `MetricList`. È disponibile una voce per il totale `db.load.avg` e tre voci ciascuna per la `db.load.avg` divisione in base a uno dei primi tre stati di attesa. Poiché esisteva una dimensione di raggruppamento (a differenza del primo esempio), deve esserci una chiave per ogni raggruppamento della metrica. Può esserci una sola chiave per ciascun parametro, come nel caso d'uso del parametro contatore di base.

Recupero della media di carico del DB per Top Query

L'esempio seguente raggruppa in `db.wait_state` base alle prime 10 istruzioni di query. Esistono due gruppi diversi per le istruzioni di interrogazione:

- `db.query`— L'istruzione di interrogazione completa, ad esempio


```

{"find":"customers","filter":{"FirstName":"Jesse"},"sort":{"key":
{"$numberInt":"1"}}}

```
- `db.query_tokenized`— L'istruzione di interrogazione tokenizzata, ad esempio


```

{"find":"customers","filter":{"FirstName":"?"},"sort":{"key":
{"$numberInt":"?"}},"limit":{"$numberInt":"?"}}

```

Quando si analizzano le prestazioni del database, può essere utile considerare come un unico elemento logico le istruzioni di query che differiscono solo in base ai relativi parametri. Pertanto, puoi utilizzare `db.query_tokenized` durante le query. Tuttavia, specialmente se sei interessato a `explain()`, a volte è più utile esaminare istruzioni di query complete con parametri. Esiste una relazione padre-figlio tra le query tokenizzate e quelle complete, con più query complete (figli) raggruppate sotto la stessa query tokenizzata (principale).

Il comando in questo esempio è simile a quello in [Recupero della media di carico del DB per i principali stati di attesa](#). Tuttavia, il file `query.json` presenta i seguenti contenuti.

```
[
  {
    "Metric": "db.load.avg",
    "GroupBy": { "Group": "db.query_tokenized", "Limit": 10 }
  }
]
```

Nell'esempio seguente viene utilizzato `db.query_tokenized`.

Per Linux, macOS o 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
```

Per 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
```

Questo esempio esegue una query di durata superiore a 1 ora, con un minuto. `period-in-seconds`

L'esempio specifica la metrica `db.load.avg` e una dei primi sette `GroupBy` stati di attesa.

Per i dettagli sui valori validi per questo esempio, consulta il riferimento [DimensionGroup](#) all'API Performance Insights.

La risposta è simile a quella riportata di seguito.

```
{
  "AlignedStartTime": "2022-04-04T06:00:00+00:00",
  "AlignedEndTime": "2022-04-04T06:15:00+00:00",
  "Identifier": "db-NQF3TTMFQ3GT0KIMJ0DMC3KQQ4",
  "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
```

Questa risposta contiene 11 voci `MetricList` (1 in totale, 10 delle principali query tokenizzate), con 24 voci all'ora per ogni voce. `DataPoints`

Per le query tokenizzate, ci sono tre voci in ogni elenco di dimensioni:

- `db.query_tokenized.statement`— L'istruzione di interrogazione tokenizzata.
- `db.query_tokenized.db_id` — L'ID sintetico che Performance Insights genera per te. Questo esempio restituisce l'ID sintetico `pi-1064184600`.
- `db.query_tokenized.id` – L'ID della query all'interno di Performance Insights.

Nella AWS Management Console, questo ID è detto Support ID (ID supporto). Si chiama questo perché l'ID è dati che il AWS Support può esaminare per facilitare la risoluzione di un problema relativo al database. AWS prende molto seriamente la sicurezza e la privacy dei tuoi dati e quasi tutti i dati vengono archiviati crittografati con la tua chiave master cliente (CMK) AWS KMS. Pertanto, nessuno all'interno di AWS può accedere a tali dati. Nell'esempio precedente, sia `tokenized.statement` che `tokenized.db_id` vengono archiviati crittografati. Se riscontri un problema con il database, AWS Support può aiutarti facendo riferimento al Support ID (ID supporto).

Quando si eseguo query, potrebbe essere utile specificare un Group in GroupBy. Tuttavia, per un controllo più dettagliato dei dati restituiti, occorre specificare l'elenco delle dimensioni. Ad esempio, se tutto ciò di cui si necessita è `db.query_tokenized.statement`, è possibile aggiungere l'attributo `Dimensions` al file `query.json`.

```
[
  {
    "Metric": "db.load.avg",
    "GroupBy": {
      "Group": "db.query_tokenized",
      "Dimensions":["db.query_tokenized.statement"],
      "Limit": 10
    }
  }
]
```

Recupero della media di carico del DB filtrata per Query

La query dell'API corrispondente in questo esempio è simile al comando in [Recupero della media di carico del DB per Top Query](#). Tuttavia, il file `query.json` presenta i seguenti contenuti.

```
[
  {
    "Metric": "db.load.avg",
    "GroupBy": { "Group": "db.wait_state", "Limit": 5 },
  }
]
```

```

    "Filter": { "db.query_tokenized.id": "AKIAIOSFODNN7EXAMPLE" }
  }
]

```

In questa risposta, tutti i valori vengono filtrati in base al contributo della query tokenizzata AKIAIOSFODNN7EXAMPLE specificata nel file query.json. Le chiavi potrebbero anche seguire un ordine diverso rispetto a una query senza filtro, poiché sono i primi cinque stati di attesa che hanno influito sulla query filtrata.

CloudWatch Metriche Amazon per Performance Insights

Performance Insights pubblica automaticamente le metriche su Amazon CloudWatch. Gli stessi dati possono essere interrogati da Performance Insights, ma l'inserimento delle metriche CloudWatch semplifica l'aggiunta di allarmi. CloudWatch Agevola inoltre l'aggiunta dei parametri ai pannelli di controllo di CloudWatch esistenti.

Parametro	Descrizione
DBLoad	Il numero di sessioni attive per Amazon DocumentDB. Generalmente, si richiedono i dati per il numero medio di sessioni attive. In Performance Insights, questi dati sono oggetto di query come <code>db.load.avg</code> .
DBLoadCPU	Il numero di sessioni attive in cui il tipo di stato di attesa è CPU. In Performance Insights, questi dati vengono interrogati come <code>db.load.avg</code> , filtrati in base al tipo di stato di attesa. CPU
CPU DB LoadNon	Il numero di sessioni attive in cui il tipo di stato di attesa non è CPU.

Note

Queste metriche vengono pubblicate su CloudWatch solo in caso di carico sull'istanza DB.

Puoi esaminare queste metriche utilizzando la CloudWatch consoleAWS CLI, l'o l' CloudWatchAPI.

Ad esempio, puoi ottenere le statistiche per la DBLoad metrica eseguendo il [get-metric-statistics](#) comando.

```
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
```

Questo esempio genera un output simile a quello riportato di seguito.

```
{  
  "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"
}

```

Puoi utilizzare la funzione matematica `DB_PERF_INSIGHTS` metrica nella CloudWatch console per interrogare i parametri dei contatori di Amazon DocumentDB Performance Insights. La `DB_PERF_INSIGHTS` funzione include anche la `DBLoad` metrica a intervalli inferiori al minuto. Puoi impostare CloudWatch allarmi su queste metriche. Per maggiori dettagli su come creare un allarme, consulta [Creazione di un allarme sui parametri contatore di Performance Insights da un database AWS](#).

Per ulteriori informazioni su CloudWatch, consulta [Cos'è Amazon? CloudWatch](#) nella Guida per CloudWatch l'utente di Amazon.

Performance Insights per le contrometriche

Le metriche dei contatori sono metriche del sistema operativo nella dashboard di Performance Insights. Per agevolare l'individuazione e l'analisi di problemi legati alle prestazioni, è possibile correlare i parametri contatore ai carichi dei database.

Contatori del sistema operativo in Performance Insights

I seguenti contatori del sistema operativo sono disponibili con DocumentDB Performance Insights.

Contatore	Tipo	Parametro
active	memory	os.memory.active
buffers	memory	os.memory.buffers
cached	memory	os.memory.cached
dirty	memory	os.memory.dirty

Contatore	Tipo	Parametro
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.cpuUtilization.idle
system	cpuUtilization	os.cpuUtilization.system
total	cpuUtilization	os.cpuUtilization.total
user	cpuUtilization	os.cpuUtilization.user
wait	cpuUtilization	os.cpuUtilization.wait
one	loadAverageMinute	sistema operativo. loadAverageMinute.uno
fifteen	loadAverageMinute	così. loadAverageMinute.quindici
cinque	loadAverageMinute	così. loadAverageMinute.cinque
cached	swap	os.swap.cached
free	swap	os.swap.free
in	swap	os.swap.in
out	swap	os.swap.out

Contatore	Tipo	Parametro
total	swap	os.swap.total
rx	network	os.network.rx
tx	network	os.network.tx
numVCPUs	general	os.general.numVCPUs

Sviluppo con Amazon DocumentDB

Queste sezioni trattano lo sviluppo con Amazon DocumentDB (con compatibilità con MongoDB).

Argomenti

- [Connessione programmatica ad Amazon DocumentDB](#)
- [Utilizzo di Change Streams con Amazon DocumentDB](#)
- [Usando AWS Lambda con Change Streams](#)
- [Utilizzo della convalida dello schema JSON](#)
- [Connessione ad Amazon DocumentDB come set di repliche](#)
- [Connessione a un cluster Amazon DocumentDB dall'esterno di un Amazon VPC](#)
- [Connessione a un cluster Amazon DocumentDB da Studio 3T](#)
- [Connect ad Amazon DocumentDB tramite DataGrip](#)
- [Connect tramite Amazon EC2](#)
- [Connect tramite il driver JDBC di Amazon DocumentDB](#)
- [Connect tramite il driver ODBC di Amazon DocumentDB](#)

Connessione programmatica ad Amazon DocumentDB

Questa sezione contiene esempi di codice che dimostrano come connettersi ad Amazon DocumentDB (con compatibilità con MongoDB) utilizzando diversi linguaggi. Gli esempi sono suddivisi in due sezioni diverse, a seconda che sul cluster con cui ti connetti sia abilitato o meno il protocollo Transport Layer Security (TLS). Per impostazione predefinita, TLS è abilitato sui cluster Amazon DocumentDB. È comunque possibile disattivarlo, se necessario. Per ulteriori informazioni, consulta [Crittografia dei dati in transito](#).

Se stai tentando di connetterti al tuo Amazon DocumentDB dall'esterno del VPC in cui risiede il cluster, consulta [Connessione a un cluster Amazon DocumentDB dall'esterno di un Amazon VPC](#).

Prima di connetterti al cluster, devi sapere se sul cluster è abilitato il protocollo TLS. La sezione successiva illustra come determinare il valore del parametro `tls` del cluster tramite la AWS Management Console o l'AWS CLI. Seguendo tale procedura potrai trovare e applicare il codice di esempio appropriato.

Argomenti

- [Determinazione del valore del parametro `tls`](#)
- [Connessione con TLS abilitato](#)
- [Connessione con TLS disabilitato](#)

Determinazione del valore del parametro `tls`

Determinare se nel cluster è abilitato TLS è un processo in due fasi che puoi eseguire utilizzando o. AWS Management Console AWS CLI

1. Determinare il gruppo di parametri che regola il cluster.

Using the AWS Management Console

1. [Accedi a e apri AWS Management Console la console Amazon DocumentDB all'indirizzo `https://console.aws.amazon.com/docdb`.](https://console.aws.amazon.com/docdb)
2. Nel pannello di navigazione a sinistra, seleziona Cluster.
3. Nell'elenco dei cluster selezionare il nome del cluster.
4. La pagina risultante mostra i dettagli del cluster selezionato. Scorri verso il basso fino a Cluster details (Dettagli del cluster). Nella parte inferiore della sezione, individua il nome del gruppo di parametri sotto Cluster parameter group (Gruppo di parametri del cluster).

Using the AWS CLI

Il AWS CLI codice seguente determina quale parametro governa il cluster. Assicurarsi di sostituire `sample-cluster` con il nome del cluster.

```
aws docdb describe-db-clusters \  
  --db-cluster-identifier sample-cluster \  
  --query 'DBClusters[*].[DBClusterIdentifier,DBClusterParameterGroup]'
```

L'aspetto dell'output di questa operazione è simile al seguente.

```
[  
  [  
    "sample-cluster",  
    "sample-parameter-group"  ]  
]
```

```
    ]
  ]
```

- Determinare il valore del parametro **tls** nel gruppo di parametri del cluster.

Using the AWS Management Console

- Nel riquadro di navigazione scegliere **Parameter groups** (Gruppi di parametri).
- Nella finestra **Cluster parameter groups** (Gruppi di parametri cluster), selezionare il gruppo di parametri del cluster.
- La pagina risultante mostra i parametri del gruppo di parametri del cluster. Puoi vedere il valore del parametro **tls** qui. Per informazioni sulla modifica di questo parametro, consulta [Modifica dei gruppi di parametri del cluster Amazon DocumentDB](#).

Using the AWS CLI

È possibile utilizzare il `describe-db-cluster-parameters` AWS CLI comando per visualizzare i dettagli dei parametri nel gruppo di parametri del cluster.

- **--describe-db-cluster-parameters**— Per elencare tutti i parametri all'interno di un gruppo di parametri e i relativi valori.
- **--db-cluster-parameter-group name**: obbligatorio. Il nome del gruppo di parametri del cluster.

```
aws docdb describe-db-cluster-parameters \
  --db-cluster-parameter-group-name sample-parameter-group
```

L'aspetto dell'output di questa operazione è simile al seguente.

```
{
  "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 supporta gli endpoint FIPS 140-3 a partire dai cluster Amazon DocumentDB 5.0 (versione del motore 3.0.3727) in queste regioni: ca-central-1, us-west-2, us-east-1, us-east-2, -1. us-gov-east us-gov-west

Dopo aver determinato il valore del parametro `tls`, continuare con la connessione al cluster utilizzando uno degli esempi di codice nelle seguenti sezioni.

- [Connessione con TLS abilitato](#)
- [Connessione con TLS disabilitato](#)

Connessione con TLS abilitato

Per visualizzare un esempio di codice per la connessione programmatica a un cluster Amazon DocumentDB abilitato per TLS, scegli la scheda appropriata per la lingua che desideri utilizzare.

Per crittografare i dati in transito, scarica la chiave pubblica per Amazon DocumentDB `global-bundle.pem` denominata utilizzando la seguente operazione.

```
wget https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem
```

Se l'applicazione è su Microsoft Windows e richiede un file PKCS7, puoi scaricare il bundle di certificati PKCS7. Questo bundle contiene i certificati intermedi e root all'indirizzo <https://truststore.pki.rds.amazonaws.com/global/global-bundle.p7b>.

Python

Il codice seguente mostra come connettersi ad Amazon DocumentDB usando Python quando TLS è abilitato.

```
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

Il codice seguente mostra come connettersi ad Amazon DocumentDB utilizzando Node.js quando TLS è abilitato.

```
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':'DocDB;'}, function(err, result){
        //Print the result to the screen
        console.log(result);

        //Close the connection
        client.close()
      });
    });
  });
```

PHP

Il codice seguente mostra come connettersi ad Amazon DocumentDB utilizzando PHP quando TLS è abilitato.

```
<?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 MongoClient("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->sampldatabase->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

Il codice seguente mostra come connettersi ad Amazon DocumentDB utilizzando Go quando TLS è abilitato.

Note

A partire dalla versione 1.2.1, il driver MongoDB Go utilizzerà solo il primo certificato del server CA trovato in `sslcertificateauthorityfile`. Il codice di esempio riportato di seguito risolve questa limitazione aggiungendo manualmente tutti i certificati server trovati in `sslcertificateauthorityfile` su una configurazione TLS personalizzata utilizzata durante la creazione del client.

```
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

Quando ci si connette a un cluster Amazon DocumentDB abilitato per TLS da un'applicazione Java, il programma deve utilizzare AWS il file di autorità di certificazione (CA) fornito per convalidare la connessione. Per utilizzare il certificato Amazon RDS CA, procedi come segue:

1. Scarica il file Amazon RDS CA da <https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem>.
2. Creare uno store attendibile con il certificato CA contenuto nel file eseguendo i comandi indicati di seguito. Assicurarsi di modificare `<keystorePassword>` con un valore diverso. Se si accede a uno store attendibile che contiene sia il vecchio certificato CA (`rds-`

ca-2015-root.pem) sia il nuovo certificato CA (rds-ca-2019-root.pem), è possibile importare il pacchetto di certificati nell'archivio attendibilità.

Il seguente script è uno script di esempio shell che importa il bundle di certificati in un archivio di trust su un sistema operativo Linux. Nell'esempio seguente, sostituisci ogni *segnaposto dell'input utente* con le tue informazioni. In particolare, ovunque si trovi la directory di esempio "mydir" nello script, sostituiscila con una directory creata per questa attività.

```
mydir=/tmp/certs
truststore=${mydir}/rds-truststore.jks
storepassword=<truststorePassword>

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
```

Il seguente script è uno script di shell di esempio che importa il bundle di certificati in un archivio di trust su un sistema operativo Linux.

```

mydir=/tmp/certs
truststore=${mydir}/rds-truststore.jks
storepassword=<truststorePassword>

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

```

- Utilizzalo keystore nel tuo programma impostando le seguenti proprietà di sistema nell'applicazione prima di effettuare una connessione al cluster Amazon DocumentDB.

```

javax.net.ssl.trustStore: <truststore>
javax.net.ssl.trustStorePassword: <truststorePassword>

```

- Il codice seguente mostra come connettersi ad Amazon DocumentDB utilizzando Java quando TLS è abilitato.

```

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 = "<truststorePassword>";

        System.setProperty("javax.net.ssl.trustStore", truststore);
        System.setProperty("javax.net.ssl.trustStorePassword",
truststorePassword);

        MongoClient mongoClient = MongoClient.create(connectionString);

        MongoDBDatabase 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

Il codice seguente mostra come connettersi ad Amazon DocumentDB utilizzando C# / .NET quando TLS è abilitato.

```
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.pem_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);
    }
}
}
```

mongo shell

Il codice seguente mostra come connettersi e interrogare Amazon DocumentDB utilizzando la shell mongo quando TLS è abilitato.

1. Connect ad Amazon DocumentDB con la shell mongo. Se utilizzi una versione mongo shell precedente alla 4.2, usa il seguente codice per connetterti.

```
mongo --ssl --host sample-cluster.node.us-east-1.docdb.amazonaws.com:27017 --
sslCAFile global-bundle.pem --username <sample-user> --password <password>
```

Se stai usando una versione uguale o superiore alla 4.2, usa il seguente codice per connetterti. Le scritture riutilizzabili non sono supportate in AWS DocumentDB. Eccezione: se utilizzi mongo shell, non includere il `retryWrites=false` comando in nessuna stringa

di codice. Per impostazione predefinita, le scritture riutilizzabili sono disabilitate. L'inclusione `retryWrites=false` potrebbe causare errori nei normali comandi di lettura.

```
mongo --tls --host sample-cluster.node.us-east-1.docdb.amazonaws.com:27017 --
tlsCAFile global-bundle.pem --username <sample-user> --password <password>
```

2. Inserire un singolo documento.

```
db.myTestCollection.insertOne({'hello':'Amazon DocumentDB'})
```

3. Trovare il documento precedentemente inserito.

```
db.myTestCollection.find({'hello':'Amazon DocumentDB'})
```

R

Il codice seguente mostra come connettersi ad Amazon DocumentDB con R utilizzando mongolite <https://jeroen.github.io/mongolite/> () quando TLS è abilitato.

```
#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

Il codice seguente mostra come connettersi ad Amazon DocumentDB con Ruby quando TLS è abilitato.

```
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
```

Connessione con TLS disabilitato

Per visualizzare un esempio di codice per la connessione programmatica a un cluster Amazon DocumentDB disabilitato per TLS, scegli la scheda relativa alla lingua che desideri utilizzare.

Python

Il codice seguente mostra come connettersi ad Amazon DocumentDB usando Python quando TLS è disabilitato.

```
## 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

Il codice seguente mostra come connettersi ad Amazon DocumentDB utilizzando Node.js quando TLS è disabilitato.

```
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

Il codice seguente mostra come connettersi ad Amazon DocumentDB utilizzando PHP quando TLS è disabilitato.

```
<?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->sampldatabase->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

Il codice seguente mostra come connettersi ad Amazon DocumentDB utilizzando Go quando TLS è disabilitato.

```
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

Il codice seguente mostra come connettersi ad Amazon DocumentDB utilizzando Java quando TLS è disabilitato.

```
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);

        MongoDBDatabase 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

Il codice seguente mostra come connettersi ad Amazon DocumentDB utilizzando C# / .NET quando TLS è disabilitato.

```
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);
        }
    }
}
```

mongo shell

Il codice seguente mostra come connettersi e interrogare Amazon DocumentDB utilizzando la shell mongo quando TLS è disabilitato.

1. Connect ad Amazon DocumentDB con la shell mongo.

```
mongo --host mycluster.node.us-east-1.docdb.amazonaws.com:27017 --  
username <sample-user> --password <password>
```

2. Inserire un singolo documento.

```
db.myTestCollection.insertOne({'hello':'Amazon DocumentDB'})
```

3. Trovare il documento precedentemente inserito.

```
db.myTestCollection.find({'hello':'Amazon DocumentDB'})
```

R

Il codice seguente mostra come connettersi ad Amazon DocumentDB con R usando mongolite <https://jeroen.github.io/mongolite/> () quando TLS è disabilitato.

```
#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

Il codice seguente mostra come connettersi ad Amazon DocumentDB con Ruby quando TLS è disabilitato.

```
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
```

Utilizzo di Change Streams con Amazon DocumentDB

La funzionalità Change Streams di Amazon DocumentDB (compatibile con MongoDB) fornisce una sequenza temporale di eventi di modifica che si verificano all'interno delle raccolte del cluster. Puoi leggere gli eventi da un flusso di modifica per implementare molti casi d'uso diversi, inclusi i seguenti:

- Notifica di modifica
- Ricerca di testo completo con Amazon OpenSearch Servizio (OpenSearch Servizio)
- Analisi con Amazon Redshift

Le applicazioni possono utilizzare i flussi di modifica per sottoscrivere tutte le modifiche ai dati su singole raccolte. Gli eventi di flussi di modifica vengono ordinati man mano che si verificano nel cluster e vengono archiviati per 3 ore (valore predefinito) dopo la registrazione dell'evento. Il periodo di conservazione può essere esteso fino a 7 giorni utilizzando il `change_stream_log_retention_duration` parametro. Per modificare il periodo di conservazione del change stream, consulta [Modifica della durata di conservazione del log del Change Stream](#).

Argomenti

- [Operazioni supportate](#)
- [Fatturazione](#)
- [Restrizioni](#)
- [Abilitazione dei flussi di modifica](#)
- [Esempio: utilizzo di flussi di modifica con Python](#)
- [Ricerca di un documento completo](#)
- [Ripresa di un flusso di modifiche](#)
- [Ripresa di un flusso di modifiche con `startAtOperationTime`](#)
- [Transazioni nei flussi di modifica](#)
- [Modifica della durata di conservazione del registro del flusso di modifica](#)

Operazioni supportate

Amazon DocumentDB supporta le seguenti operazioni per i flussi di modifica:

- Tutti gli eventi di modifica supportati in `MongoDBdb.collection.watch()`, `db.watch()` e `client.watch()` API.
- Ricerca completa dei documenti per gli aggiornamenti.
- Fasi di aggregazione: `$match`, `$project`, `$redact`, e `$addFieldse$replaceRoot`.
- Ripresa di un flusso di modifiche da un token di ripristino
- Ripresa di un flusso di modifiche da un timestamp utilizzando `startAtOperation` (applicabile ad Amazon DocumentDB v4.0+)

Fatturazione

La funzionalità dei flussi di modifica di Amazon DocumentDB è disabilitata per impostazione predefinita e non comporta costi aggiuntivi finché non viene abilitata. L'utilizzo di flussi di modifiche in un cluster comporta costi di archiviazione e iOS di lettura e scrittura aggiuntivi. È possibile utilizzare il `modifyChangeStreams` Funzionamento tramite API per abilitare questa funzionalità per il cluster. Per ulteriori informazioni sui prezzi, consulta [Prezzi di Amazon DocumentDB](#).

Restrizioni

I flussi di modifica presentano le seguenti limitazioni in Amazon DocumentDB:

- I flussi di modifiche possono essere aperti solo da una connessione all'istanza principale di un cluster Amazon DocumentDB. La lettura dai flussi di modifica su un'istanza di replica non è attualmente supportata. Quando si richiama l'operazione API `watch()`, è necessario specificare una preferenza di lettura **primary** per assicurare che tutte le letture siano indirizzate all'istanza primaria (consulta la sezione [Esempio](#)).
- Gli eventi scritti in un flusso di modifiche per una raccolta sono disponibili per un massimo di 7 giorni (l'impostazione predefinita è 3 ore). I dati dei flussi di modifiche vengono eliminati dopo la finestra della durata di conservazione del log, anche se non si sono verificate nuove modifiche.
- Un'operazione di scrittura di lunga durata su una raccolta come `updateMany` o `deleteMany` può temporaneamente bloccare la scrittura degli eventi dei flussi di modifica fino al completamento della lunga operazione di scrittura.
- Amazon DocumentDB non supporta il registro delle operazioni di MongoDB (`oplog`).
- Con Amazon DocumentDB, devi abilitare esplicitamente i flussi di modifica su una determinata raccolta.
- Se la dimensione totale di un evento di flussi di modifica (inclusi i dati di modifica e il documento completo, se richiesto) è maggiore di 16 MB, il client incontrerà un errore di lettura nei flussi di modifiche.
- Il driver Ruby attualmente non è supportato durante l'utilizzo di `utilizzodb.watch()` o `client.watch()` con Amazon DocumentDB v3.6.

Abilitazione dei flussi di modifica

Puoi abilitare i flussi di modifica di Amazon DocumentDB per tutte le raccolte all'interno di un determinato database o solo per raccolte selezionate. Di seguito sono riportati esempi di come

abilitare i flussi di modifica per diversi casi d'uso utilizzando la shell mongo. Le stringhe vuote vengono trattate come caratteri jolly quando si specificano i nomi del database e della raccolta.

```
//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});
```

I flussi di modifica saranno abilitati per una raccolta se una delle seguenti condizioni è vera:

- Sia il database sia la raccolta sono abilitati in modo esplicito.
- Il database contenente la raccolta è abilitato.
- Tutti i database sono abilitati.

L'eliminazione di una raccolta da un database non disabilita i flussi di modifica per tale raccolta se il database padre dispone anche di flussi di modifiche abilitati o se tutti i database nel cluster sono abilitati. Se viene creata una nuova raccolta con lo stesso nome della raccolta eliminata, i flussi di modifica verranno abilitati per tale raccolta.

È possibile elencare tutti i flussi di modifiche abilitati del cluster utilizzando la fase della pipeline di aggregazione `$listChangeStreams`. Tutte le fasi di aggregazione supportate da Amazon DocumentDB possono essere utilizzate nella pipeline per ulteriori elaborazioni. Se una raccolta precedentemente abilitata è stata disabilitata, non verrà visualizzata nell'output `$listChangeStreams`.

```
//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: {}}));
```

Esempio: utilizzo di flussi di modifica con Python

Di seguito è riportato un esempio di utilizzo di un flusso di modifiche di Amazon DocumentDB con Python a livello di raccolta.

```
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}}}
"""
```

Di seguito è riportato un esempio di utilizzo di un flusso di modifiche di Amazon DocumentDB con Python a livello di database.

```
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'}
"""

```

Ricerca di un documento completo

L'evento di modifica dell'aggiornamento non include il documento completo, ma include solo la modifica apportata. Se il caso d'uso richiede il documento completo interessato da un aggiornamento, è possibile abilitare la ricerca completa del documento all'apertura del flusso.

Il documento `fullDocument` per un evento di aggiornamento del flusso di modifiche rappresenta la versione più recente del documento aggiornato al momento della ricerca del documento. Se si sono verificate modifiche tra l'operazione di aggiornamento e la ricerca `fullDocument`, il documento `fullDocument` potrebbe non rappresentare lo stato del documento al momento dell'aggiornamento.

```

#Create a stream object with update lookup enabled
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()

#Output:
{'_id': {'_data': '015daf9b7c00000001010000000100009025'},
'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}}
```

Ripresa di un flusso di modifiche

È possibile riprendere un flusso di modifiche successivamente utilizzando un token di ripresa, che è uguale al campo `_id` dell'ultimo documento dell'evento di modifica recuperato.

```
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': '015daf9c5b00000001010000000100009025'}
"""

#Python provides a nice shortcut for getting a stream's resume token
print(stream.resume_token)

"""
Output
{'_data': '015daf9c5b00000001010000000100009025'}
"""

#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': '015f7e8f0c000000060100000006000fe038'},
'operationType': 'update',
'clusterTime': Timestamp(1602129676, 6),
'ns': {'db': 'bar', 'coll': 'foo'},
'documentKey': {'_id': ObjectId('5f7e8f0ac423bafb9adba2')},
'fullDocument': {'_id': ObjectId('5f7e8f0ac423bafb9adba2'), 'x': 5},
'updateDescription': {'updatedFields': {'x': 5}, 'removedFields': []}}
"""
#Followed by the insert
print(stream.try_next())

"""
#Output:
{'_id': {'_data': '015f7e8f0c000000070100000007000fe038'},
'operationType': 'insert',
'clusterTime': Timestamp(1602129676, 7),
'ns': {'db': 'bar', 'coll': 'foo'},
'documentKey': {'_id': ObjectId('5f7e8f0cbf8c233ed577eb94')},
'fullDocument': {'_id': ObjectId('5f7e8f0cbf8c233ed577eb94'), 'y': 5}}
"""

```

Ripresa di un flusso di modifiche con `startAtOperationTime`

È possibile riprendere un flusso di modifiche in un secondo momento da un determinato timestamp utilizzando `startAtOperationTime`.

Note

La capacità di usare `startAtOperationTime` è disponibile in Amazon DocumentDB 4.0+. Quando si utilizza `startAtOperationTime`, il cursore del flusso di modifica

restituirà solo le modifiche avvenute in corrispondenza o dopo il timestamp specificato. `llstartAtOperationTime` e `resumeAfter` i comandi si escludono a vicenda e quindi non possono essere usati insieme.

```
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': '015f7e941a000000030100000003000fe038'},
'operationType': 'update',
'clusterTime': Timestamp(1602130970, 3),
'ns': {'db': 'bar', 'coll': 'foo'},
```

```
'documentKey': {'_id': ObjectId('5f7e9417c423bafb9adbb1')},
'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('5f7e94ffc423bafb9adbb2')},
'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}}
"""
```

Transazioni nei flussi di modifica

Gli eventi Change Stream non conterranno eventi derivanti da transazioni non eseguite e/o interrotte. Ad esempio, se inizi una transazione con una `INSERT` operazione e una `UPDATE` operazione e. Se il tuo `INSERT` operazione ha successo, ma il `UPDATE` operazione fallisce, la transazione verrà annullata. Poiché questa transazione è stata annullata, il flusso di modifiche non conterrà alcun evento relativo a questa transazione.

Modifica della durata di conservazione del registro del flusso di modifica

È possibile modificare la durata di conservazione del registro del flusso di modifiche in modo che sia compresa tra 1 ora e 7 giorni utilizzando il `AWS Management Console` o il `AWS CLI`.

Using the AWS Management Console

Per modificare la durata di conservazione del registro del flusso di modifica

1. Accedi all'AWS Management Console e apri la console Amazon DocumentDB all'indirizzo <https://console.aws.amazon.com/docdb>.
2. Nel riquadro di navigazione scegliere Parameter groups (Gruppi di parametri).

Tip

Se il riquadro di navigazione non viene visualizzato sul lato sinistro della schermata, scegliere l'icona del menu (☰) nell'angolo in alto a sinistra della pagina.


3. Nel riquadro Parameter groups (Gruppi di parametri) scegliere il gruppo di parametri cluster associato al cluster. Per identificare il gruppo di parametri del cluster associato al cluster, consulta [Determinazione del gruppo di parametri di un cluster Amazon DocumentDB](#).
4. La pagina risultante mostra i parametri e i relativi dettagli corrispondenti per questo gruppo di parametri del cluster. Selezionare il parametro `change_stream_log_retention_duration`.
5. In alto a destra della pagina, scegliere Edit (Modifica) per modificare il valore del parametro. La `change_stream_log_retention_duration` il parametro può essere modificato per essere compreso tra 1 ora e 7 giorni.
6. Apportare la modifica, quindi scegliere Modify cluster parameter (Modifica parametro cluster) per salvare le modifiche. Per annullare le modifiche, selezionare Cancel (Annulla).

Using the AWS CLI

Per modificare il parametro `change_stream_log_retention_duration` di un gruppo di parametri del cluster, utilizzare l'operazione `modify-db-cluster-parameter-group` con i parametri seguenti.

- **--db-cluster-parameter-group-name**: obbligatorio. Il nome del gruppo di parametri del cluster che stai modificando. Per identificare il gruppo di parametri del cluster associato al cluster, consulta [Determinazione del gruppo di parametri di un cluster Amazon DocumentDB](#).

- **--parameters**: obbligatorio. Il parametro che stai modificando. Ogni voce del parametro deve includere:
 - **ParameterName**— Il nome del parametro che state modificando. In questo caso, è `change_stream_log_retention_duration`
 - **ParameterValue**— Il nuovo valore per questo parametro.
 - **ApplyMethod**— Come si desidera applicare le modifiche a questo parametro. I valori consentiti sono `immediate` e `pending-reboot`.

 Note

I parametri con `ApplyType` per `static` devono avere `ApplyMethod` per `pending-reboot`.

1. Per modificare i valori del parametro `change_stream_log_retention_duration`, eseguire il comando seguente e sostituire `parameter-value` con il valore a cui si desidera modificare il parametro.

Per Linux, macOS o 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"
```

Per 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"
```

L'aspetto dell'output di questa operazione è simile al seguente (formato JSON).

```
{
  "DBClusterParameterGroupName": "sample-parameter-group"
```

```
}
```

2. Attendi almeno 5 minuti.
3. Elenca i valori dei parametri di `sample-parameter-group` per essere certo che le modifiche siano state apportate.

Per Linux, macOS o Unix:

```
aws docdb describe-db-cluster-parameters \  
  --db-cluster-parameter-group-name sample-parameter-group
```

Per Windows:

```
aws docdb describe-db-cluster-parameters ^  
  --db-cluster-parameter-group-name sample-parameter-group
```

L'aspetto dell'output di questa operazione è simile al seguente (formato JSON).

```
{  
  "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

La conservazione dei log del flusso di modifiche non eliminerà i log più vecchi di quelli configurati con `change_stream_log_retention_duration` valore fino a quando la dimensione del registro non è superiore a (>) 51.200 MB.

Usando AWS Lambda con Change Streams

Amazon DocumentDB è integrato con AWS Lambda in modo da poter utilizzare le funzioni Lambda per elaborare i record in un flusso di modifiche. La mappatura delle sorgenti degli eventi Lambda è una risorsa che può essere utilizzata per richiamare le funzioni Lambda al fine di elaborare eventi Amazon DocumentDB che non richiamano direttamente Lambda. Con Amazon DocumentDB change stream come fonte di eventi, puoi creare applicazioni basate sugli eventi che rispondono alle modifiche dei dati. Ad esempio, puoi utilizzare le funzioni Lambda per elaborare nuovi documenti, tenere traccia degli aggiornamenti di documenti esistenti o registrare i documenti eliminati.

Puoi configurare una mappatura dell'origine degli eventi per inviare i record dal flusso di modifiche di Amazon DocumentDB a una funzione Lambda. Gli eventi possono essere inviati uno alla volta o raggruppati per una maggiore efficienza e verranno elaborati in ordine. È possibile configurare il comportamento di batch della mappatura delle sorgenti degli eventi in base alla durata di una finestra temporale specifica (da 0 a 300 secondi) o al numero di record in batch (limite massimo di 10.000 record). Puoi creare più mappature delle sorgenti degli eventi per elaborare gli stessi dati con più funzioni Lambda o per elaborare elementi distinti da più flussi con un'unica funzione.

Se la funzione restituisce un errore, Lambda riprova il batch finché non viene elaborato correttamente. Nel caso in cui gli eventi nel flusso di modifiche siano scaduti, Lambda disabiliterà la mappatura delle sorgenti degli eventi. In questo caso, puoi creare una nuova mappatura delle sorgenti degli eventi e configurarla con una posizione iniziale a tua scelta. Le mappature delle origini eventi Lambda elaborano gli eventi almeno una volta a causa della natura distribuita dei relativi poller. Di conseguenza, in rari casi, la tua funzione Lambda potrebbe ricevere eventi duplicati. Segui le migliori pratiche per lavorare con AWS Lambda funzioni e crea funzioni idempotenti per evitare

problemi relativi a eventi duplicati. Per ulteriori informazioni, vedere [Usando AWS Lambda console con Amazon DocumentDB](#) nella AWS Lambda Guida per gli sviluppatori.

Come best practice in materia di prestazioni, la funzione Lambda deve essere di breve durata. Per evitare di introdurre ritardi di elaborazione non necessari, inoltre, non dovrebbe eseguire una logica complessa. In particolare, per un flusso a velocità elevata, è meglio attivare flussi di lavoro Step Function di post-elaborazione asincrona rispetto a funzioni Lambda sincrone a lunga durata. Per ulteriori informazioni su AWS Lambda, consulta la [Guida per sviluppatori di AWS Lambda](#).

Restrizioni

Di seguito sono riportate le limitazioni da considerare quando si lavora con Amazon DocumentDB e AWS Lambda:

- AWS Lambda è attualmente supportato solo su Amazon DocumentDB 4.0 e 5.0.
- AWS Lambda attualmente non è supportato su cluster elastici o cluster globali.
- AWS Lambda le dimensioni del payload non possono superare i 6 MB. Per ulteriori informazioni sulle dimensioni dei batch Lambda, consulta «Comportamento in batch» in [Mappature delle sorgenti degli eventi Lambda](#) sezione nella AWS Lambda Guida per gli sviluppatori.

Utilizzo della convalida dello schema JSON

Utilizzando l'operatore di interrogazione di `$jsonSchema` valutazione, puoi convalidare i documenti inseriti nelle tue raccolte.

Argomenti

- [Creazione e utilizzo della convalida dello schema JSON](#)
- [Parole chiave supportate](#)
- [Limitazioni](#)

Creazione e utilizzo della convalida dello schema JSON

Creazione di una raccolta con convalida dello schema

È possibile creare una raccolta con regole `createCollection` operative e di convalida. Queste regole di convalida vengono applicate durante gli inserimenti o gli aggiornamenti dei documenti

Amazon DocumentDB. Il seguente esempio di codice mostra le regole di convalida per un insieme di dipendenti:

```
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"
} )
```

Inserimento di un documento valido

L'esempio seguente inserisce documenti conformi alle regole di convalida dello schema di cui sopra:

```
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})
```

Inserimento di un documento non valido

L'esempio seguente inserisce documenti che non sono conformi alle regole di convalida dello schema di cui sopra. In questo esempio, il valore EmployeeID non è una stringa:

```
db.employees.insert({
  "name" : { "firstName" : "Carol" , "lastName" : "Smith"},
  "employeeId": 720 ,
  "salary": 1000.0
})
```

Questo esempio mostra una sintassi errata all'interno del documento.

Modifica di una raccolta

Il collMod comando viene utilizzato per aggiungere o modificare le regole di convalida della raccolta esistente. L'esempio seguente aggiunge un campo stipendio all'elenco dei campi obbligatori:

```
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
}
} )
```

Indirizzare i documenti aggiunti prima della modifica delle regole di convalida

Per indirizzare i documenti che sono stati aggiunti alla tua raccolta prima della modifica delle regole di convalida, utilizza i seguenti `validationLevel` modificatori:

- `strict`: applica le regole di convalida a tutti gli inserti e gli aggiornamenti.
- `moderate`: applica le regole di convalida ai documenti validi esistenti. Durante gli aggiornamenti, i documenti non validi esistenti non vengono controllati.

Nell'esempio seguente, dopo aver aggiornato le regole di convalida sulla raccolta denominata «dipendenti», il campo stipendio è obbligatorio. L'aggiornamento del seguente documento avrà esito negativo:

```
db.runCommand({
  update: "employees",
  updates: [{
    q: { "employeeId": "c721a" },
    u: { age: 25 , salary : 1000},
    upsert: true }]
})
```

Amazon DocumentDB restituisce il seguente output:

```
{
  "n" : 0,
```

```

    "nModified" : 0,
    "writeErrors" : [
      {
"index" : 0,
        "code" : 121,
        "errmsg" : "Document failed validation"
      }
    ],
    "ok" : 1,
    "operationTime" : Timestamp(1234567890, 1)
  }

```

L'aggiornamento del livello di convalida per moderate consente l'aggiornamento corretto del documento precedente:

```

db.runCommand({
  "collMod" : "employees",
  validationLevel : "moderate"
})

db.runCommand({
  update: "employees",
  updates: [{
    q: { "employeeId": "c721a" },
    u: { age: 25 , salary : 1000},
    upsert: true }]
})

```

Amazon DocumentDB restituisce il seguente output:

```

{
  "n" : 1,
  "nModified" : 1,
  "ok" : 1,
  "operationTime" : Timestamp(1234567890, 1)
}

```

Recupero di documenti con \$jsonSchema

L'\$jsonSchema operatore può essere utilizzato come filtro per interrogare i documenti che corrispondono allo schema JSON. Si tratta di un operatore di primo livello che può essere presente nei documenti di filtro come campo di primo livello o utilizzato con operatori di query come \$and\$or,

e. \$nor Gli esempi seguenti mostrano l'uso di \$JsonSchema come filtro singolo e con altri operatori di filtro:

Documento inserito in una raccolta di «dipendenti»:

```
{ "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 }
```

Raccolta filtrata solo con l'\$jsonSchemaoperatore:

```
db.employees.find({
  $jsonSchema: { required: ["age"] } })
```

Amazon DocumentDB restituisce il seguente output:

```
{ "_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 }
```

Raccolta filtrata con l'\$jsonSchemaoperatore e un altro operatore:

```
db.employees.find({
  $or: [{ $jsonSchema: { required: ["age", "name"]}},
  { salary: { $lte:1000}}]});
```

Amazon DocumentDB restituisce il seguente output:

```
{ "_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 }
```

Raccolta filtrata con l'`$jsonSchema` operatore e all'`$match` interno del filtro aggregato:

```
db.employees.aggregate(  
  [{ $match: {  
    $jsonSchema: {  
      required: ["name", "employeeId"],  
      properties: {"salary" : {"bsonType": "double"}}  
    }  
  }  
}]  
)
```

Amazon DocumentDB restituisce il seguente output:

```
{  
  "_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  
}
```

Visualizzazione delle regole di convalida esistenti

Per visualizzare le regole di convalida esistenti su una raccolta, usa:

```
db.runCommand({
  listCollections: 1,
  filter: { name: 'employees' }
})
```

Amazon DocumentDB restituisce il seguente output:

```
{
  "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)
}
```

Parole chiave supportate

I seguenti campi sono supportati nei collMod comandi create and:

- **Validator**— Supporta l'operatore `$jsonSchema`.
- **ValidationLevel**— Supporta i valori `off`, `strict` e `moderate`.
- **ValidationAction**— Supporta il valore `error`.

L'operatore `$JsonSchema` supporta le seguenti parole chiave:

- `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`

Limitazioni

Le seguenti limitazioni si applicano alla convalida: `$jsonSchema`

- Le raccolte non mantengono le regole di convalida quando le operazioni di scrittura con fase di `$out` aggregazione scrivono nella raccolta. Per ottenere documenti validi nella raccolta di output, si consiglia di utilizzare il `$jsonSchema` filtro nella fase di aggregazione prima della `$out` fase di `$match` aggregazione. La convalida dello schema può essere riapplicata alla raccolta degli output dopo la fase di aggregazione. `$out`

```
db.foo.aggregate([{$match: {$jsonSchema: {...}}], {$out: "bar"}]);  
db.runCommand("collMod": "bar", validator: {$jsonSchema: {...}})
```

- Amazon DocumentDB restituisce l'errore «Document failed validation» quando un'operazione non soddisfa la regola di convalida.
- Amazon DocumentDB non supporta `bypassDocumentValidation` l'azione operativa.
`db.runCommand`
- I cluster elastici di Amazon DocumentDB non sono supportati. `$jsonSchema`

Connessione ad Amazon DocumentDB come set di repliche

Durante lo sviluppo su Amazon DocumentDB (con compatibilità con MongoDB), ti consigliamo di connetterti al cluster come set di repliche e distribuire le letture alle istanze di replica utilizzando le funzionalità di preferenza di lettura integrate del driver. Questa sezione illustra ulteriormente il significato e la modalità della connessione al cluster Amazon DocumentDB come set di repliche utilizzando l'SDK per Python come esempio.

Amazon DocumentDB dispone di tre endpoint che puoi utilizzare per connetterti al cluster:

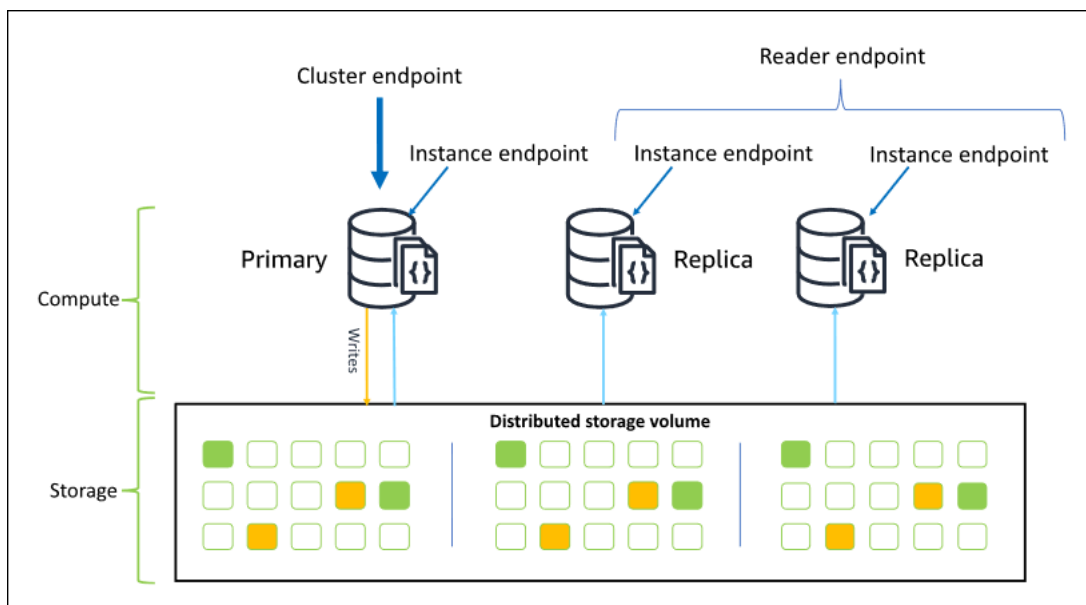
- Endpoint del cluster
- Endpoint di lettura
- Endpoint dell'istanza

Nella maggior parte dei casi, quando ti connetti ad Amazon DocumentDB, è opportuno utilizzare l'endpoint del cluster. Si tratta di un CNAME che punta all'istanza primaria nel cluster, come mostrato nel seguente diagramma.

Quando si utilizza un tunnel SSH, si consiglia di connettersi al cluster utilizzando l'endpoint del cluster e di non tentare di connettersi in modalità set di repliche (ad esempio, specificando `replicaSet=rs0` nella stringa di connessione) poiché si verificherà un errore.

Note

Per ulteriori informazioni sugli endpoint Amazon DocumentDB, consulta [Endpoint Amazon DocumentDB](#).



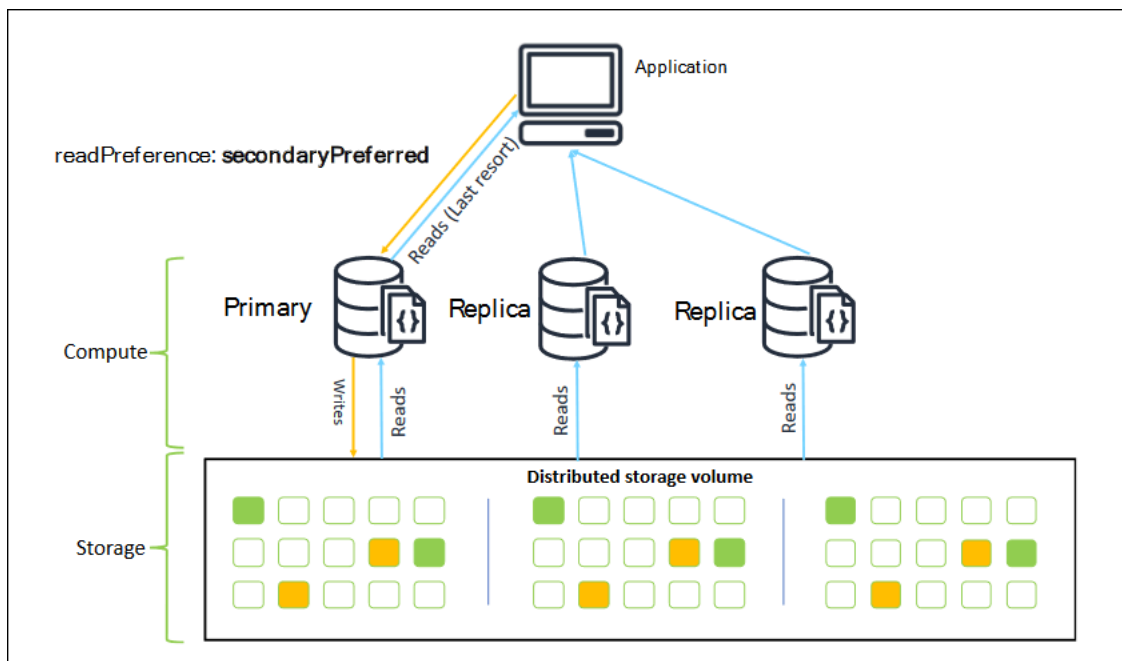
Utilizzando l'endpoint del cluster, puoi connetterti al cluster in modalità set di repliche. Puoi quindi utilizzare le funzionalità integrate del driver delle preferenze di lettura. Nell'esempio seguente, specificando `/?replicaSet=rs0` indichi all'SDK che desideri connetterti come set di repliche. Se ometti `/?replicaSet=rs0`, il client instrada tutte le richieste all'endpoint del cluster, ovvero all'istanza primaria.

```
## 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')
```

Il vantaggio della connessione come set di repliche è che consente all'SDK di rilevare automaticamente la topografia del cluster, anche quando le istanze vengono aggiunte o rimosse dal cluster. Puoi quindi utilizzare il cluster in modo più efficiente instradando le richieste di lettura alle istanze di replica.

Quando ti connetti come set di repliche, puoi specificare `readPreference` per la connessione. Se specifichi una preferenza di lettura di `secondaryPreferred`, il client instrada le query di lettura alle repliche e le query di scrittura all'istanza primaria (come nel diagramma seguente). Le risorse del cluster vengono in tal modo utilizzate meglio. Per ulteriori informazioni, consultare [Opzioni per le preferenze di lettura](#).

```
## 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')
```



Le letture dalle repliche di Amazon DocumentDB sono consistenti finali. Restituiscono i dati nello stesso ordine in cui sono stati scritti sull'istanza primaria e spesso con un ritardo di replica

inferiore a 50 ms. Puoi monitorare il ritardo di replica per il cluster utilizzando i parametri di `Amazon CloudWatchDBInstanceReplicaLag` e `DBClusterReplicaLagMaximum`. Per ulteriori informazioni, consultare [Monitoraggio di Amazon DocumentDB con CloudWatch](#).

A differenza dell'architettura di database monolitica tradizionale, Amazon DocumentDB separa storage ed elaborazione. Data questa architettura moderna, ti consigliamo di dimensionare la lettura sulle istanze di replica. Le letture sulle istanze di replica non bloccano le scritture replicate dall'istanza primaria. Puoi aggiungere fino a 15 istanze di replica di lettura in un cluster e dimensionare fino a milioni di letture al secondo.

Il vantaggio principale della connessione come set di repliche e della distribuzione delle letture alle repliche è quello di aumentare il numero delle risorse complessive nel cluster disponibili per l'applicazione. Ti consigliamo di connetterti come set di repliche come best practice. Inoltre, consigliamo in genere questa connessione nei seguenti scenari:

- Stai utilizzando quasi il 100% di CPU sull'istanza primaria.
- Il numero di riscontri nella cache del buffer è vicino a zero.
- Raggiungi i limiti di connessione o cursore per una singola istanza.

L'aumento delle dimensioni di un'istanza cluster è un'opzione e, in alcuni casi, può essere il modo migliore per dimensionare il cluster. Tuttavia, devi anche considerare come utilizzare al meglio le repliche già presenti nel cluster. In questo modo puoi incrementare le dimensioni senza aumentare i costi derivanti dall'utilizzo di un tipo di istanza più grande. Ti consigliamo inoltre di monitorare e inviare avvisi su questi limiti (ovvero `CPUUtilization`, `DatabaseConnections`, e `BufferCacheHitRatio`) utilizzando gli allarmi di CloudWatch in modo da sapere quando una risorsa viene utilizzata in modo intensivo.

Per ulteriori informazioni, consulta i seguenti argomenti:

- [Best practice per Amazon DocumentDB](#)
- [Quote e limiti di Amazon DocumentDB](#)

Utilizzo delle connessioni del cluster

Considera lo scenario in cui si utilizzano tutte le connessioni del cluster. Ad esempio, un'istanza `r5.2xlarge` ha un limite di 4.500 connessioni (e 450 cursori aperti). Se crei un cluster Amazon DocumentDB a tre istanze e ti connetti solo all'istanza primaria utilizzando l'endpoint del cluster,

i limiti del cluster per le connessioni e i cursori aperti sono rispettivamente 4.500 e 450. Puoi raggiungere questi limiti se stai creando applicazioni che utilizzano molti processi di lavoro che vengono attivati in container. I container aprono una serie di connessioni tutte in una volta sola e saturano il cluster.

Puoi invece connetterti al cluster Amazon DocumentDB come set di repliche e distribuire le letture alle istanze di replica. Puoi quindi triplicare in modo efficace il numero di connessioni e cursori disponibili nel cluster a 13.500 e 1.350 rispettivamente. L'aggiunta di più istanze al cluster aumenta solo il numero di connessioni e cursori per carichi di lavoro di lettura. Se devi aumentare il numero di connessioni per le scritture nel cluster, ti consigliamo di aumentare le dimensioni dell'istanza.

Note

Il numero di connessioni le istanze `large`, `xlarge` e `2xlarge` aumenta con le dimensioni dell'istanza fino a 4.500. Il numero massimo di connessioni per istanza per le istanze `4xlarge` o superiori è 4.500. Per ulteriori informazioni sui limiti in base ai tipi di istanza, consulta [Limiti di istanze](#).

In genere non è consigliabile connettersi al cluster utilizzando la preferenza di lettura `secondary` perché se non ci sono istanze di replica nel cluster, le letture non vanno a buon fine. Ad esempio, supponiamo di avere un cluster Amazon DocumentDB a due istanze con un'istanza primaria e una replica. Se la replica presenta un problema, le richieste di lettura da un pool di connessioni impostato come `secondary` non vanno a buon fine. Il vantaggio di `secondaryPreferred` è che se il client non è in grado di trovare un'istanza di replica idonea a cui connettersi, esegue il fallback sull'istanza primaria per le letture.

Pool di connessione multipli

In alcuni scenari, le letture in un'applicazione devono avere la consistenza lettura dopo scrittura che può essere servita solo dall'istanza primaria in Amazon DocumentDB. In questi scenari, è possibile creare due pool di connessioni client: uno per le scritture e uno per le letture che richiedono la consistenza lettura dopo scrittura. Per effettuare questa operazione, il codice sarà simile al seguente.

```
## 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')
```

Un'altra opzione consiste nel creare un singolo pool di connessioni e sovrascrivere la preferenza di lettura per una determinata raccolta.

```
##Specify the collection and set the read preference level for that collection  
col = db.review.with_options(read_preference=ReadPreference.SECONDARY_PREFERRED)
```

Riepilogo

Per utilizzare meglio le risorse del cluster, ti consigliamo di connetterti al cluster utilizzando la modalità set di repliche. Se è adatto per la tua applicazione, puoi dimensionare la lettura dell'applicazione distribuendo le letture alle istanze di replica.

Connessione a un cluster Amazon DocumentDB dall'esterno di un Amazon VPC

I cluster Amazon DocumentDB (con compatibilità MongoDB) sono distribuiti all'interno di un Amazon Virtual Private Cloud (Amazon VPC). È possibile accedervi direttamente dalle istanze Amazon EC2 o da altri AWS servizi distribuiti nello stesso Amazon VPC. Inoltre, è possibile accedere ad Amazon DocumentDB da istanze EC2 o altri AWS servizi in diversi VPC nella stessa Regione AWS o in altre regioni tramite peering VPC.

Tuttavia, supponiamo che il tuo caso d'uso richieda che tu (o la tua applicazione) acceda alle risorse Amazon DocumentDB dall'esterno del VPC del cluster. In tal caso, puoi utilizzare il tunneling SSH (noto anche come port forwarding) per accedere alle tue risorse Amazon DocumentDB.

La discussione approfondita sul tunneling SSH non rientra negli scopi di questo argomento. Per ulteriori informazioni sul tunneling SSH, consulta quanto segue:

- [Tunnel SSH](#)
- L'[esempio sull'inoltro alla porta SSH](#) e, in particolare, la sezione sull'[inoltro locale](#)

Per creare un tunnel SSH, sarà necessaria un'istanza Amazon EC2 in esecuzione nello stesso Amazon VPC del cluster Amazon DocumentDB. Puoi utilizzare un'istanza EC2 esistente nello stesso VPC del cluster o crearne una. Per ulteriori informazioni, consulta l'argomento rilevante per il tuo sistema operativo:

- [Nozioni base sulle istanze Amazon EC2 Linux](#)
- [Nozioni base sulle istanze Amazon EC2 Windows](#)

In genere, puoi connetterti a un'istanza EC2 con il comando seguente:

```
ssh -i "ec2Access.pem" ubuntu@ec2-34-229-221-164.compute-1.amazonaws.com
```

In tal caso, sarà possibile configurare un tunnel SSH per il cluster Amazon DocumentDB `sample-cluster.node.us-east-1.docdb.amazonaws.com` eseguendo il seguente comando sul computer locale. Il flag `-L` viene utilizzato per inoltrare una porta locale. Quando si utilizza un tunnel SSH, si consiglia di connettersi al cluster utilizzando l'endpoint del cluster e di non tentare di connettersi in modalità set di repliche (ad esempio, specificando `replicaSet=rs0` nella stringa di connessione) poiché si verificherà un errore.

```
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
```

Dopo la creazione del tunnel SSH, tutti i comandi a cui invii `localhost:27017` vengono inoltrati al cluster Amazon DocumentDB in `sample-cluster` esecuzione in Amazon VPC. Se il Transport Layer Security (TLS) è abilitato sul tuo cluster Amazon DocumentDB, devi scaricare la chiave pubblica per Amazon DocumentDB da <https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem>. La seguente operazione scarica questo file:

```
wget https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem
```

Note

TLS è abilitato per impostazione predefinita per i nuovi cluster Amazon DocumentDB. Tuttavia, è possibile effettuare la disabilitazione. Per ulteriori informazioni, consulta [Gestione delle impostazioni TLS del cluster Amazon DocumentDB](#).

Per connetterti al tuo cluster Amazon DocumentDB dall'esterno di Amazon VPC, usa il seguente comando.

```
mongo --sslAllowInvalidHostnames --ssl --sslCAFile global-bundle.pem --username  
<yourUsername> --password <yourPassword>
```

Connessione a un cluster Amazon DocumentDB da Studio 3T

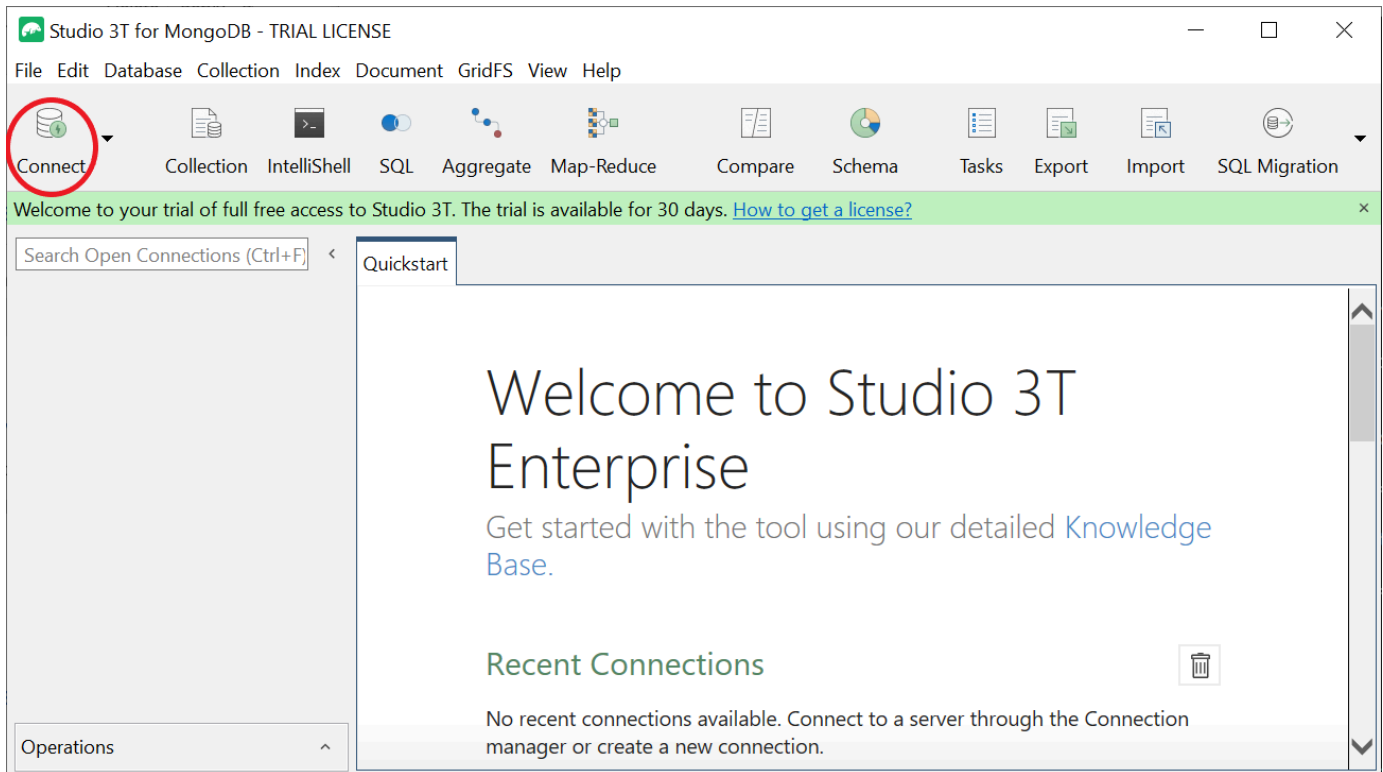
[Studio 3T](#) è una GUI e IDE popolare per sviluppatori e ingegneri dei dati che lavorano con MongoDB. Offre diverse potenti funzionalità, visualizzazioni ad albero, tabella e JSON dei dati, facile importazione/esportazione in CSV, JSON, SQL e BSON/MongoDump, un'opzione di interrogazione flessibile, un' drag-and-drop interfaccia utente visiva, una shell mongo integrata con completamento automatico, un editor di pipeline di aggregazione e supporto per query SQL.

Prerequisiti

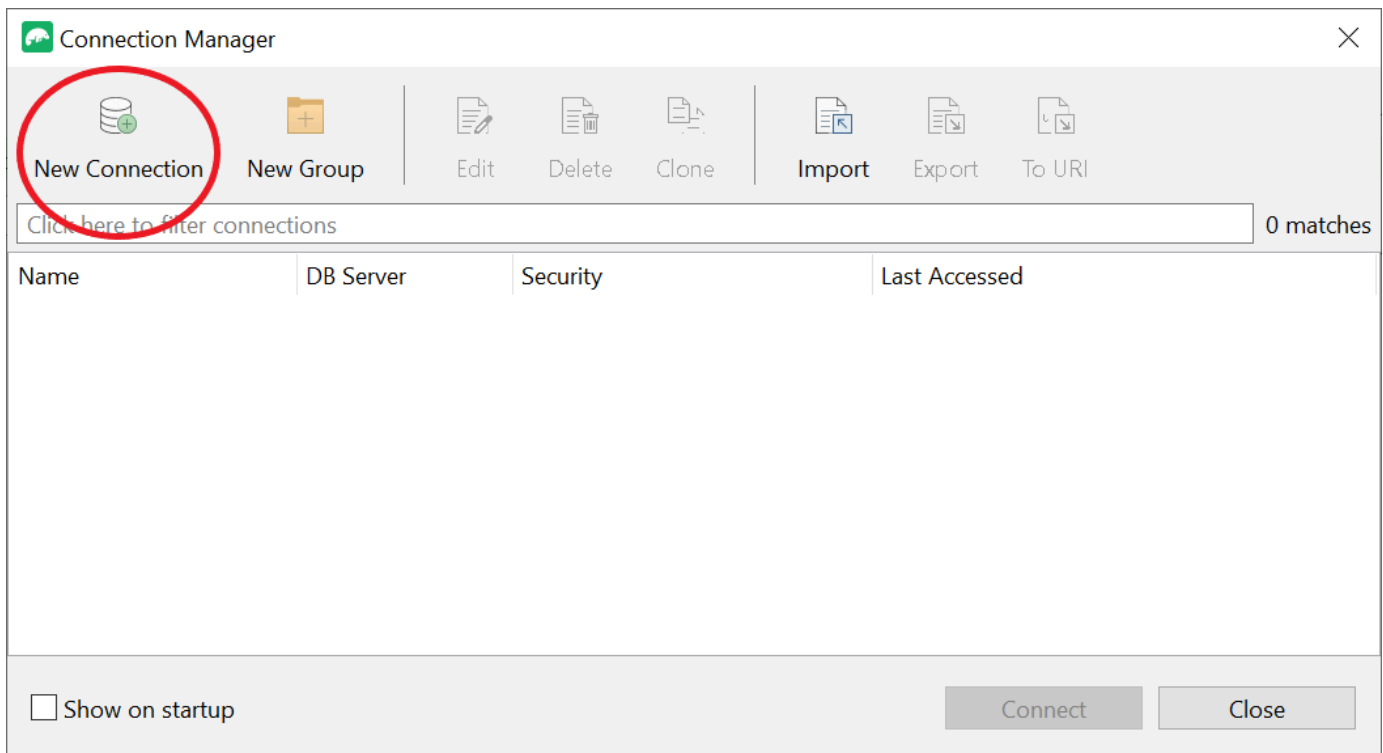
- Se non disponi già di un cluster Amazon DocumentDB in esecuzione su Amazon EC2, segui le istruzioni su come [connetterti con Amazon EC2](#).
- Se non disponi di Studio 3T, [scaricalo](#) e installalo.

Connect con Studio 3T

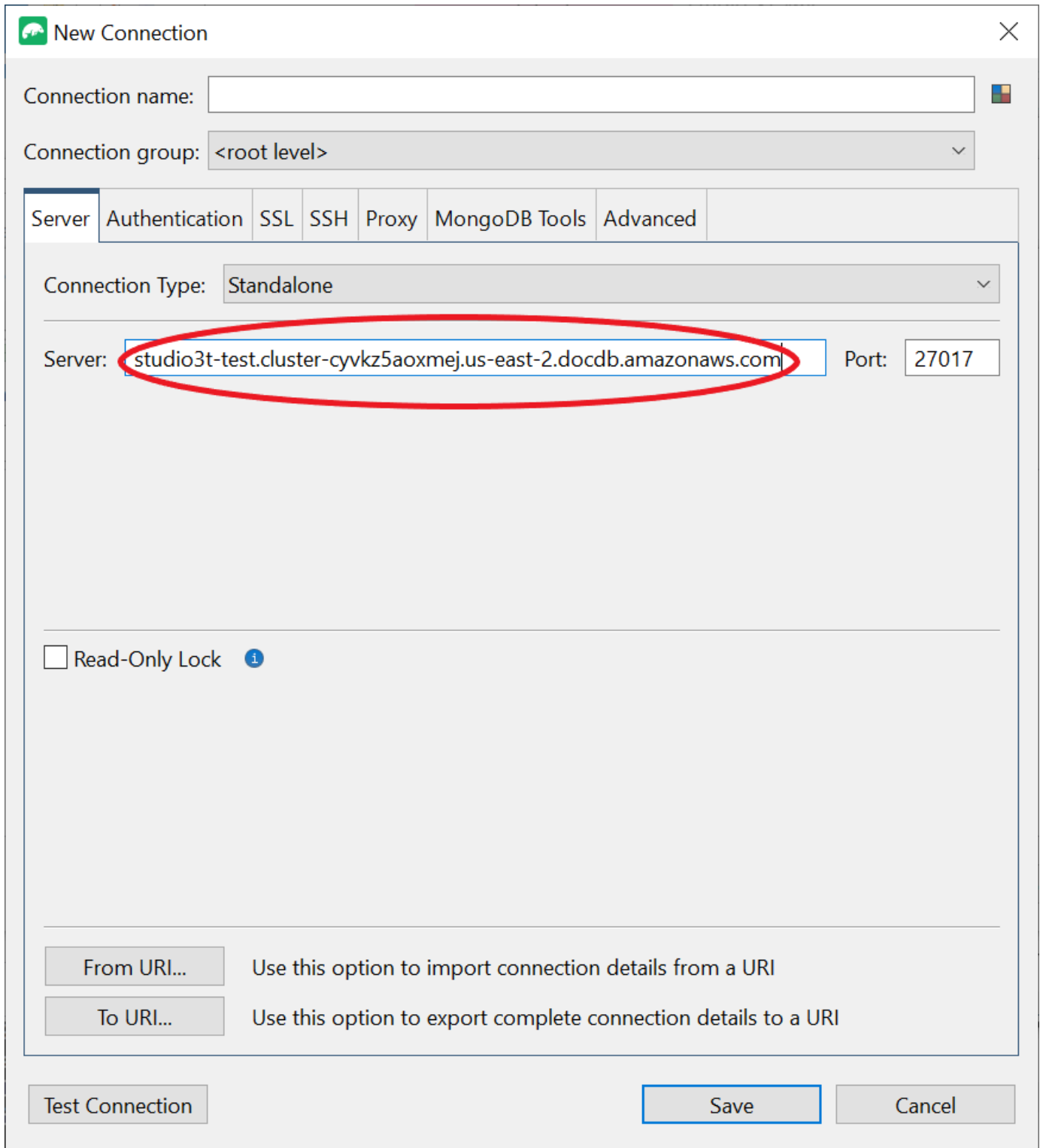
1. Scegli Connect nell'angolo in alto a sinistra della barra degli strumenti.



2. Scegli Nuova connessione nell'angolo in alto a sinistra della barra degli strumenti.



3. Nella scheda Server, nel campo Server, inserisci le informazioni sull'endpoint del cluster.



New Connection

Connection name:

Connection group: <root level>

Server | Authentication | SSL | SSH | Proxy | MongoDB Tools | Advanced

Connection Type: Standalone

Server: Port:

Read-Only Lock ?

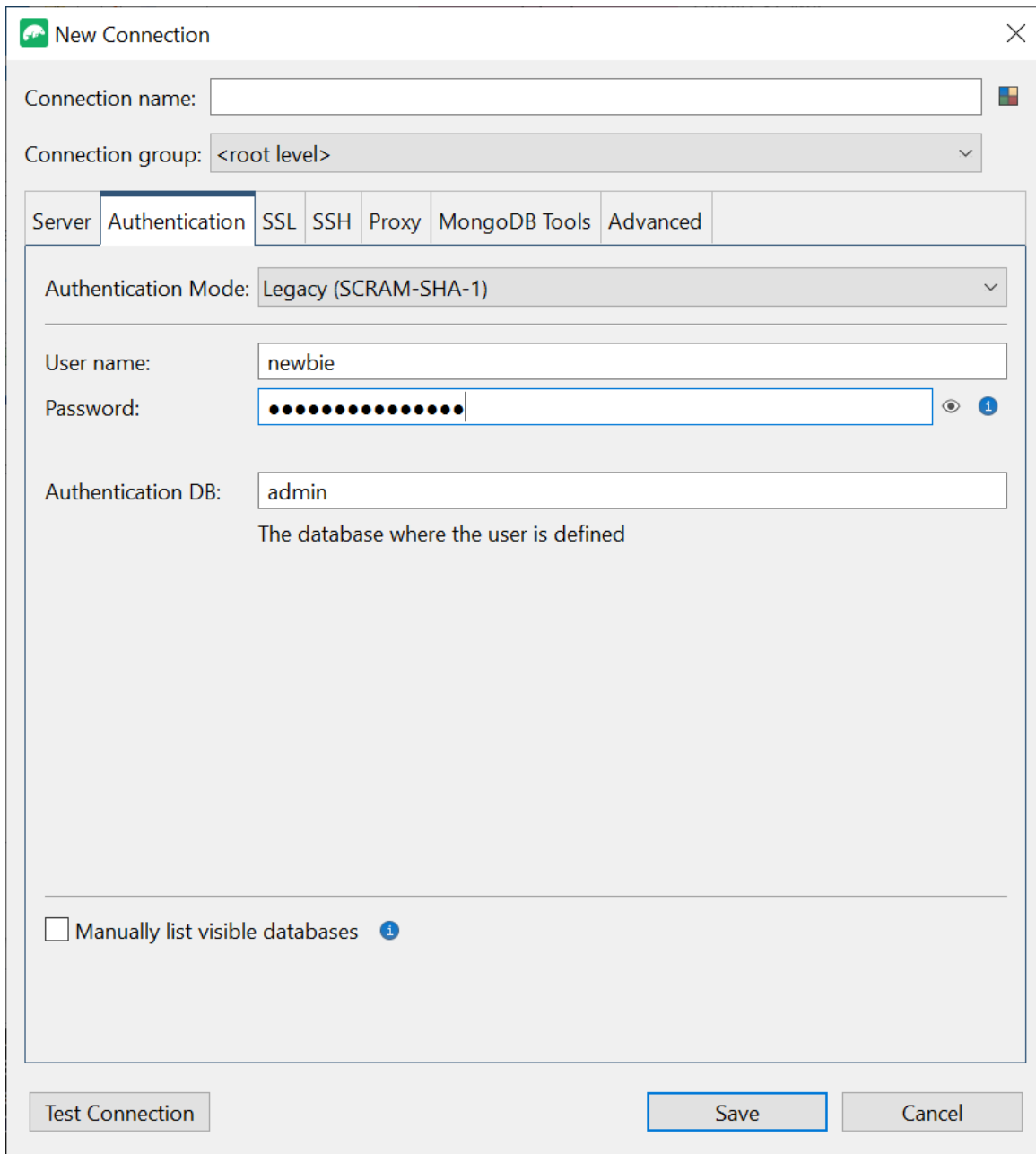
Use this option to import connection details from a URI

Use this option to export complete connection details to a URI

Note

Non riesci a trovare l'endpoint del tuo cluster? Basta seguire i passaggi riportati [qui](#).

- Scegli la scheda Autenticazione e seleziona Legacy nel menu a discesa per la modalità di autenticazione.



The screenshot shows the 'New Connection' dialog box with the 'Authentication' tab selected. The 'Authentication Mode' dropdown is set to 'Legacy (SCRAM-SHA-1)'. The 'User name' field contains 'newbie'. The 'Password' field is masked with 12 dots. The 'Authentication DB' field contains 'admin', with a note below it stating 'The database where the user is defined'. At the bottom, there is a checkbox for 'Manually list visible databases' which is unchecked. The 'Save' button is highlighted with a blue border.


- Inserisci il tuo nome utente e le tue credenziali nei campi Nome utente e Password.
- Scegli la scheda SSL e seleziona la casella Usa il protocollo SSL per connetterti.

The screenshot shows the 'New Connection' dialog box in Studio 3T. The 'SSL' tab is selected, and the following options are visible:

- Use SSL protocol to connect
- Use own Root CA file (--sslCAFile)
 - Text field: C:\Users\suphatra\Downloads\rds-combined-ca-bundle.pem
- Accept server SSL certificates trusted by the operating system
- Accept any server SSL certificates
- Use Client Certificate (--sslPEMKeyFile)
 - Client Certificate: [Text field]
 - Passphrase: [Text field]
 - My client certificate is not protected by a passphrase
- Allow invalid hostnames (--sslAllowInvalidHostnames)
- Use Server Name Indication (Advanced)
 - SNI Host Name: [Text field]

Buttons at the bottom: Test Connection, Save, Cancel.

7. Scegli Usa il tuo file Root CA. Aggiungi quindi il certificato Amazon DocumentDB (puoi saltare questo passaggio se SSL è disabilitato sul tuo cluster DocumentDB). Seleziona la casella per consentire nomi host non validi.

 New Connection ✕

Connection name:

Connection group: <root level> ▼

Server Authentication **SSL** SSH Proxy MongoDB Tools Advanced

Use SSL protocol to connect

Use own Root CA file (--sslCAFile)

🔍 i

Accept server SSL certificates trusted by the operating system

Accept any server SSL certificates

Use Client Certificate (--sslPEMKeyFile)

Client Certificate: 🔍 i

Passphrase: 👁 i

My client certificate is not protected by a passphrase

Allow invalid hostnames (--sslAllowInvalidHostnames) i

Use Server Name Indication (Advanced) i

SNI Host Name:

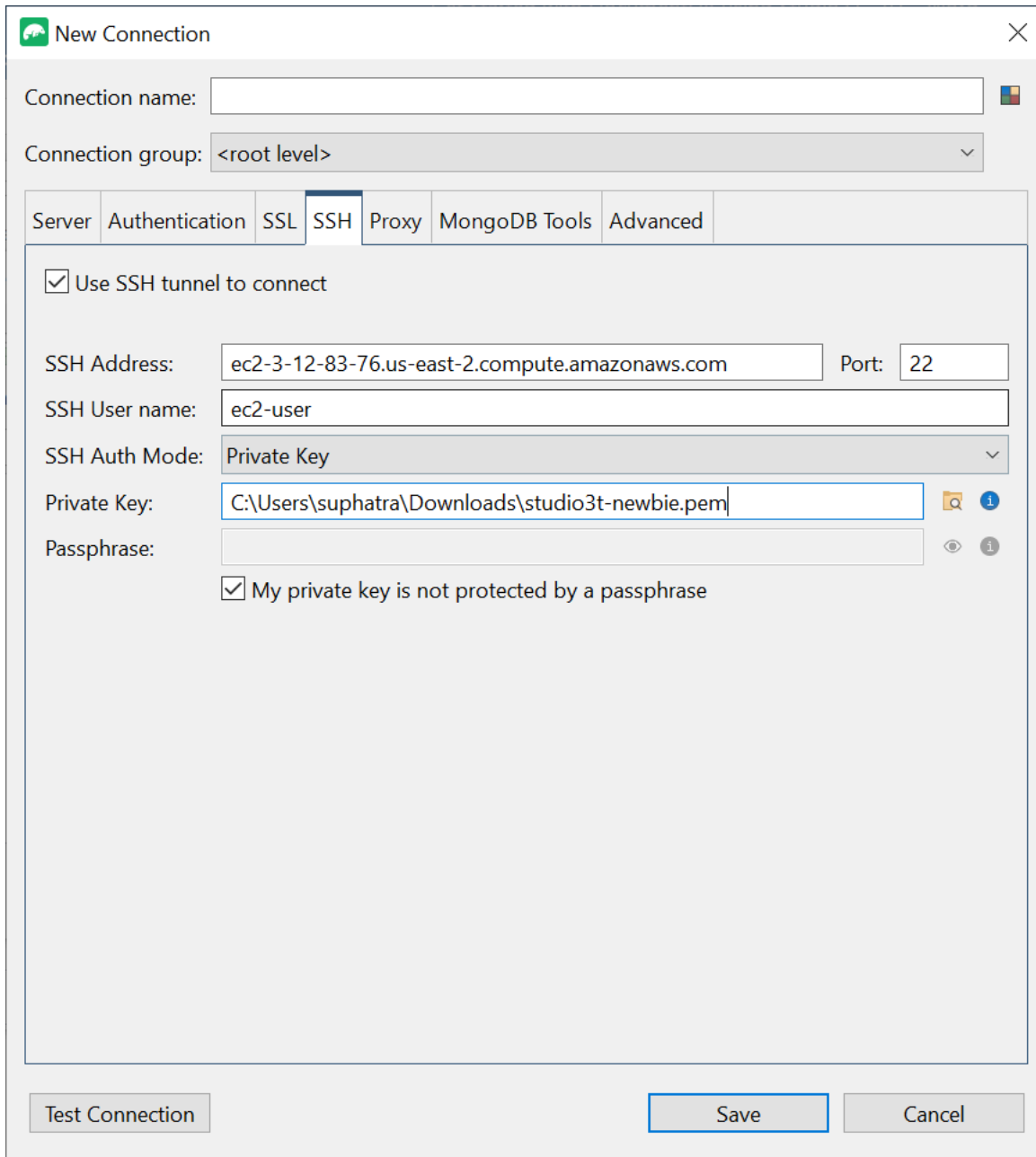
i Note

Non hai il certificato? Puoi scaricarlo con il seguente comando:

```
wget https://truststore.pki.rds.amazonaws.com/global/global-  
bundle.pem
```

8. Se ti connetti da una macchina client esterna ad Amazon VPC, devi creare un tunnel SSH. Lo farai nella scheda SSH.
 - a. Seleziona la casella Usa tunnel SSH e inserisci l'indirizzo SSH nel campo Indirizzo SSH. Questa è la tua istanza Public DNS (IPV4). Puoi ottenere questo URL dalla tua console di [gestione Amazon EC2](#).
 - b. Inserisci il tuo nome utente. Questo è il nome utente della tua istanza Amazon EC2
 - c. Per la modalità di autenticazione SSH, seleziona Chiave privata. Nel campo Chiave privata, scegli l'icona di ricerca dei file da individuare e scegli la chiave privata della tua istanza Amazon EC2. Questo è il file.pem (key pair) che hai salvato durante la creazione dell'istanza nella console Amazon EC2.
 - d. Se sei su un computer client Linux/macOS, potresti dover modificare i permessi della tua chiave privata usando il seguente comando:

```
chmod 400 /fullPathToYourPemFile/<yourKey>.pem
```



The screenshot shows the 'New Connection' dialog box in Studio 3T. The 'SSH' tab is selected, and the following configuration is visible:

- Connection name: [Empty text box]
- Connection group: <root level>
- Use SSH tunnel to connect:
- SSH Address: ec2-3-12-83-76.us-east-2.compute.amazonaws.com
- Port: 22
- SSH User name: ec2-user
- SSH Auth Mode: Private Key
- Private Key: C:\Users\suphatra\Downloads\studio3t-newbie.pem
- Passphrase: [Empty text box]
- My private key is not protected by a passphrase:

Buttons at the bottom: Test Connection, Save, Cancel.

Note

Questa istanza Amazon EC2 deve trovarsi nello stesso gruppo di sicurezza e VPC di Amazon del cluster DocumentDB. Puoi ottenere l'indirizzo SSH, il nome utente e la chiave privata dalla tua console di [gestione Amazon EC2](#).

9. Ora verifica la tua configurazione scegliendo il pulsante Test di connessione.

New Connection

Connection name:

Connection group: <root level>

Server Authentication SSL SSH Proxy MongoDB Tools Advanced

Connection Type: Standalone

Server: robo3t-test.cluster-cyvkz5aoxmej.us-east-2.docdb.amazonaws.com Port: 27017

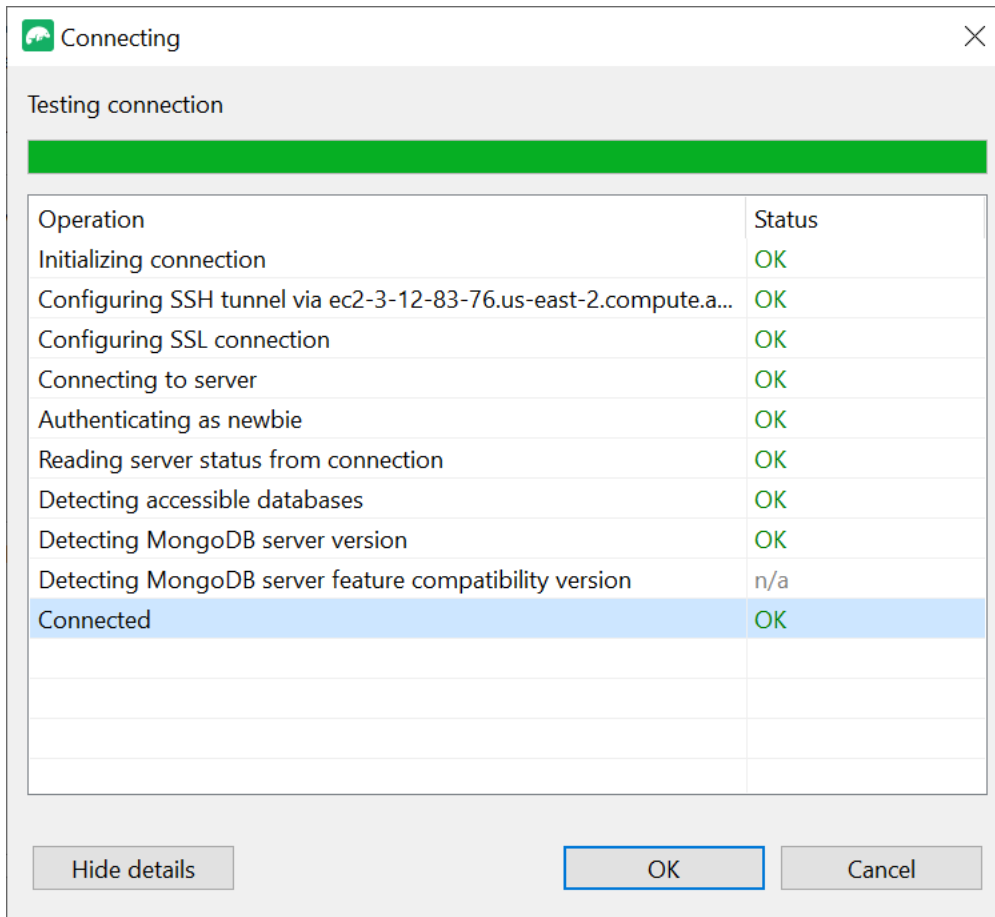
Read-Only Lock ?

From URI... Use this option to import connection details from a URI

To URI... Use this option to export complete connection details to a URI

Test Connection Save Cancel

- Una finestra di diagnostica dovrebbe caricare una barra verde per indicare che il test ha avuto esito positivo. Ora scegli OK per chiudere la finestra di diagnostica.



11. Scegli Salva per salvare la connessione per utilizzi futuri.

New Connection

Connection name:

Connection group: <root level>

Server Authentication SSL SSH Proxy MongoDB Tools Advanced

Connection Type: Standalone

Server: Port:

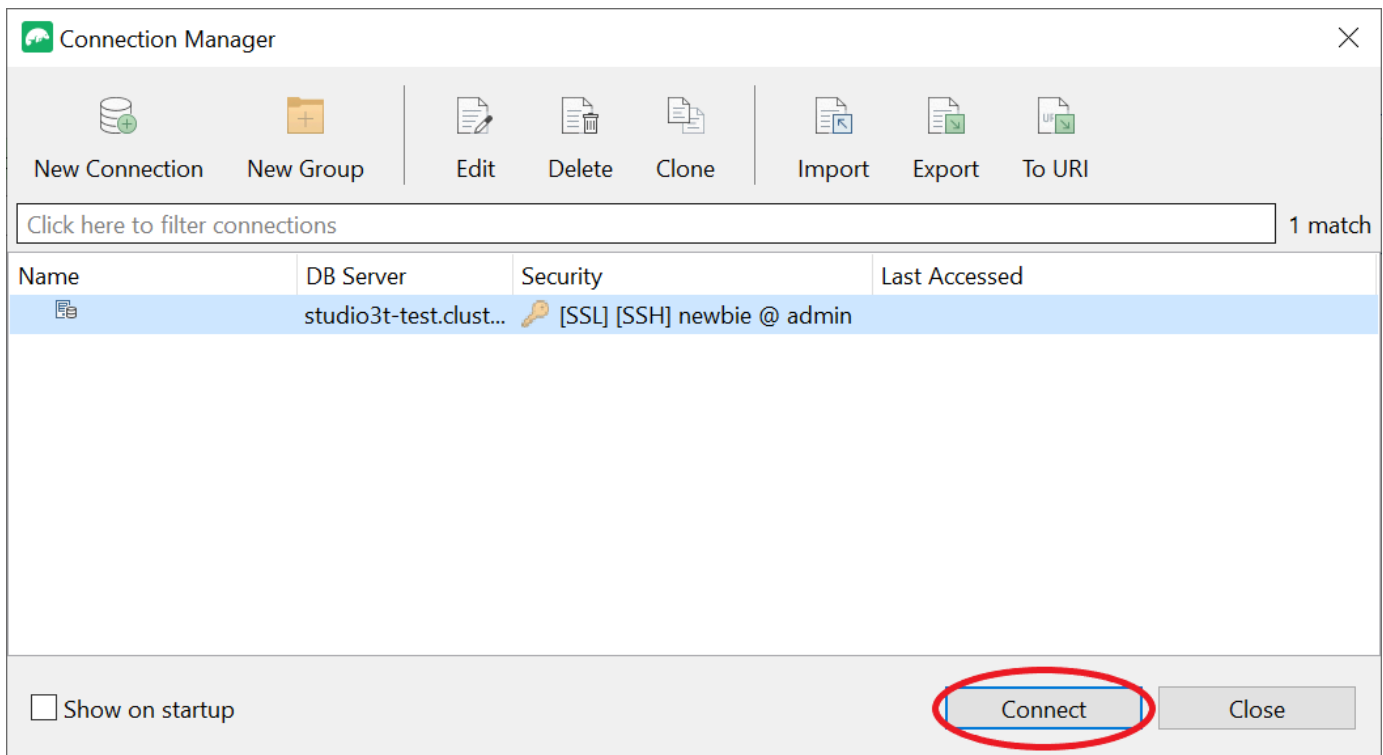
Read-Only Lock ?

From URI... Use this option to import connection details from a URI

To URI... Use this option to export complete connection details to a URI

Test Connection **Save** Cancel

12. Ora seleziona il tuo cluster e scegli Connect.



Complimenti! Ora sei connesso correttamente al tuo cluster Amazon DocumentDB tramite Studio 3T.

Connect ad Amazon DocumentDB tramite DataGrip

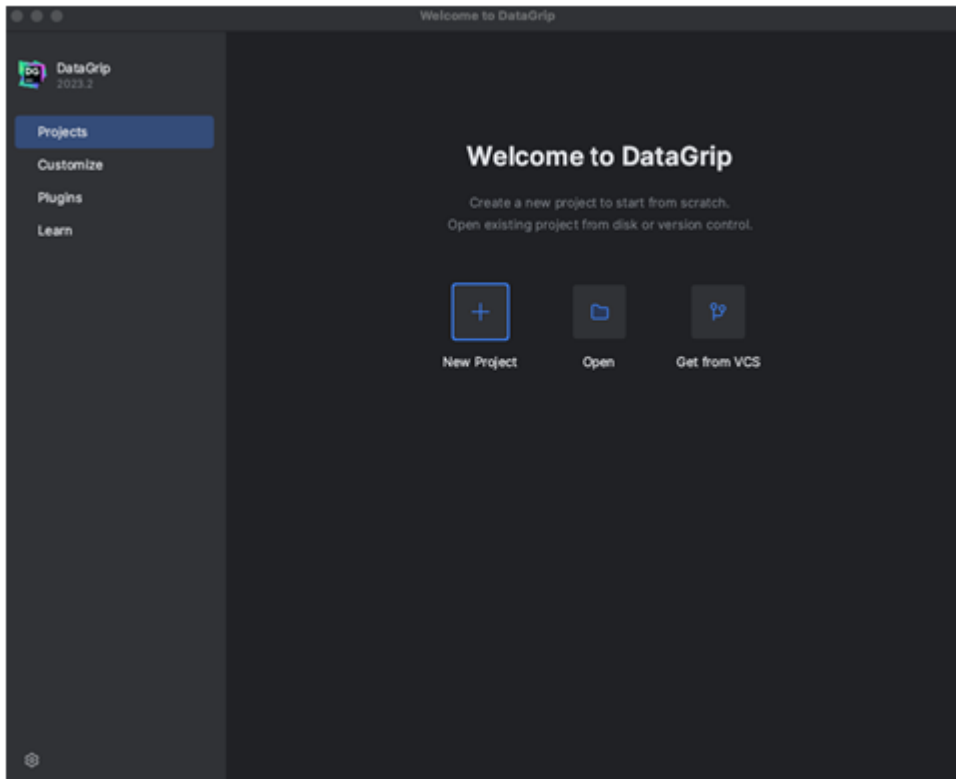
[DataGrip](#) è un potente ambiente di sviluppo integrato (IDE) che supporta vari sistemi di database, incluso Amazon DocumentDB. Questa sezione illustra i passaggi per connettersi al cluster Amazon DocumentDB utilizzando DataGrip, in modo da gestire e interrogare facilmente i dati utilizzando un'interfaccia grafica.

Prerequisiti

- DataGrip IDE installato sulla tua macchina. Puoi scaricarlo da [JetBrains](#).
- Un'istanza Amazon EC2 in esecuzione nello stesso VPC del cluster Amazon DocumentDB. Utilizzerai questa istanza per stabilire un tunnel sicuro dal tuo computer locale ad Amazon DocumentDBCluster. Segui le istruzioni su come farlo. [Connect tramite Amazon EC2](#)
- Alternativa a un'istanza Amazon EC2, a una connessione VPN o se stai già accedendo alla tua AWS infrastruttura utilizzando una VPN sicura. Se preferisci questa opzione, segui le istruzioni per [accedere in modo sicuro ad Amazon AWS Client VPN DocumentDB](#) utilizzando.

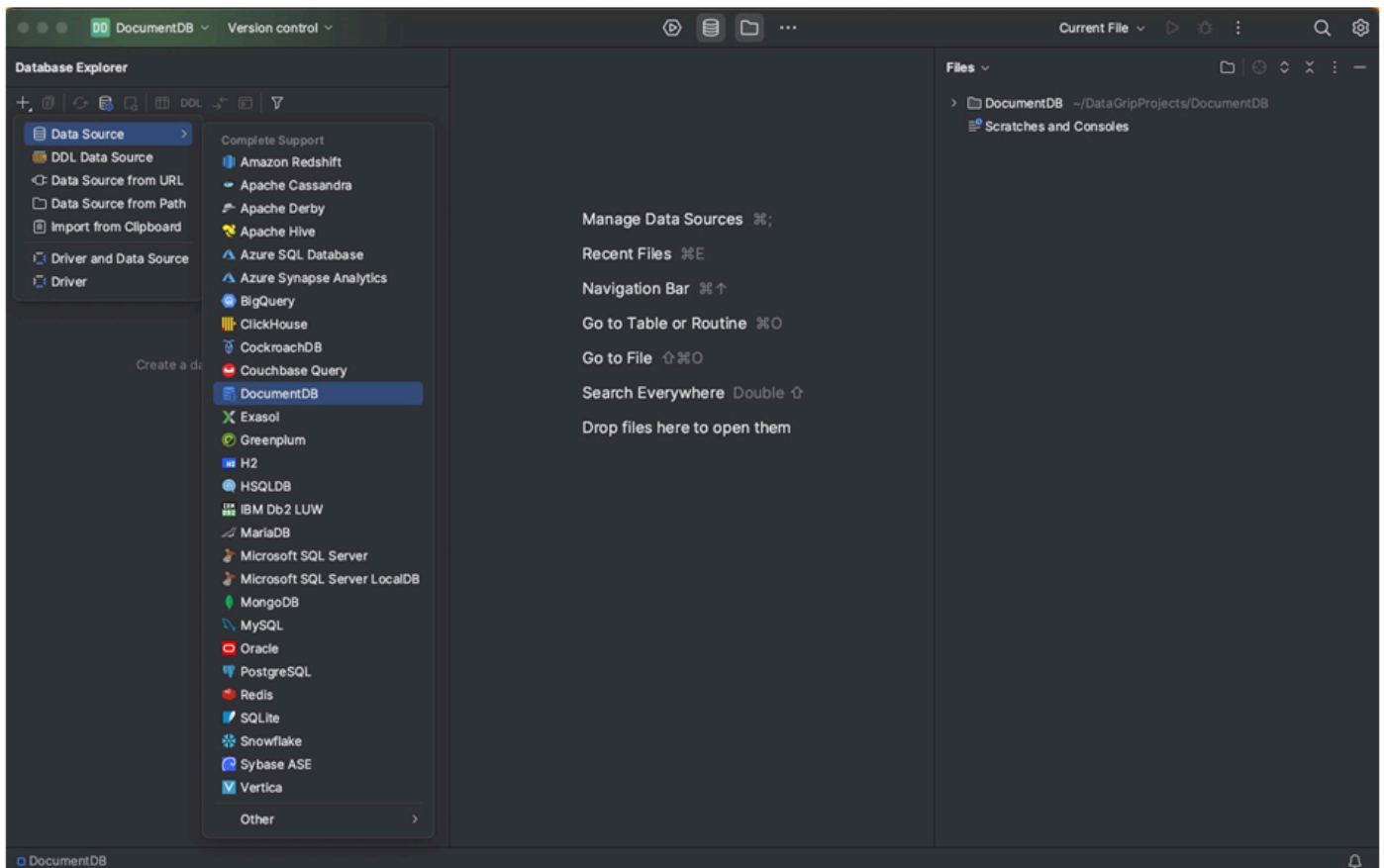
Connect usando DataGrip

1. Avvia DataGrip sul tuo computer e crea un nuovo progetto.

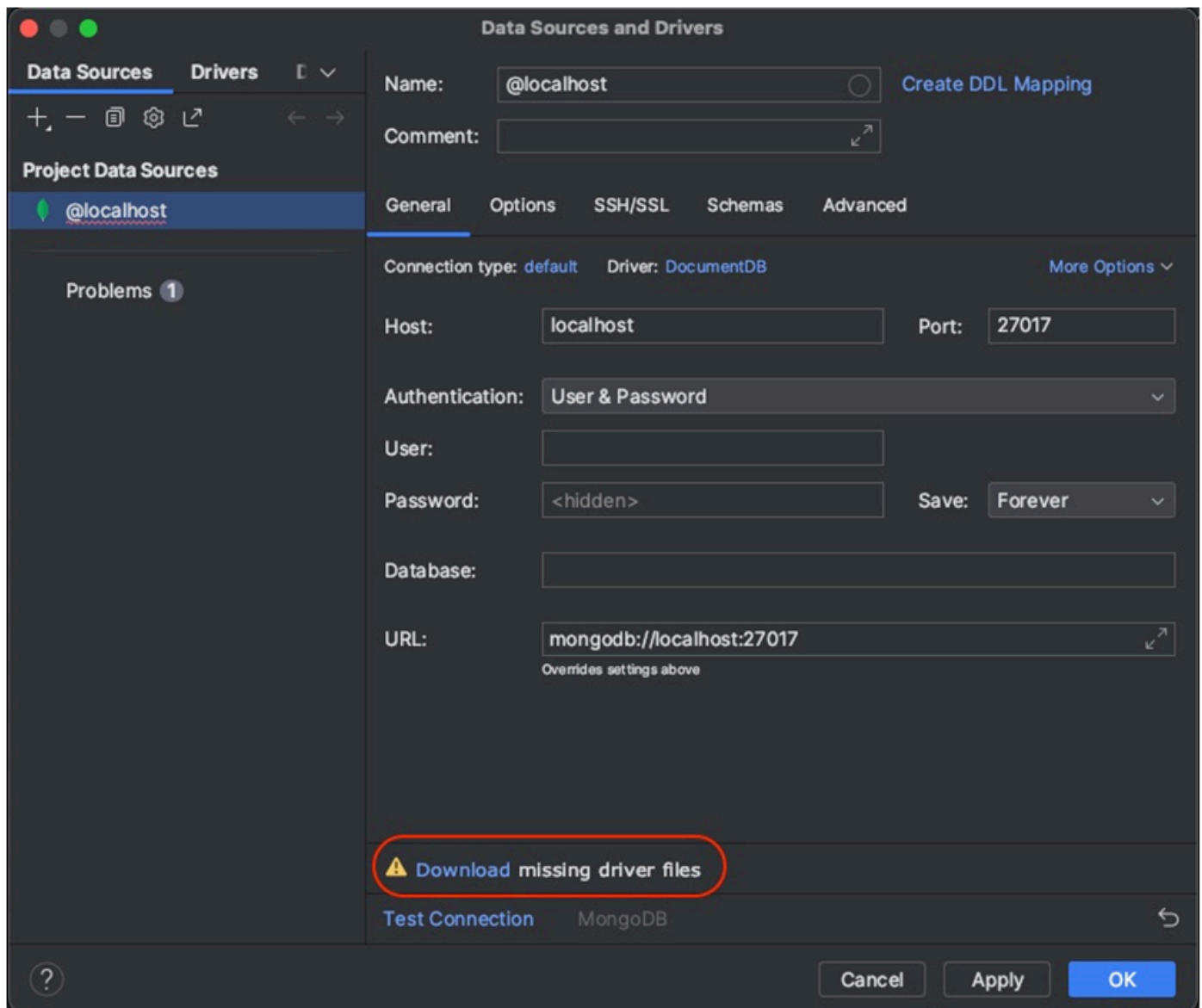


2. Aggiungi una nuova fonte di dati utilizzando uno dei seguenti modi:

- a. Dal menu principale, accedi a File — Nuovo — Origine dati e seleziona DocumentDB
- b. In Database Explorer, fate clic sulla nuova icona (+) nella barra degli strumenti. Vai a Data Source e seleziona DocumentDB.

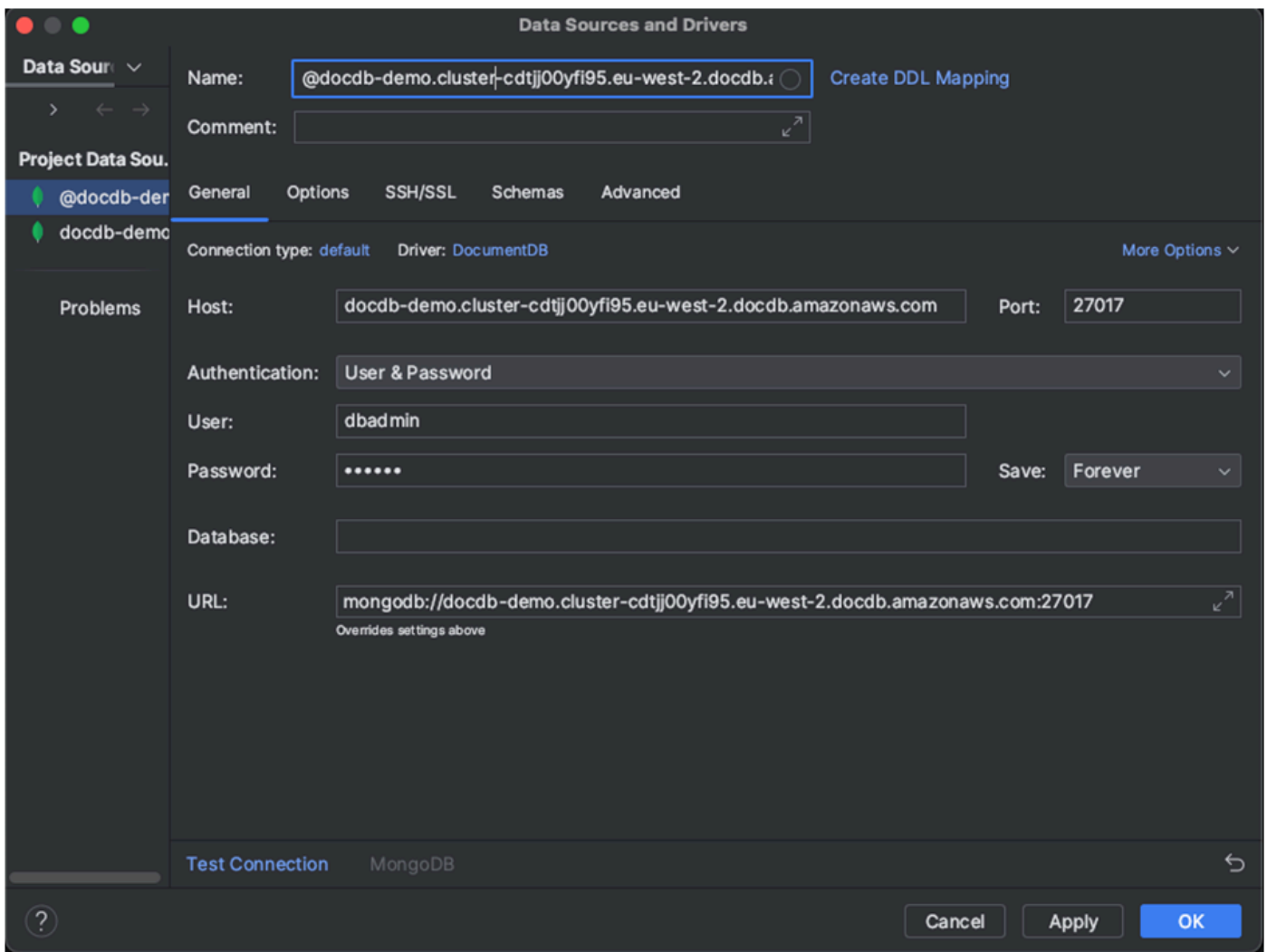


3. Nella pagina Fonti dati della scheda Generale, controlla se è presente il link Scarica i file dei driver mancanti nella parte inferiore dell'area delle impostazioni di connessione. Fai clic su questo link per scaricare i driver necessari per interagire con un database. Per un link per il download diretto, consulta i driver [JetBrains JDBC](#).



4. Nella scheda Generale, specifica i dettagli della connessione:

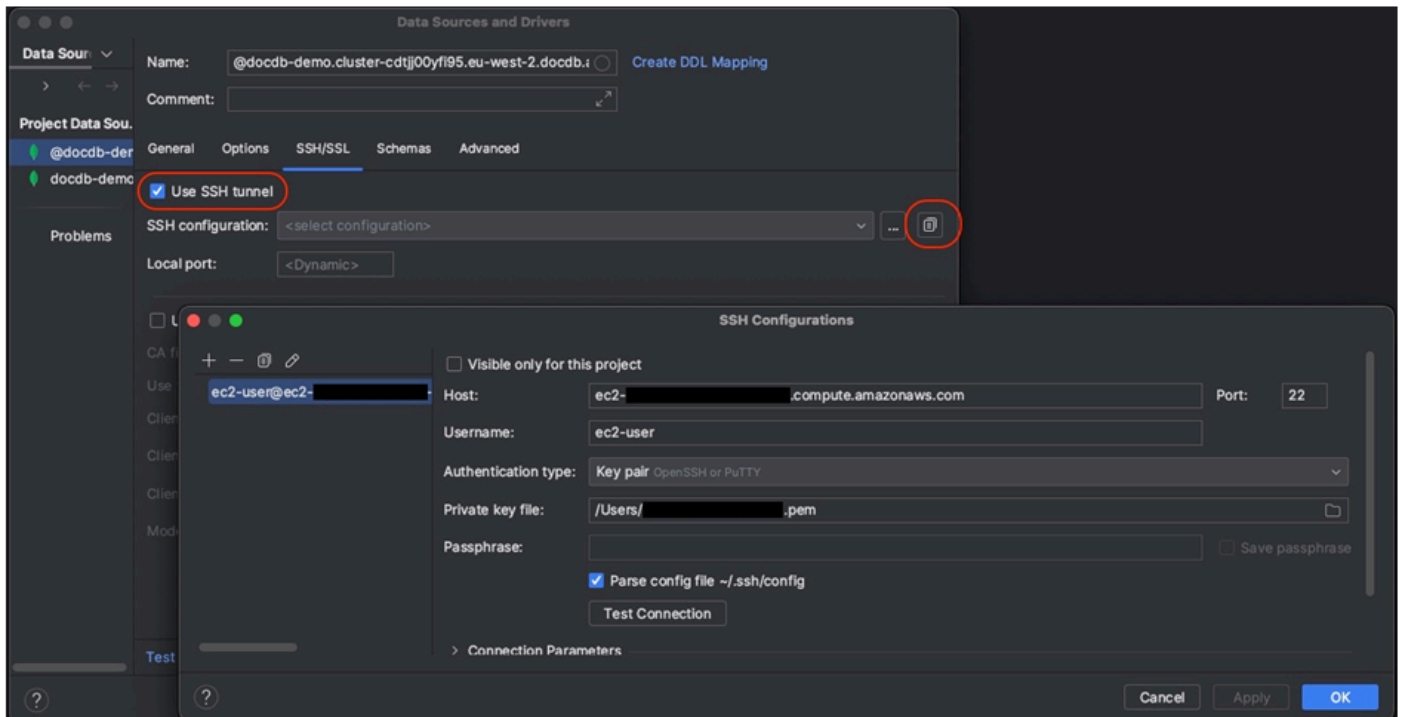
- a. Nel campo Host, specifica l'endpoint del cluster Amazon DocumentDB.
- b. La porta è già impostata su 27017. Modificala se il cluster è stato distribuito su una porta diversa.
- c. Per l'autenticazione, scegli Utente e password.
- d. Inserisci le informazioni relative al nome utente e alla password.
- e. Il campo Database è facoltativo. È possibile specificare il database a cui connettersi.
- f. Il campo URL viene completato automaticamente man mano che aggiungi i dettagli di cui sopra.



5. Nella scheda SSH/SSL, abilita Usa tunnel SSH, quindi fai clic sull'icona per aprire la finestra di dialogo di configurazione SSH. Immettere le seguenti informazioni:
 - a. nel campo Host, inserisci il nome host della tua istanza Amazon EC2.
 - b. Inserisci il nome utente e la password per la tua istanza Amazon EC2.
 - c. Per Tipo di autenticazione, scegli Coppia di chiavi.
 - d. Inserisci il tuo file di chiave privata.

Note

Se utilizzi l'opzione VPN, non è necessario configurare il tunnel SSH.



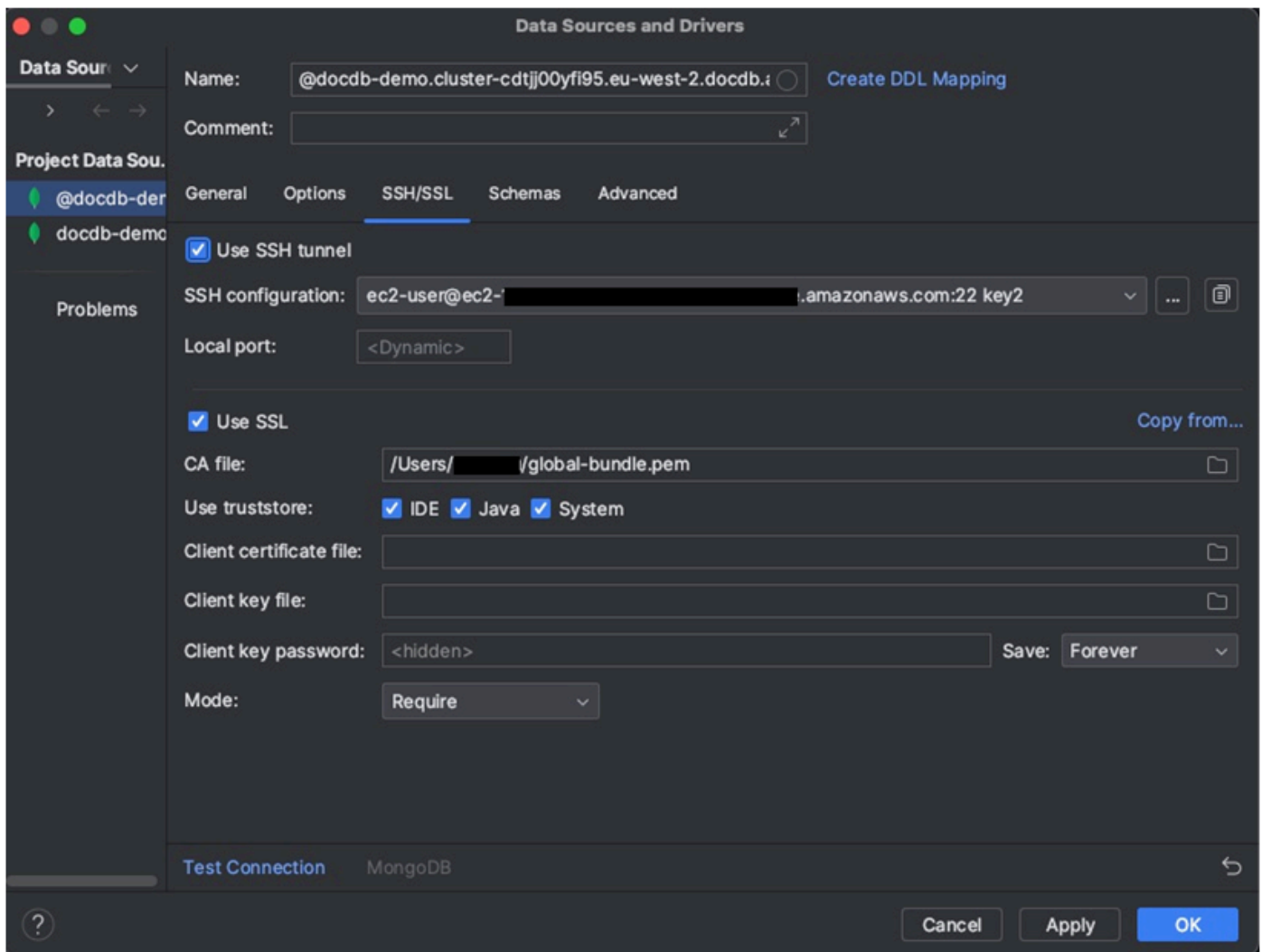
- Nella scheda SSH/SSL, abilita Usa SSL. Nel campo File CA, inserisci la posizione del file sul `global-bundle.pem` tuo computer. Per Mode, lascia l'opzione Richiedi.

Note

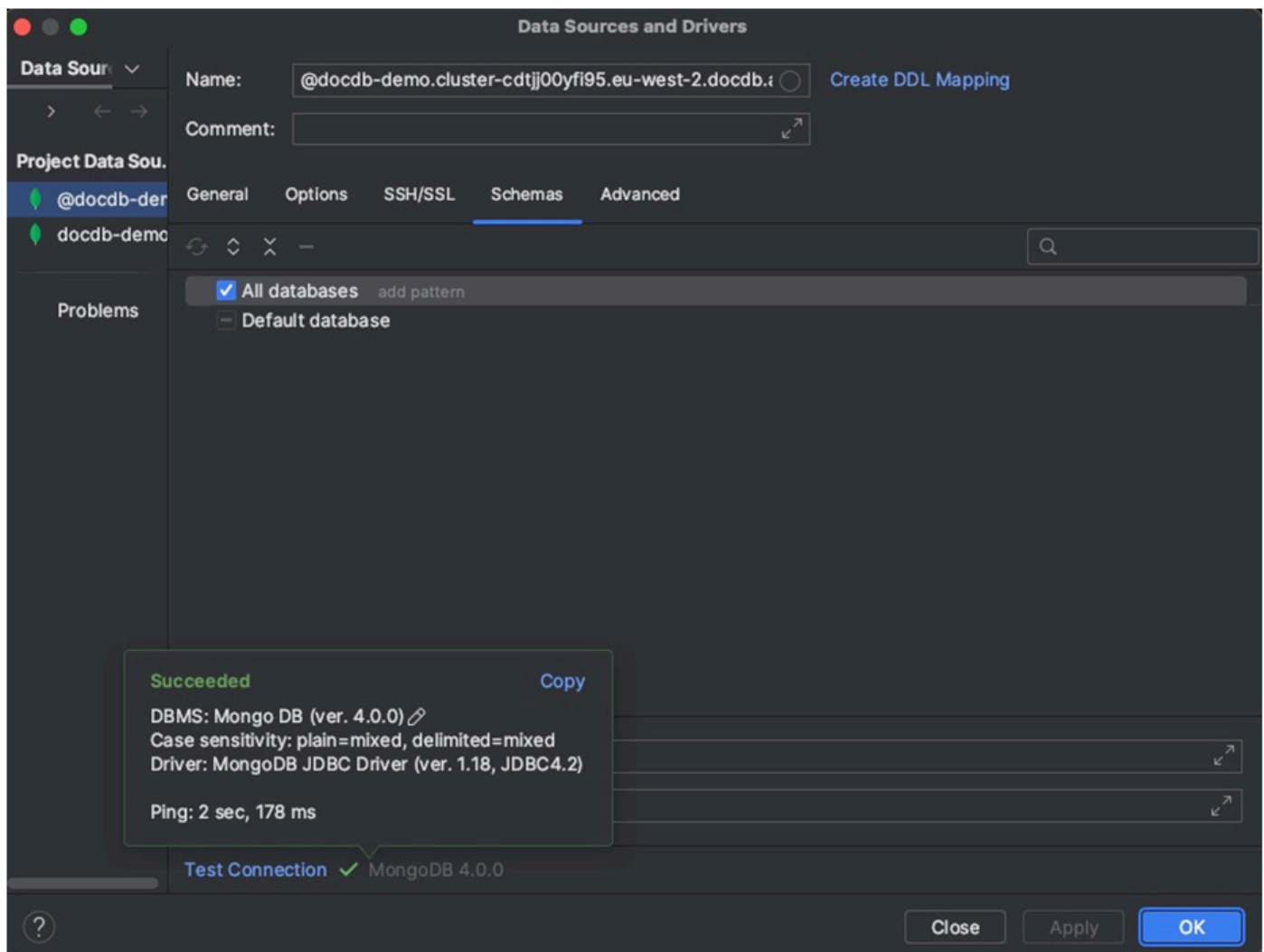
Puoi scaricare il certificato da questa posizione o con questo comando: `wget https://aws.amazon.com/https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem`

Note

Se ti connetti al cluster elastico di Amazon DocumentDB, non devi specificare il file CA. Lascia selezionata l'opzione Usa SSL e tutte le altre opzioni ai valori predefiniti.



7. Nella scheda Schemi, scegli Tutti i database o inserisci il filtro «*: *» nel campo Schema pattern. Fai clic sul link Test Connection per testare la connessione.



8. Una volta che la connessione è stata testata correttamente, fai clic su OK per salvare la configurazione dell'origine dati.

DataGrip caratteristiche

DataGrip offre diverse funzionalità per aiutarti a lavorare con Amazon DocumentDB in modo efficiente:

- SQL Editor: scrivi ed esegui query di tipo SQL sulle tue raccolte DocumentDB utilizzando l'editor SQL in DataGrip
- Visual Query Builder: utilizza il generatore di query visive per creare query graficamente senza scrivere codice SQL.

- **Gestione dello schema:** gestisci facilmente lo schema del tuo database, inclusa la creazione, la modifica e l'eliminazione delle raccolte.
- **Visualizzazione dei dati:** visualizza e analizza i dati utilizzando vari strumenti di visualizzazione disponibili in. DataGrip
- **Esportazione e importazione di dati:** trasferisci dati tra Amazon DocumentDB e altri database utilizzando le funzionalità DataGrip di esportazione e importazione di.

Consulta la [DataGrip documentazione](#) ufficiale per funzionalità e suggerimenti più avanzati su come lavorare con Amazon DocumentDB e altri sistemi di database.

Connect tramite Amazon EC2

Questa sezione descrive come configurare la connettività tra un cluster Amazon DocumentDB e Amazon EC2 e accedere al cluster Amazon DocumentDB dall'istanza Amazon EC2.

Esistono due opzioni per configurare la connessione EC2:

- [Connetti automaticamente la tua istanza EC2 a un database Amazon DocumentDB](#): utilizza la funzionalità di connessione automatica nella console EC2 per configurare automaticamente la connessione tra l'istanza EC2 e un database Amazon DocumentDB nuovo o esistente. Questa connessione consente al traffico di viaggiare tra l'istanza EC2 e il database Amazon DocumentDB. Questa opzione viene in genere utilizzata per testare e creare nuovi gruppi di sicurezza.
- [Connetti manualmente l'istanza EC2 al database Amazon DocumentDB](#): configura la connessione tra l'istanza EC2 e il database Amazon DocumentDB configurando e assegnando manualmente i gruppi di sicurezza per riprodurre la configurazione creata dalla funzionalità di connessione automatica. Questa opzione viene in genere utilizzata per modificare impostazioni più avanzate e utilizzare i gruppi di sicurezza esistenti.

Prerequisiti

Indipendentemente dall'opzione, e prima di creare il primo cluster Amazon DocumentDB, devi fare quanto segue:

Crea un account Amazon Web Services (AWS)

Prima di iniziare a utilizzare Amazon DocumentDB, devi disporre di un account Amazon Web Services (AWS). L' AWS account è gratuito. Paghi solo per i servizi e le risorse che utilizzi.

Se non ne possiedi uno Account AWS, completa i seguenti passaggi per crearne uno.

Per iscriverti a un Account AWS

1. Apri la pagina all'indirizzo <https://portal.aws.amazon.com/billing/signup>.
2. Segui le istruzioni online.

Nel corso della procedura di registrazione riceverai una telefonata, durante la quale sarà necessario inserire un codice di verifica attraverso la tastiera del telefono.

Quando ti iscrivi a un Account AWS, Utente root dell'account AWS viene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come best practice di sicurezza, [assegna l'accesso amministrativo a un utente amministrativo](#) e utilizza solo l'utente root per eseguire [attività che richiedono l'accesso di un utente root](#).

Facoltativamente, imposta le autorizzazioni necessarie AWS Identity and Access Management (IAM).

L'accesso alla gestione delle risorse di Amazon DocumentDB come cluster, istanze e gruppi di parametri del cluster richiede credenziali che AWS possono essere utilizzate per autenticare le richieste. Per ulteriori informazioni, consulta [Identity and Access Management per Amazon DocumentDB](#).

1. Nella barra di ricerca di AWS Management Console, digita IAM e seleziona IAM nel menu a discesa visualizzato.
2. Una volta che sei nella console IAM, seleziona Utenti dal pannello di navigazione.
3. Seleziona il tuo nome utente.
4. Fai clic sul pulsante Aggiungi autorizzazioni.
5. Seleziona Attach existing policies directly (Collega direttamente le policy esistenti).
6. Digita AmazonDocDBFullAccess nella barra di ricerca e selezionala quando appare nei risultati della ricerca.
7. Fai clic sul pulsante blu in basso che dice Avanti: revisione.
8. Fai clic sul pulsante blu in basso che dice Aggiungi autorizzazioni.

Crea un Amazon Virtual Private Cloud (Amazon VPC)

A seconda dell'ambiente in cui Regione AWS ti trovi, potresti avere o meno un VPC predefinito già creato. Se non disponi di un VPC predefinito, completa il passaggio 1 della [Guida introduttiva](#)

[ad Amazon VPC nella Amazon VPC User Guide](#). Questa operazione richiederà meno di cinque minuti.

Connect Amazon EC2 automaticamente

Argomenti

- [Connetti automaticamente un'istanza EC2 a un nuovo database Amazon DocumentDB](#)
- [Connetti automaticamente un'istanza EC2 a un database Amazon DocumentDB esistente](#)
- [Panoramica della connettività automatica con un'istanza EC2](#)
- [Visualizzazione delle risorse di calcolo connesse](#)

Prima di configurare una connessione tra un'istanza EC2 e un nuovo database Amazon DocumentDB, assicurati di soddisfare i requisiti descritti in [Panoramica della connettività automatica con un'istanza EC2](#). Se apporti modifiche ai gruppi di sicurezza dopo aver configurato la connettività, le modifiche potrebbero influire sulla connessione tra l'istanza EC2 e il database Amazon DocumentDB.

Note

Puoi configurare automaticamente una connessione tra un'istanza EC2 e un database Amazon DocumentDB solo utilizzando l'AWS Management Console. Non puoi configurare automaticamente una connessione con l'API AWS CLI o Amazon DocumentDB.

Connetti automaticamente un'istanza EC2 a un nuovo database Amazon DocumentDB

Il processo seguente presuppone che tu abbia completato i passaggi indicati nell'[Prerequisiti](#) argomento.

Fasi

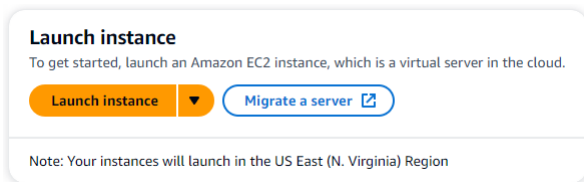
- [Fase 1: creare un'istanza Amazon EC2](#)
- [Fase 2: creare un cluster Amazon DocumentDB](#)
- [Fase 3: Connettiti alla tua istanza Amazon EC2](#)
- [Passaggio 4: installa la shell mongo](#)
- [Fase 5: Gestione del TLS di Amazon DocumentDB](#)

- [Fase 6: Connettiti al tuo cluster Amazon DocumentDB](#)
- [Fase 7: Inserimento e interrogazione dei dati](#)
- [Fase 8: Esplora](#)

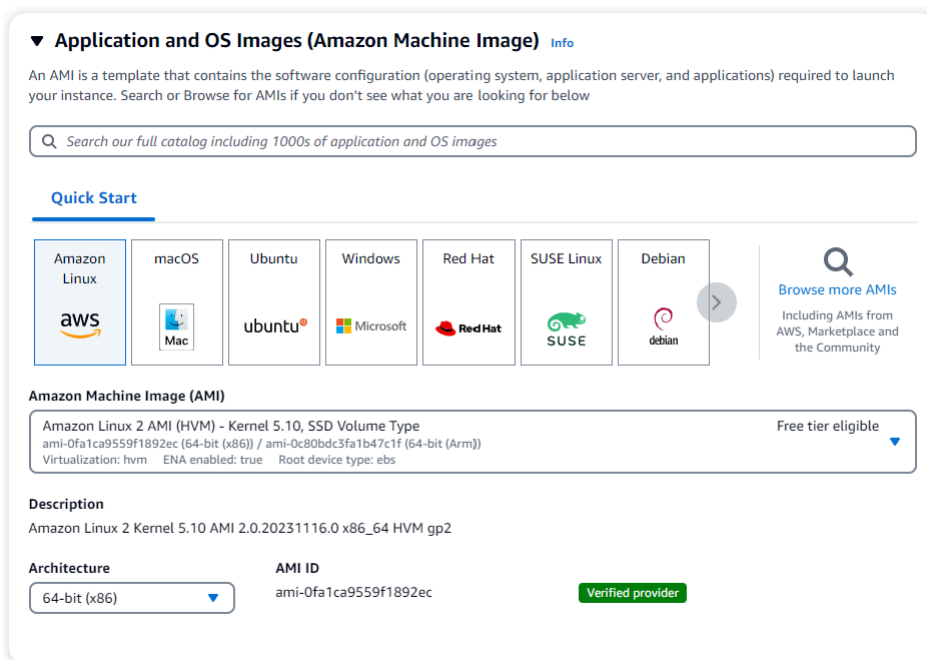
Fase 1: creare un'istanza Amazon EC2

In questa fase, creerai un'istanza Amazon EC2 nella stessa regione e Amazon VPC che utilizzerai successivamente per il provisioning del tuo cluster Amazon DocumentDB.

1. Sulla console Amazon EC2, scegli Launch instance.



2. Inserisci un nome o un identificatore nel campo Nome situato nella sezione Nome e tag.
3. Nell'elenco a discesa Amazon Machine Image (AMI), individua l'AMI Amazon Linux 2 e selezionala.



4. Individua e scegli t3.micro nell'elenco a discesa del tipo di istanza.

▼ Instance type [Info](#) | [Get advice](#)

Instance type

t3.micro
Family: t3 2 vCPU 1 GiB Memory Current generation: true
On-Demand SUSE base pricing: 0.0104 USD per Hour On-Demand Linux base pricing: 0.0104 USD per Hour
On-Demand RHEL base pricing: 0.0704 USD per Hour On-Demand Windows base pricing: 0.0196 USD per Hour

All generations [Compare instance types](#)

Additional costs apply for AMIs with pre-installed software

5. Nella sezione Key pair (login), inserisci l'identificatore di una coppia di chiavi esistente o scegli Crea nuova coppia di chiavi.

▼ Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

Select [Create new key pair](#)

È necessario fornire una coppia di chiavi Amazon EC2.

Se disponi di una coppia di chiavi Amazon EC2:

- Seleziona una coppia di chiavi, scegli la tua coppia di chiavi dall'elenco.
- Devi già avere il file della chiave privata (file.pem o .ppk) disponibile per accedere alla tua istanza Amazon EC2.

Se non disponi di una coppia di chiavi Amazon EC2:

- Scegli Crea nuova coppia di chiavi, viene visualizzata la finestra di dialogo Crea coppia di chiavi.
- Inserisci un nome nel campo Nome della coppia di chiavi.
- Scegli il tipo di coppia di chiavi e il formato del file della chiave privata.
- Scegliere Create key pair (Crea coppia di chiavi).

Create key pair ✕

Key pair name
Key pairs allow you to connect to your instance securely.

The name can include upto 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type


RSA
RSA encrypted private and public key pair

ED25519
ED25519 encrypted private and public key pair

Private key file format

.pem
For use with OpenSSH

.ppk
For use with PuTTY

⚠ When prompted, store the private key in a secure and accessible location on your computer. **You will need it later to connect to your instance.** [Learn more](#) 

[Cancel](#) [Create key pair](#)

i Note

Per motivi di sicurezza, consigliamo vivamente di utilizzare una coppia di chiavi per la connettività SSH e Internet all'istanza EC2.

6. Facoltativo: nella sezione Impostazioni di rete, in Firewall (gruppi di sicurezza), scegli Crea gruppo di sicurezza o Seleziona gruppo di sicurezza esistente.

▼ Network settings [Info](#) Edit

Network [Info](#)
vpc-02c0445657b77542c

Subnet [Info](#)
No preference (Default subnet in any availability zone)

Auto-assign public IP [Info](#)
Enable

Firewall (security groups) [Info](#)
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group
 Select existing security group

We'll create a new security group called 'launch-wizard-1' with the following rules:

Allow SSH traffic from Helps you connect to your instance Anywhere
0.0.0.0/0

Allow HTTPS traffic from the internet To set up an endpoint, for example when creating a web server

Allow HTTP traffic from the internet To set up an endpoint, for example when creating a web server

⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only. ×

Se hai scelto di selezionare un gruppo di sicurezza esistente, selezionane uno dall'elenco a discesa Gruppi di sicurezza comuni.

Se hai scelto di creare un nuovo gruppo di sicurezza, controlla tutte le regole di autorizzazione al traffico che si applicano alla tua connettività EC2.

7. Nella sezione Riepilogo, esamina la configurazione EC2 e scegli Launch instance, se corretta. Modifica i gruppi di sicurezza.

▼ Summary

Number of instances [Info](#)
1

Software Image (AMI)
Amazon Linux 2 Kernel 5.10 AMI...[read more](#)
ami-0fa1ca9559f1892ec

Virtual server type (instance type)
t3.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 8 GiB

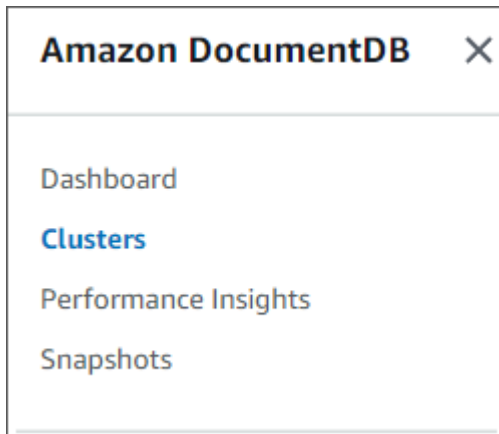
ⓘ **Free tier:** In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet. ×

[Review commands](#)
[Cancel](#)
[Launch instance](#)

Fase 2: creare un cluster Amazon DocumentDB

Durante il provisioning dell'istanza Amazon EC2, creerai il tuo cluster Amazon DocumentDB.

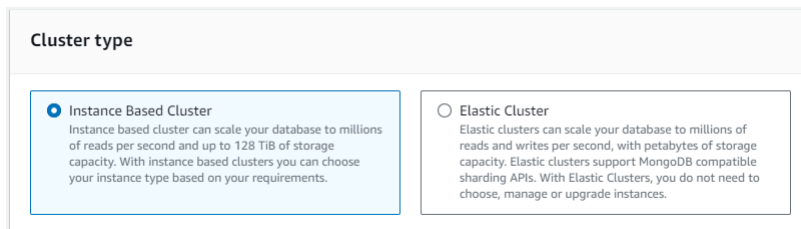
1. Accedi alla console Amazon DocumentDB e scegli Clusters dal pannello di navigazione.



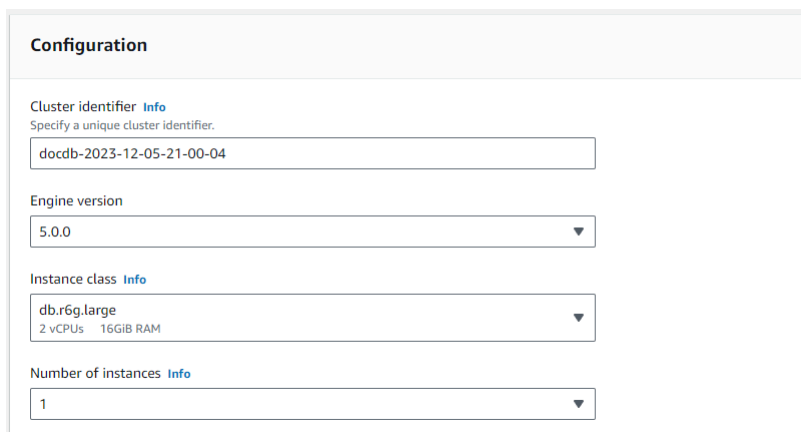
2. Scegli Crea.



3. Lascia l'impostazione del tipo di cluster sull'impostazione predefinita di Instance Based Cluster.



4. Per Numero di istanze, scegli 1. Ciò ridurrà al minimo i costi. Lascia le altre impostazioni ai valori predefiniti.



5. Per Connettività, scegli Connetti a una risorsa di calcolo EC2. Questa è l'istanza EC2 che hai creato nella Fase 1.

Connectivity ↻

Compute resources
Choose whether to set up a connection to a compute resource for this database. Setting up a connection will automatically change connectivity settings so that the compute resource can connect to this database.

Connect to an EC2 compute resource
Set up a connection to an EC2 compute resource for this database.

Don't connect to an EC2 compute resource
Don't set up a connection to a compute resource for this database.

EC2 Instance
Choose the EC2 instance to add as the compute resource for this database. A VPC security group is added to this EC2 instance. A VPC security group is also added to the database with an inbound rule that allows the EC2 instance to access the database.

i After a database is created, you can't change its VPC.

i Note

La connessione a una risorsa di calcolo EC2 crea automaticamente un gruppo di sicurezza per la connessione delle risorse di calcolo EC2 al cluster Amazon DocumentDB. Una volta completata la creazione del cluster e desideri visualizzare il gruppo di sicurezza appena creato, vai all'elenco dei cluster e scegli l'identificatore del cluster. Nella scheda Connettività e sicurezza, vai a Gruppi di sicurezza e trova il tuo gruppo in Nome del gruppo di sicurezza (ID). Conterrà il nome del tuo cluster e avrà un aspetto simile a questo: docdb-ec2-docdb-2023-12-11-21-33-41 : i-0e4bb09985d2bbc4c (sg-0238e0b0bf0f73877).

- Per l'autenticazione, inserisci le credenziali di accesso. Importante: ti serviranno le credenziali di accesso per autenticare il cluster in un passaggio successivo.

Authentication

Username Info
Specify an alphanumeric string that defines the login ID for the user.

Username must start with a letter and contain 1 to 63 characters

Password Info **Confirm password** Info

Password must be at least eight characters long and cannot contain a / (slash), " (double quote) or @ (at symbol).

- Attiva Mostra impostazioni avanzate.

i **The estimated hourly cost for 1 db.r6g.large instance(s) is \$0.29/hr.**
With Amazon DocumentDB you are charged for instances, storage, IOPS, backups, and data transfer. Please see our [pricing page](#) and [cost optimization documentation](#) for more information.

Show advanced settings
Cancel
Create cluster

- Nella sezione Impostazioni di rete, per i gruppi di sicurezza Amazon VPC, scegli DemoDocDB.

Network settings

Virtual Private Cloud (VPC) [Info](#)
VPC defines the virtual networking environment for this cluster.

Only VPCs with a corresponding subnet group are listed. Once a cluster is created, the VPC cannot be changed.

Subnet group [Info](#)
A subnet group is a collection of subnets that are within a VPC.

VPC security groups
A security group acts as a virtual firewall for your instance to control inbound and outbound traffic.

- Scegli Create cluster (Crea cluster).

Create cluster

Fase 3: Connettiti alla tua istanza Amazon EC2

Per installare la shell mongo, devi prima connetterti alla tua istanza Amazon EC2. L'installazione della mongo shell ti consente di connetterti e interrogare il tuo cluster Amazon DocumentDB. Completa questa procedura:

- Sulla console Amazon EC2, accedi alle tue istanze e verifica se l'istanza che hai appena creato è in esecuzione. In caso affermativo, seleziona l'istanza facendo clic sull'ID dell'istanza.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
aws-cloud9-D...	i-0413cea24ed66b250	Stopped	t2.micro	-	No alarms	us-east-1c
Sample Server	i-0e4bb09985d2bbc4c	Running	t3.micro	2/2 checks passed	No alarms	us-east-1a

- Scegli Connetti.

Instance summary for i-0e4bb09985d2bbc4c (Sample Server) Info

Updated less than a minute ago

Refresh
Connect
Instance state ▼
Actions ▼

<p>Instance ID i-0e4bb09985d2bbc4c (Sample Server)</p> <p>IPV6 address -</p> <p>Hostname type IP name: ip-172-31-41-131.ec2.internal</p> <p>Answer private resource DNS name IPv4 (A)</p> <p>Auto-assigned IP address 54.87.99.44 [Public IP]</p> <p>IAM Role -</p> <p>IMDSv2 Required</p>	<p>Public IPv4 address 54.87.99.44 open address</p> <p>Instance state ● Running</p> <p>Private IP DNS name (IPv4 only) ip-172-31-41-131.ec2.internal</p> <p>Instance type t3.micro</p> <p>VPC ID vpc-02c0445657b77542c</p> <p>Subnet ID subnet-06676048a6487a578</p>	<p>Private IPv4 addresses 172.31.41.131</p> <p>Public IPv4 DNS ec2-54-87-99-44.compute-1.amazonaws.com open address</p> <p>Elastic IP addresses -</p> <p>AWS Compute Optimizer finding No recommendations available for this instance.</p> <p>Auto Scaling Group name -</p>
---	---	--

3. Esistono quattro opzioni a schede per il metodo di connessione: Amazon EC2 Instance Connect, Session Manager, client SSH o console seriale EC2. Devi sceglierne una e seguirne le istruzioni. Al termine, scegli Connect.

EC2 Instance Connect
Session Manager
SSH client
EC2 serial console

Instance ID
i-0e4bb09985d2bbc4c (Sample Server)

Connection Type

Connect using EC2 Instance Connect
Connect using the EC2 Instance Connect browser-based client, with a public IPv4 address.

Connect using EC2 Instance Connect Endpoint
Connect using the EC2 Instance Connect browser-based client, with a private IPv4 address and a VPC endpoint.

Public IP address
54.87.99.44

User name
Enter the user name defined in the AMI used to launch the instance. If you didn't define a custom user name, use the default user name, ec2-user.

Note: In most cases, the default user name, ec2-user, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.

i Note

Se l'indirizzo IP è cambiato dopo aver iniziato questa procedura dettagliata o se si torna all'ambiente in un secondo momento, è necessario aggiornare la regola in entrata del gruppo di demoEC2 sicurezza per abilitare il traffico in entrata dal nuovo indirizzo API.

Passaggio 4: installa la shell mongo

Ora puoi installare la mongo shell, un'utilità da riga di comando che usi per connettere e interrogare il tuo cluster Amazon DocumentDB. Segui le istruzioni riportate di seguito per installare la shell mongo per il tuo sistema operativo.

On Amazon Linux

Per installare la shell Mongo in Amazon Linux

1. Crea il file del repository. Nella riga di comando dell'istanza EC2, esegui il seguente comando:

```
echo -e "[mongodb-org-5.0] \nname=MongoDB Repository\nbaseurl=https://\nrepo.mongodb.org/yum/amazon/2/mongodb-org/5.0/x86_64/\nngpgcheck=1 \nenabled=1\nngpgkey=https://www.mongodb.org/static/pgp/server-5.0.asc" | sudo tee /etc/\nyum.repos.d/mongodb-org-5.0.repo
```

2. Al termine, installa la shell mongo eseguendo il seguente comando:

```
sudo yum install -y mongodb-org-shell
```

On Ubuntu 18.04

Per installare la shell Mongo in Ubuntu 18.04

1. Importa la chiave pubblica che verrà utilizzata dal sistema di gestione dei pacchetti.

```
sudo apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv\n2930ADAE8CAF5059EE73BB4B58712A2291FA4AD5
```

2. Crea l'elenco di file `/etc/apt/sources.list.d/mongodb-org-3.6.list` per MongoDB utilizzando il comando appropriato per la versione di Ubuntu.

Ubuntu 18.04

```
echo "deb [ arch=amd64,arm64 ] https://repo.mongodb.org/apt/ubuntu xenial/\nmongodb-org/3.6 multiverse" | sudo tee /etc/apt/sources.list.d/mongodb-\norg-3.6.list
```

Note

Il comando precedente installerà la shell mongo 3.6 per Bionic e Xenial.

3. Ricarica il database del pacchetto locale utilizzando il comando seguente:

```
sudo apt-get update
```

4. Installa la shell MongoDB.

```
sudo apt-get install -y mongodb-org-shell
```

Per informazioni sull'installazione di versioni precedenti di MongoDB nel sistema Ubuntu, consulta [Installazione di MongoDB Community Edition in Ubuntu](#).

On other operating systems

Per installare la shell Mongo in altri sistemi operativi, vedi l'argomento relativo all'[installazione di MongoDB Community Edition](#) nella documentazione relativa a MongoDB.

Fase 5: Gestione del TLS di Amazon DocumentDB

Scarica il certificato CA per Amazon DocumentDB con il seguente codice: `wget https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem`

Note

Transport Layer Security (TLS) è abilitato di default per tutti i nuovi cluster Amazon DocumentDB. Per ulteriori informazioni, consulta [Gestione delle impostazioni TLS del cluster Amazon DocumentDB](#).

Fase 6: Connettiti al tuo cluster Amazon DocumentDB

1. Nella console Amazon DocumentDB, in Clusters, individua il cluster. Scegli il cluster che hai creato facendo clic sull'identificatore del cluster.

Cluster identifier	Role	Engine version	Region & AZ	Status
docdb-2023-12-06-13-47-11	Regional cluster	5.0.0	us-east-1	available
docdb-2023-12-06-13-47-11	Primary instance	5.0.0	us-east-1a	available

2. Nella scheda Connettività e sicurezza, individua Connect to this cluster with the mongo shell nella casella Connect:

Connect

Getting Started Guide | Enabling/Disabling TLS | Connecting programmatically

Download the Amazon DocumentDB Certificate Authority (CA) certificate required to authenticate to your cluster [Copy](#)

```
wget https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem
```

Connect to this cluster with the mongo shell [Copy](#)

```
mongo --ssl --host docdb-2023-12-06-13-47-11.cluster-cozt4xr9xv9b.us-east-1.docdb.amazonaws.com:27017 --sslCAFile global-bundle.pem --username sampleUser --password <insertYourPassword>
```

Connect to this cluster with an application [Copy](#)

```
mongodb://sampleUser:<insertYourPassword>@docdb-2023-12-06-13-47-11.cluster-cozt4xr9xv9b.us-east-1.docdb.amazonaws.com:27017/?tls=true&tlsCAFile=global-bundle.pem&replicaSet=rs0&readPreference=secondaryPreferred&retryWrites=false
```

Copia la stringa di connessione fornita e incollala nel tuo terminale.

Apporta le seguenti modifiche:

- Assicurati di avere il nome utente corretto nella stringa.
- Ometti `<insertYourPassword>` in modo che ti venga richiesta la password dalla shell mongo quando ti connetti.

La stringa di connessione dovrebbe essere simile alla seguente:

```
mongo --ssl host docdb-2020-02-08-14-15-11.  
cluster.region.docdb.amazonaws.com:27107 --sslCAFile global-bundle.pem  
--username demoUser --password
```

3. Premi invio nel tuo terminale. Ora ti verrà richiesta la password. Inserisci la password.
4. Quando inserisci la password e riesci a visualizzare il `rs0:PRIMARY>` prompt, sei connesso correttamente al tuo cluster Amazon DocumentDB.

Hai problemi di connessione? Vedi [Risoluzione dei problemi di Amazon DocumentDB](#).

Fase 7: Inserimento e interrogazione dei dati

Ora che sei connesso al cluster, puoi eseguire alcune query per acquisire familiarità con l'utilizzo di un database di documenti.

1. Per inserire un singolo documento, inserisci quanto segue:

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

2. Otterrete il seguente risultato:

```
WriteResult({ "nInserted" : 1 })
```

3. Puoi leggere il documento che hai scritto con il `findOne()` comando (perché restituisce solo un singolo documento). Inserisci quanto segue:

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

4. Si ottiene il seguente risultato:

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

5. Per eseguire qualche altra domanda, considera un caso d'uso dei profili di gioco. Innanzitutto, inserisci alcune voci in una raccolta intitolata `profiles`. Inserisci quanto segue:

```
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}
  ])
```

6. Si ottiene il seguente risultato:

```
{ "acknowledged" : true, "insertedIds" : [ 1, 2, 3, 4 ] }
```

7. Utilizzate il `find()` comando per restituire tutti i documenti nella raccolta dei profili. Inserisci quanto segue:

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

8. Otterrai un output che corrisponderà ai dati che hai digitato nel passaggio 5.

9. Usa una query per un singolo documento usando un filtro. Inserisci quanto segue:

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

10. Dovresti recuperare questo risultato:

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

11. Ora proviamo a trovare un profilo e modificarlo usando il `findAndModify` comando. Daremo all'utente Matt altri dieci punti con il seguente codice:

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

12. Otterrete il seguente risultato (notate che il suo punteggio non è ancora aumentato):

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

```
"score" : 202
}
```

13. Puoi verificare che il suo punteggio sia cambiato con la seguente domanda:

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

14. Si ottiene il seguente risultato:

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

Fase 8: Esplora

Complimenti! Hai completato con successo la Guida rapida ad Amazon DocumentDB.

Qual è il prossimo passo? Scopri come sfruttare appieno questo potente database con alcune delle sue funzionalità più popolari:

- [Gestione di Amazon DocumentDB](#)
- [Dimensionamento](#)
- [Backup e ripristino](#)

Note

Per risparmiare sui costi, puoi interrompere il cluster Amazon DocumentDB per ridurre i costi o eliminare il cluster. Per impostazione predefinita, dopo 30 minuti di inattività, l' AWS Cloud9 ambiente interromperà l'istanza Amazon EC2 sottostante.

Connetti automaticamente un'istanza EC2 a un database Amazon DocumentDB esistente

La procedura seguente presuppone che tu abbia un cluster Amazon DocumentDB esistente e un'istanza Amazon EC2 esistente.

Accedi al tuo cluster Amazon DocumentDB e configura la connessione Amazon EC2

1. Accedi al tuo cluster Amazon DocumentDB.

- a. [Accedi a e apri AWS Management Console la console Amazon DocumentDB all'indirizzo https://console.aws.amazon.com/docdb](https://console.aws.amazon.com/docdb).
- b. Nel pannello di navigazione scegliere Clusters (Cluster).

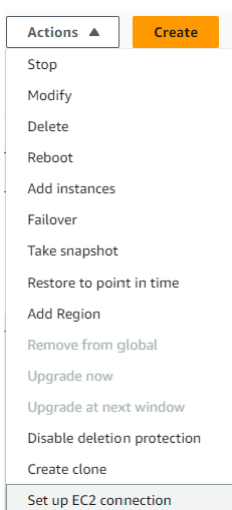
 Tip

Se il riquadro di navigazione non viene visualizzato sul lato sinistro della schermata, scegliere l'icona del menu (☰) nell'angolo in alto a sinistra della pagina.

- c. Specificate il cluster che desiderate scegliendo il pulsante a sinistra del nome del cluster.

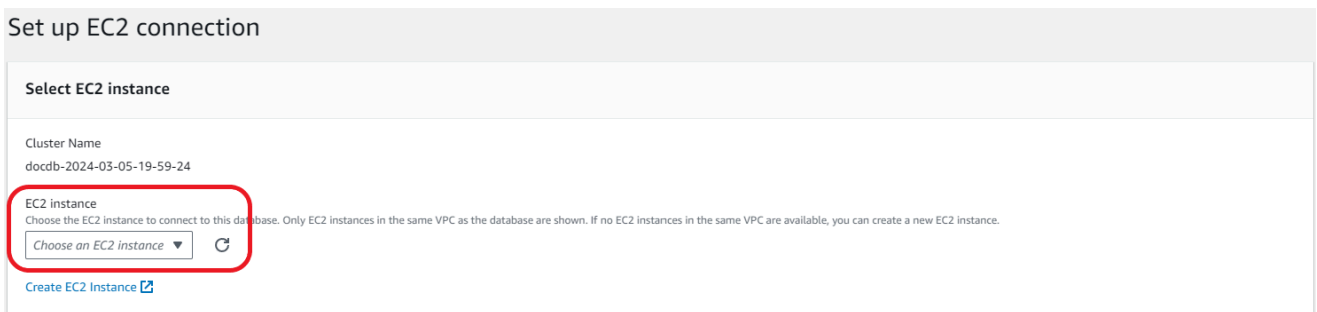
2. Configura la connessione Amazon EC2.

- a. Scegli Azioni, quindi scegli Configura connessione EC2.



Viene visualizzata la finestra di dialogo Configura connessione EC2.

- b. Nel campo dell'istanza EC2, scegli l'istanza EC2 che desideri connettere al tuo cluster.



c. Scegli Continua.

Viene visualizzata la finestra di dialogo Rivedi e conferma.

d. Assicurati che le modifiche siano corrette. Quindi scegli Configura connessione.

Review and confirm

Connection summary

You are setting up a connection between DocumentDB database docdb-2024-03-05-19-59-24 and EC2 instance i-0413cea24ed66b250

To set up a connection between the database and the EC2 instance, VPC security group docdb-ec2-docdb-2024-03-05-19-59-24:i-0413cea24ed66b250 is added to the DocumentDB cluster, and VPC security group ec2-docdb-docdb-2024-03-05-19-59-24:i-0413cea24ed66b250 is added to the EC2 instance.

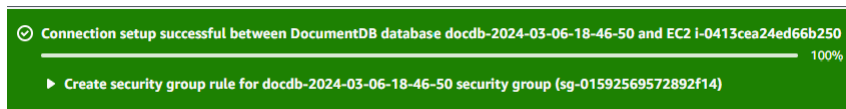
Changes to EC2 instance: i-0413cea24ed66b250

Attribute	Current value	New value
Security groups	aws-cloud9-DocumentDBCloud9-9c5f0bc9ff074715afd9d3e4fb7d6fba-InstanceSecurityGroup-1URT6OYVALT77	aws-cloud9-DocumentDBCloud9-9c5f0bc9ff074715afd9d3e4fb7d6fba-InstanceSecu

Changes to DocumentDB cluster: docdb-2024-03-05-19-59-24

Attribute	Current value	New value
Security groups	sg-021d234a0a3a2c2fe	sg-021d234a0a3a2c2fe, docdb-ec2-docdb-2024-03-05-19-59-24:i-0413cea24ed66b250

In caso di successo, viene visualizzata la seguente verifica:



Panoramica della connettività automatica con un'istanza EC2

Quando configuri una connessione tra un'istanza EC2 e un database Amazon DocumentDB, Amazon DocumentDB configura automaticamente il gruppo di sicurezza VPC per l'istanza EC2 e per il database Amazon DocumentDB.

Di seguito sono riportati i requisiti per connettere un'istanza EC2 con un database Amazon DocumentDB:

- L'istanza EC2 deve esistere nello stesso VPC del database Amazon DocumentDB.

Se nello stesso VPC non esistono istanze EC2, allora la console fornisce un collegamento per crearne una.

- L'utente che configura la connettività deve disporre delle autorizzazioni per eseguire le seguenti operazioni Amazon EC2:

- `ec2:AuthorizeSecurityGroupEgress`
- `ec2:AuthorizeSecurityGroupIngress`
- `ec2:CreateSecurityGroup`
- `ec2:DescribeInstances`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeSecurityGroups`
- `ec2:ModifyNetworkInterfaceAttribute`
- `ec2:RevokeSecurityGroupEgress`

Se l'istanza database e l'istanza EC2 si trovano in zone di disponibilità diverse, è possibile che all'account vengano addebitati costi tra zone di disponibilità.

Quando configuri una connessione a un'istanza EC2, Amazon DocumentDB agisce in base alla configurazione corrente dei gruppi di sicurezza associati al database Amazon DocumentDB e all'istanza EC2, come descritto nella tabella seguente:

Configurazione attuale del gruppo di sicurezza di Amazon DocumentDB	Configurazione del gruppo di sicurezza EC2 corrente	Azione di Amazon DocumentDB
Esistono uno o più gruppi di sicurezza associati al database Amazon DocumentDB con un nome che corrisponde al modello. DocumentDB-ec2-n Un gruppo di sicurezza che corrisponde al modello non è stato modificato. Questo gruppo di sicurezza include una sola regola in uscita con il gruppo di sicurezza VPC dell'istanza EC2 come origine.	Esistono uno o più gruppi di sicurezza associati all'istanza EC2 con un nome che corrisponde al modello DocumentDB-ec2-n (dove n è un numero). Un gruppo di sicurezza che corrisponde al modello non è stato modificato. Questo gruppo di sicurezza ha una sola regola in uscita con il gruppo di sicurezza VPC del database Amazon DocumentDB come origine.	Amazon DocumentDB non intraprende alcuna azione. Era già stata configurata automaticamente una connessione tra l'istanza EC2 e il database Amazon DocumentDB. Poiché esiste già una connessione tra l'istanza EC2 e il database Amazon DocumentDB, i gruppi di sicurezza non vengono modificati.

Configurazione attuale del gruppo di sicurezza di Amazon DocumentDB	Configurazione del gruppo di sicurezza EC2 corrente	Azione di Amazon DocumentDB
<p>Si applica una delle due condizioni seguenti:</p> <ul style="list-style-type: none"> • Non esiste un gruppo di sicurezza associato al database Amazon DocumentDB con un nome che corrisponda al modello. DocumentDB-ec2-n • Esistono uno o più gruppi di sicurezza associati ad Amazon DocumentDB con un nome che corrisponde al modello. DocumentDB-ec2-n Tuttavia, Amazon DocumentDB non può utilizzare nessuno di questi gruppi di sicurezza per la connessione con l'istanza EC2. Amazon DocumentDB non può utilizzare un gruppo di sicurezza che non ha una regola in entrata con il gruppo di sicurezza VPC dell'istanza EC2 come origine. Amazon DocumentDB inoltre non può utilizzare un gruppo di sicurezza che è stato modificato. Esempi di modifiche sono l'aggiunta di una regola o la modifica 	<p>Si applica una delle due condizioni seguenti:</p> <ul style="list-style-type: none"> • Non esiste un gruppo di sicurezza associato all'istanza EC2 con un nome che corrisponde al modello ec2-DocumentDB-n . • Esistono uno o più gruppi di sicurezza associati all'istanza EC2 con un nome che corrisponde al modello ec2-DocumentDB-n. Tuttavia, Amazon DocumentDB non può utilizzare nessuno di questi gruppi di sicurezza per la connessione con il database Amazon DocumentDB. Amazon DocumentDB non può utilizzare un gruppo di sicurezza che non ha una regola in uscita con il gruppo di sicurezza VPC del database Amazon DocumentDB come origine. Amazon DocumentDB inoltre non può utilizzare un gruppo di sicurezza che è stato modificato. 	<p>Azione Amazon DocumentDB: creazione di nuovi gruppi di sicurezza</p>

Configurazione attuale del gruppo di sicurezza di Amazon DocumentDB	Configurazione del gruppo di sicurezza EC2 corrente	Azione di Amazon DocumentDB
della porta di una regola esistente.		
<p>Esistono uno o più gruppi di sicurezza associati al database Amazon DocumentDB con un nome che corrisponde al modello. DocumentDB-ec2-n Un gruppo di sicurezza che corrisponde al modello non è stato modificato. Questo gruppo di sicurezza include una sola regola in uscita con il gruppo di sicurezza VPC dell'istanza EC2 come origine.</p>	<p>Esistono uno o più gruppi di sicurezza associati all'istanza EC2 con un nome che corrisponde al modello ec2-DocumentDB-n . Tuttavia, Amazon DocumentDB non può utilizzare nessuno di questi gruppi di sicurezza per la connessione con il database Amazon DocumentDB. Amazon DocumentDB non può utilizzare un gruppo di sicurezza che non ha una regola in uscita con il gruppo di sicurezza VPC del database Amazon DocumentDB come origine. Amazon DocumentDB inoltre non può utilizzare un gruppo di sicurezza che è stato modificato.</p>	<p>Azione Amazon DocumentDB: creazione di nuovi gruppi di sicurezza</p>

Configurazione attuale del gruppo di sicurezza di Amazon DocumentDB	Configurazione del gruppo di sicurezza EC2 corrente	Azione di Amazon DocumentDB
Esistono uno o più gruppi di sicurezza associati al database Amazon DocumentDB con un nome che corrisponde al modello. DocumentDB-ec2-n Un gruppo di sicurezza che corrisponde al modello non è stato modificato. Questo gruppo di sicurezza include una sola regola in uscita con il gruppo di sicurezza VPC dell'istanza EC2 come origine.	Esiste un gruppo di sicurezza EC2 valido per la connessione, ma non è associato all'istanza EC2. Questo gruppo di sicurezza ha un nome che corrisponde al modello DocumentDB-ec2-n. Non è stato modificato. Ha una sola regola in uscita con il gruppo di sicurezza VPC del database Amazon DocumentDB come origine.	Azione Amazon DocumentDB: associazione del gruppo di sicurezza EC2

Configurazione attuale del gruppo di sicurezza di Amazon DocumentDB	Configurazione del gruppo di sicurezza EC2 corrente	Azione di Amazon DocumentDB
<p>Si applica una delle due condizioni seguenti:</p> <ul style="list-style-type: none"> • Non esiste un gruppo di sicurezza associato al database Amazon DocumentDB con un nome che corrisponda al modello. DocumentDB-ec2-n • Esistono uno o più gruppi di sicurezza associati al database Amazon DocumentDB con un nome che corrisponde al modello. DocumentDB-ec2-n Tuttavia, Amazon DocumentDB non può utilizzare nessuno di questi gruppi di sicurezza per la connessione con l'istanza EC2. Amazon DocumentDB non può utilizzare un gruppo di sicurezza che non ha una regola in entrata con il gruppo di sicurezza VPC dell'istanza EC2 come origine. Amazon DocumentDB inoltre non può utilizzare un gruppo di sicurezza che è stato modificato. 	<p>Esistono uno o più gruppi di sicurezza associati all'istanza EC2 con un nome che corrisponde al modello DocumentDB-ec2-n . Un gruppo di sicurezza che corrisponde al modello non è stato modificato. Questo gruppo di sicurezza ha una sola regola in uscita con il gruppo di sicurezza VPC del database Amazon DocumentDB come origine.</p>	<p>Azione Amazon DocumentDB: creazione di nuovi gruppi di sicurezza</p>

Azione Amazon DocumentDB: creazione di nuovi gruppi di sicurezza

Amazon DocumentDB esegue le seguenti azioni:

- Crea un nuovo gruppo di sicurezza che corrisponde al modello DocumentDB-ec2-n. Questo gruppo di sicurezza include una regola in uscita con il gruppo di sicurezza VPC dell'istanza EC2 come origine. Questo gruppo di sicurezza è associato al database Amazon DocumentDB e consente all'istanza EC2 di accedere al database Amazon DocumentDB.
- Crea un nuovo gruppo di sicurezza che corrisponde al modello ec2-DocumentDB-n. Questo gruppo di sicurezza ha una regola in uscita con il gruppo di sicurezza VPC del database Amazon DocumentDB come origine. Questo gruppo di sicurezza è associato all'istanza EC2 e consente all'istanza EC2 di inviare traffico al database Amazon DocumentDB.

Azione Amazon DocumentDB: associazione del gruppo di sicurezza EC2

Amazon DocumentDB associa il gruppo di sicurezza EC2 valido ed esistente all'istanza EC2. Questo gruppo di sicurezza consente all'istanza EC2 di inviare traffico al database Amazon DocumentDB.

Visualizzazione delle risorse di calcolo connesse

Puoi usare il AWS Management Console per visualizzare le risorse di calcolo connesse a un database Amazon DocumentDB. Le risorse mostrate includono le connessioni delle risorse di calcolo configurate automaticamente. È possibile configurare la connettività delle risorse di calcolo automaticamente nei modi seguenti:

- È possibile selezionare la risorsa di calcolo quando si crea il database. Per ulteriori informazioni, consulta Creazione di un [Creazione di un cluster Amazon DocumentDB](#) cluster DB Multi-AZ.
- È possibile configurare la connettività tra un database esistente e una risorsa di calcolo. Per ulteriori informazioni, consulta [Connect Amazon EC2 automaticamente](#).

Le risorse di calcolo elencate non includono quelle connesse al database manualmente. Ad esempio, è possibile consentire manualmente a una risorsa di calcolo di accedere a un database aggiungendo una regola al gruppo di sicurezza VPC associato al database.

Per garantire la presenza della risorsa di calcolo nell'elenco, è necessario che siano soddisfatte le condizioni elencate di seguito.

- Il nome del gruppo di sicurezza associato alla risorsa di calcolo corrisponde al modello ec2-DocumentDB-n (dove n è un numero).

- Il gruppo di sicurezza associato alla risorsa di calcolo ha una regola in uscita con l'intervallo di porte impostato sulla porta utilizzata dal database Amazon DocumentDB.
- Il gruppo di sicurezza associato alla risorsa di calcolo ha una regola in uscita con l'origine impostata su un gruppo di sicurezza associato al database Amazon DocumentDB.
- Il nome del gruppo di sicurezza associato al database Amazon DocumentDB corrisponde al modello DocumentDB-ec2-n (dove n è un numero).
- Il gruppo di sicurezza associato al database Amazon DocumentDB ha una regola in entrata con l'intervallo di porte impostato sulla porta utilizzata dal database Amazon DocumentDB.
- Il gruppo di sicurezza associato al database Amazon DocumentDB ha una regola in entrata con l'origine impostata su un gruppo di sicurezza associato alla risorsa di calcolo.

Per visualizzare le risorse di calcolo connesse a un database Amazon DocumentDB

1. [Accedi a e apri AWS Management Console la console Amazon DocumentDB all'indirizzo https://console.aws.amazon.com/docdb.](https://console.aws.amazon.com/docdb)
2. Nel riquadro di navigazione, scegli Database, quindi scegli il nome del database Amazon DocumentDB.
3. Nella scheda Connettività e sicurezza, visualizza le risorse di calcolo nella sezione Risorse di calcolo connesse.

Connect Amazon EC2 manualmente

Argomenti

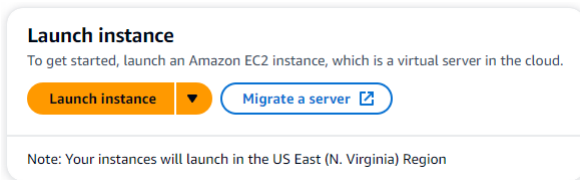
- [Fase 1: creare un'istanza Amazon EC2](#)
- [Fase 2: creazione di un gruppo di sicurezza](#)
- [Fase 3: creare un cluster Amazon DocumentDB](#)
- [Fase 4: Connettiti alla tua istanza Amazon EC2](#)
- [Passaggio 5: installa la shell mongo](#)
- [Fase 6: Gestione del TLS di Amazon DocumentDB](#)
- [Fase 7: Connettiti al tuo cluster Amazon DocumentDB](#)
- [Fase 8: Inserimento e interrogazione dei dati](#)
- [Fase 9: Esplora](#)

I passaggi seguenti presuppongono che tu abbia completato i passaggi indicati nell'[Prerequisiti](#) argomento.

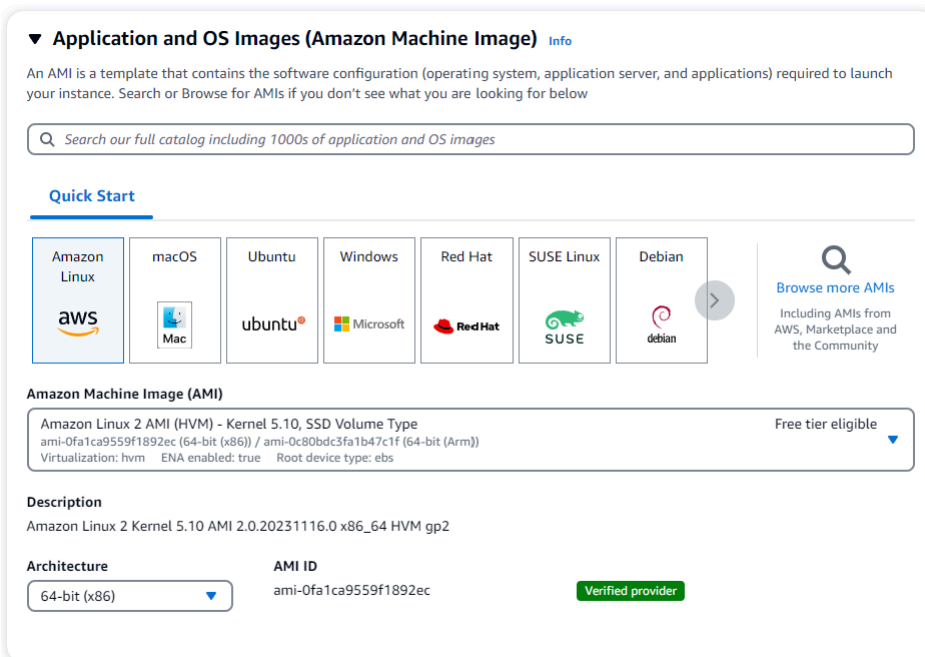
Fase 1: creare un'istanza Amazon EC2

In questa fase, creerai un'istanza Amazon EC2 nella stessa regione e Amazon VPC che utilizzerai successivamente per il provisioning del tuo cluster Amazon DocumentDB.

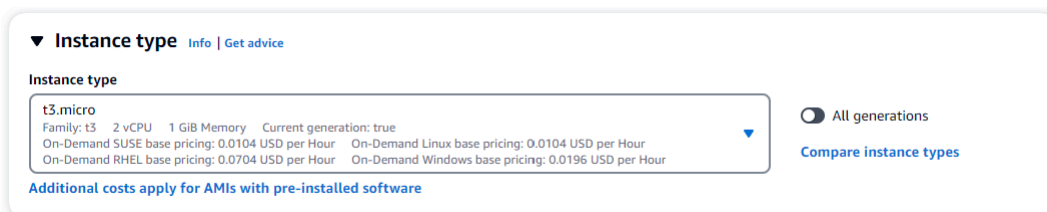
1. Sulla console Amazon EC2, scegli Launch instance.



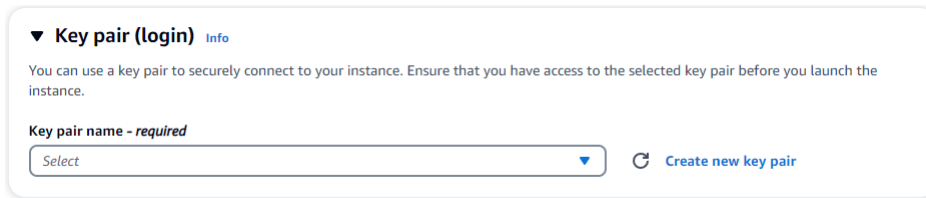
2. Inserisci un nome o un identificatore nel campo Nome situato nella sezione Nome e tag.
3. Nell'elenco a discesa Amazon Machine Image (AMI), individua l'AMI Amazon Linux 2 e selezionala.



4. Individua e scegli t3.micro nell'elenco a discesa del tipo di istanza.



5. Nella sezione Key pair (login), inserisci l'identificatore di una coppia di chiavi esistente o scegli Crea nuova coppia di chiavi.



▼ Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

Select [Create new key pair](#)

È necessario fornire una coppia di chiavi Amazon EC2.

Se disponi di una coppia di chiavi Amazon EC2:

- a. Seleziona una coppia di chiavi, scegli la tua coppia di chiavi dall'elenco.
- b. Devi già avere il file della chiave privata (file.pem o .ppk) disponibile per accedere alla tua istanza Amazon EC2.

Se non disponi di una coppia di chiavi Amazon EC2:

- a. Scegli Crea nuova coppia di chiavi, viene visualizzata la finestra di dialogo Crea coppia di chiavi.
- b. Inserisci un nome nel campo Nome della coppia di chiavi.
- c. Scegli il tipo di coppia di chiavi e il formato del file della chiave privata.
- d. Scegliere Create key pair (Crea coppia di chiavi).

Create key pair ✕

Key pair name
Key pairs allow you to connect to your instance securely.

The name can include upto 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type


RSA
RSA encrypted private and public key pair

ED25519
ED25519 encrypted private and public key pair

Private key file format

.pem
For use with OpenSSH

.ppk
For use with PuTTY

⚠ When prompted, store the private key in a secure and accessible location on your computer. **You will need it later to connect to your instance.** [Learn more](#) 

[Cancel](#) [Create key pair](#)

i Note

Per motivi di sicurezza, consigliamo vivamente di utilizzare una coppia di chiavi per la connettività SSH e Internet all'istanza EC2.

6. Nella sezione Impostazioni di rete, in Firewall (gruppi di sicurezza), scegli Crea gruppo di sicurezza o Seleziona gruppo di sicurezza esistente.

▼ **Network settings** [Info](#) [Edit](#)

Network [Info](#)
vpc-02c0445657b77542c

Subnet [Info](#)
No preference (Default subnet in any availability zone)

Auto-assign public IP [Info](#)
Enable

Firewall (security groups) [Info](#)
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group Select existing security group

We'll create a new security group called 'launch-wizard-1' with the following rules:

Allow SSH traffic from
Helps you connect to your instance

Allow HTTPS traffic from the internet
To set up an endpoint, for example when creating a web server

Allow HTTP traffic from the internet
To set up an endpoint, for example when creating a web server

⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only. ✕

Se hai scelto di selezionare un gruppo di sicurezza esistente, selezionane uno dall'elenco a discesa Gruppi di sicurezza comuni.

Se hai scelto di creare un nuovo gruppo di sicurezza, procedi come segue:

- Controlla tutte le regole di autorizzazione al traffico che si applicano alla tua connettività EC2.
- Nel campo IP, scegli Il mio IP o seleziona Personalizzato per scegliere da un elenco di blocchi CIDR, elenchi di prefissi o gruppi di sicurezza. Non consigliamo Anywhere come scelta, a meno che l'istanza EC2 non si trovi su una rete isolata, perché consente l'accesso a qualsiasi indirizzo IP all'istanza EC2.

My IP
52.95.4.16/32

- Nella sezione Riepilogo, esamina la configurazione EC2 e scegli l'istanza Launch, se corretta. Modifica i gruppi di sicurezza.

▼ **Summary**

Number of instances [Info](#)

Software Image (AMI)
Amazon Linux 2 Kernel 5.10 AMI...[read more](#)
ami-0fa1ca9559f1892ec

Virtual server type (instance type)
t3.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 8 GiB

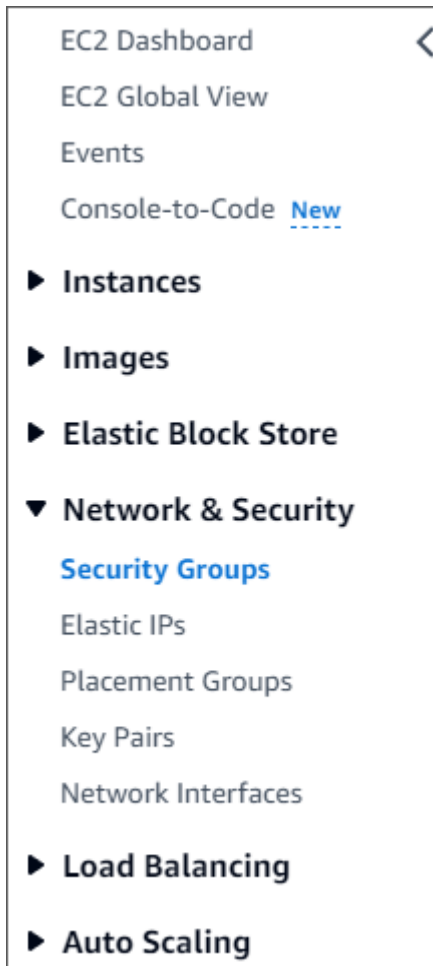
Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet. ×

[Review commands](#) [Cancel](#) [Launch instance](#)

Fase 2: creazione di un gruppo di sicurezza

Ora creerai un nuovo gruppo di sicurezza nel tuo Amazon VPC predefinito. Il gruppo di sicurezza demoDocDB consente di connettersi al cluster Amazon DocumentDB sulla porta 27017 (la porta predefinita per Amazon DocumentDB) dall'istanza Amazon EC2.

1. Nella [Console di gestione Amazon EC2](#), in Rete e sicurezza, scegli Gruppi di sicurezza.



2. Scegliere Create Security Group (Crea gruppo di sicurezza).

Create security group

3. Nella sezione Dettagli di base:
 - a. In Security group name (Nome gruppo di sicurezza) immettere demoDocDB.
 - b. In Description (Descrizione), inserire una descrizione.
 - c. Per VPC, accetta l'utilizzo del tuo VPC predefinito.

Basic details

Security group name [Info](#)

MyWebServerGroup

Name cannot be edited after creation.

Description [Info](#)

Allows SSH access to developers

VPC [Info](#)

vpc-02c0445657b77542c ▼

4. Nella sezione Regole in entrata, scegliere Aggiungi regola.
 - a. Per Type (Tipo) seleziona Custom TCP Rule (Regola TCP personalizzata).
 - b. Per Port range, inserisci. 27017
 - c. Per Destinazione, scegliete Personalizzato. Nel campo accanto, cerca il gruppo di sicurezza che hai appena chiamato demoEC2. Potrebbe essere necessario aggiornare il browser affinché la console Amazon EC2 compili automaticamente il nome sorgentedemoEC2.

Inbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info		
Custom TCP ▼	TCP	27017	Cust... ▼	Q		Delete
Add rule						

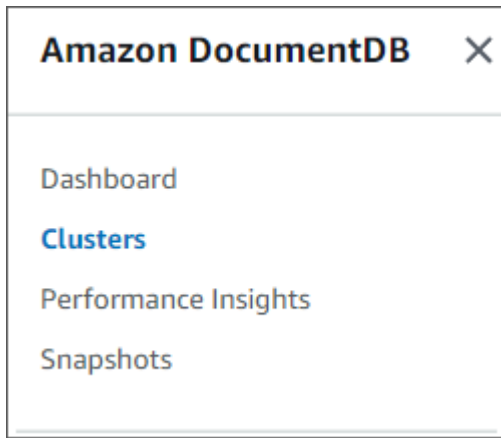
5. Accetta tutte le altre impostazioni predefinite e scegli Crea gruppo di sicurezza.

[Create security group](#)

Fase 3: creare un cluster Amazon DocumentDB

Durante il provisioning dell'istanza Amazon EC2, creerai il tuo cluster Amazon DocumentDB.

1. Accedi alla console Amazon DocumentDB e scegli Clusters dal pannello di navigazione.



2. Scegli Crea.

Create

3. Lascia l'impostazione del tipo di cluster sull'impostazione predefinita di Instance Based Cluster.

A screenshot of the "Cluster type" selection screen. It shows two options: "Instance Based Cluster" (selected with a radio button) and "Elastic Cluster". The "Instance Based Cluster" option includes a description: "Instance based cluster can scale your database to millions of reads per second and up to 128 TiB of storage capacity. With instance based clusters you can choose your instance type based on your requirements." The "Elastic Cluster" option includes a description: "Elastic clusters can scale your database to millions of reads and writes per second, with petabytes of storage capacity. Elastic clusters support MongoDB compatible sharding APIs. With Elastic Clusters, you do not need to choose, manage or upgrade instances."

4. Per Numero di istanze, scegli 1. Ciò ridurrà al minimo i costi. Lascia le altre impostazioni ai valori predefiniti.

A screenshot of the "Configuration" screen for creating a cluster. It shows the following fields: "Cluster identifier" (text input with value "docdb-2023-12-05-21-00-04"), "Engine version" (dropdown menu with value "5.0.0"), "Instance class" (dropdown menu with value "db.r6g.large" and subtext "2 vCPUs 16GiB RAM"), and "Number of instances" (dropdown menu with value "1").

5. Per la connettività, lascia l'impostazione predefinita di Non connetterti a una risorsa di calcolo EC2.

Connectivity C

Compute resources
Choose whether to set up a connection to a compute resource for this database. Setting up a connection will automatically change connectivity settings so that the compute resource can connect to this database.

Connect to an EC2 compute resource
Set up a connection to an EC2 compute resource for this database.

Don't connect to an EC2 compute resource
Don't set up a connection to a compute resource for this database.

i Note

La connessione a una risorsa di calcolo EC2 crea automaticamente gruppi di sicurezza per la connessione delle risorse di calcolo EC2 al cluster. Poiché hai creato manualmente questi gruppi di sicurezza nel passaggio precedente, dovresti selezionare Non connetterti a una risorsa di calcolo EC2 per non creare un secondo set di gruppi di sicurezza.

- Per l'autenticazione, inserisci le credenziali di accesso. Importante: ti serviranno le credenziali di accesso per autenticare il cluster in un passaggio successivo.

Authentication

Username Info
Specify an alphanumeric string that defines the login ID for the user.

Username must start with a letter and contain 1 to 63 characters

Password Info **Confirm password** Info

Password must be at least eight characters long and cannot contain a / (slash), " (double quote) or @ (at symbol).

- Attiva Mostra impostazioni avanzate.

i **The estimated hourly cost for 1 db.r6g.large instance(s) is \$0.29/hr.**
With Amazon DocumentDB you are charged for instances, storage, IOPS, backups, and data transfer. Please see our [pricing page](#) and [cost optimization documentation](#) for more information.

Show advanced settings
Cancel
Create cluster

- Nella sezione Impostazioni di rete, per i gruppi di sicurezza Amazon VPC, scegli DemoDocDB.

Network settings

Virtual Private Cloud (VPC) [Info](#)
VPC defines the virtual networking environment for this cluster.

vpc-02c0445657b77542c

Only VPCs with a corresponding subnet group are listed. Once a cluster is created, the VPC cannot be changed.

Subnet group [Info](#)
A subnet group is a collection of subnets that are within a VPC.

default

VPC security groups
A security group acts as a virtual firewall for your instance to control inbound and outbound traffic.

Select VPC security groups

default (VPC) X demoDocDB (VPC) X

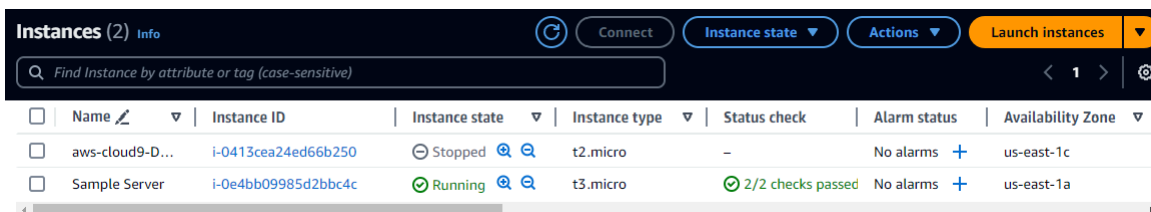
9. Scegli Create cluster (Crea cluster).

Create cluster

Fase 4: Connettiti alla tua istanza Amazon EC2

Per installare la shell mongo, devi prima connetterti alla tua istanza Amazon EC2. L'installazione della mongo shell ti consente di connetterti e interrogare il tuo cluster Amazon DocumentDB. Completa questa procedura:

1. Sulla console Amazon EC2, accedi alle tue istanze e verifica se l'istanza che hai appena creato è in esecuzione. In caso affermativo, seleziona l'istanza facendo clic sull'ID dell'istanza.



<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
<input type="checkbox"/>	aws-cloud9-D...	i-0413cea24ed66b250	Stopped	t2.micro	-	No alarms	us-east-1c
<input checked="" type="checkbox"/>	Sample Server	i-0e4bb09985d2bbc4c	Running	t3.micro	2/2 checks passed	No alarms	us-east-1a

2. Scegli Connetti.

Instance summary for i-0e4bb09985d2bbc4c (Sample Server) Info

Updated less than a minute ago

Refresh
Connect
Instance state ▼
Actions ▼

<p>Instance ID i-0e4bb09985d2bbc4c (Sample Server)</p> <p>IPV6 address -</p> <p>Hostname type IP name: ip-172-31-41-131.ec2.internal</p> <p>Answer private resource DNS name IPv4 (A)</p> <p>Auto-assigned IP address 54.87.99.44 [Public IP]</p> <p>IAM Role -</p> <p>IMDSv2 Required</p>	<p>Public IPv4 address 54.87.99.44 open address</p> <p>Instance state ● Running</p> <p>Private IP DNS name (IPv4 only) ip-172-31-41-131.ec2.internal</p> <p>Instance type t3.micro</p> <p>VPC ID vpc-02c0445657b77542c</p> <p>Subnet ID subnet-06676048a6487a578</p>	<p>Private IPv4 addresses 172.31.41.131</p> <p>Public IPv4 DNS ec2-54-87-99-44.compute-1.amazonaws.com open address</p> <p>Elastic IP addresses -</p> <p>AWS Compute Optimizer finding No recommendations available for this instance.</p> <p>Auto Scaling Group name -</p>
---	---	--

3. Esistono quattro opzioni a schede per il metodo di connessione: Amazon EC2 Instance Connect, Session Manager, client SSH o console seriale EC2. Devi sceglierne una e seguirne le istruzioni. Al termine, scegli Connect.

EC2 Instance Connect

Session Manager

SSH client

EC2 serial console

Instance ID
i-0e4bb09985d2bbc4c (Sample Server)

Connection Type

Connect using EC2 Instance Connect
Connect using the EC2 Instance Connect browser-based client, with a public IPv4 address.

Connect using EC2 Instance Connect Endpoint
Connect using the EC2 Instance Connect browser-based client, with a private IPv4 address and a VPC endpoint.

Public IP address
54.87.99.44

User name
Enter the user name defined in the AMI used to launch the instance. If you didn't define a custom user name, use the default user name, ec2-user.

Note: In most cases, the default user name, ec2-user, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.

i Note

Se l'indirizzo IP è cambiato dopo aver iniziato questa procedura dettagliata o se si torna all'ambiente in un secondo momento, è necessario aggiornare la regola in entrata del gruppo di demoEC2 sicurezza per abilitare il traffico in entrata dal nuovo indirizzo API.

Passaggio 5: installa la shell mongo

Ora puoi installare la mongo shell, un'utilità da riga di comando che usi per connettere e interrogare il tuo cluster Amazon DocumentDB. Segui le istruzioni riportate di seguito per installare la shell mongo per il tuo sistema operativo.

On Amazon Linux

Per installare la shell Mongo in Amazon Linux

1. Crea il file del repository. Nella riga di comando dell'istanza EC2, esegui il seguente comando:

```
echo -e "[mongodb-org-5.0] \nname=MongoDB Repository\nbaseurl=https://\nrepo.mongodb.org/yum/amazon/2/mongodb-org/5.0/x86_64/\nngpgcheck=1 \nenabled=1\nngpgkey=https://www.mongodb.org/static/pgp/server-5.0.asc" | sudo tee /etc/\nyum.repos.d/mongodb-org-5.0.repo
```

2. Al termine, installa la shell mongo eseguendo il seguente comando:

```
sudo yum install -y mongodb-org-shell
```

On Ubuntu 18.04

Per installare la shell Mongo in Ubuntu 18.04

1. Importa la chiave pubblica che verrà utilizzata dal sistema di gestione dei pacchetti.

```
sudo apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv\n2930ADAE8CAF5059EE73BB4B58712A2291FA4AD5
```

2. Crea l'elenco di file `/etc/apt/sources.list.d/mongodb-org-3.6.list` per MongoDB utilizzando il comando appropriato per la versione di Ubuntu.

Ubuntu 18.04

```
echo "deb [ arch=amd64,arm64 ] https://repo.mongodb.org/apt/ubuntu xenial/\nmongodb-org/3.6 multiverse" | sudo tee /etc/apt/sources.list.d/mongodb-\norg-3.6.list
```

Note

Il comando precedente installerà la shell mongo 3.6 per Bionic e Xenial.

3. Ricarica il database del pacchetto locale utilizzando il comando seguente:

```
sudo apt-get update
```

4. Installa la shell MongoDB.

```
sudo apt-get install -y mongodb-org-shell
```

Per informazioni sull'installazione di versioni precedenti di MongoDB nel sistema Ubuntu, consulta [Installazione di MongoDB Community Edition in Ubuntu](#).

On other operating systems

Per installare la shell Mongo in altri sistemi operativi, vedi l'argomento relativo all'[installazione di MongoDB Community Edition](#) nella documentazione relativa a MongoDB.

Fase 6: Gestione del TLS di Amazon DocumentDB

Scarica il certificato CA per Amazon DocumentDB con il seguente codice: `wget https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem`

Note

Transport Layer Security (TLS) è abilitato di default per tutti i nuovi cluster Amazon DocumentDB. Per ulteriori informazioni, consulta [Gestione delle impostazioni TLS del cluster Amazon DocumentDB](#).

Fase 7: Connettiti al tuo cluster Amazon DocumentDB

1. Nella console Amazon DocumentDB, in Clusters, individua il cluster. Scegli il cluster che hai creato facendo clic sull'identificatore del cluster.

Cluster identifier	Role	Engine version	Region & AZ	Status
docdb-2023-12-06-13-47-11	Regional cluster	5.0.0	us-east-1	available
docdb-2023-12-06-13-47-11	Primary instance	5.0.0	us-east-1a	available

2. Nella scheda Connettività e sicurezza, individua Connect to this cluster with the mongo shell nella casella Connect:

Connect to this cluster with the mongo shell [Copy](#)

```
mongo --ssl --host docdb-2023-12-06-13-47-11.cluster-cozt4xr9xv9b.us-east-1.docdb.amazonaws.com:27017 --sslCAFile global-bundle.pem --username sampleUser --password <insertYourPassword>
```

Copia la stringa di connessione fornita e incollala nel tuo terminale.

Apporta le seguenti modifiche:

- a. Assicurati di avere il nome utente corretto nella stringa.
- b. Ometti <insertYourPassword> in modo che ti venga richiesta la password dalla shell mongo quando ti connetti.

La stringa di connessione dovrebbe essere simile alla seguente:

```
mongo --ssl host docdb-2020-02-08-14-15-11.  
cluster.region.docdb.amazonaws.com:27107 --sslCAFile global-bundle.pem  
--username demoUser --password
```

3. Premi invio nel tuo terminale. Ora ti verrà richiesta la password. Inserisci la password.
4. Quando inserisci la password e riesci a visualizzare il `rs0:PRIMARY>` prompt, sei connesso correttamente al tuo cluster Amazon DocumentDB.

Hai problemi di connessione? Vedi [Risoluzione dei problemi di Amazon DocumentDB](#).

Fase 8: Inserimento e interrogazione dei dati

Ora che sei connesso al cluster, puoi eseguire alcune query per acquisire familiarità con l'utilizzo di un database di documenti.

1. Per inserire un singolo documento, inserisci quanto segue:

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

2. Otterrete il seguente risultato:

```
WriteResult({ "nInserted" : 1 })
```

3. Puoi leggere il documento che hai scritto con il `findOne()` comando (perché restituisce solo un singolo documento). Inserisci quanto segue:

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

4. Si ottiene il seguente risultato:

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

5. Per eseguire qualche altra domanda, considera un caso d'uso dei profili di gioco. Innanzitutto, inserisci alcune voci in una raccolta intitolata `profiles`. Inserisci quanto segue:

```
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}
  ])
```

6. Si ottiene il seguente risultato:

```
{ "acknowledged" : true, "insertedIds" : [ 1, 2, 3, 4 ] }
```

7. Utilizzate il `find()` comando per restituire tutti i documenti nella raccolta dei profili. Inserisci quanto segue:

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

8. Otterrai un output che corrisponderà ai dati che hai digitato nel passaggio 5.

9. Usa una query per un singolo documento usando un filtro. Inserisci quanto segue:

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

10. Dovresti recuperare questo risultato:

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

11. Ora proviamo a trovare un profilo e modificarlo usando il `findAndModify` comando. Daremo all'utente Matt altri dieci punti con il seguente codice:

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

12. Otterrete il seguente risultato (notate che il suo punteggio non è ancora aumentato):

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

```
"score" : 202
}
```

13. Puoi verificare che il suo punteggio sia cambiato con la seguente domanda:

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

14. Si ottiene il seguente risultato:

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

Fase 9: Esplora

Complimenti! Hai completato con successo la Guida rapida ad Amazon DocumentDB.

Qual è il prossimo passo? Scopri come sfruttare appieno questo potente database con alcune delle sue funzionalità più popolari:

- [Gestione di Amazon DocumentDB](#)
- [Dimensionamento](#)
- [Backup e ripristino](#)

Note

Per risparmiare sui costi, puoi interrompere il cluster Amazon DocumentDB per ridurre i costi o eliminare il cluster. Per impostazione predefinita, dopo 30 minuti di inattività, l' AWS Cloud9 ambiente interromperà l'istanza Amazon EC2 sottostante.

Connect tramite il driver JDBC di Amazon DocumentDB

Il driver JDBC per Amazon DocumentDB fornisce un'interfaccia relazionale SQL per gli sviluppatori e consente la connettività da strumenti di BI come Tableau e DbVisualizer.

Per informazioni più dettagliate, consulta la [documentazione del driver JDBC di Amazon DocumentDB su GitHub](#).

Argomenti

- [Nozioni di base](#)
- [Connect ad Amazon DocumentDB da Tableau Desktop](#)
- [Connect ad Amazon DocumentDB da DbVisualizer](#)
- [Generazione automatica di schemi JDBC](#)
- [Supporto SQL](#)
- [Risoluzione dei problemi](#)

Nozioni di base

Fase 1. Crea cluster Amazon DocumentDB

Se non hai creato un cluster Amazon DocumentDB, creane uno utilizzando le istruzioni nella sezione [Getting Started](#) della Amazon DocumentDB Developer Guide.

Note

DocumentDB è un servizio esclusivo di Virtual Private Cloud (VPC). Se ti connetti da una macchina locale, esterna al VPC del cluster, dovrai creare una connessione SSH a un'istanza Amazon EC2. In questo caso, avvia il cluster utilizzando le istruzioni in [Connect with EC2](#). Consulta [Utilizzo di un tunnel SSH per Connect ad Amazon DocumentDB](#) per ulteriori informazioni sul tunneling SSH e quando potrebbe essere necessario.

Fase 2. Installazione JRE o JDK

A seconda dell'applicazione di BI, potrebbe essere necessario assicurarsi che sul computer sia installata un'installazione JRE o JDK a 64 bit versione 8 o successiva. Puoi scaricare Java SE Runtime Environment 8 [qui](#).

Fase 3. Scarica il driver JDBC DocumentDB

Scarica il driver JDBC DocumentDB da [qui](#). Il driver è confezionato in un singolo file JAR (ad esempio documentdb-jdbc-1.0.0-all.jar).

Fase 4. Utilizzo di un tunnel SSH per Connect ad Amazon DocumentDB

I cluster Amazon DocumentDB (con compatibilità MongoDB) sono distribuiti all'interno di un Amazon Virtual Private Cloud (Amazon VPC). È possibile accedervi direttamente dalle istanze Amazon EC2 o da altri AWS servizi distribuiti nello stesso Amazon VPC. Inoltre, è possibile

accedere ad Amazon DocumentDB da istanze EC2a o altriAWS servizi in diversi VPC nella stessaAWS regione o in altre regioni tramite peering VPC.

Puoi utilizzare il tunneling SSH (noto anche come port forwarding) per accedere alle tue risorse Amazon DocumentDB, dall'esterno del VPC del cluster. Questo sarà il caso della maggior parte degli utenti che non eseguono la propria applicazione su una macchina virtuale nello stesso VPC del cluster DocumentDB.

Per creare un tunnel SSH, sarà necessaria un'istanza Amazon EC2 in esecuzione nello stesso Amazon VPC del cluster Amazon DocumentDB. Puoi utilizzare un'istanza EC2 esistente nello stesso VPC del cluster o crearne una. Puoi configurare un tunnel SSH per il cluster Amazon DocumentDB `sample-cluster.node.us-east-1.docdb.amazonaws.com` eseguendo il seguente comando sul tuo computer locale.

```
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
```

Il flag `-L` viene utilizzato per inoltrare una porta locale. Questo è un prerequisito per la connessione a qualsiasi strumento di BI in esecuzione su un client esterno al VPC. Una volta eseguito il passaggio precedente, puoi passare ai passaggi successivi per lo strumento di BI di tua scelta.

Per ulteriori informazioni sul tunneling SSH, consulta la documentazione sull'[uso di un tunnel SSH per connettersi ad Amazon DocumentDB](#).

Connect ad Amazon DocumentDB da Tableau Desktop

Argomenti

- [Aggiungere il driver JDBC Amazon DocumentDB](#)
- [Connessione ad Amazon DocumentDB tramite Tableau - Tunnel SSH](#)

Aggiungere il driver JDBC Amazon DocumentDB

Per connetterti ad Amazon DocumentDB da Tableau Desktop devi scaricare e installare il driver JDBC DocumentDB e il connettore DocumentDB Tableau.

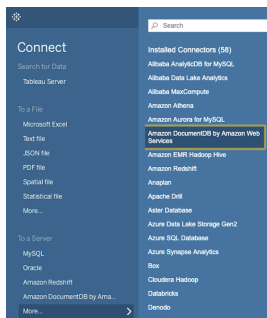
1. Scarica il file JAR del driver JDBC DocumentDB e copialo in una di queste directory in base al tuo sistema operativo:
 - Finestre -C:\Program Files\Tableau\Drivers
 - macOS -~/Library/Tableau/Drivers
2. Scarica il connettore Tableau DocumentDB (un file TACO) e copialo nella directory My Tableau Repository/Connectors.
 - Finestre -C:\Users\[user]\Documents\My Tableau Repository\Connectors
 - macOS -/Users/[user]/Documents/My Tableau Repository/Connectors

Per ulteriori informazioni, consulta la [documentazione di Tableau](#).

Connessione ad Amazon DocumentDB tramite Tableau - Tunnel SSH

Per connetterti a Tableau da un computer client esterno al VPC del cluster DocumentDB, devi configurare un tunnel SSH prima di seguire i passaggi seguenti:

1. Avvia l'applicazione Tableau Desktop.
2. Vai a Connect > A un server > Altro.
3. Scegli Amazon DocumentDB di Amazon Web Services nella sezione Connettori installati.

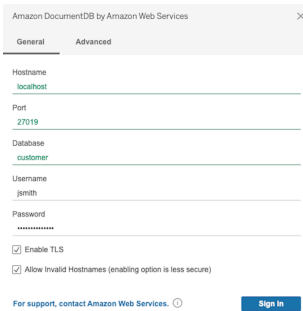


Connessione ad Amazon DocumentDB tramite Tableau - Tunnel SSH esterno

1. Immettere i parametri di connessione richiesti Hostname, Port, Database, Username e Password. I parametri di connessione nell'esempio seguente sono equivalenti alla stringa di connessione JDBC:

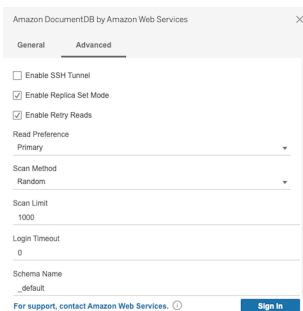
```
jdbc:documentdb://localhost:27019/test?
tls=true&tlsAllowInvalidHostnames=true&scanMethod=random&scanLimit=1000&login
```

i parametri nome utente e password passati separatamente in una raccolta di proprietà. Per ulteriori informazioni sui parametri della stringa di connessione, consulta la [documentazione github del driver JDBC di Amazon DocumentDB](#).



The screenshot shows the 'General' tab of the 'Amazon DocumentDB by Amazon Web Services' connection dialog. The fields are filled with the following values: Hostname: localhost, Port: 27019, Database: customer, Username: jsmith, Password: [masked]. There are two checked checkboxes: 'Enable TLS' and 'Allow invalid hostnames (enabling option is less secure)'. A 'Sign In' button is visible at the bottom right.

2. (Facoltativo) Le opzioni più avanzate sono disponibili nella scheda Avanzate.



The screenshot shows the 'Advanced' tab of the 'Amazon DocumentDB by Amazon Web Services' connection dialog. The 'Enable SSH Tunnel' checkbox is unchecked. The 'Enable Replica Set Mode' and 'Enable Retry Reads' checkboxes are checked. The 'Read Preference' is set to 'Primary', 'Scan Method' is 'Random', and 'Scan Limit' is '1000'. The 'Login Timeout' is '0' and the 'Schema Name' is '_default'. A 'Sign In' button is visible at the bottom right.

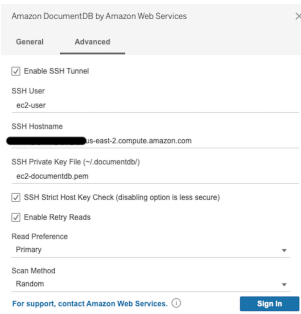
3. Selezionare Sign in (Accedi).

Connessione ad Amazon DocumentDB tramite Tableau - Tunnel SSH interno

Note

Se preferisci non configurare il tunnel SSH utilizzando un terminale, puoi utilizzare la GUI di Tableau per specificare i dettagli dell'istanza EC2 che il driver JDBC utilizzerà intrinsecamente per creare un tunnel SSH.

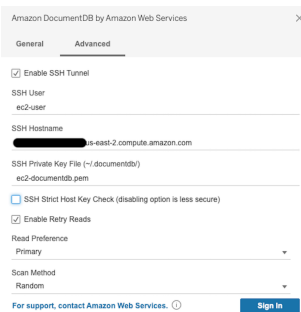
1. Nella scheda Avanzate, scegli l'opzione Abilita tunnel SSH per esaminare ulteriori proprietà.



2. Inserisci l'utente SSH, il nome host SSH e il file di chiave privata SSH.
3. (Facoltativo) È possibile disabilitare l'opzione SSH Strict Host Key Check che aggira il controllo della chiave host rispetto a un file hosts noto.

Note

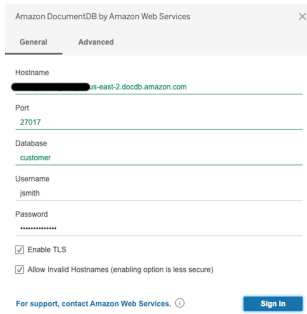
La disattivazione di questa opzione è meno sicura in quanto può portare a un [man-in-the-middle](#) attacco.



4. Inserisci i parametri richiesti: Hostname, Port, Database, Nome utente e Password.

Note

Assicurati di utilizzare l'endpoint del cluster DocumentDB e non localhost quando usi l'opzione tunnel SSH interno.



5. Selezionare Sign in (Accedi).

Connect ad Amazon DocumentDB da DbVisualizer

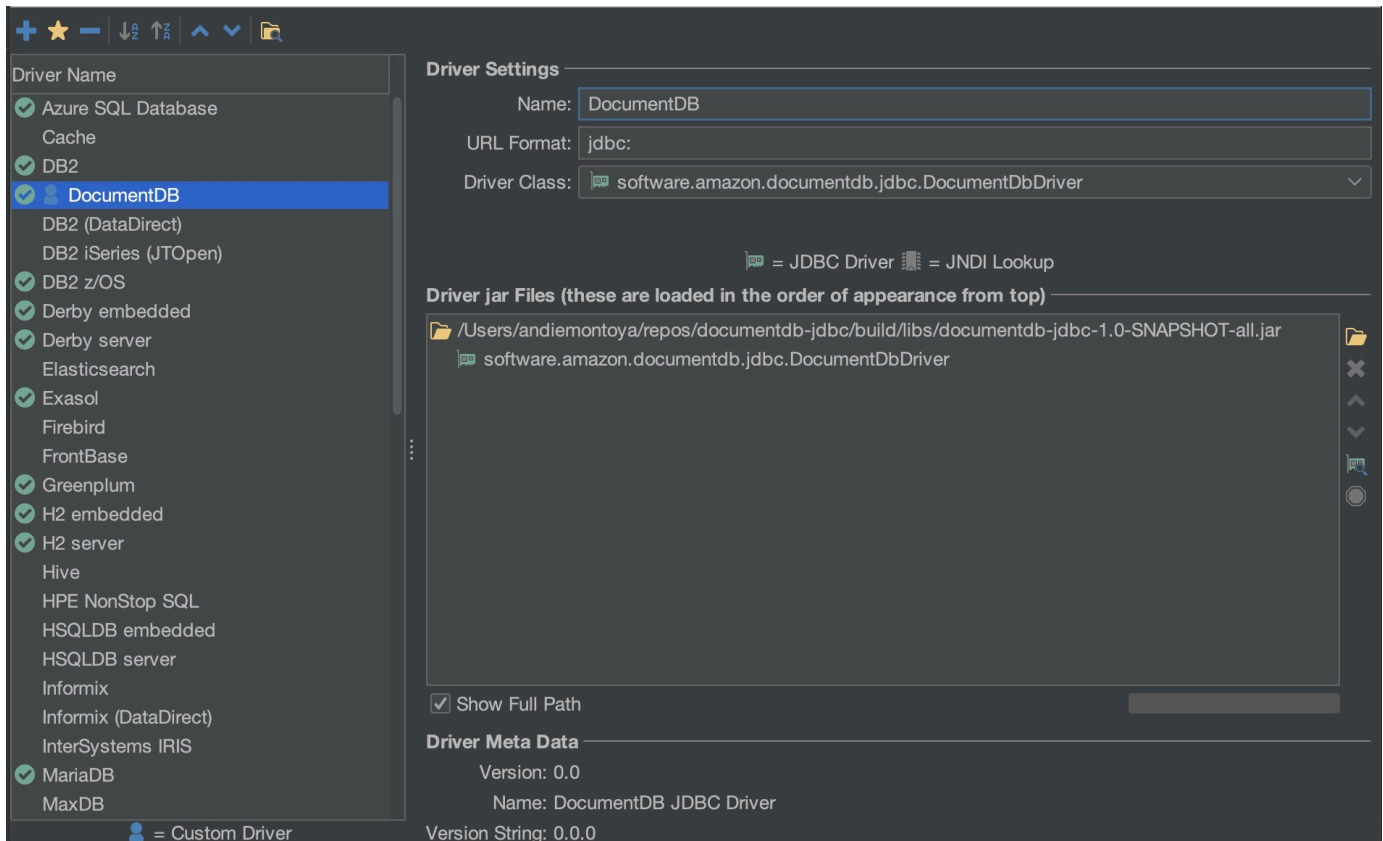
Argomenti

- [Aggiungere il driver JDBC Amazon DocumentDB](#)
- [Connessione ad Amazon DocumentDB utilizzando DbVisualizer](#)

Aggiungere il driver JDBC Amazon DocumentDB

Per connetterti ad Amazon DocumentDB da, DbVisualizer devi prima importare il driver JDBC di Amazon DocumentDB.

1. Avvia l' DbVisualizer applicazione e vai al percorso del menu: Strumenti > Driver Manager...
2. Scegli + (o nel menu, seleziona Driver > Crea driver).
3. Impostare Name (Nome) su DocumentDB.
4. Imposta il formato URL su `jdbc:documentdb://<host>[:port]/<database>[?option=value[&option=value[...]]]`
5. Scegli il pulsante della cartella, quindi seleziona il file JAR del driver JDBC di Amazon DocumentDB e scegli il pulsante Apri.
6. Verificare che il campo Classe conducente sia impostato su `software.amazon.documentdb.jdbc.DocumentDbDriver`. Le impostazioni di Driver Manager per DocumentDB dovrebbero essere simili al seguente.



7. Chiudere la finestra di dialogo. Il driver JDBC di Amazon DocumentDB sarà configurato e pronto per l'uso.

Connessione ad Amazon DocumentDB utilizzando DbVisualizer

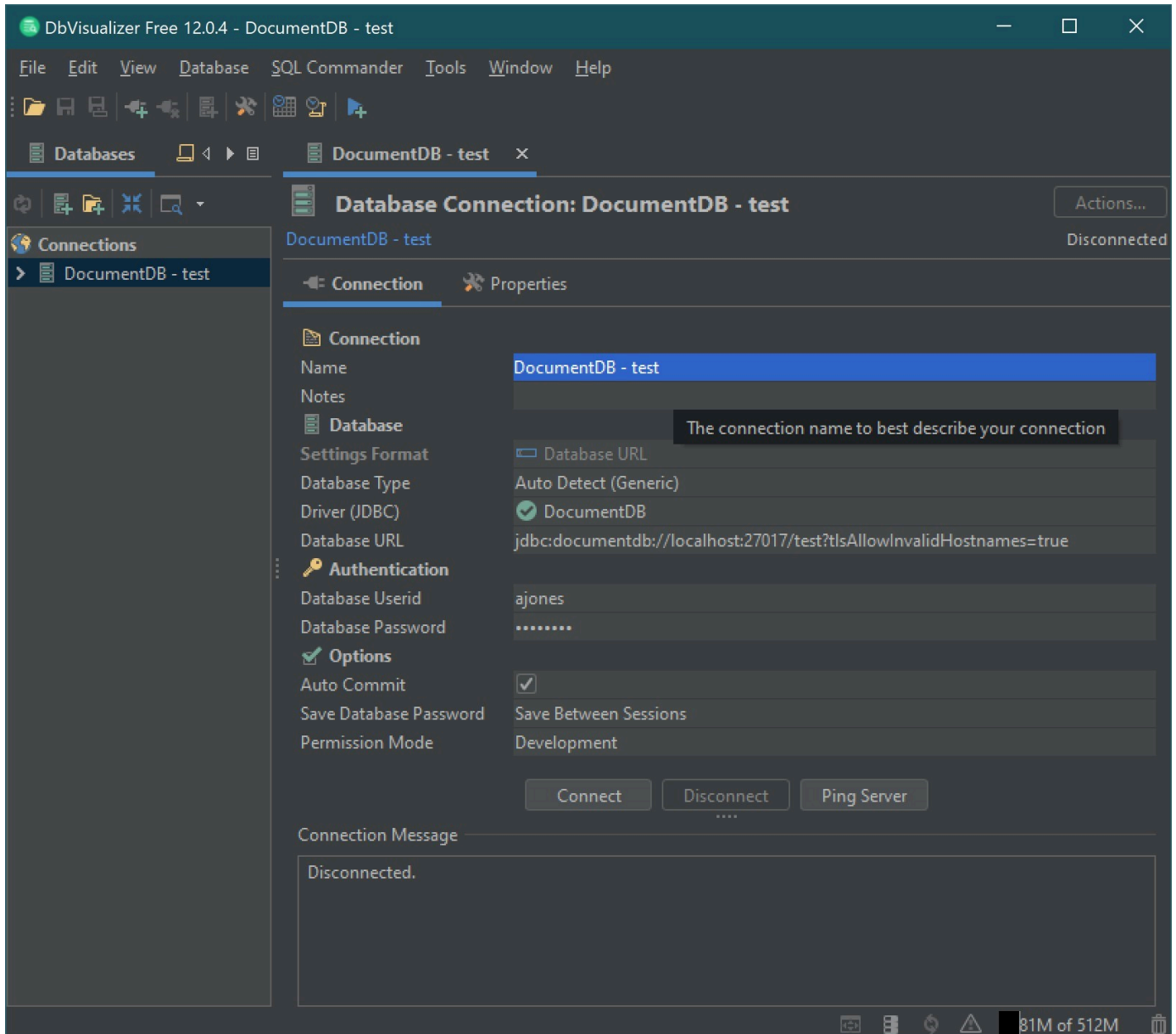
Connect ad Amazon DocumentDB utilizzando DbVisualizer

1. Se ti connetti dall'esterno del VPC del cluster Amazon DocumentDB, assicurati di aver configurato un tunnel SSH.
2. Scegliete Database > Crea connessione al database dal menu di primo livello.
3. Inserire un nome descrittivo per il campo Nome.
4. Imposta Driver (JDBC) sul driver DocumentDB creato nella sezione precedente.
5. Imposta l'URL del database sulla stringa di connessione JDBC.

Ad esempio: `jdbc:documentdb://localhost:27017/database?
tlsAllowInvalidHostnames=true`

6. Imposta l'ID utente del database sul tuo ID utente Amazon DocumentDB.
7. Imposta la password del database sulla password corrispondente per l'ID utente.

La seguente finestra di dialogo Connessione al database dovrebbe essere simile alla seguente:



8. Scegli Connect (Connetti).

Generazione automatica di schemi JDBC

Amazon DocumentDB è un database di documenti e quindi non ha il concetto di tabelle e schema. Tuttavia, gli strumenti di BI come Tableau si aspettano che il database a cui si connette presenti uno schema. In particolare, quando la connessione del driver JDBC deve ottenere lo schema per la raccolta nel database, eseguirà un sondaggio per tutte le raccolte nel database. Il driver determinerà

se esiste già una versione cache dello schema per quella raccolta. Se non esiste una versione memorizzata nella cache, campionerà la raccolta di documenti e creerà uno schema basato sul seguente comportamento.

Argomenti

- [Limitazioni alla generazione dello schema](#)
- [Opzioni del metodo di scansione](#)
- [Tipi di dati Amazon DocumentDB](#)
- [Mappatura dei campi scalari](#)
- [Gestione dei tipi di dati di oggetti e matrici](#)

Limitazioni alla generazione dello schema

Il driver JDBC DocumentDB impone un limite alla lunghezza degli identificatori a 128 caratteri. Il generatore di schemi può troncare la lunghezza degli identificatori generati (nomi di tabelle e nomi di colonne) per assicurarsi che soddisfino tale limite.

Opzioni del metodo di scansione

Il comportamento di campionamento può essere modificato utilizzando le opzioni della stringa di connessione o dell'origine dati.

- Metodo di scansione = <option>
 - random - (predefinito) - I documenti di esempio vengono restituiti in ordine casuale.
 - idForward: i documenti di esempio vengono restituiti in ordine di id.
 - idReverse: i documenti di esempio vengono restituiti in ordine inverso rispetto all'id.
 - tutti: campionano tutti i documenti della raccolta.
- scanLimit= <n>- Il numero di documenti da campionare. Il valore deve essere un numero intero positivo. Il valore predefinito è 1000. Se ScanMethod è impostato su tutto, questa opzione viene ignorata.

Tipi di dati Amazon DocumentDB

Il server DocumentDB supporta diversi tipi di dati MongoDB. Di seguito sono elencati i tipi di dati supportati e i tipi di dati JDBC associati.

Tipo di dati MongoDB	Supportato in DocumentDB	Tipo di dati JDBC
Dati binari	Sì	VARBINARY
Boolean	Sì	BOOLEAN
Doppio	Sì	DOUBLE
Intero a 32 bit	Sì	INTEGER
Numero intero a 64 bit	Sì	BIGINT
Stringa	Sì	VARCHAR
ObjectId	Sì	VARCHAR
Data	Sì	TIMESTAMP
Null	Sì	VARCHAR
Espressione regolare	Sì	VARCHAR
Time stamp	Sì	VARCHAR
MinKey	Sì	VARCHAR
MaxKey	Sì	VARCHAR
Oggetto	Sì	tavolo virtuale
Array	Sì	tavolo virtuale
Decimal128	No	DECIMAL
JavaScript	No	VARCHAR
JavaScript (con cannocchiale)	No	VARCHAR
Undefined	No	VARCHAR
Symbol	No	VARCHAR

Tipo di dati MongoDB	Supportato in DocumentDB	Tipo di dati JDBC
dBPointer (4.0+)	No	VARCHAR

Mappatura dei campi scalari

Durante la scansione di un campione di documenti da una raccolta, il driver JDBC creerà uno o più schemi per rappresentare i campioni della raccolta. In generale, un campo scalare nel documento è associato a una colonna nello schema della tabella. Ad esempio, in una raccolta denominata `team` e in un singolo documento `{ "_id" : "112233", "name" : "Alastair", "age": 25 }`, questo corrisponderebbe allo schema:

Nome tabella	Nome colonna	Tipo di dati	Chiave
squadra	ID squadra	VARCHAR	PK
squadra	name	VARCHAR	
squadra	età	INTEGER	

Promozione dei conflitti relativi ai tipi di dati

Durante la scansione dei documenti campionati, è possibile che i tipi di dati per un campo non siano coerenti da documento a documento. In questo caso, il driver JDBC promuoverà il tipo di dati JDBC a un tipo di dati comune adatto a tutti i tipi di dati dei documenti campionati.

Ad esempio:

```
{
  "_id" : "112233",
  "name" : "Alastair", "age" : 25
}

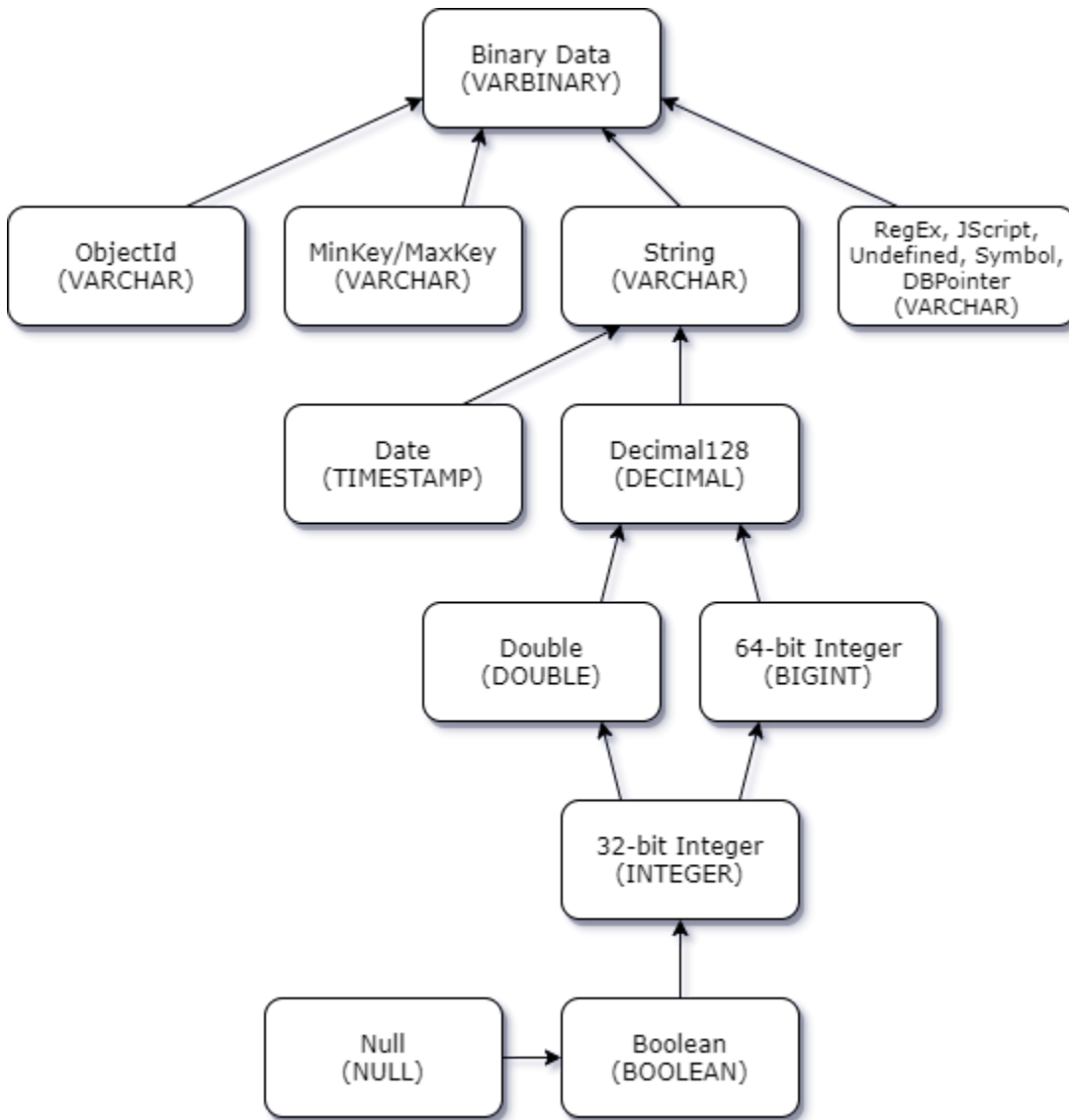
{
  "_id" : "112244",
  "name" : "Benjamin",
  "age" : "32"
}
```

Il campo età è di tipo intero a 32 bit nel primo documento ma stringa nel secondo documento. Qui il driver JDBC promuoverà il tipo di dati JDBC a VARCHAR per gestire entrambi i tipi di dati quando vengono incontrati.

Nome tabella	Nome colonna	Tipo di dati	Chiave
squadra	ID squadra	VARCHAR	PK
squadra	name	VARCHAR	
squadra	età	VARCHAR	

Promozione dei conflitti scalare-scalari

Il diagramma seguente mostra il modo in cui vengono risolti i conflitti tra tipi di dati scalari scalari.



Promozione dei conflitti di tipo scalare complesso

Come i conflitti di tipo scalare-scalare, lo stesso campo in documenti diversi può avere tipi di dati in conflitto tra complessi (array e oggetto) e scalari (interi, booleani, ecc.). Tutti questi conflitti vengono risolti (promossi) a VARCHAR per quei campi. In questo caso, i dati dell'array e dell'oggetto vengono restituiti come rappresentazione JSON.

Esempio di conflitto tra campi di tipo Embedded Array e String:

```
{
  "_id": "112233",
  "name": "George Jackson",
  "subscriptions": [
```

```

    "Vogue",
    "People",
    "USA Today"
  ]
}
{
  "_id": "112244",
  "name": "Joan Starr",
  "subscriptions": 1
}

```

L'esempio precedente corrisponde allo schema della tabella customer2:

Nome tabella	Nome colonna	Tipo di dati	Chiave
cliente 2	id cliente2	VARCHAR	PK
cliente 2	name	VARCHAR	
cliente 2	sottoscrizione	VARCHAR	

e la tabella virtuale customer1_subscriptions:

Nome tabella	Nome colonna	Tipo di dati	Chiave
customer1_abbonamenti	id cliente1	VARCHAR	PK/FK
customer1_abbonamenti	abbonamenti_index_lv10	BIGINT	PK
customer1_abbonamenti	value	VARCHAR	
customer_address	city	VARCHAR	
customer_address	Regione	VARCHAR	
customer_address	country	VARCHAR	

Nome tabella	Nome colonna	Tipo di dati	Chiave
customer_address	code	VARCHAR	

Gestione dei tipi di dati di oggetti e matrici

Finora, abbiamo solo descritto come vengono mappati i tipi di dati scalari. I tipi di dati Object e Array sono (attualmente) mappati su tabelle virtuali. Il driver JDBC creerà una tabella virtuale per rappresentare i campi dell'oggetto o dell'array in un documento. Il nome della tabella virtuale mappata concatenerà il nome della raccolta originale seguito dal nome del campo separato da un carattere di sottolineatura («_»).

La chiave primaria della tabella di base («_id») assume un nuovo nome nella nuova tabella virtuale e viene fornita come chiave esterna alla tabella di base associata.

Per i campi di tipo array incorporati, le colonne dell'indice vengono generate per rappresentare l'indice nell'array a ogni livello dell'array.

Esempio di campo oggetto incorporato

Per i campi oggetto di un documento, il driver JDBC crea una mappatura a una tabella virtuale.

```
{
  "Collection: customer",
  "_id": "112233",
  "name": "George Jackson",
  "address": {
    "address1": "123 Avenue Way",
    "address2": "Apt. 5",
    "city": "Hollywood",
    "region": "California",
    "country": "USA",
    "code": "90210"
  }
}
```

L'esempio precedente è associato allo schema per la tabella dei clienti:

Nome tabella	Nome colonna	Tipo di dati	Chiave
customer	ID cliente	VARCHAR	PK
customer	name	VARCHAR	

e la tabella virtuale customer_address:

Nome tabella	Nome colonna	Tipo di dati	Chiave
customer_address	ID cliente	VARCHAR	PC/FK
customer_address	indirizzo1	VARCHAR	
customer_address	indirizzo2	VARCHAR	
customer_address	city	VARCHAR	
customer_address	Regione	VARCHAR	
customer_address	country	VARCHAR	
customer_address	code	VARCHAR	

Esempio di campo di matrice incorporata

Per i campi di matrice in un documento, il driver JDBC crea anche una mappatura a una tabella virtuale.

```
{
  "Collection: customer1",
  "_id": "112233",
  "name": "George Jackson",
  "subscriptions": [
    "Vogue",
    "People",
    "USA Today"
  ]
}
```

L'esempio precedente è associato allo schema della tabella customer1:

Nome tabella	Nome colonna	Tipo di dati	Chiave
cliente1	id cliente1	VARCHAR	PK
cliente1	name	VARCHAR	

e la tabella virtuale customer1_subscriptions:

Nome tabella	Nome colonna	Tipo di dati	Chiave
customer1_abbonamenti	id cliente1	VARCHAR	PC/FK
customer1_abbonamenti	abbonamenti_index_lv10	BIGINT	PK
customer1_abbonamenti	value	VARCHAR	
customer_address	city	VARCHAR	
customer_address	Regione	VARCHAR	
customer_address	country	VARCHAR	
customer_address	code	VARCHAR	

Supporto SQL

Il driver JDBC di Amazon DocumentDB è un driver di sola lettura che supporta un sottoinsieme di SQL-92 e alcune estensioni comuni. Per ulteriori informazioni, consulta la [documentazione sulle limitazioni SQL](#) e [la documentazione sulle limitazioni JDBC](#).

Risoluzione dei problemi

In caso di problemi nell'utilizzo del driver JDBC di Amazon DocumentDB, consulta la [Guida alla risoluzione dei problemi](#).

Connect tramite il driver ODBC di Amazon DocumentDB

Il driver ODBC per Amazon DocumentDB fornisce un'interfaccia relazionale SQL per gli sviluppatori e consente la connettività da strumenti di BI come Power BI Desktop e Microsoft Excel.

Per informazioni più dettagliate, consulta la [documentazione del driver ODBC di Amazon DocumentDB su GitHub](#).

Argomenti

- [Nozioni di base](#)
- [Configurazione del driver ODBC Amazon DocumentDB in Windows](#)
- [Connect ad Amazon DocumentDB da Microsoft Excel](#)
- [Connect ad Amazon DocumentDB da Microsoft Power BI Desktop](#)
- [Generazione automatica di schemi](#)
- [Supporto SQL e limitazioni](#)
- [Risoluzione dei problemi](#)

Nozioni di base

Fase 1: Crea cluster Amazon DocumentDB

Se non disponi già di un cluster Amazon DocumentDB, sarà possibile iniziare.

Note

Amazon DocumentDB è un servizio esclusivamente VPC (Virtual Private Cloud). Se ti connetti da una macchina locale esterna al VPC del cluster, dovrai creare una connessione SSH a un'istanza Amazon EC2. In questo caso, avvia il cluster utilizzando le istruzioni in [Connect with EC2](#). Consulta [Utilizzo di un tunnel SSH per Connect ad Amazon DocumentDB](#) per ulteriori informazioni sul tunneling SSH e quando potrebbe essere necessario.

Fase 2. Installazione JRE o JDK

A seconda dell'applicazione di BI, potrebbe essere necessario assicurarsi che sul computer sia installata un'installazione JRE o JDK a 64 bit versione 8 o successiva. Puoi scaricare Java SE Runtime Environment 8 [qui](#).

Fase 3. Scarica il driver ODBC di Amazon DocumentDB

Scarica il driver ODBC di Amazon DocumentDB [qui](#). Scegli il programma di installazione appropriato (ad esempio, `documentdb-odbc-1.0.0.msi`). Segui la guida all'installazione.

Fase 4. Utilizzo di un tunnel SSH per Connect ad Amazon DocumentDB

I cluster Amazon DocumentDB vengono distribuiti all'interno di Amazon Virtual Private Cloud (Amazon VPC). È possibile accedervi direttamente dalle istanze Amazon EC2 o da altri AWS servizi distribuiti nello stesso Amazon VPC. Inoltre, è possibile accedere ad Amazon DocumentDB da istanze Amazon EC2 o altri AWS servizi in diversi VPC nella stessa AWS regione o in altre regioni tramite peering VPC.

Tuttavia, supponiamo che il tuo caso d'uso richieda che tu (o la tua applicazione) accediate alle risorse Amazon DocumentDB dall'esterno del VPC del cluster. Questo sarà il caso della maggior parte degli utenti che non eseguono la propria applicazione su una macchina virtuale nello stesso VPC del cluster Amazon DocumentDB. Quando ti connetti dall'esterno del VPC, puoi utilizzare il tunneling SSH (noto anche come port forwarding) per accedere alle tue risorse Amazon DocumentDB.

Per creare un tunnel SSH, sarà necessaria un'istanza Amazon EC2 in esecuzione nello stesso Amazon VPC del cluster Amazon DocumentDB. Puoi utilizzare un'istanza EC2 esistente nello stesso VPC del cluster o crearne una. Puoi configurare un tunnel SSH per il cluster Amazon DocumentDB `sample-cluster.node.us-east-1.docdb.amazonaws.com` eseguendo il seguente comando sul tuo computer locale:

```
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
```

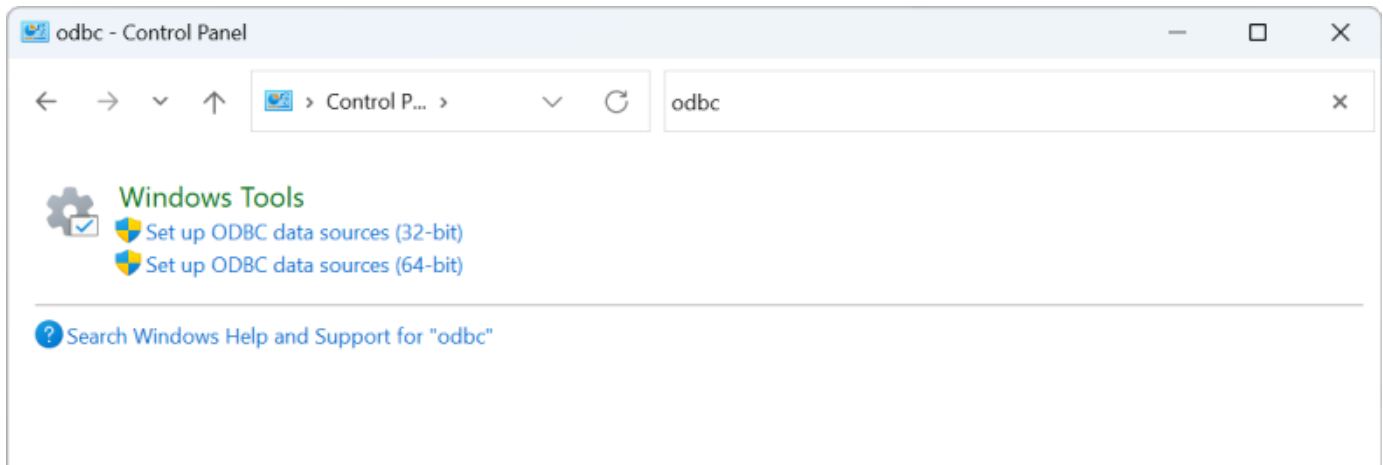
Il flag `-L` viene utilizzato per inoltrare una porta locale. Questo è un prerequisito per la connessione a qualsiasi strumento di BI in esecuzione su un client esterno al VPC. Una volta eseguito il passaggio precedente, puoi passare ai passaggi successivi per lo strumento di BI di tua scelta.

Per ulteriori informazioni sul tunneling SSH, consulta la documentazione sull'[uso di un tunnel SSH per la Connect ad Amazon DocumentDB](#).

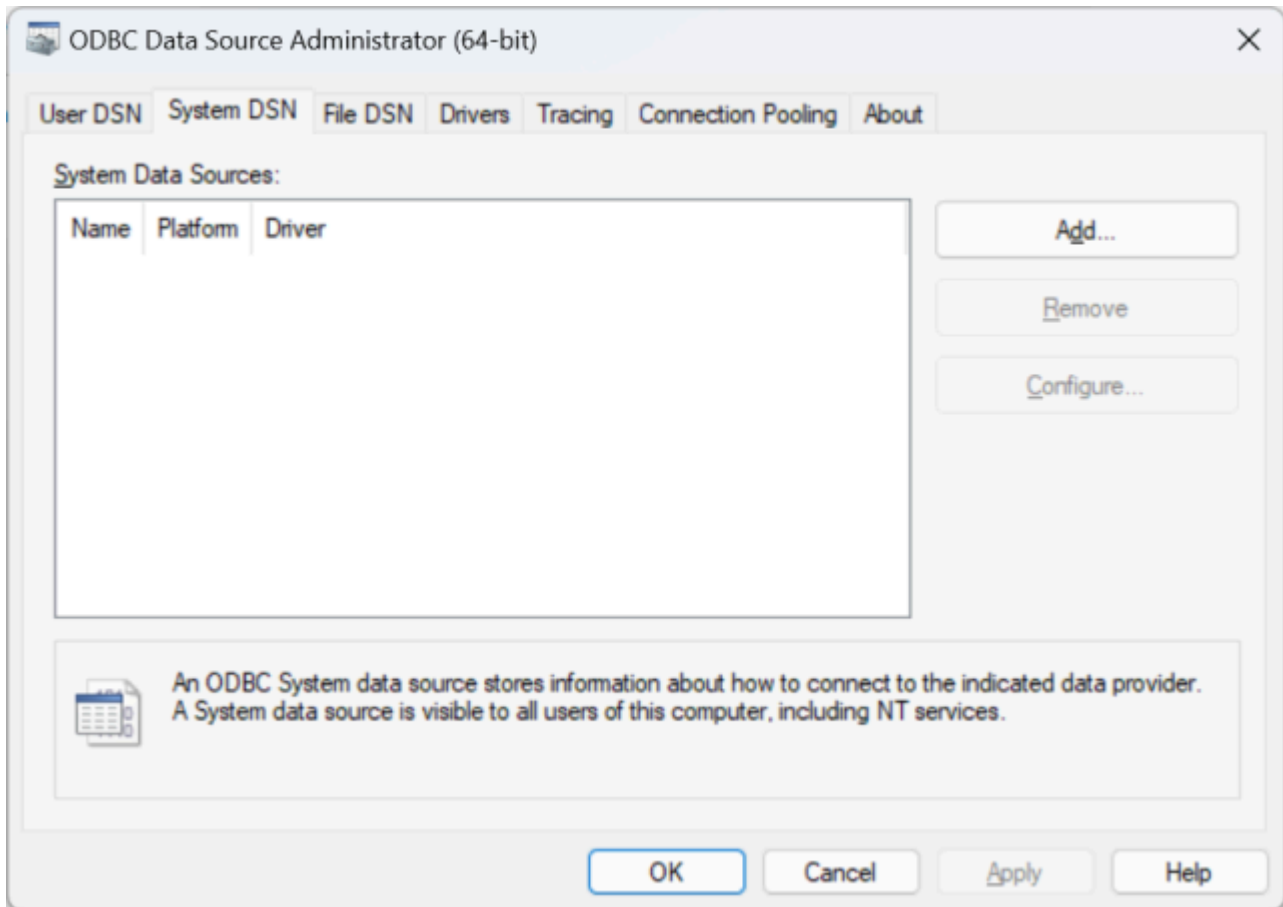
Configurazione del driver ODBC Amazon DocumentDB in Windows

Utilizza le procedure seguenti per configurare il driver ODBC Amazon DocumentDB in Windows:

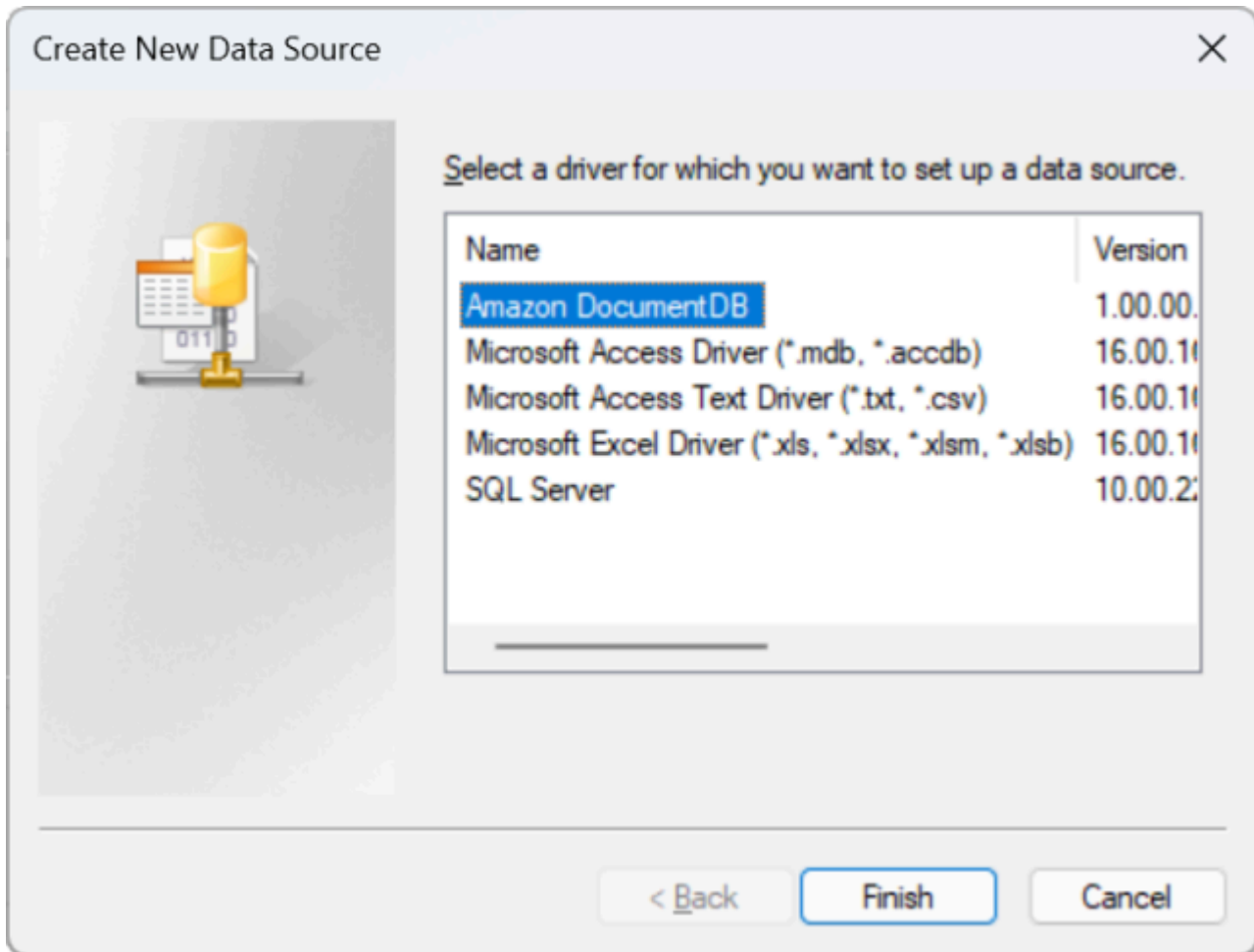
1. Apri il Pannello di controllo in Windows e cerca ODBC (oppure, nel menu, seleziona Strumenti di Windows > Origini dati ODBC (32 bit) o Origini dati ODBC (64 bit)):



2. Seleziona il driver ODBC Data Source Administrator appropriato: opta per la versione a 32 bit se è installata, altrimenti scegli la versione a 64 bit.
3. Seleziona la scheda DSN di sistema, quindi fai clic su Aggiungi... per aggiungere un nuovo DSN:



4. Scegli Amazon DocumentDB dall'elenco dei driver di origine dati:



5. Nella finestra di dialogo Configura Amazon DocumentDB DSN, completa i campi Impostazioni di configurazione, scheda TLS e Verifica connessione, quindi fai clic su Salva:

Configure Amazon DocumentDB DSN

Connection Settings

Data Source Name*: DocumentDB DSN

Hostname*: docdb-2023-04-09-00-13-17.cpluojuahk1k.us-east-2.docdb.amazonaws.c

Port*: 27017

Database*: employees

TLS SSH Tunnel Schema Logging Additional

Enable TLS

Allow Invalid Hostnames (enabling option is less secure)

TLS CA File: C:\Users\narek\global-bundle.pem

Test Connection

User: adminadmin

Password: ●●●●●●●●●●

Enter valid User and Password to test the connection settings. Test

Version: 1.0.0 Save Cancel

- Assicurati di completare il modulo Windows in modo accurato, poiché i dettagli della connessione varieranno a seconda del metodo di tunneling SSH scelto verso l'istanza EC2. Vedi i metodi di tunneling SSH [qui](#). Vedi [Sintassi e opzioni della stringa di connessione](#) per ulteriori informazioni su ciascuna proprietà.

Configure Amazon DocumentDB DSN

Connection Settings

Data Source Name*: DocumentDB DSN

Hostname*: docdb-2023-04-09-00-13-17.cpluojuahk1k.us-east-2.docdb.amazonaws.c

Port*: 27017

Database*: employees

TLS | **SSH Tunnel** | Schema | Logging | Additional

Enable SSH Tunnel

SSH User: ec2-user

SSH Hostname: ec2-18-221-174-48.us-east-2.compute.amazonaws.com

SSH Private Key File: C:\Users\narek\docdbec2keypair.pem ...

SSH Strict Host Key Check (disabling option is less secure)

SSH Known Hosts File: ...

Test Connection

User: adminadmin

Password:

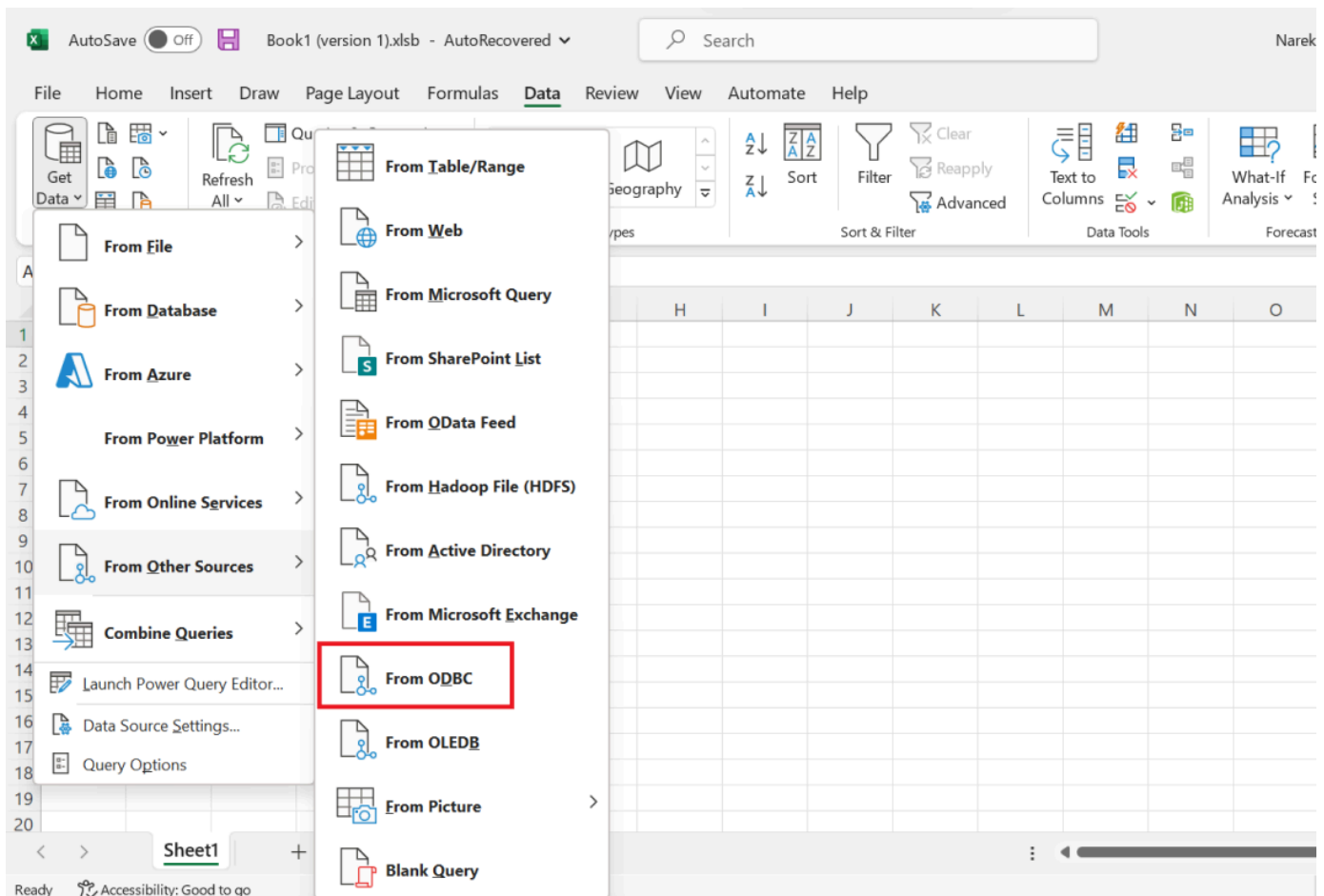
Enter valid User and Password to test the connection settings. **Test**

Version: 1.0.0 **Save** **Cancel**

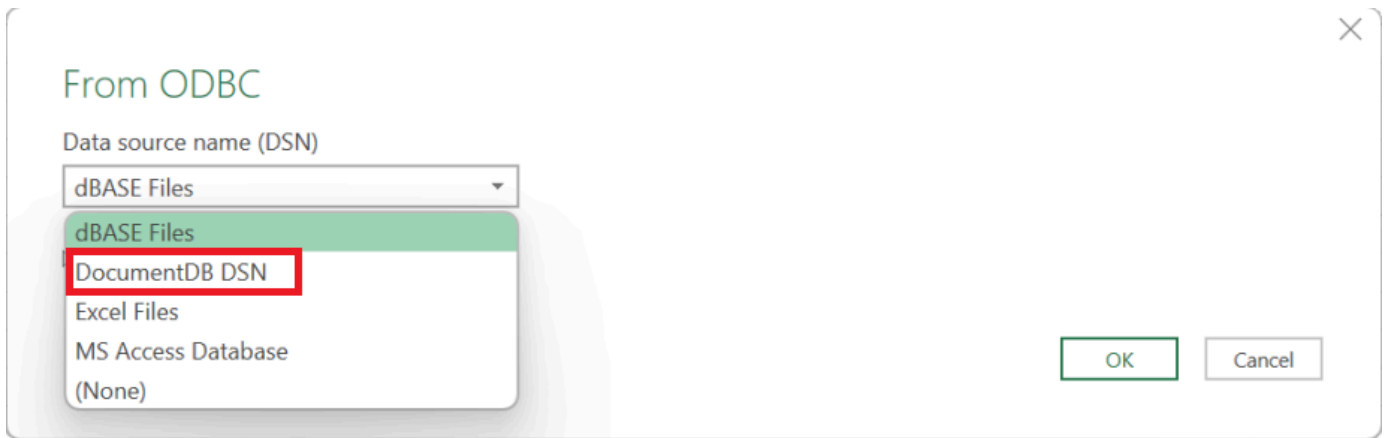
Per ulteriori informazioni sulla configurazione del driver ODBC Amazon DocumentDB su Windows, fai clic [qui](#).

Connect ad Amazon DocumentDB da Microsoft Excel

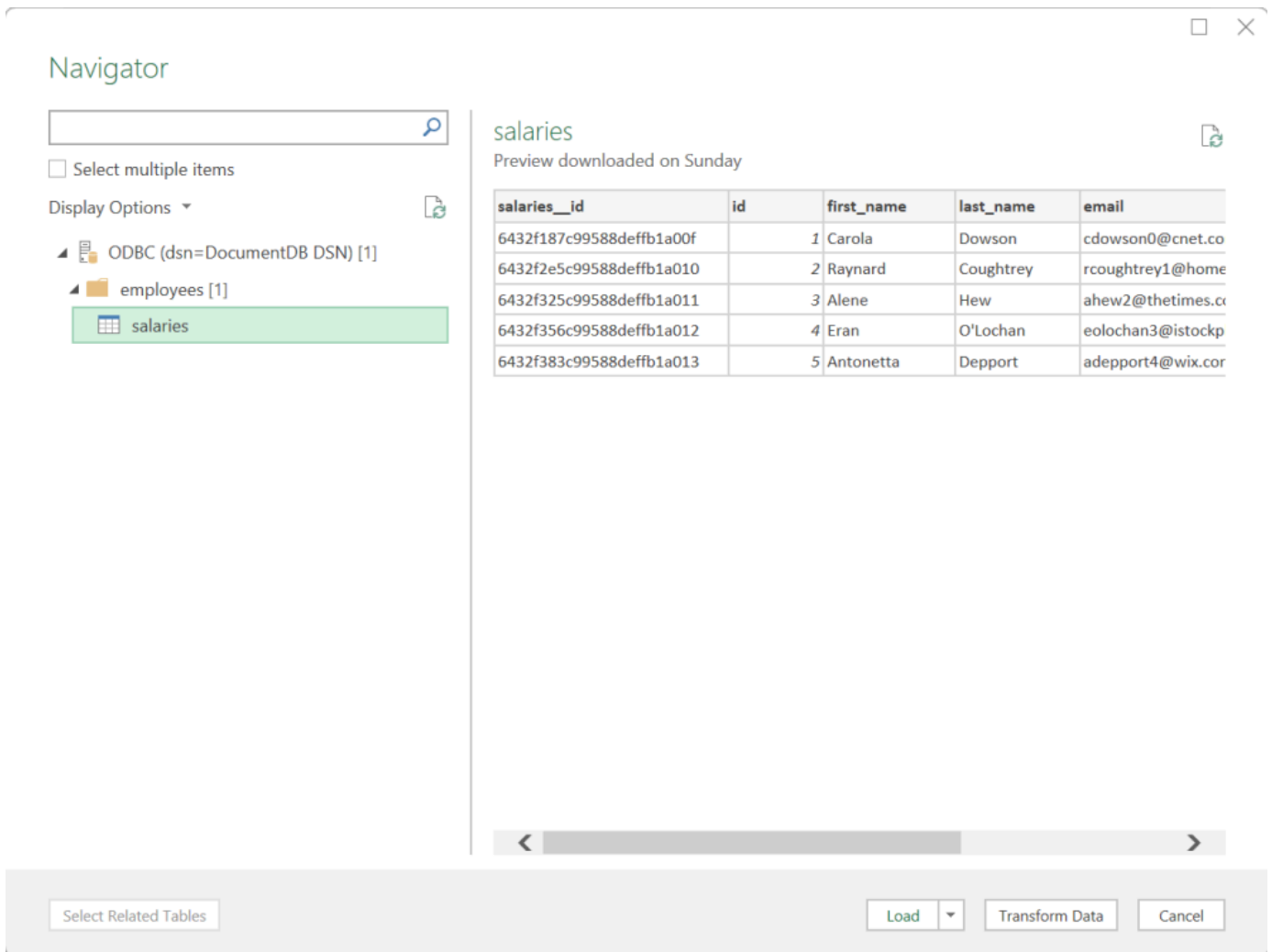
1. Assicurati che il driver Amazon DocumentDB sia stato installato e configurato correttamente. Per ulteriori informazioni, consulta [Configurazione del driver ODBC in Windows](#).
2. Avvia Microsoft Excel.
3. Accedere a Dati > Ottieni dati > Da altre fonti.
4. Scegli tra ODBC:



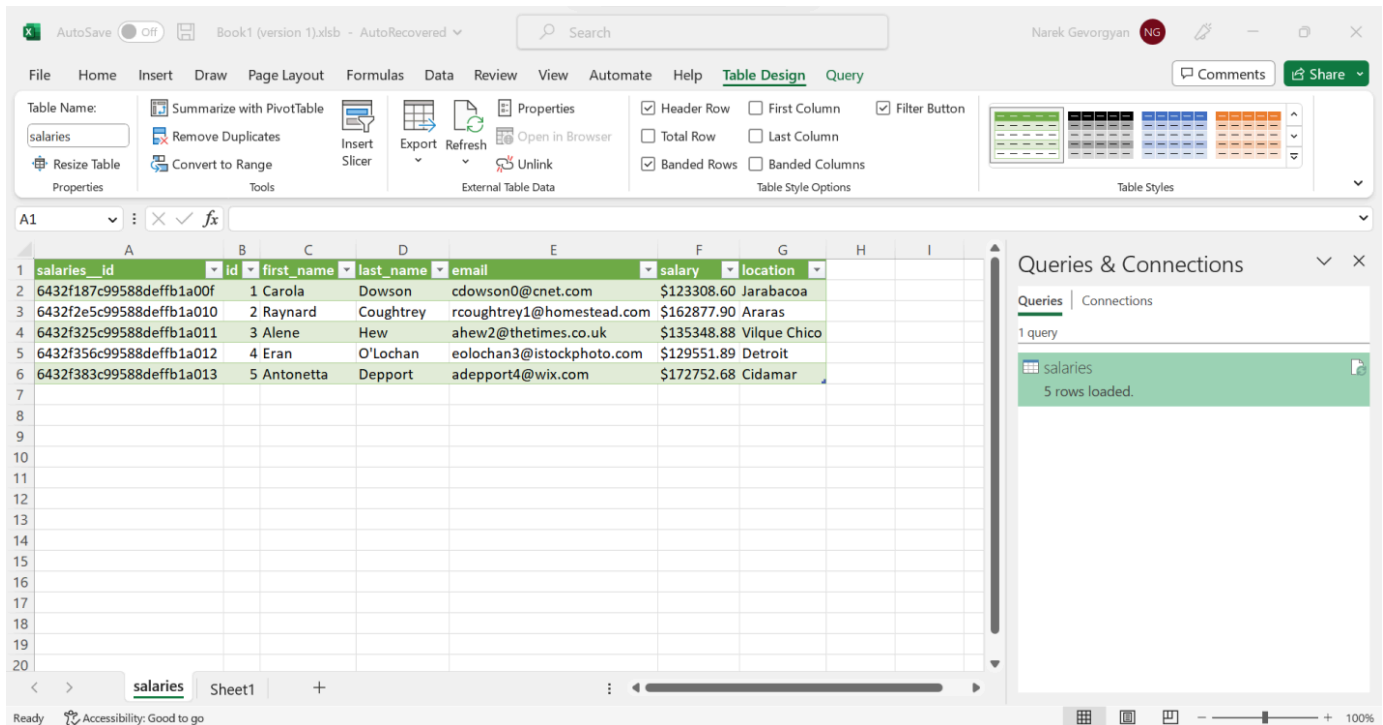
5. Seleziona l'origine dati dal menu a discesa Data source name (DSN) associato ad Amazon DocumentDB:



6. Scegli la raccolta da cui desideri caricare i dati in Excel:



7. Caricare i dati in Excel:



Connect ad Amazon DocumentDB da Microsoft Power BI Desktop

Argomenti


- [Prerequisiti](#)
- [Aggiungere un connettore personalizzato per Microsoft Power BI Desktop](#)
- [Connessione tramite il connettore personalizzato Amazon DocumentDB](#)
- [Configurazione del gateway Microsoft Power BI](#)

Prerequisiti

Prima di iniziare, assicurati che il driver ODBC di Amazon DocumentDB sia installato correttamente.

Aggiungere un connettore personalizzato per Microsoft Power BI Desktop

Copia il file `AmazonDocumentDBConnector.mez` nella cartella `<User>\Documents\Power BI Desktop\Custom Connectors\` (o nella cartella `<User>\OneDrive\Documents\Power BI Desktop\Custom Connectors` se usi OneDrive). Ciò consentirà a Power BI di accedere al connettore personalizzato. Puoi ottenere il connettore per Power BI Desktop [qui](#). Riavvia Power BI Desktop per assicurarti che il connettore sia caricato.

 Note

Il connettore personalizzato supporta solo il nome utente e la password di Amazon DocumentDB per l'autenticazione.

Connessione tramite il connettore personalizzato Amazon DocumentDB

1. Seleziona Amazon DocumentDB (Beta) da Ottieni dati e fai clic su Connect. Se ricevi un avviso relativo all'utilizzo di un servizio di terze parti, fai clic su Continua.


Get Data



All

All

Other

 Amazon DocumentDB (Beta)

Amazon DocumentDB (Beta)

Certified Connectors | Template Apps

Connect

Cancel

2. Inserisci tutte le informazioni necessarie per connetterti al tuo cluster Amazon DocumentDB, quindi fai clic su OK:



Amazon DocumentDB

HostName ⓘ

Port ⓘ

Database ⓘ

TLS (optional) ⓘ

Allow Invalid HostNames (optional) ⓘ

TLS CA File Path (optional) ⓘ

Enable SSH tunnel (optional) ⓘ

SSH tunnel user (optional) ⓘ

SSH tunnel hostname (optional) ⓘ

SSH tunnel private certificate path (optional) ⓘ

OK

Cancel

Note

A seconda della configurazione del Data Source Name (DSN) del driver ODBC, la schermata dei dettagli della connessione SSH potrebbe non essere visualizzata se sono già state fornite le informazioni necessarie nelle impostazioni DSN.

3. Scegli la modalità di connettività dati:

- **Importa:** carica tutti i dati e memorizza le informazioni su disco. I dati devono essere aggiornati e ricaricati per mostrare gli aggiornamenti dei dati.
- **Interrogazione diretta:** non carica i dati, ma esegue interrogazioni in tempo reale sui dati. Ciò significa che non è necessario aggiornare e ricaricare i dati per mostrare gli aggiornamenti dei dati.

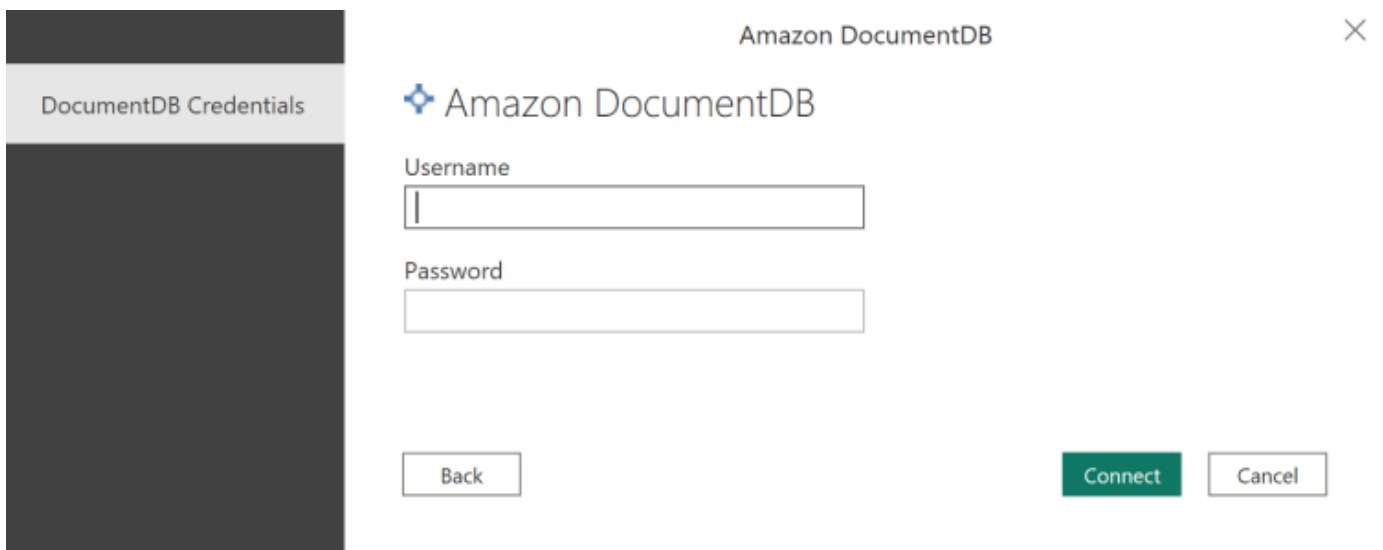


The screenshot shows a dialog box titled "Amazon DocumentDB". It contains a "DSN" field with the text "DocumentDB DSN" entered. Below this is the "Data Connectivity mode" section, with "Import" selected (indicated by a green radio button) and "DirectQuery" unselected (indicated by a grey radio button). At the bottom right, there are two buttons: "OK" (green) and "Cancel" (white).

Note

Se si utilizza un set di dati molto grande, l'importazione di tutti i dati potrebbe richiedere un periodo di tempo più lungo.

- Se è la prima volta che ti connetti a questa fonte di dati, seleziona il tipo di autenticazione e inserisci le tue credenziali quando richiesto. Quindi fai clic su Connect:



The screenshot shows a dialog box titled "Amazon DocumentDB" with a "DocumentDB Credentials" sidebar on the left. The main area contains "Username" and "Password" input fields. At the bottom, there are three buttons: "Back" (white), "Connect" (green), and "Cancel" (white).

- Nella finestra di dialogo Navigator, selezionate le tabelle del database desiderate, quindi fate clic su Carica per caricare i dati o su Trasforma dati per continuare a trasformare i dati.

Navigator

The Navigator interface shows a tree view on the left with the following structure:

- localhost: 27017: odbc-test: F...
 - odbc-test [20]
 - api_robustness_test_001
 - jni_test_001
 - jni_test_001_sub
 - jni_test_001_sub_doc
 - jni_test_001_with_array
 - jni_test_001_with_array_...
 - meta_queries_test_001
 - meta_queries_test_002
 - meta_queries_test_002_...
 - meta_queries_test_002_...
 - queries_test_001
 - queries_test_002
 - queries_test_003
 - queries_test_003_fieldA...
 - queries_test_003_fieldA...
 - queries_test_003_fieldD...
 - queries_test_003_fieldD...
 - queries_test_004

The right pane displays the data for 'queries_test_001' in a table:

queries_test_001_id	fieldDecimal128	fieldDouble	fieldString	fieldObjectId
62196dcc4d91892191475139	3.40282E+20	1.79769E+308	some Text	62196dcc4d91892

At the bottom right, there are three buttons: **Load**, **Transform Data**, and **Cancel**.

Note

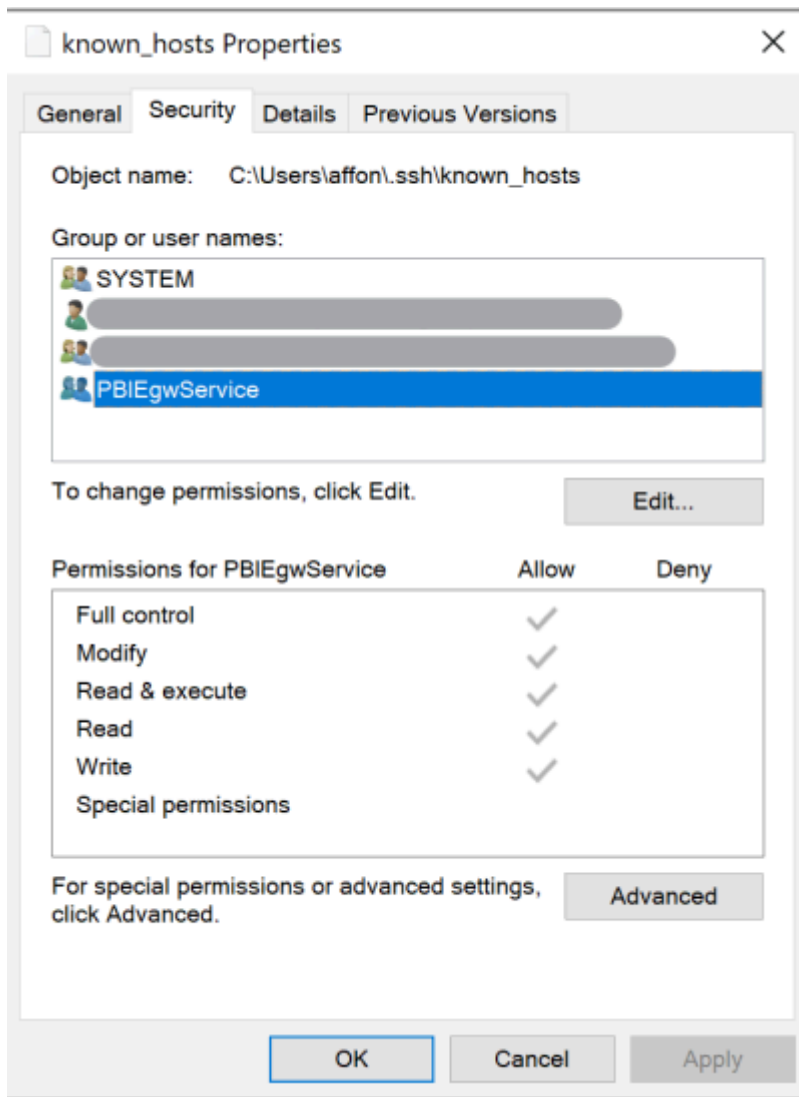
Le impostazioni dell'origine dei dati vengono salvate una volta effettuata la connessione. Per modificarli, seleziona **Trasforma dati > Impostazioni origine dati**.

Configurazione del gateway Microsoft Power BI

Prerequisiti:

- Assicurati che il connettore personalizzato funzioni con Power BI Gateway.
- Assicurati che il DSN ODBC sia stato creato nelle origini dati ODBC nella scheda Sistema sul computer in cui è installato Power BI Gateway.

Se si utilizza la funzionalità tunnel SSH interna, il file `known_hosts` deve trovarsi nel punto in cui l'account del servizio Power BI può accedervi.



Note

Ciò vale anche per qualsiasi file di cui potresti aver bisogno per stabilire una connessione al tuo cluster Amazon DocumentDB, ad esempio un file di certificato dell'autorità di certificazione (CA) (file pem).

Generazione automatica di schemi

Il driver ODBC utilizza il driver JDBC di Amazon DocumentDB tramite JNI (Java Native Interface), facendo in modo che la funzionalità di generazione automatica dello schema funzioni in modo

simile nel driver JDBC. Per ulteriori informazioni sulla generazione automatica di schemi, vedere [Generazione automatica di schemi JDBC](#). Inoltre, per ulteriori informazioni sull'architettura dei driver ODBC, fai clic [qui](#).

Supporto SQL e limitazioni

Il driver ODBC di Amazon DocumentDB è un driver di sola lettura che supporta un sottoinsieme di SQL-92 e alcune estensioni comuni. Per ulteriori informazioni, consulta la documentazione relativa al [supporto e alle limitazioni ODBC](#).

Risoluzione dei problemi

In caso di problemi nell'utilizzo del driver ODBC di Amazon DocumentDB, consulta la [Guida alla risoluzione dei problemi](#).

Quote e limiti di Amazon DocumentDB

Questo argomento descrive le quote di risorse, i limiti e i vincoli di denominazione per Amazon DocumentDB (con compatibilità con MongoDB).

Per alcune funzionalità di gestione, Amazon DocumentDB utilizza una tecnologia operativa condivisa con Amazon Relational Database Service (Amazon RDS) e Amazon Neptune.

Argomenti

- [Tipi di istanze supportati](#)
- [Regioni supportate](#)
- [Quote regionali](#)
- [Limiti di aggregazione](#)
- [Limiti del cluster](#)
- [Limiti di istanze](#)
- [Vincoli per la denominazione](#)
- [Vincoli TTL](#)
- [Limiti elastici del cluster](#)
- [Limiti degli shard del cluster elastico](#)
- [Limiti di CPU, memoria, connessione e cursore del cluster elastico per shard](#)

Tipi di istanze supportati

Amazon DocumentDB supporta istanze on-demand e i seguenti tipi di istanze:

- Ottimizzata per la memoria:
 - Tipi di istanze R6G: db.r6g.large,,,,,db.r6g.2xlarge. db.r6g.4xlarge db.r6g.8xlarge db.r6g.12xlarge db.r6g.16xlarge
 - Tipi di istanze R5: db.r5.large,,,db.r5.2xlarge,db.r5.4xlarge,db.r5.8xlarge. db.r5.12xlarge db.r5.16xlarge db.r5.24xlarge
 - Tipi di istanza R4: db.r4.large, db.r4.2xlarge, db.r4.4xlarge, db.r4.8xlarge e db.r4.16xlarge.
- Prestazioni instabili:

- Tipi di istanze T4G: db.t4g.medium
- Tipi di istanze T3: db.t3.medium

Per ulteriori informazioni sui tipi di istanze supportati e sulle loro specifiche, consulta [Specifiche per la classe di istanza](#).

Regioni supportate

Amazon DocumentDB è disponibile nelle seguenti regioni: AWS

Nome della regione	Regione	Zone di disponibilità (elaborazione)
Stati Uniti orientali (Ohio)	us-east-2	3
Stati Uniti orientali (Virginia settentrionale)	us-east-1	6
US West (Oregon)	us-west-2	4
Sud America (São Paulo)	sa-east-1	3
Asia Pacifico (Hong Kong)	ap-east-1	3
Asia Pacifico (Hyderabad)	ap-south-2	3
Asia Pacifico (Mumbai)	ap-south-1	3
Asia Pacifico (Seul)	ap-northeast-2	4
Asia Pacifico (Singapore)	ap-southeast-1	3
Asia Pacifico (Sydney)	ap-southeast-2	3
Asia Pacifico (Tokyo)	ap-northeast-1	3
Canada (Centrale)	ca-central-1	3

Nome della regione	Regione	Zone di disponibilità (elaborazione)
Regione Cina (Pechino)	cn-north-1	3
Cina (Ningxia)	cn-northwest-1	3
Europa (Francoforte)	eu-central-1	3
Europa (Irlanda)	eu-west-1	3
Europa (Londra)	eu-west-2	3
Europa (Milano)	eu-south-1	3
Europa (Parigi)	eu-west-3	3
Medio Oriente (Emirati Arabi Uniti)	me-central-1	3
AWS GovCloud (Stati Uniti occidentali)	us-gov-west-1	3
AWS GovCloud (Stati Uniti orientali)	us-gov-east-1	3

Quote regionali

Per alcune funzionalità di gestione, Amazon DocumentDB utilizza la tecnologia operativa condivisa con Amazon Relational Database Service (Amazon RDS). La tabella seguente contiene i limiti regionali condivisi tra Amazon DocumentDB e Amazon RDS.

Note

La tecnologia condivisa Amazon RDS descritta sopra si applica solo ai cluster basati su istanze Amazon DocumentDB. I cluster elastici di Amazon DocumentDB non condividono la tecnologia con Amazon RDS.

I seguenti limiti si applicano ai cluster basati su istanze di Amazon DocumentDB e sono per account per regione. AWS

Risorsa	AWS limite predefinito
Cluster	40
Gruppi di parametri di cluster	50
Abbonamenti a eventi	20
Istanze	40
Snapshot manuali dei cluster	100
Repliche di lettura per cluster	15
Gruppi di sottoreti	50
Sottoreti per gruppo di sottoreti	20
Tag per risorsa	50
Gruppi di sicurezza VPC per istanza	5

I seguenti limiti si applicano ai cluster elastici di Amazon DocumentDB e sono per AWS account per regione.

Risorsa	AWS limite predefinito
cluster elastici	20
Cluster elastici vCPU	1.024
Istantanea manuale del cluster elastico	20

È possibile utilizzare Service Quotas per richiedere un aumento per una quota, se la quota è regolabile. Alcune richieste vengono risolte automaticamente, mentre altre vengono inviate a AWS Support. È possibile tenere traccia dello stato di una richiesta di aumento della quota inviata a AWS

Support. Le richieste di aumento delle quote di servizio non ricevono supporto prioritario. Se avete una richiesta urgente, contattateci [AWS Support](#). Per ulteriori informazioni sulle quote di servizio, vedere [Cosa sono le Quote di servizio?](#)

Per richiedere un aumento della quota per Amazon DocumentDB:

1. Aprire la console Quote di servizio in <https://console.aws.amazon.com/servicequotas> e, se necessario, accedere.
2. Nel pannello di navigazione, scegliere servizi AWS .
3. Seleziona Amazon DocumentDB (con compatibilità MongoDB) o Amazon DocumentDB Elastic Cluster dall'elenco, oppure digita uno dei due nel campo di ricerca.
4. Se la quota è regolabile, è possibile selezionarne il pulsante di opzione o il nome, quindi scegliere Richiedi aumento quota in alto a destra della pagina.
5. In Modifica valore quota, immettere il nuovo valore. Questo valore deve essere maggiore di quello corrente.
6. Scegli Richiedi. Dopo aver risolto la richiesta, il valore della quota applicata per la quota viene impostato sul nuovo valore.
7. Per visualizzare eventuali richieste in sospeso o risolte di recente, scegliere Dashboard dal riquadro di navigazione. Per le richieste in sospeso, scegliere lo stato della richiesta per aprire la ricevuta della richiesta. Lo stato iniziale di una richiesta è Pending. Dopo che lo stato sarà cambiato inQuota requested, vedrai il numero del caso con. AWS Support Scegli il numero del caso per aprire il ticket della tua richiesta.

Limiti di aggregazione

La tabella seguente descrive i limiti di aggregazione in Amazon DocumentDB.

Risorsa	Limite
Numero massimo di fasi supportate	500

Limiti del cluster

La tabella seguente descrive i limiti dei cluster basati sulle istanze di Amazon DocumentDB.

Risorsa	Limite
Dimensione cluster (somma di tutte le raccolte e gli indici)	128 TiB
Dimensione raccolta (la somma di tutte le raccolte non può superare il limite del cluster) – Non include la dimensione dell'indice	32 TB
Raccolte per cluster	100.000
Database per cluster	100.000
Dimensione database (la somma di tutti i database non può superare il limite del cluster)	128 TiB
Profondità di nidificazione del documento	200 livelli
Dimensioni dei documenti	16 MB
Dimensione chiave di indice	2.048 byte
Indici per raccolta	64
Chiavi in un indice composto	32
Numero massimo di operazioni di scrittura in un singolo comando batch	100.000

Risorsa	Limite
Numero di utenti per cluster	1000

Limiti di istanze

La tabella seguente descrive i limiti di Amazon DocumentDB per istanza.

Tipo di istanza	Memoria a istanze (GiB)	Connessioni (tutte)	Limite del cursore	Transazioni aperte	Connessioni (attive)
T3. Medio	4	500	30	50	102
T4 G. medio	4	500	30	50	102
R4. Grande	15,25	1700	450	N/D	1100
R4.x grande	30,5	3400	450	N/D	2700
R 4.2 x grande	61	6800	450	N/D	4500
R 4,4 x grande	122	13600	725	N/D	4500
R 4,8 x grande	288	27200	1450	N/D	4500
R4.16 x grande	488	30000	2900	N/D	4500
R5. Grande	16	1700	450	200	1100
R5.x grande	32	3500	450	400	2700
R 5.2x grande	64	7100	450	800	4500
R 5,4x grande	128	14200	760	1600	4500
R 5,8 x grande	256	28400	1520	3200	4500

Tipo di istanza	Memoria a istanze (GiB)	Connessioni (tutte)	Limite del cursore	Transazioni aperte	Connessioni (attive)
R5.12 x grande	383	30000	2280	4800	4500
R5.16 x grande	512	30000	3040	6400	4500
R 5.24 x grande	768	30000	4560	9600	4500
R6 g. Grande	16	1700	450	200	1100
R6 G.X grande	32	3500	450	400	2700
R6 g. 2 x grande	64	7100	450	800	4500
R6 g. 4x grande	128	14200	760	1600	4500
R6 g. 8 x grande	256	28400	1520	3200	4500
R6 g. 12 x grande	383	30000	2280	4800	4500
R6 g. 16 x grande	512	30000	3040	6400	4500

È possibile monitorare e generare allarmi in base ai limiti per istanza utilizzando le seguenti CloudWatch metriche. Per ulteriori informazioni sui CloudWatch parametri di Amazon DocumentDB, consulta [Monitoraggio di Amazon DocumentDB con CloudWatch](#)

Limite	CloudWatch Metriche
Memoria di istanze	FreeableMemory
Connessioni	DatabaseConnectionsMax
Cursori	DatabaseCursorsMax
Transazioni	TransactionsOpenMax

Vincoli per la denominazione

La tabella seguente descrive i vincoli di denominazione in Amazon DocumentDB.

Risorsa	Limite predefinito
Cluster identifier (Identificatore del cluster)	<ul style="list-style-type: none"> La lunghezza è di [1—63] lettere, numeri o trattini. Il primo carattere deve essere una lettera. Non può terminare con un trattino o contenere due trattini consecutivi. Deve essere unico per tutti i cluster (tra Amazon RDS, Amazon Neptune e Amazon DocumentDB) per account e per regione. AWS
Nome raccolta: <col>	La lunghezza è di [1—57] caratteri.
Nome del database: <db>	La lunghezza è di [1-63] caratteri.
Nome raccolta completo: <db>.<col>	La lunghezza è di [3—120] caratteri.
Nome indice completo: <db>.<col>.\$<index>	La lunghezza è di [6-127] caratteri.
Nome indice: <col>.\$<index>	La lunghezza è di [3-63] caratteri.
Identificatore di istanza	<ul style="list-style-type: none"> La lunghezza è di [1-63] lettere, numeri o trattini Il primo carattere deve essere una lettera Non può terminare con un trattino o contenere due trattini consecutivi

Risorsa	Limite predefinito
	<ul style="list-style-type: none">• Deve essere unico per tutte le istanze (tra Amazon RDS, Amazon Neptune e Amazon DocumentDB) per account e per regione. AWS
Master password (Password master)	<ul style="list-style-type: none">• La lunghezza è di [8-100] caratteri ASCII stampabili.• È possibile utilizzare qualsiasi carattere ASCII stampabile eccetto i seguenti:<ul style="list-style-type: none">• / (barra)• " (virgolette doppie)• @ (simbolo chiocciola)
Nome utente master	<ul style="list-style-type: none">• La lunghezza è compresa tra 1 e 63 caratteri alfanumerici.• Il primo carattere deve essere una lettera.• Non può essere una parola riservata del motore di database.
Nome del gruppo di parametri	<ul style="list-style-type: none">• La lunghezza è compresa tra 1 e 255 caratteri alfanumerici.• Il primo carattere deve essere una lettera.• Non può terminare con un trattino o contenere due trattini consecutivi.

Vincoli TTL

Eliminazioni da un indice TTL non sono garantite all'interno di un determinato periodo di tempo e si basano sul miglior tentativo. Fattori come l'utilizzo di risorse dell'istanza, dimensioni documento e throughput complessivo possono influenzare la tempistica di un'eliminazione TTL.

Limiti elastici del cluster

La tabella seguente descrive i limiti massimi nei cluster elastici di Amazon DocumentDB.

Risorsa	Limite
Cluster elastici per regione	20
vCPU sommata tra tutti i cluster elastici per regione	1.024
Istantanee manuali del cluster per regione	20
Shards per cluster	32
Archiviazione per cluster (quando i dati sono distribuiti uniformemente tramite shard-key)	4 PiB
Connessioni al cluster	Il valore più basso di 300.000 o il numero di shard x il limite di connessione associato a vCPU per shard
UnSharded dimensione della raccolta	32 TB
Dimensione della raccolta suddivisa (quando i dati sono distribuiti uniformemente tramite shard-key)	1 PB
Database per cluster	10.000
UnSharded raccolte per cluster	100.000
Raccolte suddivise per cluster	1000

Risorsa	Limite
Utenti per cluster	100
Scrive in un unico comando batch	100.000
Indici per raccolta	64
Profondità di nidificazione del documento	100 livelli
Dimensioni dei documenti	16MB
Dimensione chiave di indice	2048 byte
Chiavi in un indice composto	32

Limiti degli shard del cluster elastico

La tabella seguente descrive i limiti massimi di shard nei cluster elastici di Amazon DocumentDB.

Risorsa	Limite
vCPU per istanza shard	64
Istanze per shard	16
Archiviazione per shard	128 TiB
Spazio di archiviazione per raccolta per frammento	32 TB

Limiti di CPU, memoria, connessione e cursore del cluster elastico per shard

La tabella seguente descrive i limiti massimi di CPU, memoria, connessione e cursore negli shard di cluster elastici di Amazon DocumentDB.

VCPUs per shard	Memoria di istanza (GiB)	Limite di connessione	Limite del cursore
2	16	1700	450
4	32	3500	450
8	64	7100	450
16	128	14200	760
32	256	28400	1520
48	383	30000	2280
64	512	30000	3040

Esecuzione di query

Questa sezione spiega tutti gli aspetti delle interrogazioni con Amazon DocumentDB.

Argomenti

- [Interrogazione di documenti](#)
- [Piano di query](#)
- [Spiega i risultati](#)
- [Interrogazione di dati geospaziali con Amazon DocumentDB](#)
- [Indice parziale](#)
- [Esecuzione di ricerche di testo con Amazon DocumentDB](#)

Interrogazione di documenti

A volte, potrebbe essere necessario cercare nell'inventario dello store online, in modo che i clienti possano vedere e acquistare ciò che vendi. Eseguire query su una raccolta è relativamente semplice, sia per le ricerche su tutti i documenti della raccolta che per quelle solo sui documenti che soddisfano un determinato criterio.

Per eseguire una query per i documenti, utilizza l'operazione `find()`. Il comando `find()` ha un parametro per documenti singoli che definisce i criteri da utilizzare nella scelta dei documenti da restituire. L'output di `find()` è un documento formattato su una sola riga di testo senza interruzioni di riga. Per formattare il documento di output per facilitare la lettura, utilizza `find().pretty()`. Tutti gli esempi di questo argomento utilizzano `.pretty()` per formattare l'output.

I seguenti esempi di codice utilizzano i quattro documenti che avete inserito nella `example` raccolta nei due esercizi precedenti `insertOne()` e `insertMany()` che si trovano nella sezione [Aggiungere documenti di Lavorare con i documenti](#).

Argomenti

- [Recupero di tutti i documenti di una raccolta](#)
- [Recupero di documenti che corrispondono a un valore di campo](#)
- [Recupero di documenti che corrispondono a un documento incorporato](#)
- [Recupero di documenti che corrispondono a un valore di campo in un documento incorporato](#)

- [Recupero di documenti che corrispondono a un array](#)
- [Recupero di documenti che corrispondono a un valore in un array](#)
- [Recupero di documenti tramite operatori](#)

Recupero di tutti i documenti di una raccolta

Per recuperare tutti i documenti nella raccolta, usa l'operazione `find()` con un documento di query vuoto.

La query seguente restituisce tutti i documenti della raccolta `example`.

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

Recupero di documenti che corrispondono a un valore di campo

Per recuperare tutti i documenti che corrispondono a un campo e a un valore, usa l'operazione `find()` con un documento di query che identifica i campi e i valori per la corrispondenza.

Usando i documenti precedenti, questa query restituisce tutti i documenti in cui il campo "Item" è uguale a "Pen".

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

Recupero di documenti che corrispondono a un documento incorporato

Per trovare tutti i documenti che corrispondono a un documento incorporato, utilizza l'operazione `find()` con un documento di query che specifica il nome del documento incorporato e tutti i campi e i valori per quel documento incorporato.

Quando si esegue il confronto di un documento incorporato, il documento incorporato del documento deve avere lo stesso nome che ha nella query. Inoltre, i campi e i valori nel documento incorporato devono corrispondere alla query.

La seguente query restituisce solo il documento "Poster Paint". Questo perché "Pen" ha valori diversi per "OnHand" e "MinOnHand" e "Spray Paint" ha un ulteriore campo (`OrderQty`) rispetto al documento di query.

```
db.example.find({"Inventory": {
```

```
"OnHand": 47,  
"MinOnHand": 50 } } ).pretty()
```

Recupero di documenti che corrispondono a un valore di campo in un documento incorporato

Per trovare tutti i documenti che corrispondono a un documento incorporato, utilizza l'operazione `find()` con un documento di query che specifica il nome del documento incorporato e tutti i campi e i valori per quel documento incorporato.

Considerati i documenti precedenti, la seguente query utilizza la "dot notation" (notazione col punto) per specificare il documento incorporato e i campi di interesse. Vengono restituiti tutti i documenti che corrispondono a questi campi, indipendentemente da quali altri campi possono essere presenti nel documento incorporato. La query restituisce "Poster Paint" e "Spray Paint" perché entrambi corrispondono ai campi e ai valori specificati.

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

Recupero di documenti che corrispondono a un array

Per trovare tutti i documenti che corrispondono a una matrice, utilizzare l'operazione `find()` con il nome della matrice richiesta e tutti i valori in quella matrice. La query restituisce tutti i documenti che hanno una matrice con quel nome in cui i valori della matrice sono identici e nello stesso ordine rispetto alla query.

La seguente query restituisce solo "Pen" perché "Poster Paint" ha un ulteriore colore (White) mentre "Spray Paint" ha i colori in un ordine diverso.

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

Recupero di documenti che corrispondono a un valore in un array

Per trovare tutti i documenti che hanno un valore specifico di matrice, utilizza l'operazione `find()` con il nome della matrice e il valore richiesto.

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

L'operazione precedente restituisce tutti e tre i documenti, in quanto ciascuno di essi dispone di una matrice denominata `Colors` e del valore "Red" all'interno della matrice. Se si specifica il valore "White", la query restituisce solo "Poster Paint".

Recupero di documenti tramite operatori

La seguente query restituisce tutti i documenti in cui il valore `Inventory.OnHand` è inferiore a 50.

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

Per un elenco degli operatori di query supportati, consulta [Operatori per query e proiezioni](#).

Piano di query

Come posso vedere il valore `executionStats` per un piano di query?

Quando si determina il motivo per cui una query viene eseguita più lentamente del previsto, può essere utile capire quali sono i valori `executionStats` per il piano di query. `executionStats` Fornisce il numero di documenti restituiti da una particolare fase (`nReturned`), la quantità di tempo di esecuzione trascorso in ogni fase (`executionTimeMillisEstimate`) e la quantità di tempo necessaria per generare un piano di query (`planningTimeMillis`). È possibile determinare le fasi più dispendiose della query per consentire di concentrare gli sforzi di ottimizzazione dall'output di `executionStats`, come illustrato negli esempi di query riportati di seguito. Il parametro `executionStats` attualmente non supporta i comandi `update` e `delete`.

Note

Amazon DocumentDB emula l'API MongoDB 3.6 su un motore di database appositamente progettato che utilizza un sistema di storage distribuito, con tolleranza ai guasti e riparazione automatica. Di conseguenza, i piani di interrogazione e l'output di `explain()` possono differire tra Amazon DocumentDB e MongoDB. I clienti che desiderano il controllo sul piano di query possono utilizzare l'operatore `$hint` per applicare la selezione di un indice preferito.

Esegui la query che vuoi ottimizzare con il comando `explain()` come segue.

```
db.runCommand({explain: {query document}}).
```



```
explain("executionStats").executionStats;
```

Di seguito è riportato un esempio di operazione.

```
db.fish.find({}).limit(2).explain("executionStats");
```

L'aspetto dell'output di questa operazione è simile al seguente.

```
{
  "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
}
```

Se si desidera vedere solo il valore `executionStats` dalla query di cui sopra, è possibile utilizzare il seguente comando. Per raccolte di piccole dimensioni, il processore di query Amazon DocumentDB può scegliere di non utilizzare un indice se i miglioramenti delle prestazioni sono trascurabili.

```
db.fish.find({}).limit(2).explain("executionStats").executionStats;
```

Cache del piano di query

Per ottimizzare le prestazioni e ridurre la durata della pianificazione, Amazon DocumentDB memorizza internamente nella cache i piani di query. Ciò consente di eseguire query con la stessa forma direttamente utilizzando un piano memorizzato nella cache.

Tuttavia, questa memorizzazione nella cache a volte può causare un ritardo casuale per la stessa query; ad esempio, l'esecuzione di una query che richiede in genere un secondo può occasionalmente impiegare dieci secondi. Questo perché, nel tempo, l'istanza del lettore ha memorizzato nella cache varie forme della query, consumando così memoria. Se si verifica questa lentezza casuale, non è necessario eseguire alcuna azione per liberare la memoria: il sistema gestirà l'utilizzo della memoria al posto dell'utente e, una volta raggiunta una certa soglia, la memoria verrà rilasciata automaticamente.

Spiega i risultati

Se desideri restituire informazioni sui piani di query, Amazon DocumentDB supporta la modalità verbosità. `queryPlanner` | `explain` risultati restituiscono il piano di query selezionato scelto dall'ottimizzatore in un formato simile al seguente:

```
{
  "queryPlanner" : {
    "plannerVersion" : <int>,
    "namespace" : <string>,
```

```
"winningPlan" : {
  "stage" : <STAGE1>,
  ...
  "inputStage" : {
    "stage" : <STAGE2>,
    ...
    "inputStage" : {
      ...
    }
  }
}
```

Le seguenti sezioni definiranno i explain risultati comuni.

Argomenti

- [Fase di scansione e filtro](#)
- [Intersezione dell'indice](#)
- [Unione dell'indice](#)
- [Intersezione/unione di indici multipli](#)
- [Indice composto](#)
- [Fase di ordinamento](#)
- [Fase a gironi](#)

Fase di scansione e filtro

L'ottimizzatore può scegliere una delle seguenti scansioni:

COLLSCAN

Questa fase è una scansione sequenziale di raccolta.

```
{
  "stage" : "COLLSCAN"
}
```

ISCAN

Questa fase esegue la scansione delle chiavi dell'indice. L'ottimizzatore può recuperare il documento in questa fase e ciò può comportare una fase FETCH aggiunta successivamente.

```
db.foo.find({"a": 1})
{
  "stage" : "IXSCAN",
  "direction" : "forward",
  "indexName" : <idx_name>
}
```

FETCH

Se l'ottimizzatore ha recuperato i documenti in una fase diversa da IXSCAN, il risultato includerà una fase FETCH. Ad esempio, la query IXSCAN di cui sopra può generare una combinazione di fasi FETCH e IXSCAN:

```
db.foo.find({"a": 1})
{
  "stage" : "FETCH",
  "inputStage" : {
    "stage" : "IXSCAN",
    "indexName" : <idx_name>
  }
}
```

IXONLYSCAN analizza solo la chiave dell'indice. La creazione di indici composti non eviterà FETCH.

Intersezione dell'indice

IXAND

Amazon DocumentDB può includere uno stage IXAND con un array InputStages di IXSCAN se può utilizzare l'intersezione degli indici. Ad esempio, possiamo vedere risultati come:

```
{
  "stage" : "FETCH",
  "inputStage" : {
```

```

    "stage" : "IXAND",
    "inputStages" : [
      {
        "stage" : "IXSCAN",
        "indexName" : "a_1"
      },
      {
        "stage" : "IXSCAN",
        "indexName" : "b_1"
      }
    ]
  }
}

```

Unione dell'indice

IXOR

Analogamente all'intersezione degli indici, Amazon DocumentDB può IXOR includere uno stage con `inputStages` un array per l'\$or operatore.

```
db.foo.find({"$or": [{"a": {"$gt": 2}}, {"b": {"$lt": 2}}]})
```

Per la query precedente, l'output di spiegazione potrebbe essere simile al seguente:

```

{
  "stage" : "FETCH",
  "inputStage" : {
    "stage" : "IXOR",
    "inputStages" : [
      {
        "stage" : "IXSCAN",
        "indexName" : "a_1"
      },
      {
        "stage" : "IXSCAN",
        "indexName" : "b_1"
      }
    ]
  }
}

```

Intersezione/unione di indici multipli

Amazon DocumentDB può combinare più fasi di intersezione o unione di indici e recuperare il risultato. Per esempio:

```
{
  "stage" : "FETCH",
  "inputStage" : {
    "stage" : "IXOR",
    "inputStages" : [
      {
        "stage" : "IXSCAN",
        ...
      },
      {
        "stage" : "IXAND",
        "inputStages" : [
          {
            "stage" : "IXSCAN",
            ...
          },
          {
            "stage" : "IXSCAN",
            ...
          }
        ]
      }
    ]
  }
}
```

L'utilizzo dell'intersezione dell'indice o degli stadi di unione non è influenzato dal tipo di indice (sparso, composto, ecc.).

Indice composto

L'utilizzo dell'indice composto di Amazon DocumentDB non è limitato nei sottoinsiemi iniziali dei campi indicizzati; può utilizzare l'indice con la parte del suffisso, ma potrebbe non essere molto efficiente.

Ad esempio, l'indice composto di { a: 1, b: -1 } può supportare tutte e tre le query seguenti:

```
db.orders.find( { a: 1 } )
```

```
db.orders.find( { b: 1 } )
```

```
db.orders.find( { a: 1, b: 1 } )
```

Fase di ordinamento

Se esiste un indice sulle chiavi di ordinamento richieste, Amazon DocumentDB può utilizzare l'indice per ottenere l'ordine. In tal caso, il risultato non includerà una SORT fase, ma piuttosto una IXSCAN fase. Se l'ottimizzatore preferisce un ordinamento semplice, includerà una fase come questa:

```
{
  "stage" : "SORT",
  "sortPattern" : {
    "a" : 1,
    "b" : -1
  }
}
```

Fase a gironi

Amazon DocumentDB supporta due diverse strategie di gruppo:

- SORT_AGGREGATE: Ordinamento aggregato su disco.
- HASH_AGGREGATE: aggregato di hash in memoria.

Interrogazione di dati geospaziali con Amazon DocumentDB

Questa sezione spiega come eseguire query sui dati geospaziali con Amazon DocumentDB. Dopo aver letto questa sezione, sarai in grado di rispondere a come archiviare, interrogare e indicizzare i dati geospaziali in Amazon DocumentDB.

Argomenti

- [Panoramica](#)

- [Indicizzazione e archiviazione di dati geospaziali](#)
- [Esecuzione di query su dati geospaziali](#)
- [Limitazioni](#)

Panoramica

I casi d'uso più comuni di Geospatial riguardano l'analisi di prossimità dei dati. Ad esempio, «trovare tutti gli aeroporti nel raggio di 50 miglia da Seattle» o «trovare i ristoranti più vicini da una determinata località». Amazon DocumentDB utilizza la specifica GeoJSON per rappresentare i dati [geospaziali](#). GeoJSON è una specifica open source per la formattazione JSON di forme in uno spazio di coordinate. Le coordinate GeoJSON catturano sia la longitudine che la latitudine, rappresentando le posizioni su una sfera simile alla Terra.

Indicizzazione e archiviazione di dati geospaziali

Amazon DocumentDB utilizza il tipo GeoJSON 'Point' per archiviare dati geospaziali. Ogni documento (o sottodocumento) GeoJSON è generalmente composto da due campi:

- `type`: la forma rappresentata, che indica ad Amazon DocumentDB come interpretare il campo «coordinate». Al momento, Amazon DocumentDB supporta solo punti
- `coordinate`, una coppia di latitudine e longitudine rappresentata come un oggetto in un array, `[longitudine, latitudine]`

Amazon DocumentDB utilizza anche indici 2dsphere per indicizzare i dati geospaziali. Amazon DocumentDB supporta i punti di indicizzazione. Amazon DocumentDB supporta l'interrogazione di prossimità con indicizzazione 2dsphere.

Prendiamo in considerazione uno scenario in cui stai creando un'applicazione per il servizio di consegna di cibo. Vuoi memorizzare diverse coppie di latitudini e longitudini di ristoranti in Amazon DocumentDB. Per farlo, ti consigliamo innanzitutto di creare un indice nel campo Geospatial che contenga la coppia di latitudine e longitudine.

```
use restaurantsdb
db.usarestaurants.createIndex({location:"2dsphere"})
```

L'output di questo comando sarebbe simile al seguente:


```
{
  "createdCollectionAutomatically" : true,
  "numIndexesBefore" : 1,
  "numIndexesAfter" : 2,
  "ok" : 1
}
```

Dopo aver creato un indice, puoi iniziare a inserire dati nella tua raccolta Amazon DocumentDB.

```
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
    ]
  }
});
```

Esecuzione di query su dati geospaziali

Amazon DocumentDB supporta l'interrogazione di prossimità, inclusione e intersezione di dati geospaziali. Un buon esempio di interrogazione di prossimità è la ricerca di tutti i punti (tutti gli aeroporti) che si trovano a meno di una certa distanza e a più di una distanza da un altro punto (città). Un buon esempio di interrogazione di inclusione consiste nel trovare tutti i punti (tutti gli aeroporti) che si trovano in una determinata area/poligono (stato di New York). Un buon esempio di interrogazione di intersezione è la ricerca di un poligono (stato) che si interseca con un punto (città). È possibile utilizzare i seguenti operatori geospaziali per ottenere informazioni dettagliate dai dati.

- **\$nearSphere**- `$nearSphere` è un operatore di ricerca che supporta la ricerca di punti dal più vicino al più lontano da un punto GeoJSON.
- **\$geoNear**- `$geoNear` è un operatore di aggregazione che supporta il calcolo della distanza in metri da un punto GeoJSON.
- **\$minDistance**- `$minDistance` è un operatore di ricerca che viene utilizzato insieme `$nearSphere` o `$geoNear` per filtrare documenti che si trovano almeno alla distanza minima specificata dal punto centrale.
- **\$maxDistance**- `$maxDistance` è un operatore di ricerca che viene utilizzato insieme `$nearSphere` o `$geoNear` per filtrare documenti che si trovano al massimo alla distanza massima specificata dal punto centrale.
- **\$geoWithin**- `$geoWithin` è un operatore di ricerca che supporta la ricerca di documenti con dati geospaziali che esistono interamente all'interno di una forma specificata, ad esempio un poligono.
- **\$geoIntersects**- `$geoIntersects` è un operatore di ricerca che supporta la ricerca di documenti i cui dati geospaziali si intersecano con un oggetto GeoJSON specificato.

Note

`$geoNear` e `$nearSphere` richiedono un indice `2dsphere` sul campo GeoJSON che usi nella tua query di prossimità.

Esempio 1

In questo esempio, imparerai come trovare tutti i ristoranti (punti) ordinati in base alla distanza più vicina da un indirizzo (punto).

Per eseguire tale interrogazione, è possibile utilizzare `$geoNear` per calcolare la distanza di un insieme di punti da un altro punto. È inoltre possibile aggiungere il `distanceMultiplier` per misurare la distanza in chilometri.

```
db.usarestaurants.aggregate([
  {
    "$geoNear":{
      "near":{
        "type":"Point",
        "coordinates":[
          -122.3516,
          47.6156
        ]
      },
      "spherical":true,
      "distanceField":"DistanceKilometers",
      "distanceMultiplier":0.001
    }
  }
])
```

Il comando precedente restituirebbe i ristoranti ordinati in base alla distanza (dalla più vicina alla più lontana) dal punto specificato. L'output di questo comando sarebbe simile al seguente

```
{ "_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 }
```

Per limitare il numero di risultati in una query, utilizzate l'opzione `limit` o.

`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
    }
  }
])
```

```
}  
])
```

Note

`$geoNearstage` supporta le num opzioni `limit` e per specificare il numero massimo di documenti da restituire. `$geoNear` restituisce un massimo di 100 documenti per impostazione predefinita se le num opzioni `limit` o non sono specificate. Questo valore viene sovrascritto dal valore dello `$limit stage`, se presente, e il valore è inferiore a 100.

Esempio 2

In questo esempio, imparerai come trovare tutti i ristoranti (punti) nel raggio di 2 chilometri da un indirizzo specifico (punto). Per eseguire tale interrogazione, è possibile utilizzare `$nearSphere` un valore minimo `$minDistance` e massimo `$maxDistance` da un punto GeoJSON

```
db.usarestaurants.find(  
  "location":{  
    "$nearSphere":{  
      "$geometry":{  
        "type":"Point",  
        "coordinates":[  
          -122.3516,  
          47.6156  
        ]  
      },  
      "$minDistance":1,  
      "$maxDistance":2000  
    }  
  },  
  {  
    "name":1  
  })
```

Il comando precedente restituirebbe i ristoranti a una distanza massima di 2 chilometri dal punto specificato. L'output di questo comando sarebbe simile al seguente

```
{ "_id" : ObjectId("611f3da985009a81ad38e74b"), "name" : "Noodle House" }
```

Limitazioni

Amazon DocumentDB non supporta l'interrogazione o l'indicizzazione di Polygons,,, e. LineString MultiPoint MultiPolygon MultiLineString GeometryCollection

Indice parziale

Un indice parziale indicizza i documenti di una raccolta che soddisfa un criterio di filtro specificato. La funzionalità di indice parziale è supportata nei cluster basati su istanze di Amazon DocumentDB 5.0.

Argomenti

- [Crea un indice parziale](#)
- [Operatori supportati](#)
- [Interrogazione utilizzando un indice parziale](#)
- [Funzionalità di indicizzazione parziale](#)
- [Limitazioni parziali dell'indice](#)

Crea un indice parziale

Per creare un indice parziale, utilizzate il `createIndex()` metodo con l'`partialFilterExpression` opzione. Ad esempio, l'operazione seguente crea un indice composto univoco nella raccolta `orders` che indicizza i documenti il cui `isDelivered` campo è impostato su `true: OrderID`

```
db.orders.createIndex(  
  {"category": 1, "CustomerId": 1, "OrderId": 1},  
  {"unique": true, "partialFilterExpression":  
    {"$and": [  
      {"OrderId": {"$exists": true}},  
      {"isDelivered": {"$eq": false}}  
    ]}  
  }  
)
```

Operatori supportati

- `$eq`
- `$exists`
- `$and` (solo al livello superiore)
- `$gt/$gte/$lt/$lte` (la scansione dell'indice viene utilizzata solo quando il filtro, previsto nella query, corrisponde esattamente all'espressione parziale del filtro) (vedi Limitazioni)

Interrogazione utilizzando un indice parziale

I seguenti modelli di interrogazione sono possibili utilizzando indici parziali:

- Il predicato della query corrisponde esattamente all'espressione del filtro dell'indice parziale:

```
db.orders.find({"$and": [
  {"OrderId": {"$exists": true}},
  {"isDelivered": {"$eq": false}}
])).explain()
```

- Il risultato previsto dal filtro di interrogazione è un sottoinsieme logico del filtro parziale:

```
db.orders.find({"$and": [
  {"OrderId": {"$exists": true}},
  {"isDelivered": {"$eq": false}},
  {"OrderAmount": {"$eq": "5"}}
])).explain()
```

- Un sottopredicato della query può essere utilizzato insieme ad altri indici:

```
db.orders.createIndex({"anotherIndex":1})
db.orders.find({ "$or": [
  {"$and": [
    {"OrderId": {"$exists": true}},
    {"isDelivered": {"$eq": false}}
  ]},
  {"anotherIndex": {"$eq": 5}}
]
}).explain()
```

Note

Un pianificatore di query può scegliere di utilizzare una scansione della raccolta anziché una scansione dell'indice se è efficiente farlo. Questo si verifica in genere per raccolte molto piccole o per query che restituirebbero una grande parte di una raccolta.

Funzionalità di indicizzazione parziale

Elenca gli indici parziali

Elenca gli indici parziali utilizzando l'operazione. `partialFilterExpression` `getIndex` Ad esempio, l'`getIndex` operazione emessa in elenca gli indici parziali con i campi `key`, `name` e `partialFilterExpressions`:

```
db.orders.getIndexes()
```

Questo esempio restituisce il seguente risultato:

```
[
  {
    "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}}
    ]
}
]
```

Espressione di filtro parziale multipla sulla stessa chiave:order

È possibile creare diversi indici parziali per le stesse combinazioni di campi (key:order). Questi indici devono avere un nome diverso.

```
db.orders.createIndex(
  {"OrderId":1},
  {
    name:"firstPartialIndex",
    partialFilterExpression:{"OrderId":{"$exists": true}}
  }
)
```

```
db.orders.createIndex(
  {"OrderId":1},
  {
    name:"secondPartialIndex",
    partialFilterExpression:{"OrderId":{"$gt": 1000}}
  }
)
```

Esegui `getIndexes` l'operazione per elencare tutti gli indici della raccolta:

```
db.orders.getIndexes()
```

Questi esempi restituiscono il seguente risultato:

```
[
  {
    "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

I nomi degli indici devono essere diversi e devono essere eliminati solo per nome.

Indici con proprietà parziali e TTL

È inoltre possibile creare indici con proprietà parziali e TTL specificando entrambe le opzioni durante la creazione dell'indice. `partialFilterExpression` `expireAfterSeconds` Ciò consente di fornire un maggiore controllo su quali documenti vengono ora rimossi da una raccolta.

Ad esempio, potresti avere un indice TTL che identifica i documenti da eliminare dopo un certo periodo di tempo. Ora puoi fornire condizioni aggiuntive su quando eliminare i documenti utilizzando l'opzione di indice parziale:

```

db.orders.createIndex(
  { "OrderTimestamp": 1 },
  {
    expireAfterSeconds: 3600 ,
    partialFilterExpression: { "isDelivered": { $eq: true } }
  }
)

```

```
}  
)
```

Questo esempio restituisce il seguente risultato:

```
{  
  "createdCollectionAutomatically" : false,  
  "numIndexesBefore" : 1,  
  "numIndexesAfter" : 2,  
  "ok" : 1,  
  "operationTime" : Timestamp(1234567890, 1)  
}
```

Eseguite l'`getIndexes` operazione per elencare gli indici presenti nella raccolta:

```
db.orders.getIndexes()  
[  
  {  
    "v" : 4,  
    "key" : {  
      "_id" : 1  
    },  
    "name" : "_id_",  
    "ns" : "test.orders"  
  }  
]
```

Questo esempio restituisce il seguente risultato:

```
[  
  {  
    "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
  }
]

```

Limitazioni parziali dell'indice

Le seguenti limitazioni si applicano alla funzionalità di indice parziale:

- Le query di disuguaglianza in Amazon DocumentDB utilizzeranno un indice parziale solo quando il predicato del filtro di query corrisponde esattamente a ed è `partialFilterExpression` dello stesso tipo di dati.

Note

`$hintNon` può essere utilizzato nemmeno per forzare `IXSCAN` nel caso precedente.

Nell'esempio seguente, `partialFilterExpression` viene applicato solo `field1` ma non `field2` a:

```

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

```

- Gli operatori A `partialFilterExpression` con array non sono supportati. La seguente operazione genererà un errore:

```

db.orders.createIndex(

```

```
  {"CustomerId":1},
  {'partialFilterExpression': {'OrderId': {'$eq': [1000, 1001, 1002]}}}
)
```

- I seguenti operatori non sono supportati nel `partialFilterExpression` campo:
 - `$all`(operatore di matrice)
 - `$mod`(operatore di matrice)
 - `$or`
 - `$xor`
 - `$not`
 - `$nor`
- Il tipo di dati dell'espressione del filtro e del filtro devono essere gli stessi.

Esecuzione di ricerche di testo con Amazon DocumentDB

La funzionalità di ricerca full text nativa di Amazon DocumentDB consente di eseguire ricerche di testo su set di dati testuali di grandi dimensioni utilizzando indici di testo per scopi speciali. Questa sezione descrive le funzionalità della funzione di indice di testo e fornisce passaggi su come creare e utilizzare indici di testo in Amazon DocumentDB. Sono inoltre elencate le limitazioni della ricerca testuale.

Argomenti

- [Funzionalità supportate](#)
- [Utilizzo dell'indice di testo di Amazon DocumentDB](#)
- [Differenze con MongoDB](#)
- [Migliori pratiche e linee guida](#)
- [Limitazioni](#)

Funzionalità supportate

La ricerca testuale di Amazon DocumentDB supporta le seguenti funzionalità compatibili con l'API MongoDB:

- Crea indici di testo su un singolo campo.
- Crea indici di testo composti che includono più di un campo di testo.

- Esegui ricerche di una o più parole.
- Controlla i risultati della ricerca utilizzando i pesi.
- Ordina i risultati della ricerca per punteggio.
- Usa l'indice di testo nella pipeline di aggregazione.
- Cerca la frase esatta.

Utilizzo dell'indice di testo di Amazon DocumentDB

Per creare un indice di testo su un campo contenente dati di tipo stringa, specifica la stringa «testo» come illustrato di seguito:

Indice a campo singolo:

```
db.test.createIndex({"comments": "text"})
```

Questo indice supporta le query di ricerca testuale nel campo stringa «comments» della raccolta specificata.

Crea un indice di testo composto su più di un campo stringa:

```
db.test.createIndex({"comments": "text", "title":"text"})
```

Questo indice supporta le query di ricerca testuale nei campi di stringhe «comments» e «title» della raccolta specificata. È possibile specificare fino a 30 campi durante la creazione di un indice di testo composto. Una volta create, le query di ricerca testuale interrogheranno tutti i campi indicizzati.

Note

È consentito un solo indice di testo per ogni raccolta.

Elencare un indice di testo in una raccolta Amazon DocumentDB

Puoi utilizzarlo `getIndexes()` nella tua collezione per identificare e descrivere gli indici, inclusi gli indici di testo, come mostrato nell'esempio seguente:

```
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
}
]
```

Dopo aver creato un indice, inizia a inserire dati nella tua raccolta Amazon DocumentDB.

```
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"}])
```

Esecuzione di query di ricerca testuale

Esegui una query di ricerca testuale composta da una sola parola

Dovrai utilizzare gli `$search` operatori `$text` e per eseguire ricerche di testo. L'esempio seguente restituisce tutti i documenti in cui il campo indicizzato di testo contiene la stringa «apple» o «apple» in altri formati come «apples»:

```
db.test.find({$text: {$search: "apple"}})
```

Output:

L'output di questo comando è simile al seguente:

```
{ "_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" }
```

Esegui una ricerca testuale composta da più parole

Puoi anche eseguire ricerche di testo di più parole sui dati di Amazon DocumentDB. Il comando seguente restituisce documenti con un campo di testo indicizzato contenente «apple» o «pie»:

```
db.test.find({$text: {$search: "apple pie"}})
```

Output:

L'output di questo comando è simile al seguente:

```
{ "_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" }
```

Esegui una ricerca testuale composta da più frasi

Per una ricerca di frasi composta da più parole, usa questo esempio:

```
db.test.find({$text: {$search: "\"apple pie\""}})
```

Output:

Il comando precedente restituisce documenti con un campo di testo indicizzato contenente la frase esatta «torta di mele». L'output di questo comando è simile al seguente:

```
{ "_id" : 4, "star_rating" : 2, "comments" : "bake the apple pie in the oven" }
```


Esegui una ricerca testuale con filtri

Puoi anche combinare la ricerca testuale con altri operatori di query per filtrare i risultati in base a criteri aggiuntivi:

```
db.test.find({$and: [{star_rating: 5}, {$text: {$search: "interest"}}]})
```

Output:

Il comando precedente restituisce documenti con un campo di testo indicizzato contenente qualsiasi forma di «interesse» e un «star_rating» pari a 5. L'output di questo comando è simile al seguente:

```
{ "_id" : 5, "star_rating" : 5, "comments" : "interesting couch" }
{ "_id" : 6, "star_rating" : 5, "comments" : "interested in couch for sale, year
2022" }
```

Limita il numero di documenti restituiti in una ricerca testuale

Puoi scegliere di limitare il numero di documenti restituiti utilizzando `limit`:

```
db.test.find({$and: [{star_rating: 5}, {$text: {$search: "couch"}}]}).limit(1)
```

Output:

Il comando precedente restituisce un risultato che soddisfa il filtro:

```
{ "_id" : 5, "star_rating" : 5, "comments" : "interesting couch" }
```

Ordina i risultati per punteggio di testo

L'esempio seguente ordina i risultati della ricerca testuale per punteggio di testo:

```
db.test.find({$text: {$search: "apple"}}, {score: {$meta: "textScore"}}).sort({score:
{$meta: "textScore"}})
```

Output:

Il comando precedente restituisce documenti con un campo di testo indicizzato contenente «apple» o «apple» negli altri formati come «apples», e ordina il risultato in base alla pertinenza del documento rispetto al termine di ricerca. L'output di questo comando è simile al seguente:

```
{ "_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 }
```

\$*texte* \$*search* sono supportati anche per aggregatecount, findAndModifyupdate, e delete comandi.

Operatori di aggregazione

Pipeline di aggregazione che utilizza **\$match**

```
db.test.aggregate(
  [ { $match: { $text: { $search: "apple pie" } } } ]
)
```

Output:

Il comando precedente restituisce i seguenti risultati:

```
{ "_id" : 1, "star_rating" : 4, "comments" : "apple is red" }
{ "_id" : 3, "star_rating" : 3, "comments" : "apple - a healthy fruit" }
{ "_id" : 4, "star_rating" : 2, "comments" : "bake the apple pie in the oven" }
{ "_id" : 2, "star_rating" : 5, "comments" : "pie is delicious" }
```

Una combinazione di altri operatori di aggregazione

```
db.test.aggregate(
  [
    { $match: { $text: { $search: "apple pie" } } },
    { $sort: { score: { $meta: "textScore" } } },
    { $project: { score: { $meta: "textScore" } } }
  ]
)
```

Output:

Il comando precedente restituisce i seguenti risultati:

```
{ "_id" : 4, "score" : 0.6079270860936958 }
{ "_id" : 1, "score" : 0.3039635430468479 }
{ "_id" : 2, "score" : 0.3039635430468479 }
{ "_id" : 3, "score" : 0.3039635430468479 }
```

Specificate più campi durante la creazione di un indice di testo

Puoi assegnare pesi a un massimo di tre campi nell'indice di testo composto. Il peso predefinito assegnato a un campo in un indice di testo è uno (1). Il peso è un parametro opzionale e deve essere compreso tra 1 e 100000.

```
db.test.createIndex(
  {
    "firstname": "text",
    "lastname": "text",
    ...
  },
  {
    weights: {
      "firstname": 5,
      "lastname": 10,
      ...
    },
    name: "name_text_index"
  }
)
```

Differenze con MongoDB

La funzionalità di indice di testo di Amazon DocumentDB utilizza un indice invertito con un algoritmo di frequenza dei termini. Per impostazione predefinita, gli indici di testo sono sparsi. A causa delle differenze nella logica di analisi, nei delimitatori di tokenizzazione e in altri modi, lo stesso set di risultati di MongoDB potrebbe non essere restituito per lo stesso set di dati o la stessa forma di query.

Esistono le seguenti differenze aggiuntive tra l'indice di testo di Amazon DocumentDB e MongoDB:

- Gli indici composti che utilizzano indici non testuali non sono supportati.
- Gli indici di testo di Amazon DocumentDB non fanno distinzione tra maiuscole e minuscole e i segni diacritici.
- L'indice di testo supporta solo la lingua inglese.

- L'indicizzazione del testo dei campi matrice (o a più chiavi) non è supportata. Ad esempio, la creazione di un indice di testo su «a» con il documento {«a»: [«apple», «pie»]} avrà esito negativo.
- L'indicizzazione del testo con caratteri jolly non è supportata.
- Gli indici di testo univoci non sono supportati.
- L'esclusione di un termine non è supportata.

Migliori pratiche e linee guida

- Per prestazioni ottimali nelle query di ricerca di testo che prevedono l'ordinamento in base a punteggi di testo, si consiglia di creare l'indice di testo prima di caricare i dati.
- Gli indici di testo richiedono spazio di archiviazione aggiuntivo per una copia interna ottimizzata dei dati indicizzati. Ciò ha implicazioni aggiuntive in termini di costi.

Limitazioni

La ricerca di testo presenta le seguenti limitazioni in Amazon DocumentDB:

- La ricerca di testo è supportata solo nei cluster basati su istanze di Amazon DocumentDB 5.0.

Risoluzione dei problemi Amazon DocumentDB

Le sezioni seguenti forniscono informazioni su come risolvere i problemi che potresti riscontrare durante l'utilizzo di Amazon DocumentDB (con compatibilità con MongoDB).

Argomenti

- [Problemi di connessione](#)
- [Creazione dell'indice](#)
- [Prestazioni e utilizzo delle risorse](#)

Problemi di connessione

Hai problemi di connessione? Di seguito sono riportati alcuni scenari comuni e come risolverli.

Argomenti

- [Impossibile connettersi a un endpoint Amazon DocumentDB](#)
- [Test della connessione a un'istanza Amazon DocumentDB](#)
- [Connessione a un endpoint non valido](#)

Impossibile connettersi a un endpoint Amazon DocumentDB

Quando provi a connetterti ad Amazon DocumentDB, il seguente è uno dei messaggi di errore più comuni che potresti ricevere.

```
connecting to: mongodb://docdb-2018-11-08-21-47-27.cluster-ccuszb3pn5e.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-ccuszb3pn5e.us-east-1.docdb.amazonaws.com:27017, connection attempt failed :
connect@src/mongo/shell/mongo.js:237:13
@(connect):1:6
exception: connect failed
```

Ciò che questo messaggio di errore significa in genere è che il tuo client (la shell mongo in questo esempio) non può accedere all'endpoint Amazon DocumentDB. Questo potrebbe accadere per vari motivi:

Argomenti

- [Connessione da endpoint pubblici](#)
- [Connessioni interregionali](#)
- [Connessione da diversi Amazon VPC](#)
- [Il gruppo di sicurezza blocca le connessioni in entrata](#)
- [Problema relativo alle preferenze di lettura del driver Java Mongo](#)

Connessione da endpoint pubblici

Stai cercando di connetterti a un cluster Amazon DocumentDB direttamente dal tuo laptop o dal tuo computer di sviluppo locale.

Il tentativo di connettersi a un cluster Amazon DocumentDB direttamente da un endpoint pubblico, come un laptop o una macchina di sviluppo locale, avrà esito negativo. Amazon DocumentDB è disponibile solo per il cloud privato virtuale (VPC) e attualmente non supporta endpoint pubblici. Pertanto, non puoi connetterti direttamente al tuo cluster Amazon DocumentDB dal tuo laptop o dall'ambiente di sviluppo locale esterno al tuo VPC.

Per connetterti a un cluster Amazon DocumentDB dall'esterno di un Amazon VPC, puoi utilizzare un tunnel SSH. Per ulteriori informazioni, consulta [Connessione a un cluster Amazon DocumentDB dall'esterno di un Amazon VPC](#). Inoltre, se il tuo ambiente di sviluppo si trova in un Amazon VPC diverso, puoi anche utilizzare VPC Peering e connetterti al tuo cluster Amazon DocumentDB da un altro Amazon VPC nella stessa regione o in un'altra regione.

Connessioni interregionali

Stai tentando di connetterti a un cluster Amazon DocumentDB in un'altra regione.

Se provi a connettersi a un cluster Amazon DocumentDB da un'istanza Amazon EC2 in una Regione diversa da quella del cluster, ad esempio, tentando di connettersi a un cluster nella Regione Stati Uniti orientali (Virginia settentrionale), (us-east-1), (us-west-2).

Per verificare la Regione del cluster Amazon DocumentDB, esegui comando. La regione è nell'endpoint.

```
aws docdb describe-db-clusters \  
  --db-cluster-identifier sample-cluster \  
  --query 'DBClusters[*].Endpoint'
```

L'aspetto dell'output di questa operazione è simile al seguente.

```
[  
  "sample-cluster.node.us-east-1.docdb.amazonaws.com"  
]
```

Per verificare la regione dell'istanza EC2, esegui il comando seguente.

```
aws ec2 describe-instances \  
  --query 'Reservations[*].Instances[*].Placement.AvailabilityZone'
```

L'aspetto dell'output di questa operazione è simile al seguente.

```
[  
  [  
    "us-east-1a"  
  ]  
]
```

Connessione da diversi Amazon VPC

Stai cercando di connetterti a un cluster Amazon DocumentDB da un VPC diverso da quello su cui è distribuito il tuo cluster.

Se sia il tuo cluster Amazon DocumentDB che l'istanza Amazon EC2 si trovano nello stesso Amazon VPC Regione AWS, ma non nello stesso Amazon VPC, non puoi connetterti direttamente al tuo cluster Amazon DocumentDB a meno che il peering VPC non sia abilitato tra i due Amazon VPC.

Per verificare Amazon VPC della tua istanza Amazon DocumentDB, esegui comando.

```
aws docdb describe-db-instances \  
  --db-instance-identifier sample-instance \  
  --query 'DBInstances[*].DBSubnetGroup.VpcId'
```

Per verificare Amazon VPC della tua istanza Amazon EC2, esegui comando.

```
aws ec2 describe-instances \  
  --query 'Reservations[*].Instances[*].VpcId'
```

Il gruppo di sicurezza blocca le connessioni in entrata

Stai tentando di connetterti a un cluster Amazon DocumentDB e il gruppo di sicurezza del cluster non consente connessioni in entrata sulla porta del cluster (porta predefinita: 27017).

Supponiamo che il tuo cluster Amazon DocumentDB e l'istanza Amazon EC2 si trovino entrambi nella stessa regione e Amazon VPC e utilizzino lo stesso gruppo di sicurezza Amazon VPC. Se non riesci a connetterti al tuo cluster Amazon DocumentDB, è probabile che il tuo gruppo di sicurezza (ovvero il firewall) del cluster non consenta connessioni in entrata sulla porta che hai scelto per il tuo cluster Amazon DocumentDB (la porta predefinita è 27017).

Per verificare la porta per il cluster Amazon DocumentDB, esegui comando.

```
aws docdb describe-db-clusters \  
  --db-cluster-identifier sample-cluster \  
  --query 'DBClusters[*].[DBClusterIdentifier,Port]'
```

Per ottenere il gruppo di sicurezza Amazon DocumentDB per il cluster, esegui comando.

```
aws docdb describe-db-clusters \  
  --db-cluster-identifier sample-cluster \  
  --query 'DBClusters[*].[VpcSecurityGroups[*],VpcSecurityGroupId]'
```

Per verificare le regole in entrata per il tuo gruppo di sicurezza, consulta i seguenti argomenti nella documentazione Amazon EC2:

- [Autorizzazione del traffico in entrata per le tue istanze Linux](#)
- [Autorizzazione del traffico in entrata per le tue istanze di Windows](#)

Problema relativo alle preferenze di lettura del driver Java Mongo

Le preferenze di lettura dei client non vengono rispettate e alcuni client non possono scrivere su Amazon DocumentDB dopo il failover a meno che non si riavviino.

Questo problema, scoperto per la prima volta in Java Mongo Driver 3.7.x, si verifica quando un client stabilisce una connessione ad Amazon DocumentDB utilizzando MongoClientSettings

e, in particolare, quando concatena il metodo. `applyToClusterSettings` Le impostazioni del `MongoClient` cluster possono essere definite utilizzando diversi metodi, ad esempio `hosts()``requiredReplicaSetName()`, `emode()`.

Quando il client specifica un solo host nel `hosts()` metodo, la modalità viene impostata su `ClusterConnectionMode.SINGLE` anziché su `ClusterConnectionMode.MULTIPLE` Ciò fa sì che il client ignori la preferenza di lettura e si connetta solo al server configurato in. `hosts()` Quindi, anche se le impostazioni del client sono inizializzate come di seguito, tutte le letture andrebbero comunque alla primaria anziché a quella secondaria.

```
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 = MongoClient.create(settings);
```

Caso di failover

Utilizzando le impostazioni di connessione client di cui sopra, se si verifica un failover e un aggiornamento ritardato del record DNS per l'endpoint del cluster writer, il client proverebbe comunque a eseguire operazioni di scrittura sul vecchio writer (ora lettore dopo failover). Ciò si traduce in un errore lato server (non master) che non viene gestito in modo appropriato dal driver Java (questo è ancora oggetto di indagine). Pertanto, il client può essere lasciato in cattivo stato fino al riavvio del server delle applicazioni, ad esempio.

Esistono due soluzioni alternative:

- I client che si connettono ad Amazon DocumentDB tramite una stringa di connessione non presenteranno questo problema, poiché `ClusterConnectionMode` verranno impostati su questa opzione `MULTIPLE` quando si impostano le preferenze di lettura.

```
MongoClientURI mongoClientURI = new MongoClientURI("mongodb://usr:pass:cluster-
endpoint:27317/test?ssl=false&replicaSet=rs0&readpreference=secondaryPreferred");
MongoClient mongoClient = MongoClient.create(mongoClientURI.getURI());
```

O usando MongoClientSettings builder con il applyConnectionString metodo.

```
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 = MongoClient.create(settings);
```

- Impostato esplicitamente suClusterConnectionMode. MULTIPLE Questo è necessario solo quando si utilizza applyToClusterSettings ehosts().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 = MongoClient.create(settings);
```

Test della connessione a un'istanza Amazon DocumentDB

Puoi verificare la connessione a un cluster utilizzando strumenti comuni di Linux o Windows.

Da un terminale Linux o Unix, puoi eseguire il test della connessione immettendo quanto segue (sostituisci `cluster-endpoint` con l'endpoint e `port` con la porta dell'istanza database):

```
nc -zv cluster-endpoint port
```

Di seguito è riportata un'operazione di esempio e il valore restituito:

```
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!
```

Connessione a un endpoint non valido

Quando ti connetti a un cluster Amazon DocumentDB e utilizzi un endpoint del cluster non valido, viene visualizzato un errore simile al seguente.

```
mongo --ssl \  
  --host sample-cluster.node.us-east-1.docdb.amazonaws.com:27017 \  
  --sslCAFile global-bundle.pem \  
  --username <user-name> \  
  --password <password>
```

L'output sarà il seguente:

```
MongoDB shell version v3.6  
connecting to: mongod://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
```

Per ottenere l'endpoint valido per un cluster, esegui il comando seguente:

```
aws docdb describe-db-clusters \  

```

```
--db-cluster-identifier sample-cluster \  
--query 'DBClusters[*].[Endpoint,Port]'
```

Per ottenere l'endpoint valido per un'istanza, esegui il comando seguente:

```
aws docdb describe-db-instances \  
--db-instance-identifier sample-instance \  
--query 'DBInstances[*].[Endpoint.Address,Endpoint.Port]'
```

Per ulteriori informazioni, consulta [Comprendere gli endpoint di Amazon DocumentDB](#).

Creazione dell'indice

I seguenti argomenti spiegano come agire in caso di mancata creazione dell'indice o indice in background.

Argomenti

- [La compilazione dell'indice non riesce](#)
- [Problemi di latenza e errori di compilazione dell'indice in background](#)

La compilazione dell'indice non riesce

Amazon DocumentDB utilizza lo storage locale su un'istanza come parte del processo di creazione dell'indice. È possibile monitorare l'utilizzo del disco utilizzando la FreeLocalStorageCloudWatchmetrica (CloudWatch -> Metrics -> DocDB -> Instance Metrics). Quando la creazione di un indice consuma tutto il disco locale e ha esito negativo, riceverai un errore. Durante la migrazione dei dati su Amazon DocumentDB, ti invitiamo a creare prima degli indici e poi a inserire i dati. Per ulteriori informazioni sulle strategie di migrazione e sulla creazione di indici, consulta [Migrazione ad Amazon DocumentDB](#) la documentazione di Amazon DocumentDB e il blog: [Migrate from MongoDB to Amazon DocumentDB usando](#) il metodo offline.

Quando si creano indici su un cluster esistente, se la creazione dell'indice richiede più tempo del previsto o non riesce, si consiglia di ridimensionare l'istanza per creare l'indice e, dopo la creazione dell'indice, di ridimensionarla nuovamente. Amazon DocumentDB ti consente di scalare rapidamente le dimensioni delle istanze in pochi minuti utilizzando AWS Management Console o ilAWS CLI. Per ulteriori informazioni, consulta [Gestione delle classi delle istanze](#). Grazie ai prezzi delle istanze al secondo, paghi solo per la risorsa che utilizzi al secondo.

Problemi di latenza e errori di compilazione dell'indice in background

Le build di indici in background in Amazon DocumentDB non vengono avviate fino al completamento di tutte le query sull'istanza principale avviate prima dell'avvio della creazione dell'indice. Se è presente una query di lunga durata, le build dell'indice in background verranno bloccate fino al termine della query e quindi il completamento può richiedere più tempo del previsto. Ciò è valido anche se le raccolte sono vuote.

Le build di indici in primo piano non presentano lo stesso comportamento di blocco. Invece, le build di indici in primo piano bloccano esclusivamente la raccolta fino al completamento della creazione dell'indice. Pertanto, per creare indici su una raccolta vuota ed evitare il blocco su query di lunga durata, suggeriamo di utilizzare build di indici in primo piano.

Note

Amazon DocumentDB consente la creazione di un solo indice in background su una raccolta in qualsiasi momento. Se le operazioni DDL (Data Definition Language) come `createIndex()` o `dropIndex()` vengono eseguite sulla stessa raccolta durante la creazione di un indice in background, tale creazione non riesce.

Prestazioni e utilizzo delle risorse

Questa sezione fornisce domande e soluzioni per problemi di diagnostica comuni nelle distribuzioni di Amazon DocumentDB. Gli esempi forniti utilizzano la shell Mongo e si riferiscono a una singola istanza. Per trovare un endpoint dell'istanza, consulta [Comprendere gli endpoint di Amazon DocumentDB](#).

Argomenti

- [Come posso determinare il numero di operazioni di inserimento, aggiornamento ed eliminazione eseguite sulla mia raccolta tramite l'API Mongo?](#)
- [Come posso analizzare le prestazioni della cache?](#)
- [Come posso trovare e terminare le query bloccate o dalla prolungata esecuzione?](#)
- [Come posso visualizzare un piano di query e ottimizzare una query?](#)
- [Come posso visualizzare un piano di query in cluster elastici?](#)
- [Come posso creare un elenco di tutte le operazioni in esecuzione su un'istanza?](#)

- [Come faccio a sapere quando una query sta facendo progressi?](#)
- [Come faccio a determinare il motivo per cui un sistema funziona improvvisamente lentamente?](#)
- [Come posso determinare la causa dell'elevato utilizzo della CPU su una o più istanze del cluster?](#)
- [Come faccio a determinare i cursori aperti su un'istanza?](#)
- [Come posso determinare la versione corrente del motore Amazon DocumentDB?](#)
- [In che modo posso analizzare l'utilizzo degli indici e identificare gli indici non utilizzati?](#)
- [Come posso identificare gli indici mancanti?](#)
- [Riepilogo delle domande utili](#)

Come posso determinare il numero di operazioni di inserimento, aggiornamento ed eliminazione eseguite sulla mia raccolta tramite l'API Mongo?

Per visualizzare il numero di operazioni di inserimento, aggiornamento ed eliminazione eseguite su una determinata raccolta, esegui il seguente comando su quella raccolta:

```
db.collection.stats()
```

L'output di questo comando descrive quanto segue nel suo `opCounters` campo:

- `numDocsIns`- Il numero di documenti inseriti in questa raccolta. Ciò include i documenti inseriti utilizzando i `insertMany` comandi `insert` and, nonché i documenti inseriti da un `upsert`.
- `numDocsUpd`- Il numero di aggiornamenti dei documenti in questa raccolta. Ciò include i documenti aggiornati utilizzando i `findAndModify` comandi `update` and.
- `numDocsDel`- Il numero di documenti eliminati da questa raccolta. Sono inclusi i documenti eliminati utilizzando i `findAndModify` comandi `deleteOne` `deleteMany` `remove`,, e.
- `LastReset`: l'ora in cui questi contatori sono stati reimpostati l'ultima volta. Le statistiche fornite da questo comando vengono ripristinate all'avvio/arresto del cluster o all'aumento/riduzione dell'istanza.

Di seguito è riportato un esempio di output dell'esecuzione. `db.collection.stats()`

```
{
  "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)
}
```

Questo comando stats deve essere usato quando si visualizzano contatori specifici della raccolta per le operazioni di inserimento, aggiornamento ed eliminazione tramite l'API Mongo. Un altro modo per visualizzare i contatori delle operazioni specifici della raccolta consiste nell'abilitare il controllo DML. Il numero di operazioni di inserimento, aggiornamento ed eliminazione su tutte le raccolte durante intervalli di un minuto può essere visualizzato in [Monitoraggio di Amazon DocumentDB con CloudWatch](#)

Come posso analizzare le prestazioni della cache?

L'analisi delle prestazioni della cache può fornire informazioni sull'efficienza del recupero dei dati e sulle prestazioni del sistema e si basa sulla quantità di dati letti dal disco rispetto alla cache.

Forniamo statistiche sulla cache sul numero di accessi alla cache (dati letti dalla cache) e errori di cache (dati che non si trovano nella cache e letti dal disco) per fornire informazioni sulle prestazioni della cache. Le statistiche della cache per una raccolta specifica possono essere trovate eseguendo il seguente comando su quella raccolta:

```
db.collection.stats()
```

I valori nel `cacheStats` campo nell'output di questo comando forniscono le statistiche della cache per la raccolta e le statistiche totali della cache per gli indici creati nella raccolta. Queste statistiche sono elencate di seguito:

- **collBlksHit**- Il numero di blocchi letti dalla cache durante le operazioni su questa raccolta.
- **collBlksRead**- Il numero di blocchi letti dal disco (cache mancante) durante le operazioni su questa raccolta.
- **collHitRatio**- Il rapporto di accesso alla cache per questa raccolta ($100 * [\text{collBlksHit} / (\text{collBlksHit} + \text{collBlksRead})]$).
- **idxBlksHit**- Il numero di blocchi letti dalla cache per ogni indice creato su questa raccolta.
- **idxBlksRead**- Il numero di blocchi letti dal disco (mancanti nella cache) per ogni indice creato su questa raccolta.
- **idxHitRatio**- Il rapporto di accessi alla cache per gli indici creati su questa raccolta ($100 * [\text{idxBlksHit} / (\text{idxBlksHit} + \text{idxBlksRead})]$).
- **lastReset**- L'ora in cui queste statistiche sono state reimpostate l'ultima volta. Le statistiche fornite da `db.collection.stats()` vengono reimpostate all'avvio/arresto del cluster o all'aumento/riduzione dell'istanza.

Utilizzando il comando è inoltre possibile trovare una suddivisione dei `idxBlksRead` campi `idxBlksHit` e per ogni indice. `indexStats` Le statistiche sulla cache specifiche dell'indice possono essere trovate eseguendo il comando seguente:

```
db.collection.aggregate([{$indexStats:{}}]).pretty()
```

Per ogni indice, nel `cacheStats` campo sono disponibili le seguenti statistiche sulla cache:

- **blksHit**- Il numero di blocchi letti dalla cache per questo indice.
- **blksRead**- Il numero di blocchi letti dal disco per questo indice.

- **blksHitRatio**- Il rapporto di accesso alla cache arrotondato a quattro cifre decimali, calcolato da.
 $100 * [\text{blksHit} / (\text{blksHit} + \text{blksRead})]$

Come posso trovare e terminare le query bloccate o dalla prolungata esecuzione?

Le query degli utenti possono essere eseguite lentamente a causa di un piano di query non ottimale o possono essere bloccate a causa di conflitti tra risorse.

Per trovare le query con esecuzione prolungata che rallentano a causa di un piano di query non ottimale o le query bloccate a causa di conflitti tra risorse, utilizza il comando `currentOp`. Puoi applicare filtri al comando per ridurre l'elenco delle query pertinenti da terminare. È necessario che `opid` sia associato alla query con esecuzione prolungata per poterla terminare.

La query seguente utilizza il comando `currentOp` per elencare tutte le query bloccate o in esecuzione per più di 10 secondi.

```
db.adminCommand({
  aggregate: 1,
  pipeline: [
    {$currentOp: {}},
    {$match:
      {$or: [
        {secs_running: {$gt: 10}},
        {WaitState: {$exists: true}}]}}}
    {$project: {_id:0, opid: 1, secs_running: 1}}],
  cursor: {}
});
```

Quindi, puoi restringere la query per trovare l'`opid` di una query in esecuzione per più di 10 secondi e terminarla.

Per trovare e terminare una query in esecuzione da più di 10 secondi

1. Trovare l'`opid` della query.

```
db.adminCommand({
  aggregate: 1,
  pipeline: [
    {$currentOp: {}},
```

```

    {$match:
      {$or:
        [{secs_running: {$gt: 10}},
         {WaitState: {$exists: true}}]}]},
    cursor: {}
  });

```

L'aspetto dell'output di questa operazione è simile al seguente (formato JSON).

```

{
  "waitedMS" : NumberLong(0),
  "cursor" : {
    "firstBatch" : [
      {
        "opid" : 24646,
        "secs_running" : 12
      }
    ],
    "id" : NumberLong(0),
    "ns" : "admin.$cmd"
  },
  "ok" : 1
}

```

2. Terminare la query utilizzando l'operazione `killOp`.

```
db.adminCommand({killOp: 1, op: 24646});
```

Come posso visualizzare un piano di query e ottimizzare una query?

Il rallentamento dell'elaborazione di una query può essere dovuto a un'esecuzione che richiede una scansione completa della raccolta per selezionare i documenti pertinenti. Talvolta, creare indici appropriati consente di accelerare l'esecuzione di una query. Per rilevare questo tipo di scenario e stabilire i campi per cui creare degli indici, puoi usare il comando `explain`.

Note

Amazon DocumentDB emula l'API MongoDB 3.6 su un motore di database appositamente progettato che utilizza un sistema di storage distribuito, con tolleranza ai guasti e riparazione automatica. Di conseguenza, i piani di interrogazione e l'output di `explain()` possono

differire tra Amazon DocumentDB e MongoDB. I clienti che desiderano il controllo sul piano di query possono utilizzare l'operatore `$hint` per applicare la selezione di un indice preferito.

Esegui la query che vuoi ottimizzare con il comando `explain` come segue.

```
db.runCommand({explain: {<query document>}})
```

Di seguito è riportato un esempio di operazione.

```
db.runCommand({explain:{
  aggregate: "sample-document",
  pipeline: [{$match: {x: {$eq: 1}}}],
  cursor: {batchSize: 1}}
});
```

L'aspetto dell'output di questa operazione è simile al seguente (formato JSON).

```
{
  "queryPlanner" : {
    "plannerVersion" : 1,
    "namespace" : "db.test",
    "winningPlan" : {
      "stage" : "COLLSCAN"
    }
  },
  "serverInfo" : {
    "host" : "...",
    "port" : ...,
    "version" : "..."
  },
  "ok" : 1
}
```

L'output precedente indica che la fase `$match` richiede la scansione delle raccolte complete e di verificare che il campo "x" di ciascun documento corrisponda a 1. Se la raccolta annovera molti documenti, la sua scansione e, di conseguenza, l'elaborazione completa della query sono molto lente. La presenza di "COLLSCAN" nell'output del comando `explain` indica che le prestazioni della query possono migliorare creando indici appropriati.

In questo esempio, la query verifica se il campo "x" è uguale a 1 in tutti i documenti. Pertanto, la creazione di un indice sul campo "x" consente alla query di evitare la scansione completa della raccolta e di utilizzare l'indice per restituire i documenti pertinenti in meno tempo.

Dopo aver creato un indice sul campo "x", l'output di `explain` è il seguente.

```
{
  "queryPlanner" : {
    "plannerVersion" : 1,
    "namespace" : "db.test",
    "winningPlan" : {
      "stage" : "IXSCAN",
      "indexName" : "x_1",
      "direction" : "forward"
    }
  },
  "serverInfo" : {
    "host" : "...",
    "port" : ...,
    "version" : "..."
  },
  "ok" : 1
}
```

La creazione di un indice sul campo "x" ha permesso alla fase `$match` di avviare una scansione dell'indice e ridurre il numero di documenti per cui valutare il predicato `"x = 1"`.

Per raccolte di piccole dimensioni, il processore di query Amazon DocumentDB può scegliere di non utilizzare un indice se i miglioramenti delle prestazioni sono trascurabili.

Come posso visualizzare un piano di query in cluster elastici?

Per esaminare un piano di query in cluster elastici, usa il `explain` comando. Di seguito è riportato un esempio di `explain` operazione su una query di ricerca destinata a una raccolta frammentata:

```
db.runCommand(
  {
    explain: { find: "cities", filter: {"name": "Seoul"}}
  }
)
```

Note

Amazon DocumentDB emula MongoDB su un motore di database creato appositamente. Di conseguenza, i piani di interrogazione e l'output di `explain()` possono differire tra Amazon DocumentDB e MongoDB. Puoi controllare il piano di interrogazione utilizzando l'`$hint` operatore per imporre la selezione di un indice preferito.

L'output di questa operazione può essere simile al seguente (formato JSON):

```
{
  "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-d7c4a0333333",
      "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)
}

```

L'output precedente mostra il piano di interrogazione per la `find` query su un cluster a tre shard. Ogni shard ha più partizioni di dati che possono avere fasi di input diverse. In questo esempio, viene eseguita una «COLLSCAN» (una scansione della raccolta) su tutte le partizioni prima che i risultati vengano uniti nella fase «PARTITION_MERGE» all'interno di ogni shard. I risultati degli shard vengono quindi uniti nella fase «SHARD_MERGE» prima di essere rispediti al client.

Come posso creare un elenco di tutte le operazioni in esecuzione su un'istanza?

In qualità di utente o utente principale, spesso si desidera elencare tutte le operazioni correnti in esecuzione su un'istanza per scopi di diagnostica e risoluzione dei problemi. Per ulteriori informazioni sulla gestione degli utenti, consulta [Gestione degli utenti Amazon DocumentDB](#).

Con la mongo shell, puoi utilizzare la seguente query per elencare tutte le operazioni in esecuzione su un'istanza Amazon DocumentDB.

```
db.adminCommand({currentOp: 1, $all: 1});
```

La query restituisce l'elenco completo di tutte le query e le attività interne del sistema attualmente operative nell'istanza.

L'aspetto dell'output di questa operazione è simile al seguente (formato JSON).

```
{
  "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
}

```

Di seguito sono riportati i valori validi per il campo "desc".

- **INTERNAL**— Attività interne al sistema come la pulizia del cursore o le attività di pulizia degli utenti non aggiornate.
- **TTLMonitor**— Il thread di monitoraggio Time to Live (TTL). Il suo stato di esecuzione si riflette nel campo "active".
- **GARBAGE_COLLECTION**— Il thread interno del Garbage Collector.
- **CONN**— La richiesta dell'utente.

- **CORSOR**— L'operazione è un cursore inattivo che attende che l'utente chiami il comando «getMore» per ottenere il successivo batch di risultati. In questo stato, il cursore consuma memoria, ma non consuma alcuna elaborazione.

L'output precedente elenca, inoltre, tutte le query degli utenti in esecuzione nel sistema. Ogni query viene eseguita in un contesto formato da un database e una raccolta, detto spazio dei nomi. Lo spazio dei nomi di una query è disponibile nel campo "ns".

A volte è necessario elencare tutte le query degli utenti in esecuzione in un determinato spazio dei nomi. Pertanto, l'output precedente deve essere filtrato in base al campo "ns". Di seguito è riportato un esempio di query per filtrare l'output. La query elenca tutte le query degli utenti attualmente in esecuzione nel database "db" e nella raccolta "test" (ovvero lo spazio dei nomi "db.test").

```
db.adminCommand({aggregate: 1,
  pipeline: [{$currentOp: {allUsers: true, idleConnections: true}},
    {$match: {ns: {$eq: "db.test"}}}],
  cursor: {}
});
```

In qualità di utente principale del sistema, puoi visualizzare le domande di tutti gli utenti e anche tutte le attività interne del sistema. Tutti gli altri utenti, invece, possono vedere solo le rispettive query.

Se il numero totale di query e attività di sistema non rientra nelle dimensioni predefinite del cursore di batch, la shell mongo genera automaticamente un oggetto iteratore 'it' che consente di visualizzare il resto dei risultati. Bisogna mantenere in esecuzione il comando 'it' fino a esaurimento dei risultati.

Come faccio a sapere quando una query sta facendo progressi?

Le query degli utenti possono essere eseguite lentamente a causa di un piano di query non ottimale o possono essere bloccate a causa di conflitti tra risorse. Il debug di questo tipo di query è un processo in più fasi che può richiedere di ripetere più volte una stessa operazione.

Innanzitutto, ai fini del debug, occorre elencare tutte le query bloccate o dall'esecuzione prolungata. La query seguente elenca tutte le query utente che sono state in esecuzione per più di 10 secondi o che sono in attesa di risorse.

```
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: {}
    });

```

Ripeti periodicamente la query precedente per determinare se l'elenco delle query cambia e per identificare le query bloccate o con esecuzione prolungata.

L'eventuale presenza del campo `WaitState` nel documento di output della query d'interesse indica che il motivo alla base del blocco o della lenta esecuzione della query è un conflitto tra le risorse. Tale conflitto potrebbe attribuirsi all'I/O, alle attività interne di sistema o ad altre query dell'utente.

L'aspetto dell'output di questa operazione è simile al seguente (formato JSON).

```

{
  "waitedMS" : NumberLong(0),
  "cursor" : {
    "firstBatch" : [
      {
        "opid" : 201,
        "command" : {
          "aggregate" : ...
        },
        "secs_running" : 208,
        "WaitState" : "IO"
      }
    ],
    "id" : NumberLong(0),
    "ns" : "admin.$cmd"
  },
  "ok" : 1
}

```

L'I/O potrebbe rivelarsi inefficace in presenza di molte query afferenti a raccolte diverse e in esecuzione simultanea sulla stessa istanza o se l'istanza dovesse risultare troppo piccola per il set di dati in cui la query viene eseguita. Se le query sono di sola lettura, puoi mitigare la situazione

precedente separando le query per ogni raccolta tra repliche separate. In caso di aggiornamenti simultanei in raccolte diverse o quando l'istanza è troppo piccola per il set di dati, la soluzione di mitigazione consiste nel ridimensionare l'istanza.

Se il conflitto tra le risorse è causato da query di altri utenti, il campo "blockedOn" nel documento di output presenta il valore "opid" della query responsabile del problema. Avvaliti della voce "opid" e segui la concatenazione dei campi "WaitState" e "blockedOn" di tutte le query per individuare la query all'inizio della catena.

Se l'attività in testa alla catena è un'operazione interna, la soluzione di mitigazione consiste nel terminare la query ed eseguirla nuovamente in un secondo momento.

Di seguito è riportato un output di esempio in cui la query di ricerca è bloccata su un blocco di raccolta di proprietà di un'altra attività.

```
{
  "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
}

```

Se "WaitState" presenta i valori "Latch", "SystemLock", "BufferLock", "BackgroundActivity" o "Other", il conflitto tra risorse è originato da attività interne di sistema. Se la situazione persiste per un lungo periodo di tempo, l'unica soluzione di mitigazione consiste nel terminare la query ed eseguirla nuovamente in un secondo momento.

Come faccio a determinare il motivo per cui un sistema funziona improvvisamente lentamente?

Di seguito sono elencati alcuni motivi comuni del rallentamento del sistema:

- Eccessivi conflitti delle risorse tra query simultanee
- Il numero di query simultanee attive aumenta nel tempo
- Attività interne di sistema, ad esempio "GARBAGE_COLLECTION"

Per monitorare l'utilizzo del sistema nel tempo, esegui periodicamente la seguente query "currentOp" e trasferisci i risultati su un archivio esterno. La query conta le query e operazioni nei vari spazi dei nomi presenti nel sistema. Puoi analizzare i risultati relativi all'utilizzo del sistema per stabilire il carico del sistema e prendere le decisioni appropriate.

```
db.adminCommand({aggregate: 1,
  pipeline: [{$currentOp: {allUsers: true, idleConnections: true}},
    {$group: {_id: {desc: "$desc", ns: "$ns", WaitState:
"$WaitState"}, count: {$sum: 1}}}],
  cursor: {}
});
```

Questa query restituisce un'aggregazione delle query eseguite nei vari spazi dei nomi e di tutte le attività interne di sistema, nonché il numero univoco degli eventuali stati di attesa per spazio dei nomi.

L'aspetto dell'output di questa operazione è simile al seguente (formato JSON).

```
{
  "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
}
```

```
}
```

L'output precedente annovera due query dell'utente nello spazio dei nomi "db.test" che sono bloccate a causa di un blocco della raccolta, una query nello spazio dei nomi "admin.\$cmd" e un'attività "TTLMonitor" interna.

Se l'output indica il blocco di molte query in stato di attesa, consulta [Come posso trovare e terminare le query bloccate o dalla prolungata esecuzione?](#)

Come posso determinare la causa dell'elevato utilizzo della CPU su una o più istanze del cluster?

Le sezioni seguenti possono aiutarti a identificare la causa dell'elevato utilizzo della CPU da parte delle istanze. I risultati possono variare a seconda del carico di lavoro.

- Per determinare il motivo per cui un'istanza viene improvvisamente eseguita lentamente, consulta [Come faccio a determinare il motivo per cui un sistema funziona improvvisamente lentamente?](#)
- Per identificare e terminare le query con esecuzione prolungata su una determinata istanza, consulta [Come posso trovare e terminare le query bloccate o dalla prolungata esecuzione?](#)
- Per capire se una query sta avanzando, consulta [Come faccio a sapere quando una query sta facendo progressi?](#)
- Per determinare il motivo per cui l'esecuzione di una query richiede molto tempo, consulta [Come posso visualizzare un piano di query e ottimizzare una query?](#)
- Per tenere traccia delle query con esecuzione prolungata nel corso del tempo, consulta [Profilazione delle operazioni di Amazon DocumentDB.](#)

A seconda del motivo dell'elevato utilizzo della CPU da parte delle istanze, può essere utile eseguire una o più delle operazioni indicate di seguito.

- Se l'istanza primaria presenta un elevato utilizzo della CPU diversamente dalle istanze di replica, valuta la possibilità di distribuire il traffico di lettura tra le repliche tramite le impostazioni delle preferenze di lettura del client (ad esempio, `secondaryPreferred`). Per ulteriori informazioni, consulta [Connessione ad Amazon DocumentDB come set di repliche.](#)

L'utilizzo delle repliche per le letture può ottimizzare l'uso delle risorse del cluster consentendo all'istanza primaria di elaborare più traffico di scrittura. Le letture dalle repliche sono consistenti finali.

- Se l'elevato utilizzo della CPU è il risultato del carico di lavoro di scrittura, la modifica delle dimensioni delle istanze del cluster in un tipo di istanza più grande aumenta il numero di core CPU disponibili per il carico di lavoro. Per ulteriori informazioni, consultare [Istanze](#) e [Specifiche per la classe di istanza](#).
- Se tutte le istanze del cluster presentano un elevato utilizzo della CPU e il carico di lavoro utilizza le repliche per le letture, l'aggiunta di più repliche al cluster aumenta le risorse disponibili per il traffico di lettura. Per ulteriori informazioni, consulta [Aggiungere un'istanza Amazon DocumentDB a un cluster](#).

Come faccio a determinare i cursori aperti su un'istanza?

Quando sei connesso a un'istanza Amazon DocumentDB, puoi usare il comando `db.runCommand("listCursors")` per elencare i cursori aperti su quell'istanza. Esiste un limite massimo di 4.560 cursori attivi aperti in un dato momento su una determinata istanza di Amazon DocumentDB, a seconda del tipo di istanza. Si consiglia generalmente di chiudere i cursori che non sono più in uso in quanto utilizzano risorse su un'istanza e prevedono un limite massimo. Vedi per i limiti specifici [Quote e limiti di Amazon DocumentDB](#).

```
db.runCommand("listCursors")
```

Come posso determinare la versione corrente del motore Amazon DocumentDB?

Per determinare la versione corrente del motore Amazon DocumentDB, esegui il comando seguente.

```
db.runCommand({getEngineVersion: 1})
```

L'aspetto dell'output di questa operazione è simile al seguente (formato JSON).

```
{ "engineVersion" : "2.x.x", "ok" : 1 }
```

Note

La versione del motore per Amazon DocumentDB 3.6 è 1.x.x e la versione del motore per Amazon DocumentDB 4.0 è 2.x.x.

In che modo posso analizzare l'utilizzo degli indici e identificare gli indici non utilizzati?

Per identificare gli indici per una determinata raccolta, eseguire il comando seguente:

```
db.collection.getIndexes()
```

Per analizzare la quantità di indici utilizzati durante le operazioni eseguite sulle raccolte, è possibile utilizzare i comandi `collStats` and `indexStats`. Per visualizzare il numero totale di scansioni eseguite utilizzando gli indici (`index scans`) rispetto al numero di scansioni eseguite senza un indice (`collection scans`), esegui il comando seguente:

```
db.collection.stats()
```

L'output di questo comando include i seguenti valori:

- **idxScans**- Il numero di scansioni eseguite su questa raccolta utilizzando un indice.
- **collScans**- Il numero di scansioni eseguite su questa raccolta senza utilizzare un indice. Queste scansioni avrebbero comportato la ricerca dei documenti della raccolta uno alla volta.
- **lastReset**- L'ora in cui questi contatori sono stati azzerati l'ultima volta. Le statistiche fornite da questo comando vengono ripristinate all'avvio/arresto del cluster o all'aumento/riduzione dell'istanza.

Un'analisi dettagliata dell'utilizzo di ciascun indice è disponibile nell'output del comando seguente. È consigliabile identificare e rimuovere regolarmente gli indici non utilizzati per migliorare le prestazioni e ridurre i costi, in quanto elimina l'elaborazione, lo storage e gli I/O non necessari utilizzati per la manutenzione degli indici.

```
db.collection.aggregate([{$indexStats:{}}]).pretty()
```

L'output di questo comando fornisce i seguenti valori per ogni indice creato nella raccolta:

- **ops**- Il numero di operazioni che hanno utilizzato l'indice. Se il carico di lavoro è in esecuzione per un periodo sufficientemente lungo e si è certi che il carico di lavoro è in uno stato costante, un valore ops pari a zero indica che l'indice non viene utilizzato affatto.
- **numDocsRead**- Il numero di documenti letti durante le operazioni che utilizzano questo indice.

- **since**- Il periodo trascorso da quando Amazon DocumentDB ha iniziato a raccogliere statistiche sull'utilizzo dell'indice, che in genere è il valore dall'ultima operazione di riavvio o manutenzione del database.
- **size**- La dimensione di questo indice in byte.

L'esempio seguente è un esempio di output ottenuto dall'esecuzione del comando precedente:

```
{
  "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" : ...
  }
}
```

```
}
```

Per determinare la dimensione complessiva dell'indice per una raccolta, eseguire il comando seguente:

```
db.collection.stats()
```

Per eliminare un indice inutilizzato, eseguire il comando seguente:

```
db.collection.dropIndex("indexName")
```

Come posso identificare gli indici mancanti?

Puoi utilizzare il [profiler Amazon DocumentDB per registrare le query lente](#). Una query che viene visualizzata ripetutamente nel log di query lento potrebbe indicare che è necessario un indice aggiuntivo per migliorare le prestazioni della query.

È possibile identificare le opportunità di indici utili cercando query a esecuzione prolungata con una o più fasi che eseguono almeno una fase COLLSCAN, il che significa che la fase di query deve leggere tutti i documenti della raccolta al fine di fornire una risposta alla query.

Nell'esempio seguente viene illustrata una query su un insieme di corse in taxi eseguite su una raccolta di grandi dimensioni.

```
db.rides.count({"fare.totalAmount":{"$gt:10.0}}))
```

Per eseguire questo esempio, la query doveva eseguire una scansione della raccolta (cioè leggere ogni singolo documento nella raccolta) poiché non vi è alcun indice sul campo `fare.totalAmount`. L'output del profiler Amazon DocumentDB per questa query è simile al seguente:

```
{
  ...
  "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"
}
```

Per velocizzare la query in questo esempio, si desidera creare un indice su `fare.totalAmount`, come illustrato di seguito.

```
db.rides.createIndex( {"fare.totalAmount": 1}, {background: true} )
```

Note

Gli indici creati in primo piano (ovvero se l'opzione `{background: true}` non è stata fornita durante la creazione dell'indice) assumono un blocco di scrittura esclusivo, che impedisce alle applicazioni di scrivere dati nella raccolta fino al completamento della compilazione dell'indice. Tenere presente questo potenziale impatto durante la creazione di indici nei cluster di produzione. Quando si creano indici, si consiglia di impostare `{background: true}`.

In generale, si desidera creare indici su campi con elevata cardinalità (ad esempio, un numero elevato di valori univoci). La creazione di un indice su un campo con bassa cardinalità può comportare un indice di grandi dimensioni che non viene utilizzato. L'ottimizzatore di query di Amazon DocumentDB considera la dimensione complessiva della raccolta e la selettività degli indici durante la creazione di un piano di query. In alcuni momenti, l'elaboratore di query selezionerà un COLLSCAN anche se è presente un indice. Ciò accade quando l'elaboratore di query stima che l'utilizzo dell'indice non produrrà un vantaggio in termini di prestazioni rispetto alla scansione dell'intera raccolta. Se si desidera forzare l'elaboratore di query affinché utilizzi un particolare indice, è possibile ricorrere all'`hint()` come illustrato di seguito.

```
db.collection.find().hint("indexName")
```

Riepilogo delle domande utili

Le seguenti query possono essere utili per monitorare le prestazioni e l'utilizzo delle risorse in Amazon DocumentDB.

- Utilizza il seguente comando per visualizzare le statistiche su una raccolta specifica, inclusi contatori operativi, statistiche sulla cache, statistiche sugli accessi e statistiche sulle dimensioni:

```
db.collection.stats()
```

- Utilizzate il comando seguente per visualizzare le statistiche su ogni indice creato in una raccolta, comprese le dimensioni dell'indice, le statistiche sulla cache specifiche dell'indice e le statistiche sull'utilizzo dell'indice:

```
db.collection.aggregate([{$indexStats: {}}]).pretty()
```

- Utilizza la seguente query per elencare tutte le attività.

```
db.adminCommand({currentOp: 1, $all: 1});
```

- Il codice seguente elenca tutte le query bloccate o con esecuzione prolungata.

```
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: {}
});
```

- Il codice seguente termina una query.

```
db.adminCommand({killOp: 1, op: <opid of running or blocked query>});
```

- Utilizza il codice seguente per ottenere una visualizzazione aggregata dello stato del sistema.

```
db.adminCommand({aggregate: 1,
  pipeline: [{$currentOp: {allUsers: true, idleConnections: true}},
    {$group: {_id: {desc: "$desc", ns: "$ns", WaitState:
"$WaitState"}, count: {$sum: 1}}}],
  cursor: {}
});
```

Amazon DocumentDB Cluster, istanze e documentazione di riferimento sulle API per la gestione delle risorse

Questa sezione descrive il cluster, l'istanza e le operazioni di gestione delle risorse per Amazon DocumentDB (con compatibilità con MongoDB) a cui è possibile accedere tramite HTTP, AWS Command Line Interface (AWS CLI), o il AWS SDK. È possibile utilizzare queste API per creare, eliminare e modificare i cluster e le istanze.

Important

Queste API vengono utilizzate solo per la gestione di cluster, istanze e risorse correlate. Per informazioni su come connettersi a un cluster Amazon DocumentDB in esecuzione, consulta [Guida introduttiva](#).

Argomenti

- [Azioni](#)
- [Tipi di dati](#)
- [Errori comuni](#)
- [Parametri comuni](#)

Azioni

Le seguenti azioni sono supportate da Amazon DocumentDB (with MongoDB compatibility):

- [AddSourceIdentifierToSubscription](#)
- [AddTagsToResource](#)
- [ApplyPendingMaintenanceAction](#)
- [CopyDBClusterParameterGroup](#)
- [CopyDBClusterSnapshot](#)
- [CreateDBCluster](#)
- [CreateDBClusterParameterGroup](#)
- [CreateDBClusterSnapshot](#)

- [CreateDBInstance](#)
- [CreateDBSubnetGroup](#)
- [CreateEventSubscription](#)
- [CreateGlobalCluster](#)
- [DeleteDBCluster](#)
- [DeleteDBClusterParameterGroup](#)
- [DeleteDBClusterSnapshot](#)
- [DeleteDBInstance](#)
- [DeleteDBSubnetGroup](#)
- [DeleteEventSubscription](#)
- [DeleteGlobalCluster](#)
- [DescribeCertificates](#)
- [DescribeDBClusterParameterGroups](#)
- [DescribeDBClusterParameters](#)
- [DescribeDBClusters](#)
- [DescribeDBClusterSnapshotAttributes](#)
- [DescribeDBClusterSnapshots](#)
- [DescribeDBEngineVersions](#)
- [DescribeDBInstances](#)
- [DescribeDBSubnetGroups](#)
- [DescribeEngineDefaultClusterParameters](#)
- [DescribeEventCategories](#)
- [DescribeEvents](#)
- [DescribeEventSubscriptions](#)
- [DescribeGlobalClusters](#)
- [DescribeOrderableDBInstanceOptions](#)
- [DescribePendingMaintenanceActions](#)
- [FailoverDBCluster](#)
- [ListTagsForResource](#)
- [ModifyDBCluster](#)

- [ModifyDBClusterParameterGroup](#)
- [ModifyDBClusterSnapshotAttribute](#)
- [ModifyDBInstance](#)
- [ModifyDBSubnetGroup](#)
- [ModifyEventSubscription](#)
- [ModifyGlobalCluster](#)
- [RebootDBInstance](#)
- [RemoveFromGlobalCluster](#)
- [RemoveSourceIdentifierFromSubscription](#)
- [RemoveTagsFromResource](#)
- [ResetDBClusterParameterGroup](#)
- [RestoreDBClusterFromSnapshot](#)
- [RestoreDBClusterToPointInTime](#)
- [StartDBCluster](#)
- [StopDBCluster](#)

Le seguenti azioni sono supportate da Amazon DocumentDB Elastic Clusters:

- [CopyClusterSnapshot](#)
- [CreateCluster](#)
- [CreateClusterSnapshot](#)
- [DeleteCluster](#)
- [DeleteClusterSnapshot](#)
- [GetCluster](#)
- [GetClusterSnapshot](#)
- [ListClusters](#)
- [ListClusterSnapshots](#)
- [ListTagsForResource](#)
- [RestoreClusterFromSnapshot](#)
- [StartCluster](#)
- [StopCluster](#)

- [TagResource](#)
- [UntagResource](#)
- [UpdateCluster](#)

Amazon DocumentDB (with MongoDB compatibility)

Le seguenti azioni sono supportate da Amazon DocumentDB (with MongoDB compatibility):

- [AddSourceIdentifierToSubscription](#)
- [AddTagsToResource](#)
- [ApplyPendingMaintenanceAction](#)
- [CopyDBClusterParameterGroup](#)
- [CopyDBClusterSnapshot](#)
- [CreateDBCluster](#)
- [CreateDBClusterParameterGroup](#)
- [CreateDBClusterSnapshot](#)
- [CreateDBInstance](#)
- [CreateDBSubnetGroup](#)
- [CreateEventSubscription](#)
- [CreateGlobalCluster](#)
- [DeleteDBCluster](#)
- [DeleteDBClusterParameterGroup](#)
- [DeleteDBClusterSnapshot](#)
- [DeleteDBInstance](#)
- [DeleteDBSubnetGroup](#)
- [DeleteEventSubscription](#)
- [DeleteGlobalCluster](#)
- [DescribeCertificates](#)
- [DescribeDBClusterParameterGroups](#)
- [DescribeDBClusterParameters](#)
- [DescribeDBClusters](#)
- [DescribeDBClusterSnapshotAttributes](#)

- [DescribeDBClusterSnapshots](#)
- [DescribeDBEngineVersions](#)
- [DescribeDBInstances](#)
- [DescribeDBSubnetGroups](#)
- [DescribeEngineDefaultClusterParameters](#)
- [DescribeEventCategories](#)
- [DescribeEvents](#)
- [DescribeEventSubscriptions](#)
- [DescribeGlobalClusters](#)
- [DescribeOrderableDBInstanceOptions](#)
- [DescribePendingMaintenanceActions](#)
- [FailoverDBCluster](#)
- [ListTagsForResource](#)
- [ModifyDBCluster](#)
- [ModifyDBClusterParameterGroup](#)
- [ModifyDBClusterSnapshotAttribute](#)
- [ModifyDBInstance](#)
- [ModifyDBSubnetGroup](#)
- [ModifyEventSubscription](#)
- [ModifyGlobalCluster](#)
- [RebootDBInstance](#)
- [RemoveFromGlobalCluster](#)
- [RemoveSourceIdentifierFromSubscription](#)
- [RemoveTagsFromResource](#)
- [ResetDBClusterParameterGroup](#)
- [RestoreDBClusterFromSnapshot](#)
- [RestoreDBClusterToPointInTime](#)
- [StartDBCluster](#)
- [StopDBCluster](#)

AddSourceIdentifierToSubscription

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Aggiunge un identificatore di origine a una sottoscrizione alle notifiche di eventi esistente.

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

SourceIdentifier

L'identificatore dell'origine dell'evento da aggiungere:

- Se il tipo di origine è un'istanza, è `DBInstanceIdentifier` necessario fornire a.
- Se il tipo di origine è un gruppo di sicurezza, è `DBSecurityGroupName` necessario fornire un.
- Se il tipo di origine è un gruppo di parametri, è `DBParameterGroupName` necessario fornire a.
- Se il tipo di origine è un'istantanea, è `DBSnapshotIdentifier` necessario fornire a.

Tipo: stringa

Campo obbligatorio: sì

SubscriptionName

Il nome dell'abbonamento di notifica degli eventi di Amazon DocumentDB a cui desideri aggiungere un identificatore di origine.

Tipo: stringa

Campo obbligatorio: sì

Elementi di risposta

Il servizio restituisce il seguente elemento.

EventSubscription

Informazioni dettagliate su un evento a cui ti sei iscritto.

Tipo: oggetto [EventSubscription](#)

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

SourceNotFound

La fonte richiesta non è stata trovata.

Codice di stato HTTP: 404

SubscriptionNotFound

Il nome dell'abbonamento non esiste.

Codice di stato HTTP: 404

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)
- [AWSSDK per JavaScript V3](#)
- [SDK AWS per PHP V3](#)
- [SDK AWS per Python](#)
- [SDK AWS per Ruby V3](#)

AddTagsToResource

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Aggiunge tag di metadati a una risorsa Amazon DocumentDB. Puoi utilizzare questi tag con i report sull'allocazione dei costi per tenere traccia dei costi associati alle risorse di Amazon DocumentDB o in Condition una dichiarazione in AWS Identity and Access Management una policy (IAM) per Amazon DocumentDB.

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

ResourceName

La risorsa Amazon DocumentDB a cui vengono aggiunti i tag. Questo valore è un Amazon Resource Name.

Tipo: stringa

Campo obbligatorio: sì

Tag.Tag.N

I tag da assegnare alla risorsa Amazon DocumentDB.

Tipo: matrice di oggetti [Tag](#)

Campo obbligatorio: sì

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

DBClusterNotFoundFault

DBClusterIdentifiernon si riferisce a un cluster esistente.

Codice di stato HTTP: 404

DBInstanceNotFound

DBInstanceIdentifiernon fa riferimento a un'istanza esistente.

Codice di stato HTTP: 404

DBSnapshotNotFound

DBSnapshotIdentifiernon fa riferimento a un'istantanea esistente.

Codice di stato HTTP: 404

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)
- [AWSSDK per V3 JavaScript](#)
- [SDK AWS per PHP V3](#)
- [SDK AWS per Python](#)
- [SDK AWS per Ruby V3](#)

ApplyPendingMaintenanceAction

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Applica un'azione di manutenzione in sospeso a una risorsa (ad esempio, a un'istanza Amazon DocumentDB).

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

ApplyAction

L'operazione di manutenzione in sospeso da applicare a questa risorsa.

Valori validi: `system-update`, `db-upgrade`

Tipo: stringa

Campo obbligatorio: sì

OptInType

Un valore che specifica il tipo di richiesta di opt-in o annulla una richiesta di opt-in. Una richiesta di consenso esplicito di tipo `immediate` non può essere annullata.

Valori validi:

- `immediate`: applica immediatamente l'azione di manutenzione.
- `next-maintenance` -Applica l'operazione di manutenzione durante la finestra di manutenzione successiva per la risorsa.
- `undo-opt-in`: annulla qualsiasi richiesta di consenso esplicito `next-maintenance` esistente.

Tipo: stringa

Campo obbligatorio: sì

ResourceIdentifier

L'Amazon Resource Name (ARN) della risorsa alla quale viene applicata l'operazione di manutenzione in sospeso.

Tipo: stringa

Campo obbligatorio: sì

Elementi di risposta

Il servizio restituisce il seguente elemento.

ResourcePendingMaintenanceActions

Rappresenta l'output di [ApplyPendingMaintenanceAction](#).

Tipo: oggetto [ResourcePendingMaintenanceActions](#)

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

InvalidDBClusterStateFault

Il cluster non è in uno stato valido.

Codice di stato HTTP: 400

InvalidDBInstanceState

L'istanza specificata non è nello stato disponibile.

Codice di stato HTTP: 400

ResourceNotFoundFault

L'ID della risorsa specificata non è stato trovato.

Codice di stato HTTP: 404

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)

- [AWSSDK per JavaScript V3](#)
- [SDK AWS per PHP V3](#)
- [SDK AWS per Python](#)
- [SDK AWS per Ruby V3](#)

CopyDBClusterParameterGroup

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Copia il gruppo di parametri del cluster specificato.

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

SourceDBClusterParameterGroupIdentifier

L'identificatore o Amazon Resource Name (ARN) per il gruppo di parametri del cluster di origine.

Vincoli:

- È necessario specificare un gruppo di parametri del cluster valido.
- Se il gruppo di parametri del cluster di origine è lo Regione AWS stesso della copia, specificare un identificatore di gruppo di parametri valido, ad esempio `my-db-cluster-param-group`, o un ARN valido.
- Se il gruppo di parametri di origine si trova in un formato Regione AWS diverso da quello della copia, specificare un gruppo di parametri del cluster valido (ARN), ad esempio.
`arn:aws:rds:us-east-1:123456789012:sample-cluster:sample-parameter-group`

Tipo: stringa

Campo obbligatorio: sì

TargetDBClusterParameterGroupDescription

Una descrizione per il gruppo di parametri del cluster copiato.

Tipo: stringa

Campo obbligatorio: sì

TargetDBClusterParameterGroupIdentifier

L'identificatore per il gruppo di parametri del cluster copiato.

Vincoli:

- Non può essere null o vuoto.

- Deve contenere da 1 a 255 lettere, numeri o trattini.
- Il primo carattere deve essere una lettera.
- Non può terminare con un trattino o contenere due trattini consecutivi.

Esempio: `my-cluster-param-group1`

Tipo: stringa

Campo obbligatorio: sì

Tag.Tag.N

I tag da assegnare al gruppo di parametri.

Tipo: matrice di oggetti [Tag](#)

Campo obbligatorio: no

Elementi di risposta

Il servizio restituisce il seguente elemento.

`DBClusterParameterGroup`

Informazioni dettagliate su un gruppo di parametri del cluster.

Tipo: oggetto [DBClusterParameterGroup](#)

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

`DBParameterGroupAlreadyExists`

Esiste già un gruppo di parametri con lo stesso nome.

Codice di stato HTTP: 400

`DBParameterGroupNotFound`

`DBParameterGroupNamenon` fa riferimento a un gruppo di parametri esistente.

Codice di stato HTTP: 404

DBParameterGroupQuotaExceeded

Questa richiesta comporterebbe il superamento del numero consentito di gruppi di parametri.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)
- [AWSSDK per JavaScript V3](#)
- [SDK AWS per PHP V3](#)
- [SDK AWS per Python](#)
- [SDK AWS per Ruby V3](#)

CopyDBClusterSnapshot

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Copia un'istantanea di un cluster.

Per copiare uno snapshot del cluster da uno snapshot del cluster manuale condiviso, `SourceDBClusterSnapshotIdentifier` deve essere l'Amazon Resource Name (ARN) dello snapshot del cluster condiviso. Puoi copiare solo uno snapshot condiviso del cluster di database, crittografato o meno, nella stessa Regione AWS.

Per annullare l'operazione di copia dopo che è in corso, elimina lo snapshot del cluster di destinazione identificato da `TargetDBClusterSnapshotIdentifier` mentre lo snapshot del cluster è in stato di copia.

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

`SourceDBClusterSnapshotIdentifier`

L'identificatore della snapshot del cluster da copiare. Questo parametro non distingue tra maiuscole e minuscole.

Vincoli:

- Deve specificare una snapshot di sistema valida nello stato disponibile.
- Se lo snapshot di origine è Regione AWS uguale alla copia, specificate un identificatore di snapshot valido.
- Se lo snapshot di origine si trova in un formato Regione AWS diverso da quello della copia, specificare un ARN di snapshot del cluster valido.

Esempio: `my-cluster-snapshot1`

Tipo: stringa

Campo obbligatorio: sì

`TargetDBClusterSnapshotIdentifier`

L'identificatore della nuova snapshot del cluster da creare dalla snapshot del cluster di origine. Questo parametro non distingue tra maiuscole e minuscole.

Vincoli:

- Deve contenere da 1 a 63 lettere, numeri o trattini.
- Il primo carattere deve essere una lettera.
- Non può terminare con un trattino o contenere due trattini consecutivi.

Esempio: `my-cluster-snapshot2`

Tipo: stringa

Campo obbligatorio: sì

CopyTags

`true` Impostare su `true` per copiare tutti i tag dallo snapshot del cluster di origine allo snapshot del cluster di destinazione e in altro modo. `false` Il valore predefinito è `false`.

Tipo: Booleano

Campo obbligatorio: no

KmsKeyId

L'ID della AWS KMS chiave per un'istantanea del cluster crittografata. L'ID della chiave AWS KMS è il nome della risorsa Amazon (ARN), l'identificatore della chiave AWS KMS o l'alias della chiave AWS KMS per la chiave di crittografia AWS KMS.

Se copi un'istantanea del cluster crittografata dal tuo Account AWS, puoi specificare un valore per `KmsKeyId` crittografare la copia con una nuova AWS KMS chiave di crittografia. Se non si specifica un valore per `KmsKeyId`, la copia dello snapshot del cluster viene crittografata con la stessa AWS KMS chiave dello snapshot del cluster di origine.

Se si copia un'istantanea del cluster crittografata condivisa da un altro Account AWS, è necessario specificare un valore per `KmsKeyId`.

Per copiare un'istantanea del cluster crittografata su un'altra Regione AWS, imposta `KmsKeyId` l'ID della AWS KMS chiave che desideri utilizzare per crittografare la copia dello snapshot del cluster nella regione di destinazione. AWS KMS le chiavi di crittografia sono specifiche del dispositivo in Regione AWS cui vengono create e non è possibile utilizzare le chiavi di crittografia l'una nell'altra Regione AWS. Regione AWS

Se si copia un'istantanea del cluster non crittografata e si specifica un valore per il `KmsKeyId` parametro, viene restituito un errore.

Tipo: string

Campo obbligatorio: no

PreSignedUrl

L'URL che contiene una richiesta firmata Signature Version 4 per l'azione CopyDBClusterSnapshot API in Regione AWS quella che contiene lo snapshot del cluster di origine da copiare. È necessario utilizzare il PreSignedUrl parametro quando si copia uno snapshot del cluster da un altro. Regione AWS

Se utilizzate uno strumento AWS SDK o ilAWS CLI, potete specificare SourceRegion (o --source-region perAWS CLI) invece di specificare manualmente. PreSignedUrl La specificazione SourceRegion genera automaticamente un URL prefirmato che rappresenta una richiesta valida per l'operazione che può essere eseguita nell'origine. Regione AWS

L'URL predefinito deve essere una richiesta valida per l'azione CopyDBClusterSnapshot API che può essere eseguita nell'origine Regione AWS che contiene lo snapshot del cluster da copiare. La richiesta URL prefirmata deve contenere i seguenti valori di parametro:

- SourceRegion- L'ID della regione che contiene l'istantanea da copiare.
- SourceDBClusterSnapshotIdentifier- L'identificatore per l'istantanea del cluster crittografata da copiare. L'identificatore deve essere nel formato Amazon Resource Name (ARN) per la Regione AWS di origine. Ad esempio, se stai copiando un'istantanea del cluster crittografata da us-east-1Regione AWS, il tuo SourceDBClusterSnapshotIdentifier avrà un aspetto simile al seguente: `arn:aws:rds:us-east-1:12345678012:sample-cluster:sample-cluster-snapshot`
- TargetDBClusterSnapshotIdentifier- L'identificatore per la nuova istantanea del cluster da creare. Questo parametro non fa distinzione tra maiuscole e minuscole.

Tipo: string

Campo obbligatorio: no

Tag.Tag.N

I tag da assegnare allo snapshot del cluster.

Tipo: matrice di oggetti [Tag](#)

Campo obbligatorio: no

Elementi di risposta

Il seguente elemento viene restituito dal servizio.

DBClusterSnapshot

Informazioni dettagliate su un'istantanea del cluster.

Tipo: oggetto [DBClusterSnapshot](#)

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

DBClusterSnapshotAlreadyExistsFault

È già disponibile un'istantanea del cluster con l'identificatore specificato.

Codice di stato HTTP: 400

DBClusterSnapshotNotFoundFault

`DBClusterSnapshotIdentifier` non fa riferimento a un'istantanea del cluster esistente.

Codice di stato HTTP: 404

InvalidDBClusterSnapshotStateFault

Il valore fornito non è uno stato valido di snapshot del cluster.

Codice di stato HTTP: 400

InvalidDBClusterStateFault

Il cluster non è in uno stato valido.

Codice di stato HTTP: 400

KMSKeyNotAccessibleFault

Si è verificato un errore durante l'accesso a una AWS KMS chiave.

Codice di stato HTTP: 400

SnapshotQuotaExceeded

La richiesta comporterebbe il superamento del numero consentito di istantanee.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)
- [AWSSDK per V3 JavaScript](#)
- [SDK AWS per PHP V3](#)
- [SDK AWS per Python](#)
- [SDK AWS per Ruby V3](#)

CreateDBCluster

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Crea un nuovo cluster Amazon DocumentDB.

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

DBClusterIdentifier

Identificatore del cluster. Questo parametro è archiviato come stringa in minuscolo.

Vincoli:

- Deve contenere da 1 a 63 lettere, numeri o trattini.
- Il primo carattere deve essere una lettera.
- Non può terminare con un trattino o contenere due trattini consecutivi.

Esempio: `my-cluster`

Tipo: stringa

Campo obbligatorio: sì

Engine

Il nome del motore di database da utilizzare per questo cluster.

Valori validi: `docdb`

Tipo: stringa

Campo obbligatorio: sì

AvailabilityZones. AvailabilityZoneN.

Elenco delle zone di disponibilità Amazon EC2 in cui possono essere create istanze nel cluster.

Tipo: matrice di stringhe

Campo obbligatorio: no

BackupRetentionPeriod

Il numero di giorni durante i quali vengono conservati i backup automatici. È necessario specificare un valore minimo pari a 1.

Impostazione predefinita: 1

Vincoli:

- Il valore deve essere compreso tra 1 e 35.

Tipo: integer

Campo obbligatorio: no

DBClusterParameterGroupName

Il nome del gruppo di parametri del cluster da associare a questo cluster.

Tipo: string

Campo obbligatorio: no

DBSubnetGroupName

Gruppo di sottoreti da associare a questo cluster.

Vincoli: deve corrispondere al nome di un oggetto `DBSubnetGroup` esistente. Non deve essere predefinito.

Esempio: `mySubnetgroup`

Tipo: string

Campo obbligatorio: no

DeletionProtection

Specifica se questo cluster può essere eliminato. Se `DeletionProtection` è abilitato, il cluster non può essere eliminato a meno che non venga modificato e `DeletionProtection` disabilitato. `DeletionProtection` protegge i cluster dall'eliminazione accidentale.

Tipo: Booleano

Campo obbligatorio: no

EnableCloudwatchLogsExports.Member.

Un elenco di tipi di log che devono essere abilitati per l'esportazione in Amazon CloudWatch Logs. È possibile abilitare i log di audit o i log del profiler. Per ulteriori informazioni, consulta [Auditing Amazon DocumentDB Events e Profiling Amazon DocumentDB Operations](#).

Tipo: matrice di stringhe

Campo obbligatorio: no

EngineVersion

Numero di versione del motore di database da utilizzare. Per impostazione predefinita, --engine-version sarà l'ultima versione principale del motore. Per i carichi di lavoro di produzione, è consigliabile dichiarare esplicitamente questo parametro con la versione principale del motore prevista.

Tipo: string

Campo obbligatorio: no

GlobalClusterIdentifier

L'identificatore del nuovo cluster globale.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 1. Lunghezza massima di 255.

Modello: [A-Za-z][0-9A-Za-z-:._]*

Campo obbligatorio: no

KmsKeyId

Identificatore della chiave AWS KMS per un cluster crittografato.

L'identificatore della chiave AWS KMS è il nome della risorsa Amazon (ARN) per la chiave di crittografia AWS KMS. Se stai creando un cluster tramite lo stesso Account AWS che possiede la chiave di crittografia AWS KMS utilizzata per crittografare il nuovo cluster, puoi utilizzare l'alias della chiave AWS KMS al posto dell'ARN per la chiave di crittografia AWS KMS.

Se non è specificata una chiave di crittografia in KmsKeyId:

- Se il parametro StorageEncrypted è true, Amazon DocumentDB utilizza la chiave di crittografia predefinita.

AWS KMS crea la chiave di crittografia di default per l'Account AWS. L'Account AWS ha una chiave crittografica predefinita diversa per ogni Regione AWS.

Tipo: string

Campo obbligatorio: no

MasterUsername

Nome dell'utente master per il cluster.

Vincoli:

- Deve contenere da 1 a 63 lettere o numeri.
- Il primo carattere deve essere una lettera.
- Non può essere una parola riservata per il motore di database scelto.

Tipo: string

Campo obbligatorio: no

MasterUserPassword

La password per l'utente del database master. Questa password può contenere qualsiasi carattere ASCII stampabile, eccetto la barra (/), le virgolette (") o il simbolo chiocciola (@).

Vincoli: deve contenere da 8 a 100 caratteri.

Tipo: string

Campo obbligatorio: no

Port

Il numero di porta su cui le istanze del cluster accettano connessioni.

Tipo: integer

Campo obbligatorio: no

PreferredBackupWindow

Intervallo di tempo giornaliero durante il quale vengono creati i backup automatici se sono abilitati tramite il parametro `BackupRetentionPeriod`.

Il valore predefinito è una finestra di 30 minuti selezionata in modo casuale in un blocco di 8 ore per ogni Regione AWS.

Vincoli:

- Il valore deve essere nel formato `hh24:mi-hh24:mi`.
- Il valore deve essere nel fuso orario UTC (Universal Coordinated Time).
- Il valore non deve essere in conflitto con la finestra di manutenzione preferita.
- Il valore deve essere almeno di 30 minuti.

Tipo: string

Campo obbligatorio: no

PreferredMaintenanceWindow

Intervallo temporale settimanale nel fuso orario UTC (Universal Coordinated Time) durante il quale può verificarsi la manutenzione dei sistemi.

Formato: `ddd:hh24:mi-ddd:hh24:mi`

Il valore predefinito è una finestra di 30 minuti selezionata in modo casuale in un blocco di 8 ore per ogni Regione AWS, in un giorno casuale della settimana.

Giorni validi: lunedì, martedì, mercoledì, giovedì, venerdì, sabato, domenica

Vincoli: finestra di un minimo di 30 minuti.

Tipo: string

Campo obbligatorio: no

PreSignedUrl

Attualmente non è supportato.

Tipo: string

Campo obbligatorio: no

StorageEncrypted

Specifica se il cluster è crittografato.

Tipo: Booleano

Campo obbligatorio: no

StorageType

Il tipo di archiviazione da associare al cluster di database.

Per informazioni sui tipi di storage per i cluster Amazon DocumentDB, consulta le configurazioni di storage dei cluster nella Amazon DocumentDB Developer Guide.

Valori validi per il tipo di storage - `standard` | `iopt1`

Il valore predefinito è `standard`

Note

Quando si crea un cluster DocumentDB DB con il tipo di archiviazione impostato su `iopt1`, il tipo di archiviazione viene restituito nella risposta. Il tipo di archiviazione non viene restituito quando lo si imposta su `standard`

Tipo: string

Campo obbligatorio: no

Tag.Tag.N

I tag da assegnare al cluster.

Tipo: matrice di oggetti [Tag](#)

Campo obbligatorio: no

VpcSecurityGroupIds. VpcSecurityGroupIdN.

Elenco dei gruppi di sicurezza VPC EC2 da associare a questo cluster.

Tipo: matrice di stringhe

Campo obbligatorio: no

Elementi di risposta

Il servizio restituisce il seguente elemento.

DBCluster

Informazioni dettagliate su un cluster.

Tipo: oggetto [DBCluster](#)

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

DBClusterAlreadyExistsFault

Hai già un cluster con l'identificatore fornito.

Codice di stato HTTP: 400

DBClusterNotFoundFault

`DBClusterIdentifiernon` fa riferimento a un cluster esistente.

Codice di stato HTTP: 404

DBClusterParameterGroupNotFound

`DBClusterParameterGroupNamenon` fa riferimento a un gruppo di parametri del cluster esistente.

Codice di stato HTTP: 404

DBClusterQuotaExceededFault

Il cluster non può essere creato perché è stata raggiunta la quota massima consentita di cluster.

Codice di stato HTTP: 403

DBInstanceNotFound

`DBInstanceIdentifiernon` fa riferimento a un'istanza esistente.

Codice di stato HTTP: 404

DBSubnetGroupDoesNotCoverEnoughAZs

Le sottoreti del gruppo di sottoreti devono coprire almeno due zone di disponibilità, a meno che non esista una sola zona di disponibilità.

Codice di stato HTTP: 400

DBSubnetGroupNotFoundFault

`DBSubnetGroupName` non fa riferimento a un gruppo di sottoreti esistente.

Codice di stato HTTP: 404

GlobalClusterNotFoundFault

`GlobalClusterIdentifier` non si riferisce a un cluster globale esistente.

Codice di stato HTTP: 404

InsufficientStorageClusterCapacity

Lo spazio di archiviazione disponibile non è sufficiente per l'azione corrente. È possibile risolvere questo errore aggiornando il gruppo di sottoreti in modo che utilizzi zone di disponibilità diverse con più spazio di archiviazione disponibile.

Codice di stato HTTP: 400

InvalidDBClusterStateFault

Il cluster non è in uno stato valido.

Codice di stato HTTP: 400

InvalidDBInstanceState

L'istanza specificata non è nello stato disponibile.

Codice di stato HTTP: 400

InvalidDBSubnetGroupStateFault

Il gruppo di sottoreti non può essere eliminato perché è in uso.

Codice di stato HTTP: 400

InvalidGlobalClusterStateFault

L'operazione richiesta non può essere eseguita mentre il cluster si trova in questo stato.

Codice di stato HTTP: 400

InvalidSubnet

La sottorete richiesta non è valida oppure sono state richieste più sottoreti che non si trovano tutte in un cloud privato virtuale (VPC) comune.

Codice di stato HTTP: 400

InvalidVPCNetworkStateFault

Il gruppo di sottoreti non copre tutte le zone di disponibilità dopo la creazione a causa delle modifiche apportate.

Codice di stato HTTP: 400

KMSKeyNotAccessibleFault

Si è verificato un errore durante l'accesso a una AWS KMS chiave.

Codice di stato HTTP: 400

StorageQuotaExceeded

La richiesta comporterebbe il superamento della quantità di storage consentita disponibile in tutte le istanze.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)
- [AWSSDK per V3 JavaScript](#)
- [SDK AWS per PHP V3](#)
- [SDK AWS per Python](#)
- [SDK AWS per Ruby V3](#)

CreateDBClusterParameterGroup

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Crea un nuovo gruppo di parametri del cluster.

I parametri in un gruppo di parametri del cluster si applicano a tutte le istanze in un cluster.

Un gruppo di parametri del cluster viene creato inizialmente con i parametri predefiniti per il motore di database utilizzato dalle istanze nel cluster. In Amazon DocumentDB, non è possibile apportare modifiche direttamente al gruppo di parametri del default.docdb3.6 cluster. Se il tuo cluster Amazon DocumentDB utilizza il gruppo di parametri del cluster predefinito e desideri modificarne un valore, devi prima [creare un nuovo gruppo di parametri o copiare un gruppo di parametri esistente](#), modificarlo e quindi applicare il gruppo di parametri modificato al cluster. Affinché il nuovo gruppo di parametri del cluster e le impostazioni associate abbiano effetto, è necessario riavviare le istanze nel cluster senza failover. Per ulteriori informazioni, consulta [Modifica dei gruppi di parametri del cluster Amazon DocumentDB](#).

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

DBClusterParameterGroupName

Il nome del gruppo di parametri del cluster.

Vincoli:

- Non deve corrispondere al nome di un oggetto `DBClusterParameterGroup` esistente.

Note

Questo valore è archiviato come stringa in caratteri minuscoli.

Tipo: stringa

Campo obbligatorio: sì

DBParameterGroupFamily

Il nome della famiglia del gruppo di parametri del cluster.

Tipo: stringa

Campo obbligatorio: sì

Description

La descrizione del gruppo di parametri del cluster.

Tipo: stringa

Campo obbligatorio: sì

Tag.Tag.N

I tag da assegnare al gruppo di parametri del cluster.

Tipo: matrice di oggetti [Tag](#)

Campo obbligatorio: no

Elementi di risposta

Il seguente elemento viene restituito dal servizio.

DBClusterParameterGroup

Informazioni dettagliate su un gruppo di parametri del cluster.

Tipo: oggetto [DBClusterParameterGroup](#)

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

DBParameterGroupAlreadyExists

Esiste già un gruppo di parametri con lo stesso nome.

Codice di stato HTTP: 400

DBParameterGroupQuotaExceeded

Questa richiesta comporterebbe il superamento del numero consentito di gruppi di parametri.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)
- [AWSSDK per JavaScript V3](#)
- [SDK AWS per PHP V3](#)
- [SDK AWS per Python](#)
- [SDK AWS per Ruby V3](#)

CreateDBClusterSnapshot

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Crea un'istantanea di un cluster.

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

DBClusterIdentifier

L'identificatore del cluster per cui creare un'istantanea. Questo parametro non distingue tra maiuscole e minuscole.

Vincoli:

- Deve corrispondere all'identificativo di un `DBCluster` esistente.

Esempio: `my-cluster`

Tipo: stringa

Campo obbligatorio: sì

DBClusterSnapshotIdentifier

L'identificatore dello snapshot del cluster. Questo parametro è archiviato come stringa in minuscolo.

Vincoli:

- Deve contenere da 1 a 63 lettere, numeri o trattini.
- Il primo carattere deve essere una lettera.
- Non può terminare con un trattino o contenere due trattini consecutivi.

Esempio: `my-cluster-snapshot1`

Tipo: stringa

Campo obbligatorio: sì

Tag.Tag.N

I tag da assegnare allo snapshot del cluster.

Tipo: matrice di oggetti [Tag](#)

Campo obbligatorio: no

Elementi di risposta

Il servizio restituisce il seguente elemento.

DBClusterSnapshot

Informazioni dettagliate su un'istantanea del cluster.

Tipo: oggetto [DBClusterSnapshot](#)

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

DBClusterNotFoundFault

DBClusterIdentifiernon fa riferimento a un cluster esistente.

Codice di stato HTTP: 404

DBClusterSnapshotAlreadyExistsFault

Hai già un'istantanea del cluster con l'identificatore specificato.

Codice di stato HTTP: 400

InvalidDBClusterSnapshotStateFault

Il valore fornito non è uno stato valido dello snapshot del cluster.

Codice di stato HTTP: 400

InvalidDBClusterStateFault

Il cluster non è in uno stato valido.

Codice di stato HTTP: 400

SnapshotQuotaExceeded

La richiesta comporterebbe il superamento del numero consentito di istantanee.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)
- [AWSSDK per V3 JavaScript](#)
- [SDK AWS per PHP V3](#)
- [SDK AWS per Python](#)
- [SDK AWS per Ruby V3](#)

CreateDBInstance

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Crea una nuova istanza.

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

DBClusterIdentifier

Identificatore del cluster a cui apparterrà l'istanza.

Tipo: stringa

Campo obbligatorio: sì

DBInstanceClass

La capacità di calcolo e di memoria dell'istanza, ad esempio `db.r5.large`.

Tipo: stringa

Campo obbligatorio: sì

DBInstanceIdentifier

L'identificatore delle istanze. Questo parametro è archiviato come stringa in minuscolo.

Vincoli:

- Deve contenere da 1 a 63 lettere, numeri o trattini.
- Il primo carattere deve essere una lettera.
- Non può terminare con un trattino o contenere due trattini consecutivi.

Esempio: `mydbinstance`

Tipo: stringa

Campo obbligatorio: sì

Engine

Nome del motore di database da utilizzare per questa istanza.

Valore valido: `docdb`

Tipo: stringa

Campo obbligatorio: sì

AutoMinorVersionUpgrade

Questo parametro non si applica ad Amazon DocumentDB. Amazon DocumentDB non esegue aggiornamenti di versione secondari indipendentemente dal valore impostato.

Impostazione predefinita: false

Tipo: Booleano

Campo obbligatorio: no

AvailabilityZone

Zona di disponibilità Amazon EC2 in cui viene creata l'istanza.

Impostazione predefinita: una zona di disponibilità casuale scelta dal sistema nella Regione AWS dell'endpoint.

Esempio: us-east-1d

Tipo: string

Campo obbligatorio: no

CACertificateIdentifier

L'identificatore del certificato CA da utilizzare per il certificato del server dell'istanza DB.

Per ulteriori informazioni, consulta [Updating your Amazon DocumentDB TLS Certificates](#) and [Encrypting Data in Transit nella](#) Amazon DocumentDB Developer Guide.

Tipo: string

Campo obbligatorio: no

CopyTagsToSnapshot

Un valore che indica se copiare i tag dall'istanza database sugli snapshot dell'istanza database. Per impostazione predefinita i tag non vengono copiati.

Tipo: Booleano

Campo obbligatorio: no

EnablePerformanceInsights

Un valore che indica se abilitare Performance Insights per l'istanza del database. Per ulteriori informazioni, consulta la sezione [Utilizzo di Amazon Performance Insights](#).

Tipo: Booleano

Campo obbligatorio: no

PerformanceInsightsKMSKeyId

Identificatore di chiave AWS KMS per la crittografia dei dati di Performance Insights.

L'identificatore della AWS KMS chiave è l'ARN della chiave, l'ID chiave, l'alias ARN o il nome alias per la chiave KMS.

Se non specifichi un valore per PerformanceInsights KMSKeyId, Amazon DocumentDB utilizza la tua chiave KMS predefinita. Esiste una chiave KMS predefinita per il tuo account Amazon Web Services. Il tuo account Amazon Web Services ha una chiave KMS predefinita diversa per ogni regione Amazon Web Services.

Tipo: string

Campo obbligatorio: no

PreferredMaintenanceWindow

Intervallo di tempo settimanale durante il quale può venire eseguita la manutenzione del sistema, nel fuso orario UTC (Universal Coordinated Time).

Formato: ddd:hh24:mi-ddd:hh24:mi

Il valore predefinito è una finestra di 30 minuti selezionata in modo casuale in un blocco di 8 ore per ogni Regione AWS, in un giorno casuale della settimana.

Giorni validi: lunedì, martedì, mercoledì, giovedì, venerdì, sabato, domenica

Vincoli: finestra di un minimo di 30 minuti.

Tipo: string

Campo obbligatorio: no

PromotionTier

Un valore che specifica l'ordine in cui una replica di Amazon DocumentDB viene promossa all'istanza principale dopo un errore dell'istanza primaria esistente.

Impostazione predefinita: 1

Valori validi: 0-15

Tipo: integer

Campo obbligatorio: no

Tag.Tag.N

I tag da assegnare all'istanza. Puoi assegnare fino a 10 tag a un'istanza.

Tipo: matrice di oggetti [Tag](#)

Campo obbligatorio: no

Elementi di risposta

Il seguente elemento viene restituito dal servizio.

DBInstance

Informazioni dettagliate su un'istanza.

Tipo: oggetto [DBInstance](#)

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

AuthorizationNotFound

L'IP CIDR o il gruppo di sicurezza Amazon EC2 specificato non sono autorizzati per il gruppo di sicurezza specificato.

Amazon DocumentDB potrebbe inoltre non essere autorizzato a eseguire le azioni necessarie per tuo conto utilizzando IAM.

Codice di stato HTTP: 404

DBClusterNotFoundFault

DBClusterIdentifier non fa riferimento a un cluster esistente.

Codice di stato HTTP: 404

DBInstanceAlreadyExists

Hai già un'istanza con l'identificatore specificato.

Codice di stato HTTP: 400

DBParameterGroupNotFound

DBParameterGroupName non fa riferimento a un gruppo di parametri esistente.

Codice di stato HTTP: 404

DBSecurityGroupNotFound

DBSecurityGroupName non fa riferimento a un gruppo di sicurezza esistente.

Codice di stato HTTP: 404

DBSubnetGroupDoesNotCoverEnoughAZs

Le sottoreti del gruppo di sottoreti devono coprire almeno due zone di disponibilità, a meno che non esista una sola zona di disponibilità.

Codice di stato HTTP: 400

DBSubnetGroupNotFoundFault

DBSubnetGroupName non fa riferimento a un gruppo di sottoreti esistente.

Codice di stato HTTP: 404

InstanceQuotaExceeded

La richiesta comporterebbe il superamento del numero consentito di istanze.

Codice di stato HTTP: 400

InsufficientDBInstanceCapacity

La classe di istanza specificata non è disponibile nella zona di disponibilità specificata.

Codice di stato HTTP: 400

InvalidDBClusterStateFault

Il cluster non è in uno stato valido.

Codice di stato HTTP: 400

InvalidSubnet

La sottorete richiesta non è valida oppure sono state richieste più sottoreti che non si trovano tutte in un cloud privato virtuale (VPC) comune.

Codice di stato HTTP: 400

InvalidVPCNetworkStateFault

Il gruppo di sottoreti non copre tutte le zone di disponibilità dopo la creazione a causa delle modifiche apportate.

Codice di stato HTTP: 400

KMSKeyNotAccessibleFault

Si è verificato un errore durante l'accesso a una AWS KMS chiave.

Codice di stato HTTP: 400

StorageQuotaExceeded

La richiesta comporterebbe il superamento della quantità di storage consentita disponibile in tutte le istanze.

Codice di stato HTTP: 400

StorageTypeNotSupported

L'archiviazione dello spazio specificato non `StorageType` può essere associata all'istanza DB.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)
- [AWSSDK per JavaScript V3](#)
- [SDK AWS per PHP V3](#)
- [SDK AWS per Python](#)
- [SDK AWS per Ruby V3](#)

CreateDBSubnetGroup

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Crea un nuovo gruppo di sottoreti. I gruppi di sottoreti devono contenere almeno una sottorete in almeno due zone di disponibilità in. Regione AWS

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

DBSubnetGroupDescription

La descrizione per il gruppo di sottoreti.

Tipo: stringa

Campo obbligatorio: sì

DBSubnetGroupName

Il nome del gruppo di sottoreti. Questo valore è archiviato come stringa in caratteri minuscoli.

Vincoli: devono contenere un massimo di 255 lettere, numeri, punti, trattini bassi, spazi o trattini. Non deve essere predefinito.

Esempio: mySubnetgroup

Tipo: stringa

Campo obbligatorio: sì

SubnetIds. SubnetIdentifierN.

Gli ID di sottorete Amazon EC2 per il gruppo di sottoreti.

Tipo: matrice di stringhe

Campo obbligatorio: sì

Tag.Tag.N

Il tag da assegnare al gruppo di sottoreti.

Tipo: matrice di oggetti [Tag](#)

Campo obbligatorio: no

Elementi di risposta

Il seguente elemento viene restituito dal servizio.

DBSubnetGroup

Informazioni dettagliate su un gruppo di sottoreti.

Tipo: oggetto [DBSubnetGroup](#)

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

DBSubnetGroupAlreadyExists

DBSubnetGroupName è già utilizzato da un gruppo di sottoreti esistente.

Codice di stato HTTP: 400

DBSubnetGroupDoesNotCoverEnoughAZs

Le sottoreti del gruppo di sottoreti devono coprire almeno due zone di disponibilità, a meno che non esista una sola zona di disponibilità.

Codice di stato HTTP: 400

DBSubnetGroupQuotaExceeded

La richiesta comporterebbe il superamento del numero consentito di gruppi di sottoreti.

Codice di stato HTTP: 400

DBSubnetQuotaExceededFault

La richiesta comporterebbe il superamento del numero consentito di sottoreti in un gruppo di sottoreti.

Codice di stato HTTP: 400

InvalidSubnet

La sottorete richiesta non è valida oppure sono state richieste più sottoreti che non si trovano tutte in un cloud privato virtuale (VPC) comune.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)
- [AWSSDK per V3 JavaScript](#)
- [SDK AWS per PHP V3](#)
- [SDK AWS per Python](#)
- [SDK AWS per Ruby V3](#)

CreateEventSubscription

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Crea un abbonamento per la notifica degli eventi di Amazon DocumentDB. Questa azione richiede un argomento Amazon Resource Name (ARN) creato utilizzando la console Amazon DocumentDB, la console Amazon SNS o l'API Amazon SNS. Per ottenere un ARN con Amazon SNS, devi creare un argomento in Amazon SNS e abbonarti all'argomento. L'ARN viene visualizzato nella console Amazon SNS.

Puoi specificare il tipo di fonte (`SourceType`) di cui desideri ricevere una notifica. Puoi anche fornire un elenco di fonti Amazon DocumentDB (`SourceIds`) che attivano gli eventi e puoi fornire un elenco di categorie di eventi (`EventCategories`) per gli eventi di cui desideri ricevere notifiche. Ad esempio, puoi specificare `SourceType = db-instance` `SourceIds = mydbinstance1, mydbinstance2` e `EventCategories = Availability, Backup`.

Se si specificano entrambi `SourceType` e `SourceIds` (ad esempio `SourceType = db-instance` e `SourceIdentifier = myDBInstance1`), si riceve una notifica di tutti gli `db-instance` eventi relativi all'origine specificata. Se specifichi `SourceType` ma non specifichi `SourceIdentifier`, riceverai una notifica degli eventi per quel tipo di sorgente per tutte le tue fonti Amazon DocumentDB. Se non specifichi `SourceType` né `SourceIdentifier`, riceverai una notifica degli eventi generati da tutte le fonti Amazon DocumentDB appartenenti al tuo account cliente.

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

`SnsTopicArn`

L'Amazon Resource Name (ARN) dell'argomento SNS creato per la notifica di eventi. Amazon SNS crea l'ARN quando crei un argomento e ti iscrivi.

Tipo: stringa

Campo obbligatorio: sì

`SubscriptionName`

Il nome dell'abbonamento.

Vincoli: il nome deve contenere meno di 255 caratteri.

Tipo: stringa

Campo obbligatorio: sì

Enabled

Un valore booleano; impostato `true` per attivare l'abbonamento, impostato per `false` a creare l'abbonamento ma non attivarlo.

Tipo: Booleano

Campo obbligatorio: no

EventCategories. EventCategoryN.

Un elenco di categorie di eventi a `SourceType` cui desideri iscriverti.

Tipo: matrice di stringhe

Campo obbligatorio: no

SourceIds. SourceIdN.

L'elenco di identificatori di origini di eventi per le quali vengono restituiti gli eventi. Se non è specificato, tutte le origini sono incluse nella risposta. Un identificatore deve iniziare con una lettera e deve contenere solo caratteri ASCII, cifre e trattini, non può terminare con un trattino o contenere due trattini consecutivi.

Vincoli:

- Se `SourceIds` vengono forniti, `SourceType` devono essere forniti anche.
- Se il tipo di origine è un'istanza, è `DBInstanceIdentifier` necessario fornire a.
- Se il tipo di origine è un gruppo di sicurezza, è `DBSecurityGroupName` necessario fornire un.
- Se il tipo di origine è un gruppo di parametri, è `DBParameterGroupName` necessario fornire a.
- Se il tipo di origine è un'istantanea, è `DBSnapshotIdentifier` necessario fornire a.

Tipo: matrice di stringhe

Campo obbligatorio: no

SourceType

Il tipo di origine che genera gli eventi. Ad esempio, se desideri ricevere una notifica degli eventi generati da un'istanza, devi impostare questo parametro su `db-instance`. Se questo valore non viene specificato, vengono restituiti tutti gli eventi.

Valori validi: `db-instance`, `db-cluster`, `db-parameter-group`, `db-security-group`, `db-cluster-snapshot`

Tipo: string

Campo obbligatorio: no

Tag.Tag.N

I tag da assegnare all'abbonamento all'evento.

Tipo: matrice di oggetti [Tag](#)

Campo obbligatorio: no

Elementi di risposta

Il servizio restituisce il seguente elemento.

EventSubscription

Informazioni dettagliate su un evento a cui ti sei iscritto.

Tipo: oggetto [EventSubscription](#)

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

EventSubscriptionQuotaExceeded

Hai raggiunto il numero massimo di iscrizioni agli eventi.

Codice di stato HTTP: 400

SNSInvalidTopic

Amazon SNS ha risposto che c'è un problema con l'argomento specificato.

Codice di stato HTTP: 400

SNSNoAuthorization

Non sei autorizzato a pubblicare sull'argomento SNS Amazon Resource Name (ARN).

Codice di stato HTTP: 400

SNSTopicArnNotFound

L'argomento SNS Amazon Resource Name (ARN) non esiste.

Codice di stato HTTP: 404

SourceNotFound

La fonte richiesta non è stata trovata.

Codice di stato HTTP: 404

SubscriptionAlreadyExist

Il nome di abbonamento fornito esiste già.

Codice di stato HTTP: 400

SubscriptionCategoryNotFound

La categoria fornita non esiste.

Codice di stato HTTP: 404

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)
- [AWSSDK per JavaScript V3](#)
- [SDK AWS per PHP V3](#)
- [SDK AWS per Python](#)
- [SDK AWS per Ruby V3](#)

CreateGlobalCluster

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Crea un cluster globale Amazon DocumentDB che può estendersi su più di un cluster. Regioni AWS Il cluster globale contiene un cluster primario con funzionalità di lettura/scrittura e fino a cluster secondari di sola lettura. I cluster globali utilizzano la replica rapida basata sullo storage tra regioni con latenze inferiori a un secondo, utilizzando un'infrastruttura dedicata senza alcun impatto sulle prestazioni del carico di lavoro.

È possibile creare un cluster globale inizialmente vuoto e quindi aggiungervi un cluster primario e uno secondario. In alternativa, è possibile specificare un cluster esistente durante l'operazione di creazione e questo cluster diventa il cluster principale del cluster globale.

Note

Questa azione si applica solo ai cluster Amazon DocumentDB.

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

GlobalClusterIdentifier

L'identificatore del cluster del nuovo cluster globale.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 1. Lunghezza massima di 255.

Modello: `[A-Za-z][0-9A-Za-z-:._]*`

Campo obbligatorio: sì

DatabaseName

Nome per il database, composto da un massimo di 64 caratteri alfanumerici. Se non fornisci un nome, Amazon DocumentDB non creerà un database nel cluster globale che stai creando.

Tipo: string

Campo obbligatorio: no

DeletionProtection

L'impostazione di protezione dall'eliminazione per il nuovo cluster globale. Il cluster globale non può essere eliminato quando è abilitata la protezione dall'eliminazione.

Tipo: Booleano

Campo obbligatorio: no

Engine

Il nome del motore di database da utilizzare per questo cluster.

Tipo: string

Campo obbligatorio: no

EngineVersion

La versione del motore del cluster globale.

Tipo: string

Campo obbligatorio: no

SourceDBClusterIdentifier

L'Amazon Resource Name (ARN) da utilizzare come cluster primario del cluster globale. Questo parametro è facoltativo.

Tipo: string

Campo obbligatorio: no

StorageEncrypted

L'impostazione di crittografia dello storage per il nuovo cluster globale.

Tipo: Booleano

Campo obbligatorio: no

Elementi di risposta

Il servizio restituisce il seguente elemento.

GlobalCluster

Un tipo di dati che rappresenta un cluster globale Amazon DocumentDB.

Tipo: oggetto [GlobalCluster](#)

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

DBClusterNotFoundFault

`DBClusterIdentifier` non si riferisce a un cluster esistente.

Codice di stato HTTP: 404

GlobalClusterAlreadyExistsFault

`GlobalClusterIdentifier` esiste già. Scegli un nuovo identificatore globale del cluster (nome univoco) per creare un nuovo cluster globale.

Codice di stato HTTP: 400

GlobalClusterQuotaExceededFault

Il numero di cluster globali per questo account è già al massimo consentito.

Codice di stato HTTP: 400

InvalidDBClusterStateFault

Il cluster non è in uno stato valido.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)

- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)
- [AWSSDK per JavaScript V3](#)
- [SDK AWS per PHP V3](#)
- [SDK AWS per Python](#)
- [SDK AWS per Ruby V3](#)

DeleteDBCluster

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Elimina un cluster precedentemente fornito. Quando si elimina un cluster, tutti i backup automatici per quel cluster vengono eliminati e non possono essere ripristinati. Le istantanee manuali del cluster DB del cluster specificato non vengono eliminate.

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

DBClusterIdentifier

L'identificatore del cluster per il cluster da eliminare. Questo parametro non fa distinzione tra maiuscole e minuscole.

Vincoli:

- Deve corrispondere a un esistente `DBClusterIdentifier`.

Tipo: stringa

Campo obbligatorio: sì

FinalDBSnapshotIdentifier

L'identificatore dello snapshot del cluster nuovo creato quando `SkipFinalSnapshot` è impostato su `false`

Note

Se si specifica questo parametro e si imposta anche il `SkipFinalShapshot` parametro su `true`, viene generato un errore.

Vincoli:

- Deve contenere da 1 a 255 lettere, numeri o trattini.
- Il primo carattere deve essere una lettera.
- Non può terminare con un trattino o contenere due trattini consecutivi.

Tipo: string

Campo obbligatorio: no

SkipFinalSnapshot

Determina se viene creata un'istantanea finale del cluster prima dell'eliminazione del cluster. Se specificato, `true` viene creata alcuna istantanea del cluster. Se specificato, `false` viene creata un'istantanea del cluster prima dell'eliminazione del cluster DB.

Note

In caso `SkipFinalSnapshot false` affermativo, è necessario specificare un `FinalDBSnapshotIdentifier` parametro.

Impostazione predefinita: `false`

Tipo: Booleano

Campo obbligatorio: no

Elementi di risposta

Il servizio restituisce il seguente elemento.

DBCluster

Informazioni dettagliate su un cluster.

Tipo: oggetto [DBCluster](#)

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

DBClusterNotFoundFault

`DBClusterIdentifier` non si riferisce a un cluster esistente.

Codice di stato HTTP: 404

DBClusterSnapshotAlreadyExistsFault

Hai già un'istantanea del cluster con l'identificatore specificato.

Codice di stato HTTP: 400

InvalidDBClusterSnapshotStateFault

Il valore fornito non è uno stato valido dello snapshot del cluster.

Codice di stato HTTP: 400

InvalidDBClusterStateFault

Il cluster non è in uno stato valido.

Codice di stato HTTP: 400

SnapshotQuotaExceeded

La richiesta comporterebbe il superamento del numero consentito di istantanee.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)
- [AWSSDK per V3 JavaScript](#)
- [SDK AWS per PHP V3](#)
- [SDK AWS per Python](#)
- [SDK AWS per Ruby V3](#)

DeleteDBClusterParameterGroup

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Elimina un gruppo di parametri del cluster specificato. Il gruppo di parametri del cluster da eliminare non può essere associato a nessun cluster.

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

DBClusterParameterGroupName

Il nome del gruppo di parametri del cluster.

Vincoli:

- Deve essere il nome di un gruppo di parametri del cluster esistente.
- Non è possibile eliminare un gruppo di parametri di cluster predefinito.
- Non può essere associato a nessun cluster.

Tipo: stringa

Campo obbligatorio: sì

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

DBParameterGroupNotFound

DBParameterGroupName non fa riferimento a un gruppo di parametri esistente.

Codice di stato HTTP: 404

InvalidDBParameterGroupState

Il gruppo di parametri è in uso o si trova in uno stato non valido. Se state cercando di eliminare il gruppo di parametri, non potete eliminarlo quando il gruppo di parametri si trova in questo stato.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)
- [AWSSDK per JavaScript V3](#)
- [SDK AWS per PHP V3](#)
- [SDK AWS per Python](#)
- [SDK AWS per Ruby V3](#)

DeleteDBClusterSnapshot

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Elimina un'istantanea del cluster. Se si copia lo snapshot, l'operazione di copia viene terminata.

Note

L'istantanea del cluster deve trovarsi `available` nello stato in cui deve essere eliminata.

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

DBClusterSnapshotIdentifier

L'identificatore dello snapshot del cluster da eliminare.

Vincoli: deve essere il nome di un'istantanea del cluster esistente nello stato `available`

Tipo: stringa

Campo obbligatorio: sì

Elementi di risposta

Il servizio restituisce il seguente elemento.

DBClusterSnapshot

Informazioni dettagliate su un'istantanea del cluster.

Tipo: oggetto [DBClusterSnapshot](#)

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

DBClusterSnapshotNotFoundFault

`DBClusterSnapshotIdentifier` non fa riferimento a un'istantanea del cluster esistente.

Codice di stato HTTP: 404

InvalidDBClusterSnapshotStateFault

Il valore fornito non è uno stato valido di snapshot del cluster.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)
- [AWSSDK per V3 JavaScript](#)
- [SDK AWS per PHP V3](#)
- [SDK AWS per Python](#)
- [SDK AWS per Ruby V3](#)

DeleteDBInstance

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Elimina un'istanza precedentemente fornita.

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

DBInstanceIdentifier

L'identificatore dell'istanza da eliminare. Questo parametro non fa distinzione tra maiuscole e minuscole.

Vincoli:

- Deve corrispondere al nome di un'istanza esistente.

Tipo: stringa

Campo obbligatorio: sì

Elementi di risposta

Il servizio restituisce il seguente elemento.

DBInstance

Informazioni dettagliate su un'istanza.

Tipo: oggetto [DBInstance](#)

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

DBInstanceNotFound

DBInstanceIdentifier non fa riferimento a un'istanza esistente.

Codice di stato HTTP: 404

DBSnapshotAlreadyExists

DBSnapshotIdentifier è già utilizzato da un'istanza esistente.

Codice di stato HTTP: 400

InvalidDBClusterStateFault

Il cluster non è in uno stato valido.

Codice di stato HTTP: 400

InvalidDBInstanceState

L'istanza specificata non è nello stato disponibile.

Codice di stato HTTP: 400

SnapshotQuotaExceeded

La richiesta comporterebbe il superamento del numero consentito di istantanee.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)
- [AWSSDK per V3 JavaScript](#)
- [SDK AWS per PHP V3](#)
- [SDK AWS per Python](#)
- [SDK AWS per Ruby V3](#)

DeleteDBSubnetGroup

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Elimina un gruppo di sottoreti.

Note

Il gruppo di sottoreti di database specificato non deve essere associato ad alcuna istanza database.

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

DBSubnetGroupName

Il nome del gruppo di sottoreti di database da eliminare.

Note

Non è possibile eliminare il gruppo di sottoreti di default.

Vincoli:

Deve corrispondere il nome di un oggetto DBSubnetGroup esistente. Non deve essere predefinito.

Esempio: mySubnetgroup

Tipo: stringa

Campo obbligatorio: sì

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

DBSubnetGroupNotFoundFault

DBSubnetGroupNameon fa riferimento a un gruppo di sottoreti esistente.

Codice di stato HTTP: 404

InvalidDBSubnetGroupStateFault

Il gruppo di sottoreti non può essere eliminato perché è in uso.

Codice di stato HTTP: 400

InvalidDBSubnetStateFault

La sottorete non è nello stato disponibile.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)
- [AWSSDK per V3 JavaScript](#)
- [SDK AWS per PHP V3](#)
- [SDK AWS per Python](#)
- [SDK AWS per Ruby V3](#)

DeleteEventSubscription

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Elimina una sottoscrizione di notifica di eventi Amazon DocumentDB.

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

SubscriptionName

Il nome dell'abbonamento di notifica degli eventi di Amazon DocumentDB che desideri eliminare.

Tipo: stringa

Campo obbligatorio: sì

Elementi di risposta

Il servizio restituisce il seguente elemento.

EventSubscription

Informazioni dettagliate su un evento a cui ti sei iscritto.

Tipo: oggetto [EventSubscription](#)

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

InvalidEventSubscriptionState

È possibile che qualcun altro stia modificando un abbonamento. Attendi qualche secondo e riprova.

Codice di stato HTTP: 400

SubscriptionNotFound

Il nome dell'abbonamento non esiste.

Codice di stato HTTP: 404

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)
- [AWSSDK per JavaScript V3](#)
- [SDK AWS per PHP V3](#)
- [SDK AWS per Python](#)
- [SDK AWS per Ruby V3](#)

DeleteGlobalCluster

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Elimina un cluster globale. I cluster primari e secondari devono essere già scollegati o eliminati prima di tentare di eliminare un cluster globale.

Note

Questa azione si applica solo ai cluster Amazon DocumentDB.

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

GlobalClusterIdentifier

L'identificatore del cluster globale da eliminare.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 1. Lunghezza massima di 255.

Modello: `[A-Za-z][0-9A-Za-z-:._]*`

Campo obbligatorio: sì

Elementi di risposta

Il servizio restituisce il seguente elemento.

GlobalCluster

Un tipo di dati che rappresenta un cluster globale Amazon DocumentDB.

Tipo: oggetto [GlobalCluster](#)

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

GlobalClusterNotFoundFault

`GlobalClusterIdentifier` non si riferisce a un cluster globale esistente.

Codice di stato HTTP: 404

InvalidGlobalClusterStateFault

L'operazione richiesta non può essere eseguita mentre il cluster si trova in questo stato.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)
- [AWSSDK per JavaScript V3](#)
- [SDK AWS per PHP V3](#)
- [SDK AWS per Python](#)
- [SDK AWS per Ruby V3](#)

DescribeCertificates

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Restituisce un elenco di certificati di autorità di certificazione (CA) forniti da Amazon DocumentDB a tale scopo. Account AWS

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

CertificateIdentifier

L'identificatore del certificato fornito dall'utente. Se viene specificato questo parametro, vengono restituite le informazioni relative solo al certificato specificato. Se questo parametro viene omissso, viene restituito un elenco contenente un massimo di MaxRecords certificati. Questo parametro non distingue tra maiuscole e minuscole.

Vincoli

- Deve corrispondere a un esistenteCertificateIdentifier.

Tipo: string

Campo obbligatorio: no

Filtri.Filter.N

Questo parametro non è attualmente supportato.

Tipo: matrice di oggetti [Filter](#)

Campo obbligatorio: no

Marker

Token di paginazione opzionale fornito da una richiesta DescribeCertificates precedente. Se questo parametro viene specificato, la risposta include solo i record oltre il contrassegno, fino al valore specificato da MaxRecords.

Tipo: string

Campo obbligatorio: no

MaxRecords

Numero massimo di record da includere nella risposta. Se sono presenti più record rispetto al valore di `MaxRecords` specificato, nella risposta viene incluso un token di paginazione detto contrassegno (oggetto `Marker`), per permettere di recuperare i risultati rimanenti.

Impostazione predefinita: 100

Vincoli:

- Minimo: 20
- Massimo: 100

Tipo: integer

Campo obbligatorio: no

Elementi di risposta

I seguenti elementi vengono restituiti dal servizio.

Certificati.Certificate.N

Un elenco di certificati a tal fine. Account AWS

Tipo: matrice di oggetti [Certificate](#)

Marker

Un token di impaginazione opzionale fornito se il numero di record recuperati è maggiore di `MaxRecords`. Se viene specificato questo parametro, il marker specifica il record successivo nell'elenco. Includendo il valore di `Marker` nella successiva chiamata a `DescribeCertificates` ottiene la pagina successiva dei certificati.

Tipo: stringa

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

CertificateNotFound

`CertificateIdentifiernon` fa riferimento a un certificato esistente.

Codice di stato HTTP: 404

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)
- [AWSSDK per JavaScript V3](#)
- [SDK AWS per PHP V3](#)
- [SDK AWS per Python](#)
- [SDK AWS per Ruby V3](#)

DescribeDBClusterParameterGroups

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Restituisce un elenco di descrizioni `DBClusterParameterGroup`. Se viene specificato un `DBClusterParameterGroupName` parametro, l'elenco contiene solo la descrizione del gruppo di parametri del cluster specificato.

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

`DBClusterParameterGroupName`

Il nome di uno specifico gruppo di parametri del cluster per cui restituire i dettagli.

Vincoli:

- Se fornito, deve corrispondere al nome di un esistente `DBClusterParameterGroup`.

Tipo: string

Campo obbligatorio: no

`Filtri.Filtro.N`

Questo parametro non è attualmente supportato.

Tipo: matrice di oggetti [Filter](#)

Campo obbligatorio: no

`Marker`

Token di paginazione opzionale fornito da una richiesta precedente. Se questo parametro viene specificato, la risposta include solo i record oltre il contrassegno, fino al valore specificato da `MaxRecords`.

Tipo: string

Campo obbligatorio: no

`MaxRecords`

Numero massimo di record da includere nella risposta. Se esistono più record rispetto al `MaxRecords` valore specificato, nella risposta viene incluso un token di impaginazione (marker) in modo da poter recuperare i risultati rimanenti.

Impostazione predefinita: 100

Vincoli: minimo 20, massimo 100.

Tipo: integer

Campo obbligatorio: no

Elementi di risposta

I seguenti elementi vengono restituiti dal servizio.

DB ClusterParameterGroups D.B.N. ClusterParameterGroup

Un elenco di gruppi di parametri del cluster.

Tipo: matrice di oggetti [DBClusterParameterGroup](#)

Marker

Token di paginazione opzionale fornito da una richiesta precedente. Se questo parametro viene specificato, la risposta include solo i record oltre il contrassegno, fino al valore specificato da `MaxRecords`.

Tipo: stringa

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

DBParameterGroupNotFound

`DBParameterGroupNotfound` fa riferimento a un gruppo di parametri esistente.

Codice di stato HTTP: 404

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)

- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)
- [AWSSDK per JavaScript V3](#)
- [SDK AWS per PHP V3](#)
- [SDK AWS per Python](#)
- [SDK AWS per Ruby V3](#)

DescribeDBClusterParameters

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Restituisce l'elenco dettagliato dei parametri per un particolare gruppo di parametri del cluster.

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

DBClusterParameterGroupName

Il nome di uno specifico gruppo di parametri del cluster per cui restituire i dettagli dei parametri.

Vincoli:

- Se fornito, deve corrispondere al nome di un esistente `DBClusterParameterGroup`.

Tipo: stringa

Campo obbligatorio: sì

Filtri.Filtro.N

Questo parametro non è attualmente supportato.

Tipo: matrice di oggetti [Filter](#)

Campo obbligatorio: no

Marker

Token di paginazione opzionale fornito da una richiesta precedente. Se questo parametro viene specificato, la risposta include solo i record oltre il contrassegno, fino al valore specificato da `MaxRecords`.

Tipo: string

Campo obbligatorio: no

MaxRecords

Numero massimo di record da includere nella risposta. Se esistono più record rispetto al `MaxRecords` valore specificato, nella risposta viene incluso un token di impaginazione (marker) in modo da poter recuperare i risultati rimanenti.

Impostazione predefinita: 100

Vincoli: minimo 20, massimo 100.

Tipo: integer

Campo obbligatorio: no

Source

Un valore che indica la restituzione solo di parametri per una determinata origine. Le origini dei parametri possono essere `engine`, `service` o `customer`.

Tipo: string

Campo obbligatorio: no

Elementi di risposta

I seguenti elementi vengono restituiti dal servizio.

Marker

Token di paginazione opzionale fornito da una richiesta precedente. Se questo parametro viene specificato, la risposta include solo i record oltre il contrassegno, fino al valore specificato da `MaxRecords`.

Tipo: stringa

Parametri.Parameter.N

Fornisce un elenco di parametri per il gruppo di parametri del cluster.

Tipo: matrice di oggetti [Parameter](#)

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

DBParameterGroupNotFound

`DBParameterGroupNamenon` fa riferimento a un gruppo di parametri esistente.

Codice di stato HTTP: 404

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)
- [AWSSDK per JavaScript V3](#)
- [SDK AWS per PHP V3](#)
- [SDK AWS per Python](#)
- [SDK AWS per Ruby V3](#)

DescribeDBClusters

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Restituisce informazioni sui cluster Amazon DocumentDB forniti. Questa operazione API supporta l'impaginazione. Per alcune funzionalità di gestione come la gestione del ciclo di vita di cluster e istanze, Amazon DocumentDB sfrutta la tecnologia operativa condivisa con Amazon RDS e Amazon Neptune. Utilizza il parametro `filterName=engine,Values=docdb filter` per restituire solo i cluster Amazon DocumentDB.

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

`DBClusterIdentifier`

L'identificatore del cluster fornito dall'utente. Se viene specificato questo parametro, vengono restituite le informazioni provenienti solo dal cluster specifico. Questo parametro non fa distinzione tra maiuscole e minuscole.

Vincoli:

- Se fornito, deve corrispondere a un valore esistente `DBClusterIdentifier`.

Tipo: string

Campo obbligatorio: no

`Filtri.Filtro.N`

Un filtro che specifica uno o più cluster da descrivere.

Filtri supportati:

- `db-cluster-id`- Accetta identificatori di cluster e Amazon Resource Names (ARN) del cluster. L'elenco dei risultati include solo informazioni sui cluster identificati da questi ARN.

Tipo: matrice di oggetti [Filter](#)

Campo obbligatorio: no

`Marker`

Token di paginazione opzionale fornito da una richiesta precedente. Se questo parametro viene specificato, la risposta include solo i record oltre il contrassegno, fino al valore specificato da `MaxRecords`.

Tipo: string

Campo obbligatorio: no

MaxRecords

Numero massimo di record da includere nella risposta. Se esistono più record rispetto al `MaxRecords` valore specificato, nella risposta viene incluso un token di impaginazione (marker) in modo da poter recuperare i risultati rimanenti.

Impostazione predefinita: 100

Vincoli: minimo 20, massimo 100.

Tipo: integer

Campo obbligatorio: no

Elementi di risposta

I seguenti elementi vengono restituiti dal servizio.

`dbclusters.dbcluster.n`

Un elenco di cluster.

Tipo: matrice di oggetti [DBCluster](#)

Marker

Token di paginazione opzionale fornito da una richiesta precedente. Se questo parametro viene specificato, la risposta include solo i record oltre il contrassegno, fino al valore specificato da `MaxRecords`.

Tipo: stringa

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

DBClusterNotFoundFault

`DBClusterIdentifiernon` fa riferimento a un cluster esistente.

Codice di stato HTTP: 404

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)
- [AWSSDK per JavaScript V3](#)
- [SDK AWS per PHP V3](#)
- [SDK AWS per Python](#)
- [SDK AWS per Ruby V3](#)

DescribeDBClusterSnapshotAttributes

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Restituisce un elenco di nomi e valori degli attributi dello snapshot del cluster per uno snapshot manuale del cluster DB.

Quando si condividono istantanee con altri Account AWS, `DescribeDBClusterSnapshotAttributes` restituisce l'attributo `restoreattribute` e un elenco di ID per coloro Account AWS che sono autorizzati a copiare o ripristinare l'istananea manuale del cluster. Se `all` è inclusa nell'elenco di valori dell'attributo `restoreattribute`, l'istananea manuale del cluster è pubblica e può essere copiata o ripristinata da tutti. Account AWS

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

`DBClusterSnapshotIdentifier`

L'identificatore dell'istananea del cluster di cui descrivere gli attributi.

Tipo: stringa

Campo obbligatorio: sì

Elementi di risposta

Il servizio restituisce il seguente elemento.

`DBClusterSnapshotAttributesResult`

Informazioni dettagliate sugli attributi associati a uno snapshot del cluster.

Tipo: oggetto [DBClusterSnapshotAttributesResult](#)

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

`DBClusterSnapshotNotFoundFault`

`DBClusterSnapshotIdentifier` non fa riferimento a un'istananea del cluster esistente.

Codice di stato HTTP: 404

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)
- [AWSSDK per V3 JavaScript](#)
- [SDK AWS per PHP V3](#)
- [SDK AWS per Python](#)
- [SDK AWS per Ruby V3](#)

DescribeDBClusterSnapshots

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Restituisce informazioni sulle istantanee del cluster. Questa operazione API supporta l'impaginazione.

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

DBClusterIdentifier

L'ID del cluster per cui recuperare l'elenco delle istantanee del cluster. Questo parametro non può essere utilizzato con il `DBClusterSnapshotIdentifier` parametro. Questo parametro non distingue tra maiuscole e minuscole.

Vincoli:

- Se fornito, deve corrispondere all'identificatore di un esistente `DBCluster`.

Tipo: string

Campo obbligatorio: no

DBClusterSnapshotIdentifier

Un identificatore di istantanea del cluster specifico da descrivere. Questo parametro non può essere utilizzato con il `DBClusterIdentifier` parametro. Questo valore è archiviato come stringa in caratteri minuscoli.

Vincoli:

- Se fornito, deve corrispondere all'identificatore di un esistente `DBClusterSnapshot`.
- Se questo identificatore è per uno snapshot automatizzato, anche il parametro `SnapshotType` deve essere specificato.

Tipo: string

Campo obbligatorio: no

Filtri.Filtro.N

Questo parametro non è attualmente supportato.

Tipo: matrice di oggetti [Filter](#)

Campo obbligatorio: no

IncludePublic

Impostato `true` per includere istantanee manuali del cluster che sono pubbliche e possono essere copiate o ripristinate da chiunque e in altro modo. Account AWS `false` Il valore predefinito è `false`.

Tipo: Booleano

Campo obbligatorio: no

IncludeShared

È impostata `true` per includere istantanee manuali condivise del cluster provenienti da altri utenti Account AWS che sono Account AWS state autorizzate a copiare o ripristinare e in altro modo. `false` Il valore predefinito è `false`.

Tipo: Booleano

Campo obbligatorio: no

Marker

Token di paginazione opzionale fornito da una richiesta precedente. Se questo parametro viene specificato, la risposta include solo i record oltre il contrassegno, fino al valore specificato da `MaxRecords`.

Tipo: string

Campo obbligatorio: no

MaxRecords

Numero massimo di record da includere nella risposta. Se esistono più record rispetto al `MaxRecords` valore specificato, nella risposta viene incluso un token di impaginazione (marker) in modo da poter recuperare i risultati rimanenti.

Impostazione predefinita: 100

Vincoli: minimo 20, massimo 100.

Tipo: integer

Campo obbligatorio: no

SnapshotType

Il tipo di istantanee del cluster da restituire. È possibile specificare uno dei seguenti valori:

- `automated`- Restituisci tutte le istantanee del cluster che Amazon DocumentDB ha creato automaticamente per te. Account AWS
- `manual`- Restituisci tutte le istantanee del cluster che hai creato manualmente per il tuo. Account AWS
- `shared`- Restituisci tutte le istantanee manuali del cluster che sono state condivise con il tuo. Account AWS
- `public`- Restituisce tutte le istantanee del cluster che sono state contrassegnate come pubbliche.

Se non si specifica un `SnapshotType` valore, vengono restituite istantanee del cluster sia automatiche che manuali. È possibile includere istantanee condivise del cluster con questi risultati impostando il `IncludeShared` parametro su `true`. È possibile includere istantanee pubbliche del cluster con questi risultati impostando il `IncludePublic` parametro su `true`.

I parametri `IncludePublic` e `IncludeShared` non sono applicabili ai valori `SnapshotType` di `manual` o `automated`. Il parametro `IncludePublic` non è applicabile quando `SnapshotType` è impostato su `shared`. Il parametro `IncludeShared` non è applicabile quando `SnapshotType` è impostato su `public`.

Tipo: string

Campo obbligatorio: no

Elementi di risposta

I seguenti elementi vengono restituiti dal servizio.

DB ClusterSnapshots D.B N. ClusterSnapshot

Fornisce un elenco di istantanee del cluster.

Tipo: matrice di oggetti [DBClusterSnapshot](#)

Marker

Token di paginazione opzionale fornito da una richiesta precedente. Se questo parametro viene specificato, la risposta include solo i record oltre il contrassegno, fino al valore specificato da `MaxRecords`.

Tipo: stringa

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

DBClusterSnapshotNotFoundFault

`DBClusterSnapshotIdentifiernon` fa riferimento a un'istantanea del cluster esistente.

Codice di stato HTTP: 404

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)
- [AWSSDK per V3 JavaScript](#)
- [SDK AWS per PHP V3](#)
- [SDK AWS per Python](#)
- [SDK AWS per Ruby V3](#)

DescribeDBEngineVersions

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Restituisce un elenco dei motori disponibili.

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

DBParameterGroupFamily

Il nome di una specifica famiglia di gruppi di parametri per cui restituire i dettagli.

Vincoli:

- Se fornito, deve corrispondere a uno esistente `DBParameterGroupFamily`.

Tipo: string

Campo obbligatorio: no

DefaultOnly

Indica che solo la versione predefinita del motore specificato o una combinazione di motore e versione principale viene restituita.

Tipo: Booleano

Campo obbligatorio: no

Engine

Il motore di database da restituire.

Tipo: string

Campo obbligatorio: no

EngineVersion

La versione del motore di database da restituire.

Esempio: 3.6.0

Tipo: string

Campo obbligatorio: no

Filtri.Filtro.N

Questo parametro non è attualmente supportato.

Tipo: matrice di oggetti [Filter](#)

Campo obbligatorio: no

ListSupportedCharacterSets

Se questo parametro viene specificato e il modulo di richiesta supporta il parametro `CharacterSetName` per `CreateDBInstance`, la risposta include un elenco di set di caratteri supportati per ciascuna versione del motore.

Tipo: Booleano

Campo obbligatorio: no

ListSupportedTimezones

Se questo parametro viene specificato e il modulo di richiesta supporta il parametro `TimeZone` per `CreateDBInstance`, la risposta include un elenco di fusi orari supportati per ciascuna versione del motore.

Tipo: Booleano

Campo obbligatorio: no

Marker

Token di paginazione opzionale fornito da una richiesta precedente. Se questo parametro viene specificato, la risposta include solo i record oltre il contrassegno, fino al valore specificato da `MaxRecords`.

Tipo: string

Campo obbligatorio: no

MaxRecords

Numero massimo di record da includere nella risposta. Se esistono più record rispetto al `MaxRecords` valore specificato, nella risposta viene incluso un token di impaginazione (marker) in modo da poter recuperare i risultati rimanenti.

Impostazione predefinita: 100

Vincoli: minimo 20, massimo 100.

Tipo: integer

Campo obbligatorio: no

Elementi di risposta

I seguenti elementi vengono restituiti dal servizio.

DB EngineVersions D.B N. EngineVersion

Informazioni dettagliate su una o più versioni del motore.

Tipo: matrice di oggetti [DBEngineVersion](#)

Marker

Token di paginazione opzionale fornito da una richiesta precedente. Se questo parametro viene specificato, la risposta include solo i record oltre il contrassegno, fino al valore specificato da `MaxRecords`.

Tipo: stringa

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)

- [AWSSDK per JavaScript V3](#)
- [SDK AWS per PHP V3](#)
- [SDK AWS per Python](#)
- [SDK AWS per Ruby V3](#)

DescribeDBInstances

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Restituisce informazioni sulle istanze Amazon DocumentDB assegnate. Quest'API supporta la paginazione.

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

DBInstanceIdentifier

L'identificatore dell'istanza fornito dall'utente. Se viene specificato questo parametro, vengono restituite solo le informazioni relative all'istanza specifica. Questo parametro non fa distinzione tra maiuscole e minuscole.

Vincoli:

- Se fornito, deve corrispondere all'identificatore di un'esistenteDBInstance.

Tipo: string

Campo obbligatorio: no

Filtri.Filtro.N

Un filtro che specifica una o più istanze da descrivere.

Filtri supportati:

- `db-cluster-id`- Accetta identificatori di cluster e Amazon Resource Names (ARN) del cluster. L'elenco dei risultati include solo le informazioni sulle istanze associate ai cluster identificati da questi ARN.
- `db-instance-id`- Accetta identificatori di istanza e ARN di istanze. L'elenco dei risultati include solo le informazioni sulle istanze identificate da questi ARN.

Tipo: matrice di oggetti [Filter](#)

Campo obbligatorio: no

Marker

Token di paginazione opzionale fornito da una richiesta precedente. Se questo parametro viene specificato, la risposta include solo i record oltre il contrassegno, fino al valore specificato da `MaxRecords`.

Tipo: string

Campo obbligatorio: no

MaxRecords

Numero massimo di record da includere nella risposta. Se esistono più record rispetto al `MaxRecords` valore specificato, nella risposta viene incluso un token di impaginazione (marker) in modo da poter recuperare i risultati rimanenti.

Impostazione predefinita: 100

Vincoli: minimo 20, massimo 100.

Tipo: integer

Campo obbligatorio: no

Elementi di risposta

I seguenti elementi vengono restituiti dal servizio.

`dbInstances.dbInstance`.

Informazioni dettagliate su una o più istanze.

Tipo: matrice di oggetti [DBInstance](#)

Marker

Token di paginazione opzionale fornito da una richiesta precedente. Se questo parametro viene specificato, la risposta include solo i record oltre il contrassegno, fino al valore specificato da `MaxRecords`.

Tipo: stringa

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

DBInstanceNotFound

`DBInstanceIdentifiernon` fa riferimento a un'istanza esistente.

Codice di stato HTTP: 404

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)
- [AWSSDK per JavaScript V3](#)
- [SDK AWS per PHP V3](#)
- [SDK AWS per Python](#)
- [SDK AWS per Ruby V3](#)

DescribeDBSubnetGroups

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Restituisce un elenco di descrizioni DBSubnetGroup. Se DBSubnetGroupName viene specificato a, l'elenco conterrà solo le descrizioni del specificato. DBSubnetGroup

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

DBSubnetGroupName

Il nome del gruppo di sottoreti per cui restituire i dettagli.

Tipo: string

Campo obbligatorio: no

Filtri.Filter.N

Questo parametro non è attualmente supportato.

Tipo: matrice di oggetti [Filter](#)

Campo obbligatorio: no

Marker

Token di paginazione opzionale fornito da una richiesta precedente. Se questo parametro viene specificato, la risposta include solo i record oltre il contrassegno, fino al valore specificato da MaxRecords.

Tipo: string

Campo obbligatorio: no

MaxRecords

Numero massimo di record da includere nella risposta. Se esistono più record rispetto al MaxRecords valore specificato, nella risposta viene incluso un token di impaginazione (marker) in modo da poter recuperare i risultati rimanenti.

Impostazione predefinita: 100

Vincoli: minimo 20, massimo 100.

Tipo: integer

Campo obbligatorio: no

Elementi di risposta

I seguenti elementi vengono restituiti dal servizio.

DB SubnetGroups D.B.N. SubnetGroup

Informazioni dettagliate su uno o più sottoreti.

Tipo: matrice di oggetti [DBSubnetGroup](#)

Marker

Token di paginazione opzionale fornito da una richiesta precedente. Se questo parametro viene specificato, la risposta include solo i record oltre il contrassegno, fino al valore specificato da `MaxRecords`.

Tipo: stringa

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

DBSubnetGroupNotFoundFault

`DBSubnetGroupNamenon` fa riferimento a un gruppo di sottoreti esistente.

Codice di stato HTTP: 404

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)
- [SDK AWS per Go](#)

- [SDK AWS per Java V2](#)
- [AWSSDK per V3 JavaScript](#)
- [SDK AWS per PHP V3](#)
- [SDK AWS per Python](#)
- [SDK AWS per Ruby V3](#)

DescribeEngineDefaultClusterParameters

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Restituisce il motore predefinito e le informazioni del parametro di sistema per il motore del cluster di database .

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

DBParameterGroupFamily

Il nome della famiglia del gruppo di parametri del cluster per cui restituire le informazioni sui parametri del motore.

Tipo: stringa

Campo obbligatorio: sì

Filtri.Filter.N

Questo parametro non è attualmente supportato.

Tipo: matrice di oggetti [Filter](#)

Campo obbligatorio: no

Marker

Token di paginazione opzionale fornito da una richiesta precedente. Se questo parametro viene specificato, la risposta include solo i record oltre il contrassegno, fino al valore specificato da `MaxRecords`.

Tipo: string

Campo obbligatorio: no

MaxRecords

Numero massimo di record da includere nella risposta. Se esistono più record rispetto al `MaxRecords` valore specificato, nella risposta viene incluso un token di impaginazione (marker) in modo da poter recuperare i risultati rimanenti.

Impostazione predefinita: 100

Vincoli: minimo 20, massimo 100.

Tipo: integer

Campo obbligatorio: no

Elementi di risposta

Il servizio restituisce il seguente elemento.

EngineDefaults

Contiene il risultato di una chiamata riuscita dell'`DescribeEngineDefaultClusterParameters`operazione.

Tipo: oggetto [EngineDefaults](#)

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)
- [AWSSDK per V3 JavaScript](#)
- [SDK AWS per PHP V3](#)
- [SDK AWS per Python](#)
- [SDK AWS per Ruby V3](#)

DescribeEventCategories

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Visualizza un elenco di categorie per tutti i tipi di origini di eventi, oppure, se specificato, per un determinato tipo di origine.

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

Filtri.Filtro.N

Questo parametro non è attualmente supportato.

Tipo: matrice di oggetti [Filter](#)

Campo obbligatorio: no

SourceType

Il tipo di origine che genera gli eventi.

Valori validi: db-instance, db-parameter-group, db-security-group

Tipo: string

Campo obbligatorio: no

Elementi di risposta

Il servizio restituisce il seguente elemento.

EventCategoriesMapList. EventCategoriesMapN.

Un elenco di mappe delle categorie di eventi.

Tipo: matrice di oggetti [EventCategoriesMap](#)

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)
- [AWSSDK per JavaScript V3](#)
- [SDK AWS per PHP V3](#)
- [SDK AWS per Python](#)
- [SDK AWS per Ruby V3](#)

DescribeEvents

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Restituisce eventi relativi a istanze, gruppi di sicurezza, istantanee e gruppi di parametri DB degli ultimi 14 giorni. È possibile ottenere eventi specifici per una particolare istanza DB, gruppo di sicurezza, snapshot o gruppo di parametri fornendo il nome come parametro. Per impostazione predefinita, vengono restituiti gli eventi dell'ultima ora.

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

Duration

Il numero di minuti per il quale recuperare gli eventi.

Impostazione predefinita: 60

Tipo: integer

Campo obbligatorio: no

EndTime

La fine dell'intervallo di tempo per il quale recuperare gli eventi, specificato nel formato ISO 8601.

Esempio: 2009-07-08T18:00Z

Tipo: Timestamp

Campo obbligatorio: no

EventCategories. EventCategoryN.

Un elenco di categorie di eventi che attivano le notifiche per un abbonamento alla notifica di eventi.

Tipo: matrice di stringhe

Campo obbligatorio: no

Filtri.Filter.N

Questo parametro non è attualmente supportato.

Tipo: matrice di oggetti [Filter](#)

Campo obbligatorio: no

Marker

Token di paginazione opzionale fornito da una richiesta precedente. Se questo parametro viene specificato, la risposta include solo i record oltre il contrassegno, fino al valore specificato da `MaxRecords`.

Tipo: string

Campo obbligatorio: no

MaxRecords

Numero massimo di record da includere nella risposta. Se esistono più record rispetto al `MaxRecords` valore specificato, nella risposta viene incluso un token di impaginazione (marker) in modo da poter recuperare i risultati rimanenti.

Impostazione predefinita: 100

Vincoli: minimo 20, massimo 100.

Tipo: integer

Campo obbligatorio: no

SourceIdentifier

L'identificatore dell'origine dell'evento in base a cui vengono restituiti gli eventi. Se non è specificato, tutte le origini sono incluse nella risposta.

Vincoli:

- Se `SourceIdentifier` fornito, `SourceType` deve essere fornito anche.
- Se il tipo di sorgente è `DBInstance`, `DBInstanceIdentifier` deve essere fornito un.
- Se il tipo di fonte è `DBSecurityGroup`, `DBSecurityGroupName` deve essere fornito a.
- Se il tipo di fonte è `DBParameterGroup`, `DBParameterGroupName` deve essere fornito a.
- Se il tipo di fonte è `DBSnapshot`, `DBSnapshotIdentifier` deve essere fornito a.
- Non può terminare con un trattino o contenere due trattini consecutivi.

Tipo: string

Campo obbligatorio: no

SourceType

L'origine eventi per la quale recuperare gli eventi. Se non viene specificato alcun valore, tutti gli eventi vengono restituiti.

Tipo: stringa

Valori validi: `db-instance` | `db-parameter-group` | `db-security-group` | `db-snapshot` | `db-cluster` | `db-cluster-snapshot`

Campo obbligatorio: no

StartTime

L'inizio dell'intervallo di tempo per il quale recuperare gli eventi, specificato nel formato ISO 8601.

Esempio: `2009-07-08T18:00Z`

Tipo: Timestamp

Campo obbligatorio: no

Elementi di risposta

I seguenti elementi vengono restituiti dal servizio.

Events.Event.N

Informazioni dettagliate su uno o più eventi.

Tipo: matrice di oggetti [Event](#)

Marker

Token di paginazione opzionale fornito da una richiesta precedente. Se questo parametro viene specificato, la risposta include solo i record oltre il contrassegno, fino al valore specificato da `MaxRecords`.

Tipo: stringa

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)
- [AWSSDK per JavaScript V3](#)
- [SDK AWS per PHP V3](#)
- [SDK AWS per Python](#)
- [SDK AWS per Ruby V3](#)

DescribeEventSubscriptions

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Elenca tutte le descrizioni di sottoscrizioni per un account cliente. La descrizione di un abbonamento include

SubscriptionName,SNSTopicARN,CustomerID,SourceType,SourceID,CreationTime,eStatus.

Se si specifica unSubscriptionName, elenca la descrizione di tale abbonamento.

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

Filtri.Filtro.N

Questo parametro non è attualmente supportato.

Tipo: matrice di oggetti [Filter](#)

Campo obbligatorio: no

Marker

Token di paginazione opzionale fornito da una richiesta precedente. Se questo parametro viene specificato, la risposta include solo i record oltre il contrassegno, fino al valore specificato da MaxRecords.

Tipo: string

Campo obbligatorio: no

MaxRecords

Numero massimo di record da includere nella risposta. Se esistono più record rispetto al MaxRecords valore specificato, nella risposta viene incluso un token di impaginazione (marker) in modo da poter recuperare i risultati rimanenti.

Impostazione predefinita: 100

Vincoli: minimo 20, massimo 100.

Tipo: integer

Campo obbligatorio: no

SubscriptionName

Il nome dell'abbonamento di notifica degli eventi di Amazon DocumentDB che desideri descrivere.

Tipo: string

Campo obbligatorio: no

Elementi di risposta

I seguenti elementi vengono restituiti dal servizio.

EventSubscriptionsList. EventSubscriptionN.

Un elenco di sottoscrizioni a eventi.

Tipo: matrice di oggetti [EventSubscription](#)

Marker

Token di paginazione opzionale fornito da una richiesta precedente. Se questo parametro viene specificato, la risposta include solo i record oltre il contrassegno, fino al valore specificato da `MaxRecords`.

Tipo: stringa

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

SubscriptionNotFound

Il nome dell'abbonamento non esiste.

Codice di stato HTTP: 404

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)
- [AWSSDK per JavaScript V3](#)
- [SDK AWS per PHP V3](#)
- [SDK AWS per Python](#)
- [SDK AWS per Ruby V3](#)

DescribeGlobalClusters

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Restituisce informazioni sui cluster globali di Amazon DocumentDB. Quest'API supporta la paginazione.

Note

Questa azione si applica solo ai cluster Amazon DocumentDB.

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

Filtri.Filtro.N

Un filtro che specifica uno o più cluster DB globali da descrivere.

Filtri supportati: `db-cluster-id` accetta identificatori di cluster e Amazon Resource Names (ARN) del cluster. L'elenco dei risultati includerà solo informazioni sui cluster identificati da questi ARN.

Tipo: matrice di oggetti [Filter](#)

Campo obbligatorio: no

GlobalClusterIdentifier

L'identificatore del cluster fornito dall'utente. Se viene specificato questo parametro, vengono restituite le informazioni provenienti solo dal cluster specifico. Questo parametro non fa distinzione tra maiuscole e minuscole.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 1. Lunghezza massima di 255.

Modello: `[A-Za-z][0-9A-Za-z-:._]*`

Campo obbligatorio: no

Marker

Token di paginazione opzionale fornito da una richiesta `DescribeGlobalClusters` precedente. Se questo parametro viene specificato, la risposta include solo i record oltre il contrassegno, fino al valore specificato da `MaxRecords`.

Tipo: string

Campo obbligatorio: no

MaxRecords

Numero massimo di record da includere nella risposta. Se esistono più record rispetto al `MaxRecords` valore specificato, nella risposta viene incluso un token di impaginazione chiamato `marker` in modo da poter recuperare i risultati rimanenti.

Tipo: integer

Campo obbligatorio: no

Elementi di risposta

I seguenti elementi vengono restituiti dal servizio.

`GlobalClusters`. `GlobalClusterMemberN`.

Tipo: matrice di oggetti [GlobalCluster](#)

Marker

Tipo: stringa

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

GlobalClusterNotFoundFault

`GlobalClusterIdentifier` Non si riferisce a un cluster globale esistente.

Codice di stato HTTP: 404

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)
- [AWSSDK per JavaScript V3](#)
- [SDK AWS per PHP V3](#)
- [SDK AWS per Python](#)
- [SDK AWS per Ruby V3](#)

DescribeOrderableDBInstanceOptions

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Restituisce un elenco di opzioni di istanza ordinabili per il motore specificato.

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

Engine

Il nome del motore per cui recuperare le opzioni di istanza.

Tipo: stringa

Campo obbligatorio: sì

DBInstanceClass

Il valore del filtro della classe di istanza. Specificate questo parametro per mostrare solo le offerte disponibili che corrispondono alla classe di istanza specificata.

Tipo: string

Campo obbligatorio: no

EngineVersion

Valore di filtro della versione del motore. Specificate questo parametro per mostrare solo le offerte disponibili che corrispondono alla versione del motore specificata.

Tipo: string

Campo obbligatorio: no

Filtri.Filtro.N

Questo parametro non è attualmente supportato.

Tipo: matrice di oggetti [Filter](#)

Campo obbligatorio: no

LicenseModel

Valore di filtro del modello di licenza. Specificate questo parametro per mostrare solo le offerte disponibili che corrispondono al modello di licenza specificato.

Tipo: string

Campo obbligatorio: no

Marker

Token di paginazione opzionale fornito da una richiesta precedente. Se questo parametro viene specificato, la risposta include solo i record oltre il contrassegno, fino al valore specificato da `MaxRecords`.

Tipo: string

Campo obbligatorio: no

MaxRecords

Numero massimo di record da includere nella risposta. Se esistono più record rispetto al `MaxRecords` valore specificato, nella risposta viene incluso un token di impaginazione (marker) in modo da poter recuperare i risultati rimanenti.

Impostazione predefinita: 100

Vincoli: minimo 20, massimo 100.

Tipo: integer

Campo obbligatorio: no

Vpc

Il valore del filtro del cloud privato virtuale (VPC). Specifica questo parametro per visualizzare solo le offerte VPC o non VPC disponibili.

Tipo: Booleano

Campo obbligatorio: no

Elementi di risposta

I seguenti elementi vengono restituiti dal servizio.

Marker

Token di paginazione opzionale fornito da una richiesta precedente. Se questo parametro viene specificato, la risposta include solo i record oltre il contrassegno, fino al valore specificato da `MaxRecords`.

Tipo: stringa

OrderableDB .OrderableDB N. InstanceOptions InstanceOption

Le opzioni disponibili per una particolare istanza ordinabile.

Tipo: matrice di oggetti [OrderableDBInstanceOption](#)

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)
- [AWSSDK per V3 JavaScript](#)
- [SDK AWS per PHP V3](#)
- [SDK AWS per Python](#)
- [SDK AWS per Ruby V3](#)

DescribePendingMaintenanceActions

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Restituisce un elenco di risorse (ad esempio, istanze) che hanno almeno un'azione di manutenzione in sospeso.

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

Filtri.Filter.N

Un filtro che specifica una o più risorse per restituire le operazioni di manutenzione in sospeso.

Filtri supportati:

- `db-cluster-id`- Accetta identificatori di cluster e Amazon Resource Names (ARN) del cluster. L'elenco dei risultati include solo le azioni di manutenzione in sospeso per i cluster identificati da questi ARN.
- `db-instance-id`- Accetta identificatori di istanza e ARN di istanza. L'elenco dei risultati include solo le azioni di manutenzione in sospeso per le istanze DB identificate da questi ARN.

Tipo: matrice di oggetti [Filter](#)

Campo obbligatorio: no

Marker

Token di paginazione opzionale fornito da una richiesta precedente. Se questo parametro viene specificato, la risposta include solo i record oltre il contrassegno, fino al valore specificato da `MaxRecords`.

Tipo: string

Campo obbligatorio: no

MaxRecords

Numero massimo di record da includere nella risposta. Se esistono più record rispetto al `MaxRecords` valore specificato, nella risposta viene incluso un token di impaginazione (marker) in modo da poter recuperare i risultati rimanenti.

Impostazione predefinita: 100

Vincoli: minimo 20, massimo 100.

Tipo: integer

Campo obbligatorio: no

ResourceIdentifier

L'ARN della risorsa per la quale restituire operazioni di manutenzione in sospeso.

Tipo: string

Campo obbligatorio: no

Elementi di risposta

I seguenti elementi vengono restituiti dal servizio.

Marker

Token di paginazione opzionale fornito da una richiesta precedente. Se questo parametro viene specificato, la risposta include solo i record oltre il contrassegno, fino al valore specificato da `MaxRecords`.

Tipo: stringa

`PendingMaintenanceActions`. `ResourcePendingMaintenanceActionsN`.

Le azioni di manutenzione da applicare.

Tipo: matrice di oggetti [ResourcePendingMaintenanceActions](#)

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

ResourceNotFoundFault

L'ID della risorsa specificata non è stato trovato.

Codice di stato HTTP: 404

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)
- [AWSSDK per JavaScript V3](#)
- [SDK AWS per PHP V3](#)
- [SDK AWS per Python](#)
- [SDK AWS per Ruby V3](#)

FailoverDBCluster

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Impone un failover per un cluster.

Un failover per un cluster promuove una delle repliche di Amazon DocumentDB (istanze di sola lettura) nel cluster come istanza principale (lo scrittore del cluster).

In caso di errore dell'istanza primaria, Amazon DocumentDB esegue automaticamente il failover su una replica di Amazon DocumentDB, se esistente. Puoi forzare un failover per simulare un guasto di un'istanza primaria per scopi di testing.

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

DBClusterIdentifier

Un identificatore di cluster per cui forzare un failover. Questo parametro non distingue tra maiuscole e minuscole.

Vincoli:

- Deve corrispondere all'identificativo di un `DBCluster` esistente.

Tipo: string

Campo obbligatorio: no

TargetDBInstanceIdentifier

Nome dell'istanza da promuovere a istanza primaria.

È necessario specificare l'identificatore di istanza per una replica di Amazon DocumentDB nel cluster. Ad esempio, `mydbcluster-replica1`.

Tipo: string

Campo obbligatorio: no

Elementi di risposta

Il seguente elemento viene restituito dal servizio.

DBCluster

Informazioni dettagliate su un cluster.

Tipo: oggetto [DBCluster](#)

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

DBClusterNotFoundFault

`DBClusterIdentifiernon` si riferisce a un cluster esistente.

Codice di stato HTTP: 404

InvalidDBClusterStateFault

Il cluster non è in uno stato valido.

Codice di stato HTTP: 400

InvalidDBInstanceState

L'istanza specificata non è nello stato disponibile.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)
- [AWSSDK per JavaScript V3](#)
- [SDK AWS per PHP V3](#)

- [SDK AWS per Python](#)
- [SDK AWS per Ruby V3](#)

ListTagsForResource

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Elenca tutti i tag su una risorsa Amazon DocumentDB.

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

ResourceName

La risorsa Amazon DocumentDB con i tag da elencare. Questo valore è un Amazon Resource Name (ARN).

Tipo: stringa

Campo obbligatorio: sì

Filtri.Filter.N

Questo parametro non è attualmente supportato.

Tipo: matrice di oggetti [Filter](#)

Campo obbligatorio: no

Elementi di risposta

Il servizio restituisce il seguente elemento.

TagList.Tag.N

Un elenco di uno o più tag.

Tipo: matrice di oggetti [Tag](#)

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

DBClusterNotFoundFault

DBClusterIdentifiernon fa riferimento a un cluster esistente.

Codice di stato HTTP: 404

DBInstanceNotFound

DBInstanceIdentifiernon fa riferimento a un'istanza esistente.

Codice di stato HTTP: 404

DBSnapshotNotFound

DBSnapshotIdentifiernon fa riferimento a un'istantanea esistente.

Codice di stato HTTP: 404

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)
- [AWSSDK per V3 JavaScript](#)
- [SDK AWS per PHP V3](#)
- [SDK AWS per Python](#)
- [SDK AWS per Ruby V3](#)

ModifyDBCluster

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Modifica un'impostazione per un cluster Amazon DocumentDB. Puoi modificare uno o più parametri di configurazione del database specificando questi parametri e i nuovi valori nella richiesta.

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

DBClusterIdentifier

L'identificatore del cluster per il cluster che viene modificato. Questo parametro non distingue tra maiuscole e minuscole.

Vincoli:

- Deve corrispondere all'identificativo di un `DBCluster` esistente.

Tipo: stringa

Campo obbligatorio: sì

AllowMajorVersionUpgrade

Un valore che Indica che gli aggiornamenti delle versioni principali sono permessi.

Vincoli: è necessario consentire gli aggiornamenti delle versioni principali quando si specifica un valore per il `EngineVersion` parametro che è una versione principale diversa dalla versione corrente del cluster DB.

Tipo: Booleano

Campo obbligatorio: no

ApplyImmediately

Un valore che specifica se le modifiche in questa richiesta e le eventuali modifiche in sospeso vengono applicate in modo asincrono il prima possibile, indipendentemente dall'impostazione per il cluster. `PreferredMaintenanceWindow` Se questo parametro è impostato su `false`, le modifiche al cluster vengono applicate durante la finestra di manutenzione successiva.

Il `ApplyImmediately` parametro influisce solo sui `MasterUserPassword` valori `NewDBClusterIdentifier` and. Se impostate questo valore del parametro su `false`, le

modifiche ai `MasterUserPassword` valori `NewDBClusterIdentifier` and vengono applicate durante la finestra di manutenzione successiva. Tutte le altre modifiche vengono applicate immediatamente, indipendentemente dal valore del parametro `ApplyImmediately`.

Impostazione predefinita: `false`

Tipo: Booleano

Campo obbligatorio: no

BackupRetentionPeriod

Il numero di giorni durante i quali vengono conservati i backup automatici. È necessario specificare un valore minimo pari a 1.

Impostazione predefinita: 1

Vincoli:

- Il valore deve essere compreso tra 1 e 35.

Tipo: integer

Campo obbligatorio: no

CloudwatchLogsExportConfiguration

L'impostazione di configurazione per i tipi di log da abilitare per l'esportazione in Amazon CloudWatch Logs per un'istanza o un cluster specifico. Gli `DisableLogTypes` array `EnableLogTypes` and determinano quali log vengono esportati (o non esportati) in Logs. CloudWatch

Tipo: oggetto [CloudwatchLogsExportConfiguration](#)

Campo obbligatorio: no

DBClusterParameterGroupName

Il nome del gruppo di parametri del cluster da utilizzare per il cluster.

Tipo: string

Campo obbligatorio: no

DeletionProtection

Specifica se questo cluster può essere eliminato. Se `DeletionProtection` è abilitato, il cluster non può essere eliminato a meno che non venga modificato e `DeletionProtection` disabilitato. `DeletionProtection` protegge i cluster dall'eliminazione accidentale.

Tipo: Booleano

Campo obbligatorio: no

EngineVersion

Numero di versione del motore di database a cui eseguire l'aggiornamento. La modifica di questo parametro provoca un'interruzione. La modifica viene applicata durante la finestra di manutenzione successiva, a meno che il parametro `ApplyImmediately` non sia abilitato.

Per elencare tutte le versioni del motore disponibili per Amazon DocumentDB, usa il seguente comando:

```
aws docdb describe-db-engine-versions --engine docdb --query
"DBEngineVersions[].EngineVersion"
```

Tipo: string

Campo obbligatorio: no

MasterUserPassword

La password per l'utente del database master. Questa password può contenere qualsiasi carattere ASCII stampabile, eccetto la barra (/), le virgolette (") o il simbolo chiocciola (@).

Vincoli: deve contenere da 8 a 100 caratteri.

Tipo: string

Campo obbligatorio: no

NewDBClusterIdentifier

Il nuovo identificatore per il cluster quando un cluster viene rinominato. Questo valore è archiviato come stringa in caratteri minuscoli.

Vincoli:

- Deve contenere da 1 a 63 lettere, numeri o trattini.

- Il primo carattere deve essere una lettera.
- Non può terminare con un trattino o contenere due trattini consecutivi.

Esempio: `my-cluster2`

Tipo: string

Campo obbligatorio: no

Port

Numero della porta sulla quale il cluster accetta le connessioni.

Vincoli: deve essere un valore compreso tra a. 1150 65535

Impostazione predefinita: la stessa porta del cluster originale.

Tipo: integer

Campo obbligatorio: no

PreferredBackupWindow

Intervallo di tempo giornaliero durante il quale vengono creati i backup automatici, se sono abilitati tramite il parametro `BackupRetentionPeriod`.

Il valore predefinito è una finestra di 30 minuti selezionata in modo casuale in un blocco di 8 ore per ogni Regione AWS.

Vincoli:

- Il valore deve essere nel formato `hh24:mi-hh24:mi`.
- Il valore deve essere nel fuso orario UTC (Universal Coordinated Time).
- Il valore non deve essere in conflitto con la finestra di manutenzione preferita.
- Il valore deve essere almeno di 30 minuti.

Tipo: string

Campo obbligatorio: no

PreferredMaintenanceWindow

Intervallo temporale settimanale nel fuso orario UTC (Universal Coordinated Time) durante il quale può verificarsi la manutenzione dei sistemi.

Formato: `ddd:hh24:mi-ddd:hh24:mi`

Il valore predefinito è una finestra di 30 minuti selezionata in modo casuale in un blocco di 8 ore per ogni Regione AWS, in un giorno casuale della settimana.

Giorni validi: lunedì, martedì, mercoledì, giovedì, venerdì, sabato, domenica

Vincoli: finestra di un minimo di 30 minuti.

Tipo: string

Campo obbligatorio: no

StorageType

Il tipo di archiviazione da associare al cluster di database.

Per informazioni sui tipi di storage per i cluster Amazon DocumentDB, consulta le configurazioni di storage dei cluster nella Amazon DocumentDB Developer Guide.

Valori validi per il tipo di storage - `standard` | `iopt1`

Il valore predefinito è `standard`

Tipo: string

Campo obbligatorio: no

VpcSecurityGroupIds. VpcSecurityGroupIDN.

Un elenco di gruppi di sicurezza del cloud privato virtuale (VPC) a cui apparterrà il cluster.

Tipo: matrice di stringhe

Campo obbligatorio: no

Elementi di risposta

Il servizio restituisce il seguente elemento.

DBCluster

Informazioni dettagliate su un cluster.

Tipo: oggetto [DBCluster](#)

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

DBClusterAlreadyExistsFault

Hai già un cluster con l'identificatore fornito.

Codice di stato HTTP: 400

DBClusterNotFoundFault

`DBClusterIdentifier` non fa riferimento a un cluster esistente.

Codice di stato HTTP: 404

DBClusterParameterGroupNotFound

`DBClusterParameterGroupName` non fa riferimento a un gruppo di parametri del cluster esistente.

Codice di stato HTTP: 404

DBSubnetGroupNotFoundFault

`DBSubnetGroupName` non fa riferimento a un gruppo di sottoreti esistente.

Codice di stato HTTP: 404

InvalidDBClusterStateFault

Il cluster non è in uno stato valido.

Codice di stato HTTP: 400

InvalidDBInstanceState

L'istanza specificata non è nello stato disponibile.

Codice di stato HTTP: 400

InvalidDBSecurityGroupState

Lo stato del gruppo di sicurezza non consente l'eliminazione.

Codice di stato HTTP: 400

InvalidDBSubnetGroupStateFault

Il gruppo di sottoreti non può essere eliminato perché è in uso.

Codice di stato HTTP: 400

InvalidSubnet

La sottorete richiesta non è valida oppure sono state richieste più sottoreti che non si trovano tutte in un cloud privato virtuale (VPC) comune.

Codice di stato HTTP: 400

InvalidVPCNetworkStateFault

Il gruppo di sottoreti non copre tutte le zone di disponibilità dopo la creazione a causa delle modifiche apportate.

Codice di stato HTTP: 400

StorageQuotaExceeded

La richiesta comporterebbe il superamento della quantità di storage consentita disponibile in tutte le istanze.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)
- [AWSSDK per V3 JavaScript](#)
- [SDK AWS per PHP V3](#)
- [SDK AWS per Python](#)

- [SDK AWS per Ruby V3](#)

ModifyDBClusterParameterGroup

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Modifica i parametri di un gruppo di parametri del cluster. Per modificare più di un parametro, inviare un elenco di quanto segue: `ParameterName`, `ParameterValue` e `ApplyMethod`. Un massimo di 20 parametri possono essere modificati in una singola richiesta.

Note

Le modifiche apportate ai parametri dinamici vengono applicate immediatamente. Le modifiche ai parametri statici richiedono una finestra di riavvio o di manutenzione prima che la modifica possa avere effetto.

Important

Dopo aver creato un gruppo di parametri del cluster, è necessario attendere almeno 5 minuti prima di creare il primo cluster che utilizza il gruppo di parametri del cluster come gruppo predefinito. Ciò consente ad Amazon DocumentDB di completare completamente l'azione di creazione prima che il gruppo di parametri venga utilizzato come predefinito per un nuovo cluster. Questa fase è particolarmente importante per parametri che sono critici durante la creazione del database predefinito per un cluster, ad esempio il set di caratteri per il database predefinito specificato dal parametro `character_set_database`.

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

DBClusterParameterGroupName

Il nome del gruppo di parametri del cluster da modificare.

Tipo: stringa

Campo obbligatorio: sì

Parametri.Parameter.N

Un elenco di parametri nel gruppo di parametri del cluster da modificare.

Tipo: matrice di oggetti [Parameter](#)

Campo obbligatorio: sì

Elementi di risposta


Il servizio restituisce il seguente elemento.

DBClusterParameterGroupName

Il nome di un gruppo di parametri del cluster.

Vincoli:

- Deve contenere da 1 a 255 lettere o numeri.
- Il primo carattere deve essere una lettera.
- Non può terminare con un trattino o contenere due trattini consecutivi.

 Note

Questo valore è archiviato come stringa in caratteri minuscoli.

Tipo: stringa

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

DBParameterGroupNotFound

DBParameterGroupName non fa riferimento a un gruppo di parametri esistente.

Codice di stato HTTP: 404

InvalidDBParameterGroupState

Il gruppo di parametri è in uso o si trova in uno stato non valido. Se state cercando di eliminare il gruppo di parametri, non potete eliminarlo quando il gruppo di parametri si trova in questo stato.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)
- [AWSSDK per JavaScript V3](#)
- [SDK AWS per PHP V3](#)
- [SDK AWS per Python](#)
- [SDK AWS per Ruby V3](#)

ModifyDBClusterSnapshotAttribute

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Aggiunge un attributo e dei valori o rimuove un attributo e dei valori da un'istantanea manuale del cluster.

Per condividere un'istantanea manuale del `AttributeName` cluster con altri Account AWS, specifica `restore` come e utilizza il `ValuesToAdd` parametro per aggiungere un elenco di ID autorizzati a ripristinare Account AWS l'istantanea manuale del cluster. Utilizzate il valore `all` per rendere pubblica l'istantanea manuale del cluster, il che significa che può essere copiata o ripristinata da tutti. Account AWS Non aggiungete il `all` valore per le istantanee manuali del cluster che contengono informazioni private che non desiderate siano disponibili per tutti. Account AWS Se un'istantanea manuale del cluster è crittografata, può essere condivisa, ma solo specificando un elenco di Account AWS ID autorizzati per il parametro. `ValuesToAdd` Non è possibile utilizzare `all` come valore per il parametro in questo caso.

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

`AttributeName`

Il nome dell'attributo dell'istantanea del cluster da modificare.

Per gestire l'autorizzazione di altri utenti Account AWS a copiare o ripristinare un'istantanea manuale del cluster, imposta questo valore su `restore`

Tipo: stringa

Campo obbligatorio: sì

`DBClusterSnapshotIdentifier`

L'identificatore dello snapshot del cluster di cui modificare gli attributi.

Tipo: stringa

Campo obbligatorio: sì

`ValuesToAdd`. `AttributeValueN`.

Un elenco di attributi di snapshot del cluster da aggiungere all'attributo specificato da.

`AttributeName`

Per autorizzare altri utenti Account AWS a copiare o ripristinare un'istantanea manuale del cluster, imposta questo elenco in modo da includere uno o più ID. Account AWS Per rendere l'istantanea manuale del cluster ripristinabile da qualsiasi utente Account AWS, impostala su. `all` Non aggiungete il `all` valore per le istantanee manuali del cluster che contengono informazioni private che non desiderate siano disponibili per tutti. Account AWS

Tipo: matrice di stringhe

Campo obbligatorio: no

ValuesToRemove. AttributeValueN.

Un elenco di attributi di snapshot del cluster da rimuovere dall'attributo specificato da. AttributeName

Per rimuovere l'autorizzazione ad altri utenti Account AWS a copiare o ripristinare manualmente un'istantanea del cluster, imposta questo elenco in modo che includa uno o più Account AWS identificatori. Per rimuovere l'autorizzazione Account AWS a copiare o ripristinare l'istantanea del cluster, impostala su. `all` Se lo specifichiamo, un utente Account AWS il cui ID account viene aggiunto in modo esplicito all'attribute può comunque copiare o ripristinare un'istantanea manuale del cluster.

Tipo: matrice di stringhe

Campo obbligatorio: no

Elementi di risposta

Il servizio restituisce il seguente elemento.

DBClusterSnapshotAttributesResult

Informazioni dettagliate sugli attributi associati a uno snapshot del cluster.

Tipo: oggetto [DBClusterSnapshotAttributesResult](#)

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

DBClusterSnapshotNotFoundFault

DBClusterSnapshotIdentifiernon fa riferimento a un'istantanea del cluster esistente.

Codice di stato HTTP: 404

InvalidDBClusterSnapshotStateFault

Il valore fornito non è uno stato valido di snapshot del cluster.

Codice di stato HTTP: 400

SharedSnapshotQuotaExceeded

È stato superato il numero massimo di account che è possibile condividere con uno snapshot DB manuale.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)
- [AWSSDK per V3 JavaScript](#)
- [SDK AWS per PHP V3](#)
- [SDK AWS per Python](#)
- [SDK AWS per Ruby V3](#)

ModifyDBInstance

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Modifica le impostazioni per un'istanza. Puoi modificare uno o più parametri di configurazione del database specificando questi parametri e i nuovi valori nella richiesta.

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

DBInstanceIdentifier

L'identificatore delle istanze. Questo valore è archiviato come stringa in caratteri minuscoli.

Vincoli:

- Deve corrispondere all'identificativo di un DBInstance esistente.

Tipo: stringa

Campo obbligatorio: sì

ApplyImmediately

Specifica se le modifiche in questa richiesta e tutte le modifiche in sospeso vengono applicate in modo asincrono il prima possibile, indipendentemente dall'impostazione per l'istanza.

PreferredMaintenanceWindow

Se questo parametro è impostato su `false`, le modifiche all'istanza vengono applicate durante la finestra di manutenzione successiva. Alcune modifiche ai parametri possono causare un'interruzione e vengono applicate al riavvio successivo.

Impostazione predefinita: `false`

Tipo: Booleano

Campo obbligatorio: no

AutoMinorVersionUpgrade

Questo parametro non si applica ad Amazon DocumentDB. Amazon DocumentDB non esegue aggiornamenti di versione secondari indipendentemente dal valore impostato.

Tipo: Booleano

Campo obbligatorio: no

CACertificateIdentifier

Indica il certificato che deve essere associato all'istanza.

Tipo: string

Campo obbligatorio: no

CertificateRotationRestart

Specifica se l'istanza DB viene riavviata quando si ruota il certificato SSL/TLS.

Per impostazione predefinita, l'istanza DB viene riavviata quando si ruota il certificato SSL/TLS. Il certificato non viene aggiornato finché l'istanza DB non viene riavviata.

Important

Imposta questo parametro solo se non utilizzi SSL/TLS per connetterti all'istanza DB.

Se utilizzi SSL/TLS per connetterti all'istanza DB, consulta Updating Your [Amazon DocumentDB TLS Certificates and Encrypting Data in Transit nella Amazon DocumentDB Developer Guide](#).

Tipo: Booleano

Campo obbligatorio: no

CopyTagsToSnapshot

Un valore che indica se copiare tutti i tag dall'istanza DB negli snapshot dell'istanza DB. Per impostazione predefinita i tag non vengono copiati.

Tipo: Booleano

Campo obbligatorio: no

DBInstanceClass

La nuova capacità di calcolo e memoria dell'istanza, ad esempio. `db.r5.large` Non tutte le classi di istanze sono disponibili in tutte le Regioni AWS.

Se si modifica la classe dell'istanza, si verifica un'interruzione durante la modifica. La modifica viene applicata durante la finestra di manutenzione successiva, a meno che il valore di `ApplyImmediately` per questa richiesta non sia `true`.

Predefinito: utilizza l'impostazione esistente.

Tipo: string

Campo obbligatorio: no

EnablePerformanceInsights

Un valore che indica se abilitare Performance Insights per l'istanza del database. Per ulteriori informazioni, consulta la sezione [Utilizzo di Amazon Performance Insights](#).

Tipo: Booleano

Campo obbligatorio: no

NewDBInstanceIdentifier

Il nuovo identificatore di istanza per l'istanza quando si rinomina un'istanza. Quando si modifica l'identificatore dell'istanza, si verifica immediatamente un riavvio dell'istanza se si imposta su `Apply Immediately true`. Si verifica durante la finestra di manutenzione successiva, se impostata su `Apply Immediately false`. Questo valore è archiviato come stringa in caratteri minuscoli.

Vincoli:

- Deve contenere da 1 a 63 lettere, numeri o trattini.
- Il primo carattere deve essere una lettera.
- Non può terminare con un trattino o contenere due trattini consecutivi.

Esempio: `mydbinstance`

Tipo: string

Campo obbligatorio: no

PerformanceInsightsKMSKeyId

Identificatore di chiave AWS KMS per la crittografia dei dati di Performance Insights.

L'identificatore della AWS KMS chiave è l'ARN della chiave, l'ID della chiave, l'alias ARN o il nome alias per la chiave KMS.

Se non specifichi un valore per `PerformanceInsights KMSKeyId`, Amazon DocumentDB utilizza la tua chiave KMS predefinita. Esiste una chiave KMS predefinita per il tuo account Amazon Web

Services. Il tuo account Amazon Web Services ha una chiave KMS predefinita diversa per ogni regione Amazon Web Services.

Tipo: string

Campo obbligatorio: no

PreferredMaintenanceWindow

Intervallo di tempo settimanale (nel fuso orario UTC) durante il quale può verificarsi la finestra di manutenzione del sistema, che potrebbe comportare un'interruzione. La modifica di questo parametro non comporta un'interruzione tranne nella situazione seguente e la modifica viene applicata in modo asincrono il prima possibile. Se ci sono azioni in sospeso che causano il riavvio e la finestra di manutenzione viene modificata per includere l'ora corrente, la modifica di questo parametro provoca il riavvio dell'istanza. Se si sposta questa finestra all'ora corrente, devono trascorrere almeno 30 minuti tra l'ora corrente e la fine della finestra per garantire che vengano applicate le modifiche in sospeso.

Predefinito: utilizza l'impostazione esistente.

Formato: ddd:hh24:mi-ddd:hh24:mi

Giorni validi: lunedì, martedì, mercoledì, giovedì, venerdì, sabato, domenica

Vincoli: deve durare almeno 30 minuti.

Tipo: string

Campo obbligatorio: no

PromotionTier

Un valore che specifica l'ordine in cui una replica di Amazon DocumentDB viene promossa all'istanza principale dopo un errore dell'istanza primaria esistente.

Impostazione predefinita: 1

Valori validi: 0-15

Tipo: integer

Campo obbligatorio: no

Elementi di risposta

Il servizio restituisce il seguente elemento.

DBInstance

Informazioni dettagliate su un'istanza.

Tipo: oggetto [DBInstance](#)

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

AuthorizationNotFound

L'IP CIDR o il gruppo di sicurezza Amazon EC2 specificato non sono autorizzati per il gruppo di sicurezza specificato.

Amazon DocumentDB potrebbe inoltre non essere autorizzato a eseguire le azioni necessarie per tuo conto utilizzando IAM.

Codice di stato HTTP: 404

CertificateNotFound

`CertificateIdentifier` non fa riferimento a un certificato esistente.

Codice di stato HTTP: 404

DBInstanceAlreadyExists

Hai già un'istanza con l'identificatore specificato.

Codice di stato HTTP: 400

DBInstanceNotFound

`DBInstanceIdentifier` non fa riferimento a un'istanza esistente.

Codice di stato HTTP: 404

DBParameterGroupNotFound

`DBParameterGroupName` non fa riferimento a un gruppo di parametri esistente.

Codice di stato HTTP: 404

DBSecurityGroupNotFound

DBSecurityGroupNamenon fa riferimento a un gruppo di sicurezza esistente.

Codice di stato HTTP: 404

DBUpgradeDependencyFailure

L'aggiornamento non è riuscito perché una risorsa da cui dipende non può essere modificata.

Codice di stato HTTP: 400

InsufficientDBInstanceCapacity

La classe di istanza specificata non è disponibile nella zona di disponibilità specificata.

Codice di stato HTTP: 400

InvalidDBInstanceState

L'istanza specificata non è nello stato disponibile.

Codice di stato HTTP: 400

InvalidDBSecurityGroupState

Lo stato del gruppo di sicurezza non consente l'eliminazione.

Codice di stato HTTP: 400

InvalidVPCNetworkStateFault

Il gruppo di sottoreti non copre tutte le zone di disponibilità dopo la sua creazione a causa delle modifiche apportate.

Codice di stato HTTP: 400

StorageQuotaExceeded

La richiesta comporterebbe il superamento della quantità di storage consentita disponibile in tutte le istanze.

Codice di stato HTTP: 400

StorageTypeNotSupported

L'archiviazione dello spazio specificato non StorageType può essere associata all'istanza DB.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)
- [AWSSDK per JavaScript V3](#)
- [SDK AWS per PHP V3](#)
- [SDK AWS per Python](#)
- [SDK AWS per Ruby V3](#)

ModifyDBSubnetGroup

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Modifica un gruppo di sottoreti esistente. I gruppi di sottoreti devono contenere almeno una sottorete in almeno due zone di disponibilità in. Regione AWS

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

DBSubnetGroupName

Il nome del gruppo di sottoreti. Questo valore è archiviato come stringa in caratteri minuscoli. Non è possibile modificare il gruppo di sottoreti di default.

Vincoli: deve corrispondere al nome di un oggetto DBSubnetGroup esistente. Non deve essere predefinito.

Esempio: mySubnetgroup

Tipo: stringa

Campo obbligatorio: sì

SubnetIds. SubnetIdentifierN.

Gli ID di sottorete Amazon EC2 per il gruppo di sottoreti.

Tipo: matrice di stringhe

Campo obbligatorio: sì

DBSubnetGroupDescription

La descrizione per il gruppo di sottoreti.

Tipo: string

Campo obbligatorio: no

Elementi di risposta

Il servizio restituisce il seguente elemento.

DBSubnetGroup

Informazioni dettagliate su un gruppo di sottoreti.

Tipo: oggetto [DBSubnetGroup](#)

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

DBSubnetGroupDoesNotCoverEnoughAZs

Le sottoreti del gruppo di sottoreti devono coprire almeno due zone di disponibilità, a meno che non esista una sola zona di disponibilità.

Codice di stato HTTP: 400

DBSubnetGroupNotFoundFault

DBSubnetGroupNameon fa riferimento a un gruppo di sottoreti esistente.

Codice di stato HTTP: 404

DBSubnetQuotaExceededFault

La richiesta comporterebbe il superamento del numero consentito di sottoreti in un gruppo di sottoreti.

Codice di stato HTTP: 400

InvalidSubnet

La sottorete richiesta non è valida oppure sono state richieste più sottoreti che non si trovano tutte in un cloud privato virtuale (VPC) comune.

Codice di stato HTTP: 400

SubnetAlreadyInUse

La sottorete è già in uso nella zona di disponibilità.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)
- [AWSSDK per V3 JavaScript](#)
- [SDK AWS per PHP V3](#)
- [SDK AWS per Python](#)
- [SDK AWS per Ruby V3](#)

ModifyEventSubscription

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Modifica un abbonamento esistente per la notifica di eventi di Amazon DocumentDB.

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

SubscriptionName

Il nome dell'abbonamento per la notifica degli eventi di Amazon DocumentDB.

Tipo: stringa

Campo obbligatorio: sì

Enabled

Un valore booleano; impostato per `true` attivare l'abbonamento.

Tipo: Booleano

Campo obbligatorio: no

EventCategories. EventCategoryN.

Un elenco di categorie di eventi a `SourceType` cui desideri iscriverti.

Tipo: matrice di stringhe

Campo obbligatorio: no

SnsTopicArn

L'Amazon Resource Name (ARN) dell'argomento SNS creato per la notifica di eventi. L'ARN viene creato da Amazon SNS al momento della creazione di un argomento e la sottoscrizione.

Tipo: string

Campo obbligatorio: no

SourceType

Il tipo di origine che genera gli eventi. Ad esempio, se desideri ricevere una notifica degli eventi generati da un'istanza, imposta questo parametro `sudb-instance`. Se questo valore non viene specificato, vengono restituiti tutti gli eventi.

Valori validi: db-instance, db-parameter-group, db-security-group

Tipo: string

Campo obbligatorio: no

Elementi di risposta

Il servizio restituisce il seguente elemento.

EventSubscription

Informazioni dettagliate su un evento a cui ti sei iscritto.

Tipo: oggetto [EventSubscription](#)

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

EventSubscriptionQuotaExceeded

Hai raggiunto il numero massimo di iscrizioni agli eventi.

Codice di stato HTTP: 400

SNSInvalidTopic

Amazon SNS ha risposto che c'è un problema con l'argomento specificato.

Codice di stato HTTP: 400

SNSNoAuthorization

Non sei autorizzato a pubblicare sull'argomento SNS Amazon Resource Name (ARN).

Codice di stato HTTP: 400

SNSTopicArnNotFound

L'argomento SNS Amazon Resource Name (ARN) non esiste.

Codice di stato HTTP: 404

SubscriptionCategoryNotFound

La categoria fornita non esiste.

Codice di stato HTTP: 404

SubscriptionNotFound

Il nome dell'abbonamento non esiste.

Codice di stato HTTP: 404

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)
- [AWSSDK per JavaScript V3](#)
- [SDK AWS per PHP V3](#)
- [SDK AWS per Python](#)
- [SDK AWS per Ruby V3](#)

ModifyGlobalCluster

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Modifica un'impostazione per un cluster globale Amazon DocumentDB. Puoi modificare uno o più parametri di configurazione (ad esempio: protezione dall'eliminazione) o l'identificatore globale del cluster specificando questi parametri e i nuovi valori nella richiesta.

Note

Questa azione si applica solo ai cluster Amazon DocumentDB.

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

GlobalClusterIdentifier

L'identificatore del cluster globale da modificare. Questo parametro non fa distinzione tra maiuscole e minuscole.

Vincoli:

- Deve corrispondere all'identificatore di un cluster globale esistente.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 1. Lunghezza massima di 255.

Modello: `[A-Za-z][0-9A-Za-z-:._]*`

Campo obbligatorio: sì

DeletionProtection

Indica se il cluster globale ha la protezione da eliminazione abilitata. Il cluster globale non può essere eliminato quando la protezione da eliminazione è abilitata.

Tipo: Booleano

Campo obbligatorio: no

NewGlobalClusterIdentifier

Il nuovo identificatore per un cluster globale quando si modifica un cluster globale. Questo valore è archiviato come stringa in caratteri minuscoli.

- Deve contenere da 1 a 63 lettere, numeri o trattini

Il primo carattere deve essere una lettera

Non può terminare con un trattino o contenere due trattini consecutivi

Esempio: `my-cluster2`

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 1. Lunghezza massima di 255.

Modello: `[A-Za-z][0-9A-Za-z-:._]*`

Campo obbligatorio: no

Elementi di risposta

Il servizio restituisce il seguente elemento.

GlobalCluster

Un tipo di dati che rappresenta un cluster globale Amazon DocumentDB.

Tipo: oggetto [GlobalCluster](#)

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

GlobalClusterNotFoundFault

`GlobalClusterIdentifier` Non si riferisce a un cluster globale esistente.

Codice di stato HTTP: 404

InvalidGlobalClusterStateFault

L'operazione richiesta non può essere eseguita mentre il cluster si trova in questo stato.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)
- [AWSSDK per JavaScript V3](#)
- [SDK AWS per PHP V3](#)
- [SDK AWS per Python](#)
- [SDK AWS per Ruby V3](#)

RebootDBInstance

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Potrebbe essere necessario riavviare l'istanza, in genere per motivi di manutenzione. Ad esempio, se si apportano determinate modifiche o se si modifica il gruppo di parametri del cluster associato all'istanza, è necessario riavviare l'istanza affinché le modifiche abbiano effetto.

Il riavvio di un'istanza comporta il riavvio del servizio del motore di database. Il riavvio di un'istanza provoca un'interruzione momentanea, durante la quale lo stato dell'istanza è impostato su Riavvio.

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

DBInstanceIdentifier

L'identificatore delle istanze. Questo parametro è archiviato come stringa in minuscolo.

Vincoli:

- Deve corrispondere all'identificativo di un DBInstance esistente.

Tipo: stringa

Campo obbligatorio: sì

ForceFailover

Quando `true`, il riavvio viene eseguito tramite un failover Multi-AZ.

Vincolo: non è possibile specificare `true` se l'istanza non è configurata per Multi-AZ.

Tipo: Booleano

Campo obbligatorio: no

Elementi di risposta

Il seguente elemento viene restituito dal servizio.

DBInstance

Informazioni dettagliate su un'istanza.

Tipo: oggetto [DBInstance](#)

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

DBInstanceNotFound

DBInstanceIdentifiernon fa riferimento a un'istanza esistente.

Codice di stato HTTP: 404

InvalidDBInstanceState

L'istanza specificata non è nello stato disponibile.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)
- [AWSSDK per JavaScript V3](#)
- [SDK AWS per PHP V3](#)
- [SDK AWS per Python](#)
- [SDK AWS per Ruby V3](#)

RemoveFromGlobalCluster

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Scollega un cluster secondario Amazon DocumentDB da un cluster globale. Il cluster diventa un cluster autonomo con funzionalità di lettura/scrittura anziché essere di sola lettura e ricevere dati da un sistema primario in un'altra regione.

Note

Questa azione si applica solo ai cluster Amazon DocumentDB.

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

DbClusterIdentifier

L'Amazon Resource Name (ARN) che identifica il cluster che è stato separato dal cluster globale Amazon DocumentDB.

Tipo: stringa

Campo obbligatorio: sì

GlobalClusterIdentifier

L'identificatore del cluster da staccare dal cluster globale Amazon DocumentDB.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 1. Lunghezza massima di 255.

Modello: `[A-Za-z][0-9A-Za-z-:._]*`

Campo obbligatorio: sì

Elementi di risposta

Il seguente elemento viene restituito dal servizio.

GlobalCluster

Un tipo di dati che rappresenta un cluster globale Amazon DocumentDB.

Tipo: oggetto [GlobalCluster](#)

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

DBClusterNotFoundFault

`DBClusterIdentifier` non si riferisce a un cluster esistente.

Codice di stato HTTP: 404

GlobalClusterNotFoundFault

`GlobalClusterIdentifier` non si riferisce a un cluster globale esistente.

Codice di stato HTTP: 404

InvalidGlobalClusterStateFault

L'operazione richiesta non può essere eseguita mentre il cluster si trova in questo stato.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)
- [AWSSDK per JavaScript V3](#)
- [SDK AWS per PHP V3](#)

- [SDK AWS per Python](#)
- [SDK AWS per Ruby V3](#)

RemoveSourceIdentifierFromSubscription

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Rimuove un identificatore di origine da un abbonamento esistente per la notifica di eventi di Amazon DocumentDB.

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

SourceIdentifier

L'identificatore di origine da rimuovere dall'abbonamento, ad esempio l'identificatore di istanza per un'istanza o il nome di un gruppo di sicurezza.

Tipo: stringa

Campo obbligatorio: sì

SubscriptionName

Il nome dell'abbonamento di notifica degli eventi di Amazon DocumentDB da cui desideri rimuovere un identificatore di origine.

Tipo: stringa

Campo obbligatorio: sì

Elementi di risposta

Il servizio restituisce il seguente elemento.

EventSubscription

Informazioni dettagliate su un evento a cui ti sei iscritto.

Tipo: oggetto [EventSubscription](#)

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

SourceNotFound

La fonte richiesta non è stata trovata.

Codice di stato HTTP: 404

SubscriptionNotFound

Il nome dell'abbonamento non esiste.

Codice di stato HTTP: 404

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)
- [AWSSDK per JavaScript V3](#)
- [SDK AWS per PHP V3](#)
- [SDK AWS per Python](#)
- [SDK AWS per Ruby V3](#)

RemoveTagsFromResource

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Rimuove i tag di metadati da una risorsa Amazon DocumentDB.

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

ResourceName

La risorsa Amazon DocumentDB da cui vengono rimossi i tag. Questo valore è un Amazon Resource Name (ARN).

Tipo: stringa

Campo obbligatorio: sì

TagKeys.Members.

La chiave del tag (nome) del tag da rimuovere.

Tipo: matrice di stringhe

Campo obbligatorio: sì

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

DBClusterNotFoundFault

DBClusterIdentifiernon fa riferimento a un cluster esistente.

Codice di stato HTTP: 404

DBInstanceNotFound

DBInstanceIdentifiernon fa riferimento a un'istanza esistente.

Codice di stato HTTP: 404

DBSnapshotNotFound

DBSnapshotIdentifiernon fa riferimento a un'istantanea esistente.

Codice di stato HTTP: 404

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)
- [AWSSDK per V3 JavaScript](#)
- [SDK AWS per PHP V3](#)
- [SDK AWS per Python](#)
- [SDK AWS per Ruby V3](#)

ResetDBClusterParameterGroup

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Modifica i parametri di un gruppo di parametri del cluster riportandoli al valore predefinito. Per ripristinare parametri specifici, invia un elenco dei seguenti elementi: `ParameterName` e `ApplyMethod`. Per reimpostare l'intero gruppo di parametri del cluster, specificate i `ResetAllParameters` parametri `DBClusterParameterGroupName` and.

Quando si ripristina l'intero gruppo, i parametri dinamici vengono aggiornati immediatamente e i parametri statici vengono impostati in `pending-reboot` modo da avere effetto al successivo riavvio dell'istanza DB.

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

`DBClusterParameterGroupName`

Il nome del gruppo di parametri del cluster da reimpostare.

Tipo: stringa

Campo obbligatorio: sì

`Parameters.Parameter.N`

Un elenco di nomi di parametri nel gruppo di parametri del cluster da ripristinare ai valori predefiniti. Non è possibile utilizzare questo parametro se il parametro `ResetAllParameters` è impostato su `true`.

Tipo: matrice di oggetti [Parameter](#)

Campo obbligatorio: no

`ResetAllParameters`

Un valore impostato per `true` ripristinare tutti i parametri nel gruppo di parametri del cluster ai valori predefiniti e `false` altro. Non è possibile utilizzare questo parametro se c'è un elenco di nomi di parametri specificati per il parametro `Parameters`.

Tipo: Booleano

Campo obbligatorio: no

Elementi di risposta

Il servizio restituisce il seguente elemento.

DBClusterParameterGroupName

Il nome di un gruppo di parametri del cluster.

Vincoli:

- Deve contenere da 1 a 255 lettere o numeri.
- Il primo carattere deve essere una lettera.
- Non può terminare con un trattino o contenere due trattini consecutivi.

Note

Questo valore è archiviato come stringa in caratteri minuscoli.

Tipo: stringa

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

DBParameterGroupNotFound

DBParameterGroupNamenon fa riferimento a un gruppo di parametri esistente.

Codice di stato HTTP: 404

InvalidDBParameterGroupState

Il gruppo di parametri è in uso o si trova in uno stato non valido. Se state cercando di eliminare il gruppo di parametri, non potete eliminarlo quando il gruppo di parametri si trova in questo stato.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)
- [AWSSDK per JavaScript V3](#)
- [SDK AWS per PHP V3](#)
- [SDK AWS per Python](#)
- [SDK AWS per Ruby V3](#)

RestoreDBClusterFromSnapshot

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Crea un nuovo cluster da un'istantanea o da un'istantanea del cluster.

Se viene specificata un'istantanea, il cluster di destinazione viene creato dallo snapshot del DB di origine con una configurazione e un gruppo di sicurezza predefiniti.

Se viene specificata un'istantanea del cluster, il cluster di destinazione viene creato dal punto di ripristino del cluster di origine con la stessa configurazione del cluster DB di origine, tranne per il fatto che il nuovo cluster viene creato con il gruppo di sicurezza predefinito.

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

DBClusterIdentifier

Il nome del cluster da creare a partire dall'istantanea o dall'istantanea del cluster. Questo parametro non fa distinzione tra maiuscole e minuscole.

Vincoli:

- Deve contenere da 1 a 63 lettere, numeri o trattini.
- Il primo carattere deve essere una lettera.
- Non può terminare con un trattino o contenere due trattini consecutivi.

Esempio: `my-snapshot-id`

Tipo: stringa

Campo obbligatorio: sì

Engine

Il motore di database da utilizzare per il nuovo cluster.

Predefinito: lo stesso del codice sorgente.

Vincolo: deve essere compatibile con il motore del sorgente.

Tipo: stringa

Campo obbligatorio: sì

SnapshotIdentifier

L'identificatore dello snapshot o dello snapshot del cluster da cui effettuare il ripristino.

È possibile utilizzare il nome o l'Amazon Resource Name (ARN) per specificare uno snapshot del cluster. Tuttavia, è possibile utilizzare solo l'ARN per specificare uno snapshot.

Vincoli:

- Deve corrispondere all'identificatore di una snapshot esistente.

Tipo: stringa

Campo obbligatorio: sì

AvailabilityZones. AvailabilityZoneN.

Fornisce l'elenco delle zone di disponibilità di Amazon EC2 in cui è possibile creare le istanze nel cluster DB ripristinato.

Tipo: matrice di stringhe

Campo obbligatorio: no

DBClusterParameterGroupName

Nome del gruppo di parametri del cluster di database che desideri associare al cluster di database.

Tipo: stringa. Obbligatorio: No.

Se questo argomento viene omissso, viene utilizzato il gruppo di parametri predefinito del cluster DB. Se fornito, deve corrispondere al nome di un gruppo di parametri predefinito del cluster DB esistente. La stringa deve essere composta da 1 a 255 lettere, numeri o trattini. Il primo carattere deve essere una lettera e non può terminare con un trattino o contenere due trattini consecutivi.

Tipo: string

Campo obbligatorio: no

DBSubnetGroupName

Il nome del gruppo di sottoreti da utilizzare per il nuovo cluster.

Vincoli: se forniti, devono corrispondere al nome di un esistente. DBSubnetGroup

Esempio: mySubnetgroup

Tipo: string

Campo obbligatorio: no

DeletionProtection

Specifica se questo cluster può essere eliminato. Se DeletionProtection è abilitato, il cluster non può essere eliminato a meno che non venga modificato e DeletionProtection disabilitato. DeletionProtection protegge i cluster dall'eliminazione accidentale.

Tipo: Booleano

Campo obbligatorio: no

EnableCloudwatchLogsExports.membro.

Un elenco di tipi di log che devono essere abilitati per l'esportazione in Amazon CloudWatch Logs.

Tipo: matrice di stringhe

Campo obbligatorio: no

EngineVersion

La versione del motore di database da utilizzare per il nuovo cluster.

Tipo: string

Campo obbligatorio: no

KmsKeyId

L'identificatore AWS KMS chiave da utilizzare per il ripristino di un cluster crittografato da un'istantanea del database o da un'istantanea del cluster.

L'identificatore della chiave AWS KMS è il nome della risorsa Amazon (ARN) per la chiave di crittografia AWS KMS. Se si ripristina un cluster con Account AWS lo stesso proprietario della chiave di AWS KMS crittografia utilizzata per crittografare il nuovo cluster, è possibile utilizzare l'alias della AWS KMS chiave anziché l'ARN per la chiave di crittografia. AWS KMS

Se non specifichi un valore per il parametro KmsKeyId, avviene quanto segue:

- Se l'istantanea o l'istantanea del cluster in `SnapshotIdentifier` è crittografata, il cluster ripristinato viene crittografato utilizzando la AWS KMS chiave utilizzata per crittografare l'istantanea o l'istantanea del cluster.
- Se l'istantanea o l'istantanea del cluster in ingresso non `SnapshotIdentifier` è crittografata, il cluster DB ripristinato non è crittografato.

Tipo: string

Campo obbligatorio: no

Port

Il numero di porta su cui il nuovo cluster accetta le connessioni.

Vincoli: deve essere un valore compreso tra a1150. 65535

Impostazione predefinita: la stessa porta del cluster originale.

Tipo: integer

Campo obbligatorio: no

StorageType

Il tipo di archiviazione da associare al cluster di database.

Per informazioni sui tipi di storage per i cluster Amazon DocumentDB, consulta le configurazioni di storage dei cluster nella Amazon DocumentDB Developer Guide.

Valori validi per il tipo di storage - `standard` | `iopt1`

Il valore predefinito è `standard`

Tipo: string

Campo obbligatorio: no

Tags.Tag.N

I tag da assegnare al cluster ripristinato.

Tipo: matrice di oggetti [Tag](#)

Campo obbligatorio: no

VpcSecurityGroupIds. VpcSecurityGroupIdN.

Un elenco di gruppi di sicurezza del cloud privato virtuale (VPC) a cui apparterrà il nuovo cluster.

Tipo: matrice di stringhe

Campo obbligatorio: no

Elementi di risposta

Il servizio restituisce il seguente elemento.

DBCluster

Informazioni dettagliate su un cluster.

Tipo: oggetto [DBCluster](#)

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

DBClusterAlreadyExistsFault

Hai già un cluster con l'identificatore fornito.

Codice di stato HTTP: 400

DBClusterQuotaExceededFault

Il cluster non può essere creato perché hai raggiunto la quota massima consentita di cluster.

Codice di stato HTTP: 403

DBClusterSnapshotNotFoundFault

`DBClusterSnapshotIdentifiernon` fa riferimento a un'istantanea del cluster esistente.

Codice di stato HTTP: 404

DBSnapshotNotFound

`DBSnapshotIdentifiernon` fa riferimento a un'istantanea esistente.

Codice di stato HTTP: 404

DBSubnetGroupNotFoundFault

DBSubnetGroupNamenon fa riferimento a un gruppo di sottoreti esistente.

Codice di stato HTTP: 404

DBSubnetGroupNotFoundFault

DBSubnetGroupNamenon fa riferimento a un gruppo di sottoreti esistente.

Codice di stato HTTP: 404

InsufficientDBClusterCapacityFault

Il cluster non dispone di capacità sufficiente per l'operazione corrente.

Codice di stato HTTP: 403

InsufficientStorageClusterCapacity

Lo spazio di archiviazione disponibile non è sufficiente per l'azione corrente. È possibile risolvere questo errore aggiornando il gruppo di sottoreti in modo che utilizzi zone di disponibilità diverse con più spazio di archiviazione disponibile.

Codice di stato HTTP: 400

InvalidDBClusterSnapshotStateFault

Il valore fornito non è uno stato valido di snapshot del cluster.

Codice di stato HTTP: 400

InvalidDBSnapshotState

Lo stato dell'istantanea non consente l'eliminazione.

Codice di stato HTTP: 400

InvalidRestoreFault

Non è possibile eseguire il ripristino da un backup su cloud privato virtuale (VPC) su un'istanza DB non VPC.

Codice di stato HTTP: 400

InvalidSubnet

La sottorete richiesta non è valida oppure sono state richieste più sottoreti che non si trovano tutte in un cloud privato virtuale (VPC) comune.

Codice di stato HTTP: 400

InvalidVPCNetworkStateFault

Il gruppo di sottoreti non copre tutte le zone di disponibilità dopo la creazione a causa delle modifiche apportate.

Codice di stato HTTP: 400

KMSKeyNotAccessibleFault

Si è verificato un errore durante l'accesso a una AWS KMS chiave.

Codice di stato HTTP: 400

StorageQuotaExceeded

La richiesta comporterebbe il superamento della quantità di storage consentita disponibile in tutte le istanze.

Codice di stato HTTP: 400

StorageQuotaExceeded

La richiesta comporterebbe il superamento della quantità di spazio di archiviazione consentita disponibile in tutte le istanze.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)
- [SDK AWS per Go](#)

- [SDK AWS per Java V2](#)
- [AWSSDK per V3 JavaScript](#)
- [SDK AWS per PHP V3](#)
- [SDK AWS per Python](#)
- [SDK AWS per Ruby V3](#)

RestoreDBClusterToPointInTime

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Ripristina un cluster a un punto temporale arbitrario. Gli utenti possono ripristinare a qualsiasi point-in-time prima di `LatestRestorableTime` per un massimo di `BackupRetentionPeriod` giorni. Il cluster di destinazione viene creato dal cluster di origine con la stessa configurazione del cluster originale, tranne per il fatto che il nuovo cluster viene creato con il gruppo di sicurezza predefinito.

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

`DBClusterIdentifier`

Il nome del nuovo cluster da creare.

Vincoli:

- Deve contenere da 1 a 63 lettere, numeri o trattini.
- Il primo carattere deve essere una lettera.
- Non può terminare con un trattino o contenere due trattini consecutivi.

Tipo: stringa

Campo obbligatorio: sì

`SourceDBClusterIdentifier`

L'identificativo del cluster di origine dal quale eseguire il ripristino.

Vincoli:

- Deve corrispondere all'identificativo di un `DBCluster` esistente.

Tipo: stringa

Campo obbligatorio: sì

`DBSubnetGroupName`

Il nome del gruppo di sottoreti da utilizzare per il nuovo cluster.

Vincoli: se fornito, deve corrispondere al nome di un esistente. `DBSubnetGroup`

Esempio: `mySubnetgroup`

Tipo: `string`

Campo obbligatorio: `no`

DeletionProtection

Specifica se questo cluster può essere eliminato. Se `DeletionProtection` è abilitato, il cluster non può essere eliminato a meno che non venga modificato e `DeletionProtection` disabilitato. `DeletionProtection` protegge i cluster dall'eliminazione accidentale.

Tipo: `Booleano`

Campo obbligatorio: `no`

EnableCloudwatchLogsExports.Member.

Un elenco di tipi di log che devono essere abilitati per l'esportazione in Amazon CloudWatch Logs.

Tipo: matrice di stringhe

Campo obbligatorio: `no`

KmsKeyId

L'identificatore della AWS KMS chiave da utilizzare per ripristinare un cluster crittografato da un cluster crittografato.

L'identificatore della chiave AWS KMS è il nome della risorsa Amazon (ARN) per la chiave di crittografia AWS KMS. Se si ripristina un cluster con Account AWS lo stesso proprietario della chiave di AWS KMS crittografia utilizzata per crittografare il nuovo cluster, è possibile utilizzare l'alias della AWS KMS chiave anziché l'ARN per la chiave di crittografia. AWS KMS

È possibile eseguire il ripristino in un nuovo cluster e crittografare il nuovo cluster con una AWS KMS chiave diversa da quella utilizzata per crittografare il AWS KMS cluster di origine. Il nuovo cluster DB è crittografato con la AWS KMS chiave identificata dal `KmsKeyId` parametro.

Se non specifichi un valore per il parametro `KmsKeyId`, avviene quanto segue:

- Se il cluster è crittografato, il cluster ripristinato viene crittografato utilizzando la AWS KMS chiave utilizzata per crittografare il cluster di origine.
- Se il cluster non è crittografato, il cluster ripristinato non è crittografato.

Se `DBClusterIdentifier` si riferisce a un cluster non crittografato, la richiesta di ripristino viene rifiutata.

Tipo: string

Campo obbligatorio: no

Port

Il numero di porta su cui il nuovo cluster accetta le connessioni.

Vincoli: deve essere un valore compreso tra a1150. 65535

Predefinita: la porta predefinita per il motore.

Tipo: integer

Campo obbligatorio: no

RestoreToTime

La data e l'ora alle quali ripristinare il cluster.

Valori validi: un orario in formato Universal Coordinated Time (UTC).

Vincoli:

- Deve essere antecedente all'ultimo orario ripristinabile per l'istanza.
- Deve essere specificato se il parametro `UseLatestRestorableTime` non viene fornito.
- Non può essere specificato se il parametro `UseLatestRestorableTime` è `true`.
- Non può essere specificato se il parametro `RestoreType` è `copy-on-write`.

Esempio: `2015-03-07T23:45:00Z`

Tipo: Timestamp

Campo obbligatorio: no

RestoreType

Il tipo di ripristino da eseguire. È possibile specificare uno dei seguenti valori:

- `full-copy`: il nuovo cluster database viene ripristinato come una copia completa del cluster database di origine.

- `copy-on-write`: il nuovo cluster database viene ripristinato come un clone del cluster database di origine.

Vincoli: non puoi specificare `copy-on-write` se la versione del motore del cluster di database di origine è precedente alla 1.11.

Se non si specifica un valore `RestoreType`, il nuovo cluster di database viene ripristinato come una copia completa del cluster di database di origine.

Tipo: `string`

Campo obbligatorio: no

StorageType

Il tipo di archiviazione da associare al cluster di database.

Per informazioni sui tipi di storage per i cluster Amazon DocumentDB, consulta le configurazioni di storage dei cluster nella Amazon DocumentDB Developer Guide.

Valori validi per il tipo di storage - `standard` | `iopt1`

Il valore predefinito è `standard`

Tipo: `string`

Campo obbligatorio: no

Tags.Tag.N

I tag da assegnare al cluster ripristinato.

Tipo: matrice di oggetti [Tag](#)

Campo obbligatorio: no

UseLatestRestorableTime

Un valore impostato su `true` per ripristinare il cluster all'ora dell'ultimo backup ripristinabile; in alternativa è impostato su `false`.

Impostazione predefinita: `false`

Vincoli: non può essere specificato se viene fornito il parametro `RestoreToTime`.

Tipo: Booleano

Campo obbligatorio: no

VpcSecurityGroupIds. VpcSecurityGroupIdN.

Un elenco di gruppi di sicurezza VPC a cui appartiene il nuovo cluster.

Tipo: matrice di stringhe

Campo obbligatorio: no

Elementi di risposta

Il servizio restituisce il seguente elemento.

DBCluster

Informazioni dettagliate su un cluster.

Tipo: oggetto [DBCluster](#)

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

DBClusterAlreadyExistsFault

Hai già un cluster con l'identificatore fornito.

Codice di stato HTTP: 400

DBClusterNotFoundFault

DBClusterIdentiifiernon fa riferimento a un cluster esistente.

Codice di stato HTTP: 404

DBClusterQuotaExceededFault

Il cluster non può essere creato perché hai raggiunto la quota massima consentita di cluster.

Codice di stato HTTP: 403

DBClusterSnapshotNotFoundFault

DBClusterSnapshotIdentifiernon fa riferimento a un'istantanea del cluster esistente.

Codice di stato HTTP: 404

DBSubnetGroupNotFoundFault

DBSubnetGroupNamenon fa riferimento a un gruppo di sottoreti esistente.

Codice di stato HTTP: 404

InsufficientDBClusterCapacityFault

Il cluster non dispone di capacità sufficiente per l'operazione corrente.

Codice di stato HTTP: 403

InsufficientStorageClusterCapacity

Lo spazio di archiviazione disponibile non è sufficiente per l'azione corrente. È possibile risolvere questo errore aggiornando il gruppo di sottoreti in modo che utilizzi zone di disponibilità diverse con più spazio di archiviazione disponibile.

Codice di stato HTTP: 400

InvalidDBClusterSnapshotStateFault

Il valore fornito non è uno stato valido di snapshot del cluster.

Codice di stato HTTP: 400

InvalidDBClusterStateFault

Il cluster non è in uno stato valido.

Codice di stato HTTP: 400

InvalidDBSnapshotState

Lo stato dell'istantanea non consente l'eliminazione.

Codice di stato HTTP: 400

InvalidRestoreFault

Non è possibile eseguire il ripristino da un backup su cloud privato virtuale (VPC) su un'istanza DB non VPC.

Codice di stato HTTP: 400

InvalidSubnet

La sottorete richiesta non è valida oppure sono state richieste più sottoreti che non si trovano tutte in un cloud privato virtuale (VPC) comune.

Codice di stato HTTP: 400

InvalidVPCNetworkStateFault

Il gruppo di sottoreti non copre tutte le zone di disponibilità dopo la creazione a causa delle modifiche apportate.

Codice di stato HTTP: 400

KMSKeyNotAccessibleFault

Si è verificato un errore durante l'accesso a una AWS KMS chiave.

Codice di stato HTTP: 400

StorageQuotaExceeded

La richiesta comporterebbe il superamento della quantità di storage consentita disponibile in tutte le istanze.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)
- [AWSSDK per V3 JavaScript](#)
- [SDK AWS per PHP V3](#)
- [SDK AWS per Python](#)

- [SDK AWS per Ruby V3](#)

StartDBCluster

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Riavvia il cluster interrotto specificato da `DBClusterIdentifier`. Per ulteriori informazioni, consulta [Arresto e avvio di un cluster Amazon DocumentDB](#).

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

`DBClusterIdentifier`

L'identificatore del cluster da riavviare. Esempio: `docdb-2019-05-28-15-24-52`

Tipo: stringa

Campo obbligatorio: sì

Elementi di risposta

Il seguente elemento viene restituito dal servizio.

`DBCluster`

Informazioni dettagliate su un cluster.

Tipo: oggetto [DBCluster](#)

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

`DBClusterNotFoundFault`

`DBClusterIdentifier` non si riferisce a un cluster esistente.

Codice di stato HTTP: 404

`InvalidDBClusterStateFault`

Il cluster non è in uno stato valido.

Codice di stato HTTP: 400

InvalidDBInstanceState

L'istanza specificata non è nello stato disponibile.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)
- [AWSSDK per JavaScript V3](#)
- [SDK AWS per PHP V3](#)
- [SDK AWS per Python](#)
- [SDK AWS per Ruby V3](#)

StopDBCluster

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Arresta il cluster in esecuzione specificato da `DBClusterIdentifier`. Il cluster deve essere nello stato disponibile. Per ulteriori informazioni, consulta [Arresto e avvio di un cluster Amazon DocumentDB](#).

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta [Parametri comuni](#).

`DBClusterIdentifier`

L'identificatore del cluster da interrompere. Esempio: `docdb-2019-05-28-15-24-52`

Tipo: stringa

Campo obbligatorio: sì

Elementi di risposta

Il servizio restituisce il seguente elemento.

`DBCluster`

Informazioni dettagliate su un cluster.

Tipo: oggetto [DBCluster](#)

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

`DBClusterNotFoundFault`

`DBClusterIdentifier` non si riferisce a un cluster esistente.

Codice di stato HTTP: 404

`InvalidDBClusterStateFault`

Il cluster non è in uno stato valido.

Codice di stato HTTP: 400

InvalidDBInstanceState

L'istanza specificata non è nello stato disponibile.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [SDK AWS per .NET](#)
- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)
- [AWSSDK per JavaScript V3](#)
- [SDK AWS per PHP V3](#)
- [SDK AWS per Python](#)
- [SDK AWS per Ruby V3](#)

Cluster elastici Amazon DocumentDB

Le seguenti azioni sono supportate da Amazon DocumentDB Elastic Clusters:

- [CopyClusterSnapshot](#)
- [CreateCluster](#)
- [CreateClusterSnapshot](#)
- [DeleteCluster](#)
- [DeleteClusterSnapshot](#)
- [GetCluster](#)
- [GetClusterSnapshot](#)
- [ListClusters](#)

- [ListClusterSnapshots](#)
- [ListTagsForResource](#)
- [RestoreClusterFromSnapshot](#)
- [StartCluster](#)
- [StopCluster](#)
- [TagResource](#)
- [UntagResource](#)
- [UpdateCluster](#)

CopyClusterSnapshot

Servizio: Amazon DocumentDB Elastic Clusters

Copia un'istantanea di un cluster elastico.

Sintassi della richiesta

```
POST /cluster-snapshot/snapshotArn/copy HTTP/1.1
Content-type: application/json
```

```
{
  "copyTags": boolean,
  "kmsKeyId": "string",
  "tags": {
    "string" : "string"
  },
  "targetSnapshotName": "string"
}
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

snapshotArn

L'identificatore Amazon Resource Name (ARN) dello snapshot del cluster elastico.

Campo obbligatorio: sì

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

targetSnapshotName

L'identificatore del nuovo snapshot del cluster elastico da creare a partire dallo snapshot del cluster di origine. Questo parametro non distingue tra maiuscole e minuscole.

Vincoli:

- Deve contenere da 1 a 63 lettere, numeri o trattini.
- Il primo carattere deve essere una lettera.
- Non può terminare con un trattino o contenere due trattini consecutivi.

Esempio: `elastic-cluster-snapshot-5`

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 63 caratteri.

Campo obbligatorio: sì

[copyTags](#)

Impostato `true` per copiare tutti i tag dallo snapshot del cluster di origine allo snapshot del cluster elastico di destinazione. Il valore predefinito è `false`.

Tipo: Booleano

Campo obbligatorio: no

[kmsKeyId](#)

L'ID della chiave AWS KMS per un'istantanea crittografata del cluster elastico. L'ID della chiave AWS KMS è l'Amazon Resource Name (ARN) AWS, l'identificatore della chiave KMS o AWS l'alias della chiave KMS per la chiave di crittografia KMS. AWS

Se copi un'istantanea del cluster elastico crittografato dal tuo AWS account, puoi specificare un valore per crittografare la copia con una nuova chiave `KmsKeyId` di crittografia S KMS. AWS Se non specifichi un valore per `KmsKeyId`, la copia dello snapshot del cluster elastico viene crittografata con la stessa chiave AWS KMS dello snapshot del cluster elastico di origine.

Per copiare un'istantanea del cluster elastico crittografato in un'altra AWS regione, imposta `KmsKeyId` l'ID della chiave AWS KMS che desideri utilizzare per crittografare la copia dell'istantanea del cluster elastico nella regione di destinazione. AWS Le chiavi di crittografia KMS sono specifiche della AWS regione in cui vengono create e non è possibile utilizzare le chiavi di crittografia di una regione in un'altra AWS regione. AWS

Se si copia un'istantanea del cluster elastico non crittografato e si specifica un valore per il `KmsKeyId` parametro, viene restituito un errore.

Tipo: string

Campo obbligatorio: no

[tags](#)

I tag da assegnare allo snapshot del cluster elastico.

Tipo: mappatura stringa a stringa

Limitazioni di lunghezza della chiave: la lunghezza minima è 1. La lunghezza massima è 128 caratteri.

Modello di chiave: `^(?!aws:)[a-zA-Z+-._:/$]+`

Vincoli di lunghezza del valore: lunghezza minima di 0. La lunghezza massima è 256 caratteri.

Campo obbligatorio: no

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
  "snapshot": {
    "adminUserName": "string",
    "clusterArn": "string",
    "clusterCreationTime": "string",
    "kmsKeyId": "string",
    "snapshotArn": "string",
    "snapshotCreationTime": "string",
    "snapshotName": "string",
    "snapshotType": "string",
    "status": "string",
    "subnetIds": [ "string" ],
    "vpcSecurityGroupIds": [ "string" ]
  }
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

[snapshot](#)

Restituisce informazioni su uno specifico snapshot del cluster elastico.

Tipo: oggetto [ClusterSnapshot](#)

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

AccessDeniedException

Un'eccezione che si verifica quando non ci sono autorizzazioni sufficienti per eseguire un'azione.

Codice di stato HTTP: 403

ConflictException

Si è verificato un conflitto di accesso.

Codice di stato HTTP: 409

InternalServerErrorException

Si è verificato un errore interno del server.

Codice di stato HTTP: 500

ResourceNotFoundException

Impossibile trovare la risorsa specificata.

Codice di stato HTTP: 404

ServiceQuotaExceededException

La quota di servizio per l'azione è stata superata.

Codice di stato HTTP: 402

ThrottlingException

ThrottlingException verrà generata quando la richiesta viene rifiutata a causa della limitazione della richiesta.

Codice di stato HTTP: 429

ValidationException

Una struttura che definisce un'eccezione di convalida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [AWS SDK per .NET](#)
- [AWS SDK per C++](#)
- [AWS SDK for Go](#)
- [AWS SDK per Java V2](#)
- [AWS SDK per V3 JavaScript](#)
- [AWS SDK per PHP V3](#)
- [AWS SDK per Python](#)
- [AWS SDK per Ruby V3](#)

CreateCluster

Servizio: Amazon DocumentDB Elastic Clusters

Crea un nuovo cluster elastico Amazon DocumentDB e ne restituisce la struttura del cluster.

Sintassi della richiesta

```
POST /cluster HTTP/1.1
Content-type: application/json

{
  "adminUserName": "string",
  "adminUserPassword": "string",
  "authType": "string",
  "backupRetentionPeriod": number,
  "clientToken": "string",
  "clusterName": "string",
  "kmsKeyId": "string",
  "preferredBackupWindow": "string",
  "preferredMaintenanceWindow": "string",
  "shardCapacity": number,
  "shardCount": number,
  "shardInstanceCount": number,
  "subnetIds": [ "string" ],
  "tags": {
    "string" : "string"
  },
  "vpcSecurityGroupIds": [ "string" ]
}
```

Parametri della richiesta URI:

La richiesta non utilizza parametri URI.

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

adminUserName

Il nome dell'amministratore dei cluster elastici di Amazon DocumentDB.

Vincoli:

- Deve contenere da 1 a 63 lettere o numeri.
- Il primo carattere deve essere una lettera.
- Non può essere una parola riservata.

Tipo: stringa

Campo obbligatorio: sì

adminUserPassword

La password per l'amministratore dei cluster elastici di Amazon DocumentDB. La password può contenere qualsiasi carattere ASCII stampabile.

Vincoli:

- Deve contenere da 8 a 100 caratteri.
- Non può contenere una barra (/), virgolette doppie («») o il simbolo «at» (@).

Tipo: stringa

Campo obbligatorio: sì

authType

Il tipo di autenticazione utilizzato per determinare dove recuperare la password utilizzata per accedere al cluster elastico. I tipi validi sono PLAIN_TEXT o SECRET_ARN.

Tipo: stringa

Valori validi: PLAIN_TEXT | SECRET_ARN

Campo obbligatorio: sì

clusterName

Il nome del nuovo cluster elastico. Questo parametro è archiviato come stringa in minuscolo.

Vincoli:

- Deve contenere da 1 a 63 lettere, numeri o trattini.
- Il primo carattere deve essere una lettera.
- Non può terminare con un trattino o contenere due trattini consecutivi.

Esempio: my-cluster

Tipo: stringa

Campo obbligatorio: sì

[shardCapacity](#)

Il numero di vCPU assegnate a ogni shard di cluster elastico. Il massimo è 64. I valori consentiti sono 2, 4, 8, 16, 32, 64.

Tipo: integer

Campo obbligatorio: sì

[shardCount](#)

Il numero di shard assegnati al cluster elastico. Il massimo è 32.

Tipo: integer

Campo obbligatorio: sì

[backupRetentionPeriod](#)

Il numero di giorni per i quali vengono conservate le istantanee automatiche.

Tipo: integer

Campo obbligatorio: no

[clientToken](#)

Il token client per il cluster elastico.

Tipo: string

Campo obbligatorio: no

[kmsKeyId](#)

L'identificatore della chiave KMS da utilizzare per crittografare il nuovo cluster elastico.

L'identificatore della chiave KMS è l'Amazon Resource Name (ARN) per la chiave di crittografia KMS. Se stai creando un cluster utilizzando lo stesso account Amazon che possiede questa chiave di crittografia KMS, puoi utilizzare l'alias della chiave KMS anziché l'ARN come chiave di crittografia KMS.

Se non viene specificata una chiave di crittografia, Amazon DocumentDB utilizza la chiave di crittografia predefinita creata da KMS per l'account. Il tuo account ha una chiave di crittografia predefinita diversa per ogni regione Amazon.

Tipo: string

Campo obbligatorio: no

[preferredBackupWindow](#)

L'intervallo di tempo giornaliero durante il quale vengono creati i backup automatici, se i backup automatici sono abilitati, come determinato da `backupRetentionPeriod`

Tipo: string

Campo obbligatorio: no

[preferredMaintenanceWindow](#)

Intervallo temporale settimanale nel fuso orario UTC (Universal Coordinated Time) durante il quale può verificarsi la manutenzione dei sistemi.

Format: `ddd:hh24:mi-ddd:hh24:mi`

Impostazione predefinita: una finestra di 30 minuti selezionata a caso da un intervallo di tempo di 8 ore per ciascuna Regione AWS, che si verifica in un giorno casuale della settimana.

Giorni validi: lun, mar, mer, gio, ven, sab, dom

Vincoli: finestra di un minimo di 30 minuti.

Tipo: string

Campo obbligatorio: no

[shardInstanceCount](#)

Il numero di istanze di replica che si applicano a tutti gli shard del cluster elastico. `shardInstanceCount`Il valore 1 indica che esiste un'istanza di writer e tutte le istanze aggiuntive sono repliche che possono essere utilizzate per le letture e per migliorare la disponibilità.

Tipo: integer

Campo obbligatorio: no

[subnetIds](#)

Gli ID di sottorete Amazon EC2 per il nuovo cluster elastico.

Tipo: matrice di stringhe

Campo obbligatorio: no

[tags](#)

I tag da assegnare al nuovo cluster elastico.

Tipo: mappatura stringa a stringa

Limitazioni di lunghezza della chiave: la lunghezza minima è 1. La lunghezza massima è 128 caratteri.

Modello di chiave: `^(?!aws:)[a-zA-Z+-._:/$]+`

Vincoli di lunghezza del valore: lunghezza minima di 0. La lunghezza massima è 256 caratteri.

Campo obbligatorio: no

[vpcSecurityGroupIds](#)

Un elenco di gruppi di sicurezza VPC EC2 da associare al nuovo cluster elastico.

Tipo: matrice di stringhe

Campo obbligatorio: no

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
  "cluster": {
    "adminUserName": "string",
    "authType": "string",
    "backupRetentionPeriod": number,
    "clusterArn": "string",
```

```
"clusterEndpoint": "string",
"clusterName": "string",
"createTime": "string",
"kmsKeyId": "string",
"preferredBackupWindow": "string",
"preferredMaintenanceWindow": "string",
"shardCapacity": number,
"shardCount": number,
"shardInstanceCount": number,
"shards": [
  {
    "createTime": "string",
    "shardId": "string",
    "status": "string"
  }
],
"status": "string",
"subnetIds": [ "string" ],
"vpcSecurityGroupIds": [ "string" ]
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

cluster

Il nuovo cluster elastico che è stato creato.

Tipo: oggetto [Cluster](#)

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

AccessDeniedException

Un'eccezione che si verifica quando non ci sono autorizzazioni sufficienti per eseguire un'azione.

Codice di stato HTTP: 403

ConflictException

Si è verificato un conflitto di accesso.

Codice di stato HTTP: 409

InternalServerErrorException

Si è verificato un errore interno del server.

Codice di stato HTTP: 500

ServiceQuotaExceededException

La quota di servizio per l'azione è stata superata.

Codice di stato HTTP: 402

ThrottlingException

ThrottlingException verrà generata quando la richiesta viene rifiutata a causa della limitazione della richiesta.

Codice di stato HTTP: 429

ValidationException

Una struttura che definisce un'eccezione di convalida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [AWS SDK per.NET](#)
- [AWS SDK per C++](#)
- [AWS SDK for Go](#)
- [AWS SDK per Java V2](#)
- [AWS SDK per V3 JavaScript](#)
- [AWS SDK per PHP V3](#)

- [AWS SDK per Python](#)
- [AWS SDK per Ruby V3](#)

CreateClusterSnapshot

Servizio: Amazon DocumentDB Elastic Clusters

Crea un'istantanea di un cluster elastico.

Sintassi della richiesta

```
POST /cluster-snapshot HTTP/1.1
Content-type: application/json
```

```
{
  "clusterArn": "string",
  "snapshotName": "string",
  "tags": {
    "string" : "string"
  }
}
```

Parametri della richiesta URI:

La richiesta non utilizza parametri URI.

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

clusterArn

L'identificatore ARN del cluster elastico di cui si desidera creare un'istantanea.

Tipo: stringa

Campo obbligatorio: sì

snapshotName

Il nome della nuova istantanea del cluster elastico.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 63 caratteri.

Campo obbligatorio: sì

tags

I tag da assegnare alla nuova istantanea del cluster elastico.

Tipo: mappatura stringa a stringa

Limitazioni di lunghezza della chiave: la lunghezza minima è 1. La lunghezza massima è 128 caratteri.

Modello di chiave: `^(?!aws:)[a-zA-Z+ -=._:/]+$`

Vincoli di lunghezza del valore: lunghezza minima di 0. La lunghezza massima è 256 caratteri.

Campo obbligatorio: no

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
  "snapshot": {
    "adminUserName": "string",
    "clusterArn": "string",
    "clusterCreationTime": "string",
    "kmsKeyId": "string",
    "snapshotArn": "string",
    "snapshotCreationTime": "string",
    "snapshotName": "string",
    "snapshotType": "string",
    "status": "string",
    "subnetIds": [ "string" ],
    "vpcSecurityGroupIds": [ "string" ]
  }
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

[snapshot](#)

Restituisce informazioni sulla nuova istantanea del cluster elastico.

Tipo: oggetto [ClusterSnapshot](#)

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

AccessDeniedException

Un'eccezione che si verifica quando non ci sono autorizzazioni sufficienti per eseguire un'azione.

Codice di stato HTTP: 403

ConflictException

Si è verificato un conflitto di accesso.

Codice di stato HTTP: 409

InternalServerErrorException

Si è verificato un errore interno del server.

Codice di stato HTTP: 500

ResourceNotFoundException

Impossibile trovare la risorsa specificata.

Codice di stato HTTP: 404

ServiceQuotaExceededException

La quota di servizio per l'azione è stata superata.

Codice di stato HTTP: 402

ThrottlingException

ThrottlingException verrà generata quando la richiesta viene rifiutata a causa della limitazione della richiesta.

Codice di stato HTTP: 429

ValidationException

Una struttura che definisce un'eccezione di convalida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [AWS SDK per .NET](#)
- [AWS SDK per C++](#)
- [AWS SDK for Go](#)
- [AWS SDK per Java V2](#)
- [AWS SDK per V3 JavaScript](#)
- [AWS SDK per PHP V3](#)
- [AWS SDK per Python](#)
- [AWS SDK per Ruby V3](#)

DeleteCluster

Servizio: Amazon DocumentDB Elastic Clusters

Eliminare un cluster elastico.

Sintassi della richiesta

```
DELETE /cluster/clusterArn HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

[clusterArn](#)

L'identificatore ARN del cluster elastico da eliminare.

Campo obbligatorio: sì

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
  "cluster": {
    "adminUserName": "string",
    "authType": "string",
    "backupRetentionPeriod": number,
    "clusterArn": "string",
    "clusterEndpoint": "string",
    "clusterName": "string",
    "createTime": "string",
    "kmsKeyId": "string",
    "preferredBackupWindow": "string",
    "preferredMaintenanceWindow": "string",
    "shardCapacity": number,
    "shardCount": number,
```

```
"shardInstanceCount": number,
"shards": [
  {
    "createTime": "string",
    "shardId": "string",
    "status": "string"
  }
],
"status": "string",
"subnetIds": [ "string" ],
"vpcSecurityGroupIds": [ "string" ]
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

cluster

Restituisce informazioni sul cluster elastico appena eliminato.

Tipo: oggetto [Cluster](#)

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

AccessDeniedException

Un'eccezione che si verifica quando non ci sono autorizzazioni sufficienti per eseguire un'azione.

Codice di stato HTTP: 403

ConflictException

Si è verificato un conflitto di accesso.

Codice di stato HTTP: 409

InternalServerError

Si è verificato un errore interno del server.

Codice di stato HTTP: 500

ResourceNotFoundException

Impossibile trovare la risorsa specificata.

Codice di stato HTTP: 404

ThrottlingException

ThrottlingException verrà generata quando la richiesta viene rifiutata a causa della limitazione della richiesta.

Codice di stato HTTP: 429

ValidationException

Una struttura che definisce un'eccezione di convalida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [AWS SDK per .NET](#)
- [AWS SDK per C++](#)
- [AWS SDK for Go](#)
- [AWS SDK per Java V2](#)
- [AWS SDK per V3 JavaScript](#)
- [AWS SDK per PHP V3](#)
- [AWS SDK per Python](#)
- [AWS SDK per Ruby V3](#)

DeleteClusterSnapshot

Servizio: Amazon DocumentDB Elastic Clusters

Eliminare un'istantanea del cluster elastico.

Sintassi della richiesta

```
DELETE /cluster-snapshot/snapshotArn HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

[snapshotArn](#)

L'identificatore ARN dello snapshot del cluster elastico da eliminare.

Campo obbligatorio: sì

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
  "snapshot": {
    "adminUserName": "string",
    "clusterArn": "string",
    "clusterCreationTime": "string",
    "kmsKeyId": "string",
    "snapshotArn": "string",
    "snapshotCreationTime": "string",
    "snapshotName": "string",
    "snapshotType": "string",
    "status": "string",
    "subnetIds": [ "string ],
    "vpcSecurityGroupIds": [ "string ]
  }
}
```

```
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

[snapshot](#)

Restituisce informazioni sullo snapshot del cluster elastico appena eliminato.

Tipo: oggetto [ClusterSnapshot](#)

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

AccessDeniedException

Un'eccezione che si verifica quando non ci sono autorizzazioni sufficienti per eseguire un'azione.

Codice di stato HTTP: 403

ConflictException

Si è verificato un conflitto di accesso.

Codice di stato HTTP: 409

InternalServerErrorException

Si è verificato un errore interno del server.

Codice di stato HTTP: 500

ResourceNotFoundException

Impossibile trovare la risorsa specificata.

Codice di stato HTTP: 404

ThrottlingException

ThrottlingException verrà generata quando la richiesta viene rifiutata a causa della limitazione della richiesta.

Codice di stato HTTP: 429

ValidationException

Una struttura che definisce un'eccezione di convalida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [AWS SDK per .NET](#)
- [AWS SDK per C++](#)
- [AWS SDK for Go](#)
- [AWS SDK per Java V2](#)
- [AWS SDK per V3 JavaScript](#)
- [AWS SDK per PHP V3](#)
- [AWS SDK per Python](#)
- [AWS SDK per Ruby V3](#)

GetCluster

Servizio: Amazon DocumentDB Elastic Clusters

Restituisce informazioni su un cluster elastico specifico.

Sintassi della richiesta

```
GET /cluster/clusterArn HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

[clusterArn](#)

L'identificatore ARN del cluster elastico.

Campo obbligatorio: sì

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
  "cluster": {
    "adminUserName": "string",
    "authType": "string",
    "backupRetentionPeriod": number,
    "clusterArn": "string",
    "clusterEndpoint": "string",
    "clusterName": "string",
    "createTime": "string",
    "kmsKeyId": "string",
    "preferredBackupWindow": "string",
    "preferredMaintenanceWindow": "string",
    "shardCapacity": number,
    "shardCount": number,
```

```
"shardInstanceCount": number,
"shards": [
  {
    "createTime": "string",
    "shardId": "string",
    "status": "string"
  }
],
"status": "string",
"subnetIds": [ "string" ],
"vpcSecurityGroupIds": [ "string" ]
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

cluster

Restituisce informazioni su un cluster elastico specifico.

Tipo: oggetto [Cluster](#)

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

AccessDeniedException

Un'eccezione che si verifica quando non ci sono autorizzazioni sufficienti per eseguire un'azione.

Codice di stato HTTP: 403

InternalServerError

Si è verificato un errore interno del server.

Codice di stato HTTP: 500

ResourceNotFoundException

Impossibile trovare la risorsa specificata.

Codice di stato HTTP: 404

ThrottlingException

ThrottlingException verrà generata quando la richiesta viene rifiutata a causa della limitazione della richiesta.

Codice di stato HTTP: 429

ValidationException

Una struttura che definisce un'eccezione di convalida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [AWS SDK per.NET](#)
- [AWS SDK per C++](#)
- [AWS SDK for Go](#)
- [AWS SDK per Java V2](#)
- [AWS SDK per V3 JavaScript](#)
- [AWS SDK per PHP V3](#)
- [AWS SDK per Python](#)
- [AWS SDK per Ruby V3](#)

GetClusterSnapshot

Servizio: Amazon DocumentDB Elastic Clusters

Restituisce informazioni su uno specifico snapshot del cluster elastico

Sintassi della richiesta

```
GET /cluster-snapshot/snapshotArn HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

[snapshotArn](#)

L'identificatore ARN dello snapshot del cluster elastico.

Campo obbligatorio: sì

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
  "snapshot": {
    "adminUserName": "string",
    "clusterArn": "string",
    "clusterCreationTime": "string",
    "kmsKeyId": "string",
    "snapshotArn": "string",
    "snapshotCreationTime": "string",
    "snapshotName": "string",
    "snapshotType": "string",
    "status": "string",
    "subnetIds": [ "string" ],
    "vpcSecurityGroupIds": [ "string" ]
  }
}
```



```
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

[snapshot](#)

Restituisce informazioni su uno specifico snapshot del cluster elastico.

Tipo: oggetto [ClusterSnapshot](#)

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

AccessDeniedException

Un'eccezione che si verifica quando non ci sono autorizzazioni sufficienti per eseguire un'azione.

Codice di stato HTTP: 403

InternalServerError

Si è verificato un errore interno del server.

Codice di stato HTTP: 500

ResourceNotFoundException

Impossibile trovare la risorsa specificata.

Codice di stato HTTP: 404

ThrottlingException

ThrottlingException verrà generata quando la richiesta viene rifiutata a causa della limitazione della richiesta.

Codice di stato HTTP: 429

ValidationException

Una struttura che definisce un'eccezione di convalida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [AWS SDK per .NET](#)
- [AWS SDK per C++](#)
- [AWS SDK for Go](#)
- [AWS SDK per Java V2](#)
- [AWS SDK per V3 JavaScript](#)
- [AWS SDK per PHP V3](#)
- [AWS SDK per Python](#)
- [AWS SDK per Ruby V3](#)

ListClusters

Servizio: Amazon DocumentDB Elastic Clusters

Restituisce informazioni sui cluster elastici di Amazon DocumentDB forniti.

Sintassi della richiesta

```
GET /clusters?maxResults=maxResults&nextToken=nextToken HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

[maxResults](#)

Il numero massimo di risultati di snapshot del cluster elastico da ricevere nella risposta.

Intervallo valido: valore minimo di 1. valore massimo pari a 100.

[nextToken](#)

Un token di impaginazione fornito da una richiesta precedente. Se viene specificato questo parametro, la risposta include solo i record oltre questo token, fino al valore specificato da `maxResults`.

Se non ci sono più dati nella risposta, non `nextToken` verrà restituita.

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
  "clusters": [
    {
      "clusterArn": "string",
      "clusterName": "string",
```

```
    "status": "string"  
  }  
],  
"nextToken": "string"  
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

clusters

Un elenco di cluster elastici di Amazon DocumentDB.

Tipo: matrice di oggetti [ClusterInList](#)

nextToken

Un token di impaginazione fornito da una richiesta precedente. Se viene specificato questo parametro, la risposta include solo i record oltre questo token, fino al valore specificato da `maxResults`.

Se non ci sono più dati nella risposta, non `nextToken` verrà restituita.

Tipo: stringa

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

AccessDeniedException

Un'eccezione che si verifica quando non ci sono autorizzazioni sufficienti per eseguire un'azione.

Codice di stato HTTP: 403

InternalServerError

Si è verificato un errore interno del server.

Codice di stato HTTP: 500

ThrottlingException

ThrottlingException verrà generata quando la richiesta viene rifiutata a causa della limitazione della richiesta.

Codice di stato HTTP: 429

ValidationException

Una struttura che definisce un'eccezione di convalida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [AWS SDK per .NET](#)
- [AWS SDK per C++](#)
- [AWS SDK for Go](#)
- [AWS SDK per Java V2](#)
- [AWS SDK per V3 JavaScript](#)
- [AWS SDK per PHP V3](#)
- [AWS SDK per Python](#)
- [AWS SDK per Ruby V3](#)

ListClusterSnapshots

Servizio: Amazon DocumentDB Elastic Clusters

Restituisce informazioni sulle istantanee per un cluster elastico specificato.

Sintassi della richiesta

```
GET /cluster-snapshots?  
clusterArn=clusterArn&maxResults=maxResults&nextToken=nextToken&snapshotType=snapshotType  
HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

[clusterArn](#)

L'identificatore ARN del cluster elastico.

[maxResults](#)

Il numero massimo di risultati di snapshot del cluster elastico da ricevere nella risposta.

Intervallo valido: valore minimo di 20. valore massimo pari a 100.

[nextToken](#)

Un token di impaginazione fornito da una richiesta precedente. Se viene specificato questo parametro, la risposta include solo i record oltre questo token, fino al valore specificato da `maxResults`.

Se non ci sono più dati nella risposta, non `nextToken` verrà restituita.

[snapshotType](#)

Il tipo di istantanee del cluster da restituire. È possibile specificare uno dei seguenti valori:

- `automated`- Restituisci tutte le istantanee del cluster che Amazon DocumentDB ha creato automaticamente per AWS il tuo account.
- `manual`- Restituisci tutte le istantanee del cluster che hai creato manualmente per il tuo account. AWS

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
  "nextToken": "string",
  "snapshots": [
    {
      "clusterArn": "string",
      "snapshotArn": "string",
      "snapshotCreationTime": "string",
      "snapshotName": "string",
      "status": "string"
    }
  ]
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

[nextToken](#)

Un token di impaginazione fornito da una richiesta precedente. Se viene specificato questo parametro, la risposta include solo i record oltre questo token, fino al valore specificato `maxResults`.

Se non ci sono più dati nella risposta, non `nextToken` verrà restituita.

Tipo: stringa

[snapshots](#)

Un elenco di istantanee per un cluster elastico specificato.

Tipo: matrice di oggetti [ClusterSnapshotInList](#)

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

AccessDeniedException

Un'eccezione che si verifica quando non ci sono autorizzazioni sufficienti per eseguire un'azione.

Codice di stato HTTP: 403

InternalServerError

Si è verificato un errore interno del server.

Codice di stato HTTP: 500

ThrottlingException

ThrottlingException verrà generata quando la richiesta viene rifiutata a causa della limitazione della richiesta.

Codice di stato HTTP: 429

ValidationException

Una struttura che definisce un'eccezione di convalida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [AWS SDK per .NET](#)
- [AWS SDK per C++](#)
- [AWS SDK for Go](#)
- [AWS SDK per Java V2](#)
- [AWS SDK per V3 JavaScript](#)
- [AWS SDK per PHP V3](#)
- [AWS SDK per Python](#)
- [AWS SDK per Ruby V3](#)

ListTagsForResource

Servizio: Amazon DocumentDB Elastic Clusters

Elenca tutti i tag su una risorsa cluster elastica

Sintassi della richiesta

```
GET /tags/resourceArn HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

resourceArn

L'identificatore ARN della risorsa del cluster elastico.

Limitazioni di lunghezza: lunghezza minima di 1. Lunghezza massima di 1011.

Campo obbligatorio: sì

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
  "tags": {
    "string" : "string"
  }
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

tags

L'elenco di tag per la risorsa del cluster elastico specificata.

Tipo: mappatura stringa a stringa

Limitazioni di lunghezza della chiave: la lunghezza minima è 1. La lunghezza massima è 128 caratteri.

Modello di chiave: `^(?!aws:)[a-zA-Z+-._:/$]`

Vincoli di lunghezza del valore: lunghezza minima di 0. La lunghezza massima è 256 caratteri.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

InternalServerError

Si è verificato un errore interno del server.

Codice di stato HTTP: 500

ResourceNotFoundException

Impossibile trovare la risorsa specificata.

Codice di stato HTTP: 404

ThrottlingException

ThrottlingException verrà generata quando la richiesta viene rifiutata a causa della limitazione della richiesta.

Codice di stato HTTP: 429

ValidationException

Una struttura che definisce un'eccezione di convalida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [AWS SDK per.NET](#)
- [AWS SDK per C++](#)
- [AWS SDK for Go](#)
- [AWS SDK per Java V2](#)
- [AWS SDK per V3 JavaScript](#)
- [AWS SDK per PHP V3](#)
- [AWS SDK per Python](#)
- [AWS SDK per Ruby V3](#)

RestoreClusterFromSnapshot

Servizio: Amazon DocumentDB Elastic Clusters

Ripristina un cluster elastico da un'istantanea.

Sintassi della richiesta

```
POST /cluster-snapshot/snapshotArn/restore HTTP/1.1
Content-type: application/json
```

```
{
  "clusterName": "string",
  "kmsKeyId": "string",
  "shardCapacity": number,
  "shardInstanceCount": number,
  "subnetIds": [ "string" ],
  "tags": {
    "string" : "string"
  },
  "vpcSecurityGroupIds": [ "string" ]
}
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

snapshotArn

L'identificatore ARN dello snapshot del cluster elastico.

Campo obbligatorio: sì

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

clusterName

Il nome del cluster elastico.

Tipo: stringa

Campo obbligatorio: sì

[kmsKeyId](#)

L'identificatore di chiave KMS da utilizzare per crittografare il nuovo cluster elastico di cluster Amazon DocumentDB.

L'identificatore della chiave KMS è l'Amazon Resource Name (ARN) per la chiave di crittografia KMS. Se stai creando un cluster utilizzando lo stesso account Amazon che possiede questa chiave di crittografia KMS, puoi utilizzare l'alias della chiave KMS anziché l'ARN come chiave di crittografia KMS.

Se non viene specificata una chiave di crittografia qui, Amazon DocumentDB utilizza la chiave di crittografia predefinita creata da KMS per il tuo account. Il tuo account ha una chiave di crittografia predefinita diversa per ogni regione Amazon.

Tipo: string

Campo obbligatorio: no

[shardCapacity](#)

La capacità di ogni shard nel nuovo cluster elastico ripristinato.

Tipo: integer

Campo obbligatorio: no

[shardInstanceCount](#)

Il numero di istanze di replica che si applicano a tutti gli shard del cluster elastico. shardInstanceCountIl valore 1 indica che esiste un'istanza di writer e tutte le istanze aggiuntive sono repliche che possono essere utilizzate per le letture e per migliorare la disponibilità.

Tipo: integer

Campo obbligatorio: no

[subnetIds](#)

Gli ID di sottorete Amazon EC2 per il cluster elastico.

Tipo: matrice di stringhe

Campo obbligatorio: no

[tags](#)

Un elenco dei nomi di tag da assegnare al cluster elastico ripristinato, sotto forma di una matrice di coppie chiave-valore in cui la chiave è il nome del tag e il valore è il valore chiave.

Tipo: mappatura stringa a stringa

Limitazioni di lunghezza della chiave: la lunghezza minima è 1. La lunghezza massima è 128 caratteri.

Modello di chiave: `^(?!aws:)[a-zA-Z+-._:/$]+`

Vincoli di lunghezza del valore: lunghezza minima di 0. La lunghezza massima è 256 caratteri.

Campo obbligatorio: no

[vpcSecurityGroupIds](#)

Un elenco di gruppi di sicurezza VPC EC2 da associare al cluster elastico.

Tipo: matrice di stringhe

Campo obbligatorio: no

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
  "cluster": {
    "adminUserName": "string",
    "authType": "string",
    "backupRetentionPeriod": number,
    "clusterArn": "string",
    "clusterEndpoint": "string",
    "clusterName": "string",
    "createTime": "string",
    "kmsKeyId": "string",
    "preferredBackupWindow": "string",
    "preferredMaintenanceWindow": "string",
    "shardCapacity": number,
    "shardCount": number,
    "shardInstanceCount": number,
```

```
  "shards": [
    {
      "createTime": "string",
      "shardId": "string",
      "status": "string"
    }
  ],
  "status": "string",
  "subnetIds": [ "string" ],
  "vpcSecurityGroupIds": [ "string" ]
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

[cluster](#)

Restituisce informazioni su un cluster elastico ripristinato.

Tipo: oggetto [Cluster](#)

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

AccessDeniedException

Un'eccezione che si verifica quando non ci sono autorizzazioni sufficienti per eseguire un'azione.

Codice di stato HTTP: 403

ConflictException

Si è verificato un conflitto di accesso.

Codice di stato HTTP: 409

InternalServerError

Si è verificato un errore interno del server.

Codice di stato HTTP: 500

ResourceNotFoundException

Impossibile trovare la risorsa specificata.

Codice di stato HTTP: 404

ServiceQuotaExceededException

La quota di servizio per l'azione è stata superata.

Codice di stato HTTP: 402

ThrottlingException

ThrottlingException verrà generata quando la richiesta viene rifiutata a causa della limitazione della richiesta.

Codice di stato HTTP: 429

ValidationException

Una struttura che definisce un'eccezione di convalida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [AWS SDK per .NET](#)
- [AWS SDK per C++](#)
- [AWS SDK for Go](#)
- [AWS SDK per Java V2](#)
- [AWS SDK per V3 JavaScript](#)
- [AWS SDK per PHP V3](#)
- [AWS SDK per Python](#)
- [AWS SDK per Ruby V3](#)

StartCluster

Servizio: Amazon DocumentDB Elastic Clusters

Riavvia il cluster elastico interrotto specificato da `clusterArn`.

Sintassi della richiesta

```
POST /cluster/clusterArn/start HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

[clusterArn](#)

L'identificatore ARN del cluster elastico.

Campo obbligatorio: sì

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
  "cluster": {
    "adminUserName": "string",
    "authType": "string",
    "backupRetentionPeriod": number,
    "clusterArn": "string",
    "clusterEndpoint": "string",
    "clusterName": "string",
    "createTime": "string",
    "kmsKeyId": "string",
    "preferredBackupWindow": "string",
    "preferredMaintenanceWindow": "string",
    "shardCapacity": number,
    "shardCount": number,
```

```
"shardInstanceCount": number,  
"shards": [  
  {  
    "createTime": "string",  
    "shardId": "string",  
    "status": "string"  
  }  
],  
"status": "string",  
"subnetIds": [ "string" ],  
"vpcSecurityGroupIds": [ "string" ]  
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

cluster

Restituisce informazioni su un cluster elastico specifico.

Tipo: oggetto [Cluster](#)

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

AccessDeniedException

Un'eccezione che si verifica quando non ci sono autorizzazioni sufficienti per eseguire un'azione.

Codice di stato HTTP: 403

InternalServerError

Si è verificato un errore interno del server.

Codice di stato HTTP: 500

ResourceNotFoundException

Impossibile trovare la risorsa specificata.

Codice di stato HTTP: 404

ThrottlingException

ThrottlingException verrà generata quando la richiesta viene rifiutata a causa della limitazione della richiesta.

Codice di stato HTTP: 429

ValidationException

Una struttura che definisce un'eccezione di convalida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [AWS SDK per.NET](#)
- [AWS SDK per C++](#)
- [AWS SDK for Go](#)
- [AWS SDK per Java V2](#)
- [AWS SDK per V3 JavaScript](#)
- [AWS SDK per PHP V3](#)
- [AWS SDK per Python](#)
- [AWS SDK per Ruby V3](#)

StopCluster

Servizio: Amazon DocumentDB Elastic Clusters

Arresta il cluster elastico in esecuzione specificato da `clusterArn`. Il cluster elastico deve essere nello stato disponibile.

Sintassi della richiesta

```
POST /cluster/clusterArn/stop HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

[clusterArn](#)

L'identificatore ARN del cluster elastico.

Campo obbligatorio: sì

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
  "cluster": {
    "adminUserName": "string",
    "authType": "string",
    "backupRetentionPeriod": number,
    "clusterArn": "string",
    "clusterEndpoint": "string",
    "clusterName": "string",
    "createTime": "string",
    "kmsKeyId": "string",
    "preferredBackupWindow": "string",
    "preferredMaintenanceWindow": "string",
```

```
"shardCapacity": number,  
"shardCount": number,  
"shardInstanceCount": number,  
"shards": [  
  {  
    "createTime": "string",  
    "shardId": "string",  
    "status": "string"  
  }  
],  
"status": "string",  
"subnetIds": [ "string" ],  
"vpcSecurityGroupIds": [ "string" ]  
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

cluster

Restituisce informazioni su un cluster elastico specifico.

Tipo: oggetto [Cluster](#)

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

AccessDeniedException

Un'eccezione che si verifica quando non ci sono autorizzazioni sufficienti per eseguire un'azione.

Codice di stato HTTP: 403

InternalServerError

Si è verificato un errore interno del server.

Codice di stato HTTP: 500

ResourceNotFoundException

Impossibile trovare la risorsa specificata.

Codice di stato HTTP: 404

ThrottlingException

ThrottlingException verrà generata quando la richiesta viene rifiutata a causa della limitazione della richiesta.

Codice di stato HTTP: 429

ValidationException

Una struttura che definisce un'eccezione di convalida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [AWS SDK per.NET](#)
- [AWS SDK per C++](#)
- [AWS SDK for Go](#)
- [AWS SDK per Java V2](#)
- [AWS SDK per V3 JavaScript](#)
- [AWS SDK per PHP V3](#)
- [AWS SDK per Python](#)
- [AWS SDK per Ruby V3](#)

TagResource

Servizio: Amazon DocumentDB Elastic Clusters

Aggiunge tag di metadati a una risorsa cluster elastica

Sintassi della richiesta

```
POST /tags/resourceArn HTTP/1.1
Content-type: application/json
```

```
{
  "tags": {
    "string" : "string"
  }
}
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

resourceArn

L'identificatore ARN della risorsa del cluster elastico.

Limitazioni di lunghezza: lunghezza minima di 1. Lunghezza massima di 1011.

Campo obbligatorio: sì

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

tags

I tag assegnati alla risorsa del cluster elastico.

Tipo: mappatura stringa a stringa

Limitazioni di lunghezza della chiave: la lunghezza minima è 1. La lunghezza massima è 128 caratteri.

Modello di chiave: $^(?!aws:)[a-zA-Z+-._:/$]+$

Vincoli di lunghezza del valore: lunghezza minima di 0. La lunghezza massima è 256 caratteri.

Campo obbligatorio: sì

Sintassi della risposta

```
HTTP/1.1 200
```

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

InternalServerError

Si è verificato un errore interno del server.

Codice di stato HTTP: 500

ResourceNotFoundException

Impossibile trovare la risorsa specificata.

Codice di stato HTTP: 404

ThrottlingException

ThrottlingException verrà generata quando la richiesta viene rifiutata a causa della limitazione della richiesta.

Codice di stato HTTP: 429

ValidationException

Una struttura che definisce un'eccezione di convalida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [AWS SDK per.NET](#)
- [AWS SDK per C++](#)
- [AWS SDK for Go](#)
- [AWS SDK per Java V2](#)
- [AWS SDK per V3 JavaScript](#)
- [AWS SDK per PHP V3](#)
- [AWS SDK per Python](#)
- [AWS SDK per Ruby V3](#)

UntagResource

Servizio: Amazon DocumentDB Elastic Clusters

Rimuove i tag di metadati da una risorsa cluster elastica

Sintassi della richiesta

```
DELETE /tags/resourceArn?tagKeys=tagKeys HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

resourceArn

L'identificatore ARN della risorsa del cluster elastico.

Limitazioni di lunghezza: lunghezza minima di 1. Lunghezza massima di 1011.

Campo obbligatorio: sì

tagKeys

Le chiavi dei tag da rimuovere dalla risorsa del cluster elastico.

Membri dell'array: numero minimo di 0 elementi. Numero massimo di 50 item.

Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 128 caratteri.

Modello: $^(?!aws:)[a-zA-Z+-. _:/]+$

Campo obbligatorio: sì

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
```

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

InternalServerErrorException

Si è verificato un errore interno del server.

Codice di stato HTTP: 500

ResourceNotFoundException

Impossibile trovare la risorsa specificata.

Codice di stato HTTP: 404

ThrottlingException

ThrottlingException verrà generata quando la richiesta viene rifiutata a causa della limitazione della richiesta.

Codice di stato HTTP: 429

ValidationException

Una struttura che definisce un'eccezione di convalida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [AWS SDK per .NET](#)
- [AWS SDK per C++](#)
- [AWS SDK for Go](#)
- [AWS SDK per Java V2](#)
- [AWS SDK per V3 JavaScript](#)
- [AWS SDK per PHP V3](#)
- [AWS SDK per Python](#)

- [AWS SDK per Ruby V3](#)

UpdateCluster

Servizio: Amazon DocumentDB Elastic Clusters

Modifica un cluster elastico. Ciò include l'aggiornamento del nome utente/della password dell'amministratore, l'aggiornamento della versione dell'API e la configurazione di una finestra di backup e di manutenzione

Sintassi della richiesta

```
PUT /cluster/clusterArn HTTP/1.1
Content-type: application/json

{
  "adminUserPassword": "string",
  "authType": "string",
  "backupRetentionPeriod": number,
  "clientToken": "string",
  "preferredBackupWindow": "string",
  "preferredMaintenanceWindow": "string",
  "shardCapacity": number,
  "shardCount": number,
  "shardInstanceCount": number,
  "subnetIds": [ "string" ],
  "vpcSecurityGroupIds": [ "string" ]
}
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

clusterArn

L'identificatore ARN del cluster elastico.

Campo obbligatorio: sì

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

[adminUserPassword](#)

La password associata all'amministratore del cluster elastico. Questa password può contenere qualsiasi carattere ASCII stampabile, eccetto la barra (/), le virgolette (") o il simbolo chiocciola (@).

Vincoli: deve contenere da 8 a 100 caratteri.

Tipo: string

Campo obbligatorio: no

[authType](#)

Il tipo di autenticazione utilizzato per determinare dove recuperare la password utilizzata per accedere al cluster elastico. I tipi validi sono PLAIN_TEXT o SECRET_ARN.

Tipo: stringa

Valori validi: PLAIN_TEXT | SECRET_ARN

Campo obbligatorio: no

[backupRetentionPeriod](#)

Il numero di giorni per i quali vengono conservate le istantanee automatiche.

Tipo: integer

Campo obbligatorio: no

[clientToken](#)

Il token client per il cluster elastico.

Tipo: string

Campo obbligatorio: no

[preferredBackupWindow](#)

L'intervallo di tempo giornaliero durante il quale vengono creati i backup automatici, se i backup automatici sono abilitati, come determinato da `backupRetentionPeriod`

Tipo: string

Campo obbligatorio: no

[preferredMaintenanceWindow](#)

Intervallo temporale settimanale nel fuso orario UTC (Universal Coordinated Time) durante il quale può verificarsi la manutenzione dei sistemi.

Format: `ddd:hh24:mi-ddd:hh24:mi`

Impostazione predefinita: una finestra di 30 minuti selezionata a caso da un intervallo di tempo di 8 ore per ciascuna Regione AWS, che si verifica in un giorno casuale della settimana.

Giorni validi: lun, mar, mer, gio, ven, sab, dom

Vincoli: finestra di un minimo di 30 minuti.

Tipo: string

Campo obbligatorio: no

[shardCapacity](#)

Il numero di vCPU assegnate a ogni shard di cluster elastico. Il massimo è 64. I valori consentiti sono 2, 4, 8, 16, 32, 64.

Tipo: integer

Campo obbligatorio: no

[shardCount](#)

Il numero di shard assegnati al cluster elastico. Il massimo è 32.

Tipo: integer

Campo obbligatorio: no

[shardInstanceCount](#)

Il numero di istanze di replica che si applicano a tutti gli shard del cluster elastico. `shardInstanceCount`Il valore 1 indica che esiste un'istanza di writer e tutte le istanze aggiuntive sono repliche che possono essere utilizzate per le letture e per migliorare la disponibilità.

Tipo: integer

Campo obbligatorio: no

[subnetIds](#)

Gli ID di sottorete Amazon EC2 per il cluster elastico.

Tipo: matrice di stringhe

Campo obbligatorio: no

[vpcSecurityGroupIds](#)

Un elenco di gruppi di sicurezza VPC EC2 da associare al cluster elastico.

Tipo: matrice di stringhe

Campo obbligatorio: no

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
  "cluster": {
    "adminUserName": "string",
    "authType": "string",
    "backupRetentionPeriod": number,
    "clusterArn": "string",
    "clusterEndpoint": "string",
    "clusterName": "string",
    "createTime": "string",
    "kmsKeyId": "string",
    "preferredBackupWindow": "string",
    "preferredMaintenanceWindow": "string",
    "shardCapacity": number,
    "shardCount": number,
    "shardInstanceCount": number,
    "shards": [
      {
        "createTime": "string",
        "shardId": "string",
        "status": "string"
      }
    ]
  }
}
```

```
    ],  
    "status": "string",  
    "subnetIds": [ "string" ],  
    "vpcSecurityGroupIds": [ "string" ]  
  }  
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

[cluster](#)

Restituisce informazioni sul cluster elastico aggiornato.

Tipo: oggetto [Cluster](#)

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare [Errori comuni](#).

AccessDeniedException

Un'eccezione che si verifica quando non ci sono autorizzazioni sufficienti per eseguire un'azione.

Codice di stato HTTP: 403

ConflictException

Si è verificato un conflitto di accesso.

Codice di stato HTTP: 409

InternalServerError

Si è verificato un errore interno del server.

Codice di stato HTTP: 500

ResourceNotFoundException

Impossibile trovare la risorsa specificata.

Codice di stato HTTP: 404

ThrottlingException

ThrottlingException verrà generata quando la richiesta viene rifiutata a causa della limitazione della richiesta.

Codice di stato HTTP: 429

ValidationException

Una struttura che definisce un'eccezione di convalida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- [Interfaccia a riga di comando AWS](#)
- [AWS SDK per.NET](#)
- [AWS SDK per C++](#)
- [AWS SDK for Go](#)
- [AWS SDK per Java V2](#)
- [AWS SDK per V3 JavaScript](#)
- [AWS SDK per PHP V3](#)
- [AWS SDK per Python](#)
- [AWS SDK per Ruby V3](#)

Tipi di dati

I seguenti tipi di dati sono supportati da Amazon DocumentDB (with MongoDB compatibility):

- [AvailabilityZone](#)
- [Certificate](#)
- [CertificateDetails](#)
- [CloudwatchLogsExportConfiguration](#)

- [DBCluster](#)
- [DBClusterMember](#)
- [DBClusterParameterGroup](#)
- [DBClusterRole](#)
- [DBClusterSnapshot](#)
- [DBClusterSnapshotAttribute](#)
- [DBClusterSnapshotAttributesResult](#)
- [DBEngineVersion](#)
- [DBInstance](#)
- [DBInstanceStatusInfo](#)
- [DBSubnetGroup](#)
- [Endpoint](#)
- [EngineDefaults](#)
- [Event](#)
- [EventCategoriesMap](#)
- [EventSubscription](#)
- [Filter](#)
- [GlobalCluster](#)
- [GlobalClusterMember](#)
- [OrderableDBInstanceOption](#)
- [Parameter](#)
- [PendingCloudwatchLogsExports](#)
- [PendingMaintenanceAction](#)
- [PendingModifiedValues](#)
- [ResourcePendingMaintenanceActions](#)
- [Subnet](#)
- [Tag](#)
- [UpgradeTarget](#)
- [VpcSecurityGroupMembership](#)

I seguenti tipi di dati sono supportati da Amazon DocumentDB Elastic Clusters:

- [Cluster](#)
- [ClusterInList](#)
- [ClusterSnapshot](#)
- [ClusterSnapshotInList](#)
- [Shard](#)
- [ValidationExceptionField](#)

Amazon DocumentDB (with MongoDB compatibility)

I seguenti tipi di dati sono supportati da Amazon DocumentDB (with MongoDB compatibility):

- [AvailabilityZone](#)
- [Certificate](#)
- [CertificateDetails](#)
- [CloudwatchLogsExportConfiguration](#)
- [DBCluster](#)
- [DBClusterMember](#)
- [DBClusterParameterGroup](#)
- [DBClusterRole](#)
- [DBClusterSnapshot](#)
- [DBClusterSnapshotAttribute](#)
- [DBClusterSnapshotAttributesResult](#)
- [DBEngineVersion](#)
- [DBInstance](#)
- [DBInstanceStatusInfo](#)
- [DBSubnetGroup](#)
- [Endpoint](#)
- [EngineDefaults](#)
- [Event](#)
- [EventCategoriesMap](#)
- [EventSubscription](#)
- [Filter](#)

- [GlobalCluster](#)
- [GlobalClusterMember](#)
- [OrderableDBInstanceOption](#)
- [Parameter](#)
- [PendingCloudwatchLogsExports](#)
- [PendingMaintenanceAction](#)
- [PendingModifiedValues](#)
- [ResourcePendingMaintenanceActions](#)
- [Subnet](#)
- [Tag](#)
- [UpgradeTarget](#)
- [VpcSecurityGroupMembership](#)

AvailabilityZone

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Informazioni su una zona di disponibilità.

Indice

Note

Nell'elenco seguente, i parametri richiesti vengono descritti per primi.

Name

Nome della zona di disponibilità.

Tipo: string

Required: No

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [AWS SDK per Java V2](#)
- [SDK AWS per Ruby V3](#)

Certificate

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Un certificato di autorità di certificazione (CA) per unAccount AWS.

Indice

Note

Nell'elenco seguente, i parametri richiesti vengono descritti per primi.

CertificateArn

L'Amazon Resource Name (ARN) per il certificato.

Esempio: `arn:aws:rds:us-east-1::cert:rds-ca-2019`

Tipo: string

Required: No

CertificateIdentifier

La chiave univoca che identifica un certificato.

Esempio: `rds-ca-2019`

Tipo: string

Required: No

CertificateType

Il tipo di certificato.

Esempio: CA

Tipo: string

Required: No

Thumbprint

L'impronta digitale del certificato.

Tipo: string

Required: No

ValidFrom

La data e un'ora di inizio, dopo le quali il certificato è valido.

Esempio: 2019-07-31T17:57:09Z

Tipo: Timestamp

Required: No

ValidTill

La data dopo la quale il certificato non è più valido.

Esempio: 2024-07-31T17:57:09Z

Tipo: Timestamp

Required: No

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [AWS SDK per Java V2](#)
- [SDK AWS per Ruby V3](#)

CertificateDetails

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Restituisce i dettagli del certificato del server dell'istanza DB.

Per ulteriori informazioni, consulta [Updating your Amazon DocumentDB TLS Certificates](#) and [Encrypting Data in Transit nella](#) Amazon DocumentDB Developer Guide.

Indice

Note

Nell'elenco seguente, i parametri richiesti vengono descritti per primi.

CAIdentifier

L'identificatore CA del certificato CA utilizzato per il certificato del server dell'istanza DB.

Tipo: string

Campo obbligatorio: no

ValidTill

La data di scadenza del certificato del server dell'istanza DB.

Tipo: Timestamp

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [AWS SDK per Java V2](#)
- [SDK AWS per Ruby V3](#)

CloudwatchLogsExportConfiguration

Servizio: Amazon DocumentDB (with MongoDB compatibility)

— L'impostazione di configurazione per i tipi di log da abilitare per l'esportazione in per un'istanza o cluster specifico. CloudWatch

`DisableLogTypes` Gli array `EnableLogTypes` and determinano quali registri vengono esportati (o non esportati) in CloudWatch Logs. I valori all'interno di questi array dipendono dal motore utilizzato.

Indice

Note

Nell'elenco seguente, i parametri richiesti vengono descritti per primi.

`DisableLogTypes.member.N`

L'elenco dei tipi di log da disabilitare.

Tipo: matrice di stringhe

Required: No

`EnableLogTypes.member.N`

L'elenco dei tipi di log da abilitare.

Tipo: matrice di stringhe

Required: No

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [AWS SDK per Java V2](#)
- [SDK AWS per Ruby V3](#)

DBCluster

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Informazioni dettagliate su un cluster.

Indice

Note

Nell'elenco seguente, i parametri richiesti vengono descritti per primi.

AssociatedRoles.DBClusterRole.N

Fornisce un elenco dei ruoli AWS Identity and Access Management (IAM) associati al cluster. I ruoli (IAM) associati a un cluster concedono l'autorizzazione al cluster di accedere ad altri AWS servizi per conto dell'utente.

Tipo: matrice di oggetti [DBClusterRole](#)

Campo obbligatorio: no

AvailabilityZones.AvailabilityZone.N

Fornisce l'elenco delle zone di disponibilità di Amazon EC2 in cui è possibile creare le istanze del cluster.

Tipo: matrice di stringhe

Campo obbligatorio: no

BackupRetentionPeriod

Specifica il numero di giorni per i quali vengono conservati gli snapshot automatici.

Tipo: integer

Campo obbligatorio: no

CloneGroupId

Identifica il gruppo di cloni a cui è associato il cluster di database.

Tipo: string

Campo obbligatorio: no

ClusterCreateTime

Specifica l'ora in cui è stato creato il cluster, in UTC (Universal Coordinated Time).

Tipo: Timestamp

Campo obbligatorio: no

DBClusterArn

L'Amazon Resource Name (ARN) per il cluster.

Tipo: string

Campo obbligatorio: no

DBClusterIdentifier

Contiene un identificatore di cluster fornito dall'utente. Questo identificatore è la chiave univoca che identifica un cluster.

Tipo: string

Campo obbligatorio: no

DBClusterMembers.DBClusterMember.N

Fornisce l'elenco delle istanze che compongono il cluster.

Tipo: matrice di oggetti [DBClusterMember](#)

Campo obbligatorio: no

DBClusterParameterGroup

Specifica il nome del gruppo di parametri del cluster per il cluster.

Tipo: string

Campo obbligatorio: no

DbClusterResourceeld

L'identificatore Regione AWS -unique e immutabile per il cluster. Questo identificatore si trova nelle voci di AWS CloudTrail registro ogni volta che si accede alla AWS KMS chiave per il cluster.

Tipo: string

Campo obbligatorio: no

DBSubnetGroup

Specifica le informazioni sul gruppo di sottoreti associato al cluster, inclusi il nome, la descrizione e le sottoreti del gruppo di sottoreti.

Tipo: string

Campo obbligatorio: no

DeletionProtection

Specifica se questo cluster può essere eliminato. Se `DeletionProtection` è abilitato, il cluster non può essere eliminato a meno che non venga modificato e `DeletionProtection` disabilitato. `DeletionProtection` protegge i cluster dall'eliminazione accidentale.

Tipo: Booleano

Campo obbligatorio: no

EarliestRestorableTime

Il primo momento in cui è possibile ripristinare un database con point-in-time restore.

Tipo: Timestamp

Campo obbligatorio: no

EnabledCloudwatchLogsExports.member.N

Un elenco di tipi di log che questo cluster è configurato per esportare in Amazon CloudWatch Logs.

Tipo: matrice di stringhe

Campo obbligatorio: no

Endpoint

Specifica l'endpoint di connessione per l'istanza principale del cluster.

Tipo: string

Campo obbligatorio: no

Engine

Fornisce il nome del motore di database da utilizzare per questo cluster.

Tipo: string

Campo obbligatorio: no

EngineVersion

Indica la versione del motore di database.

Tipo: string

Campo obbligatorio: no

HostedZoneId

Specifica l'ID che Amazon Route 53 assegna al momento della creazione di una zona ospitata.

Tipo: string

Campo obbligatorio: no

KmsKeyId

Se `StorageEncrypted` si `true`, l'identificatore della AWS KMS chiave per il cluster crittografato.

Tipo: string

Campo obbligatorio: no

LatestRestorableTime

Specifica l'ora più recente alla quale un database può essere ripristinato con point-in-time restore.

Tipo: Timestamp

Campo obbligatorio: no

MasterUsername

Contiene il nome utente principale per il cluster.

Tipo: string

Campo obbligatorio: no

MultiAZ

Specifica se il cluster dispone di istanze in più zone di disponibilità.

Tipo: Booleano

Campo obbligatorio: no

PercentProgress

Specifica l'avanzamento dell'operazione sotto forma di percentuale.

Tipo: string

Campo obbligatorio: no

Port

Specifica la porta su cui è in ascolto il motore di database.

Tipo: integer

Campo obbligatorio: no

PreferredBackupWindow

Specifica l'intervallo di tempo giornaliero in cui vengono creati i backup automatici se questi sono abilitati, come determinato da `BackupRetentionPeriod`.

Tipo: string

Campo obbligatorio: no

PreferredMaintenanceWindow

Specifica un intervallo temporale settimanale nel fuso orario UTC (Universal Coordinated Time) durante il quale può verificarsi la manutenzione dei sistemi.

Tipo: string

Campo obbligatorio: no

ReaderEndpoint

L'endpoint di lettura per il cluster. L'endpoint di lettura per un cluster bilancia il carico delle connessioni tra le repliche di Amazon DocumentDB disponibili in un cluster. Quando i client

richiedono nuove connessioni all'endpoint del lettore, Amazon DocumentDB distribuisce le richieste di connessione tra le repliche di Amazon DocumentDB nel cluster. Questa funzionalità può aiutare a bilanciare il carico di lavoro di lettura su più repliche di Amazon DocumentDB nel cluster.

Se si verifica un failover e la replica di Amazon DocumentDB a cui sei connesso viene promossa a istanza principale, la connessione viene interrotta. Per continuare a inviare il carico di lavoro di lettura ad altre repliche di Amazon DocumentDB nel cluster, puoi riconnetterti all'endpoint di lettura.

Tipo: string

Campo obbligatorio: no

`ReadReplicaIdentifiers.ReadReplicaIdentifier.N`

Contiene uno o più identificatori dei cluster secondari associati a questo cluster.

Tipo: matrice di stringhe

Campo obbligatorio: no

`ReplicationSourceIdentifier`

Contiene l'identificatore del cluster di origine se questo cluster è un cluster secondario.

Tipo: string

Campo obbligatorio: no

`Status`

Specifica lo stato corrente di questo cluster.

Tipo: string

Campo obbligatorio: no

`StorageEncrypted`

Specifica se il cluster è crittografato.

Tipo: Booleano

Campo obbligatorio: no

StorageType

Tipo di archiviazione associato al cluster

Tipo di storage associato al cluster

Per informazioni sui tipi di storage per i cluster Amazon DocumentDB, consulta le configurazioni di storage dei cluster nella Amazon DocumentDB Developer Guide.

Valori validi per il tipo di storage - `standard` | `iopt1`

Il valore predefinito è `standard`

Tipo: string

Campo obbligatorio: no

`VpcSecurityGroups.VpcSecurityGroupMembership.N`

Fornisce un elenco di gruppi di sicurezza del cloud privato virtuale (VPC) a cui appartiene il cluster.

Tipo: matrice di oggetti [VpcSecurityGroupMembership](#)

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)
- [SDK AWS per Ruby V3](#)

DBClusterMember

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Contiene informazioni su un'istanza che fa parte di un cluster.

Indice

Note

Nell'elenco seguente, i parametri richiesti vengono descritti per primi.

DBClusterParameterGroupStatus

Imposti questo parametro del gruppo di parametri del tuo cluster database.

Tipo: string

Required: No

DBInstanceIdentifier

Specifica l'identificatore di istanza per questo membro del cluster.

Tipo: string

Required: No

IsClusterWriter

Un valore che indica `true` se il membro del cluster è l'istanza principale del cluster e `false` in altro modo.

Tipo: Booleano

Required: No

PromotionTier

Valore che specifica l'ordine di promozione di una Amazon DocumentDB Aurora a istanza principale dopo un errore di un'istanza principale esistente.

Tipo: integer

Required: No

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [AWS SDK per Java V2](#)
- [SDK AWS per Ruby V3](#)

DBClusterParameterGroup

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Informazioni dettagliate su un gruppo di parametri del cluster.

Indice

Note

Nell'elenco seguente, i parametri richiesti vengono descritti per primi.

DBClusterParameterGroupArn

Il nome della risorsa Amazon (ARN) per il gruppo di parametri del cluster.

Tipo: string

Required: No

DBClusterParameterGroupName

Fornisce il nome del gruppo di parametri del cluster.

Tipo: string

Required: No

DBParameterGroupFamily

Fornisce il nome della famiglia del gruppo di parametri con cui è compatibile questo gruppo di parametri del cluster.

Tipo: string

Required: No

Description

Fornisce la descrizione specificata dall'utente per questo gruppo di parametri del cluster.

Tipo: string

Required: No

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [AWS SDK per Java V2](#)
- [SDK AWS per Ruby V3](#)

DBClusterRole

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Descrive un ruoloAWS Identity and Access Management (IAM) associato a un cluster.

Indice

Note

Nell'elenco seguente, i parametri richiesti vengono descritti per primi.

RoleArn

Amazon Resource Name (ARN) del nome della risorsa Amazon (ARN) del nome della risorsa Amazon (ARN) del nome della risorsa Amazon (ARN) del parametro.

Tipo: string

Required: No

Status

Descrive lo stato di associazione tra IAmRole e il cluster. Il parametroStatus su uno uno uno uno uno uno uno uno valori:

- ACTIVE- L'ARN IAmRole è associato al cluster e può essere utilizzato per accedere ad altriAWS servizi per tuo conto.
- PENDING- L'ARN IAmRole viene associato al cluster.
- INVALID- L'ARN IAmRole è associato al cluster, ma il cluster non può presupporre che IamRole acceda ad altriAWS servizi per tuo conto.

Tipo: string

Required: No

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [SDK AWS per C++](#)

- [SDK AWS per Go](#)
- [AWS SDK per Java V2](#)
- [SDK AWS per Ruby V3](#)

DBClusterSnapshot

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Informazioni dettagliate su un'istantanea del cluster.

Indice

Note

Nell'elenco seguente, i parametri richiesti vengono descritti per primi.

AvailabilityZones.AvailabilityZone.N

Fornisce l'elenco delle zone di disponibilità di Amazon EC2 in cui è possibile ripristinare le istanze nello snapshot del cluster.

Tipo: matrice di stringhe

Campo obbligatorio: no

ClusterCreateTime

Specifica l'ora in cui è stato creato il cluster, in UTC (Universal Coordinated Time).

Tipo: Timestamp

Campo obbligatorio: no

DBClusterIdentifier

Specifica l'identificatore del cluster da cui è stata creata questa istantanea del cluster.

Tipo: string

Campo obbligatorio: no

DBClusterSnapshotArn

L'Amazon Resource Name (ARN) per lo snapshot del cluster.

Tipo: string

Campo obbligatorio: no

DBClusterSnapshotIdentifier

Specifica l'identificatore per lo snapshot del cluster.

Tipo: string

Campo obbligatorio: no

Engine

Specifica il nome del motore di database.

Tipo: string

Campo obbligatorio: no

EngineVersion

Fornisce la versione del motore di database per questa istantanea del cluster.

Tipo: string

Campo obbligatorio: no

KmsKeyId

In caso `StorageEncrypted true` affermativo, l'identificatore della AWS KMS chiave per lo snapshot crittografato del cluster.

Tipo: string

Campo obbligatorio: no

MasterUsername

Fornisce il nome utente principale per lo snapshot del cluster.

Tipo: string

Campo obbligatorio: no

PercentProgress

Specifica la percentuale dei dati stimati che sono stati trasferiti.

Tipo: integer

Campo obbligatorio: no

Port

Specifica la porta su cui il cluster era in ascolto al momento dell'istantanea.

Tipo: integer

Campo obbligatorio: no

SnapshotCreateTime

Fornisce l'ora in cui è stata scattata l'istantanea, in UTC.

Tipo: Timestamp

Campo obbligatorio: no

SnapshotType

Fornisce il tipo di istantanea del cluster.

Tipo: string

Campo obbligatorio: no

SourceDBClusterSnapshotArn

Se lo snapshot del cluster è stato copiato da uno snapshot del cluster di origine, l'ARN per lo snapshot del cluster di origine; in caso contrario, un valore nullo.

Tipo: string

Campo obbligatorio: no

Status

Specifica lo stato di questa istantanea del cluster.

Tipo: string

Campo obbligatorio: no

StorageEncrypted

Specifica se l'istantanea del cluster è crittografata.

Tipo: Booleano

Campo obbligatorio: no

StorageType

Tipo di storage associato allo snapshot del cluster

Per informazioni sui tipi di storage per i cluster Amazon DocumentDB, consulta le configurazioni di storage dei cluster nella Amazon DocumentDB Developer Guide.

Valori validi per il tipo di storage - `standard` | `iopt1`

Il valore predefinito è `standard`

Tipo: string

Campo obbligatorio: no

VpcId

Fornisce l'ID del cloud privato virtuale (VPC) associato allo snapshot del cluster.

Tipo: string

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [SDK AWS per Java V2](#)
- [SDK AWS per Ruby V3](#)

DBClusterSnapshotAttribute

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Contiene il nome e i valori di un attributo snapshot manuale del cluster.

Gli attributi manuali dello snapshot del cluster vengono utilizzati per autorizzare altriAccount AWS utenti a ripristinare un'istantanea manuale del cluster.

Indice

Note

Nell'elenco seguente, i parametri richiesti vengono descritti per primi.

AttributeName

Il nome dell'attributo manuale dello snapshot del cluster.

L'attributo `denominatorrestore` si riferisce all'elenco di `colorAccount AWS` che hanno il permesso di copiare o ripristinare l'istantanea manuale del cluster.

Tipo: string

Required: No

AttributeValues.AttributeValue.N

I valori per l'attributo manuale snapshot del cluster.

Se il `AttributeName` campo è impostato su `restore`, questo elemento restituisce un elenco di ID degliAccount AWS utenti autorizzati a copiare o ripristinare l'istantanea manuale del cluster. Se nell'elenco `all` è presente un valore di, l'istantanea manuale del cluster è pubblica e puòAccount AWS essere copiata o ripristinata da chiunque.

Tipo: matrice di stringhe

Required: No

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [AWS SDK per Java V2](#)
- [SDK AWS per Ruby V3](#)

DBClusterSnapshotAttributesResult

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Informazioni dettagliate sugli attributi associati a un'istantanea del cluster.

Indice

Note

Nell'elenco seguente, i parametri richiesti vengono descritti per primi.

DBClusterSnapshotAttributes.DBClusterSnapshotAttribute.N

L'elenco di attributi e valori per l'istantanea del cluster.

Tipo: matrice di oggetti [DBClusterSnapshotAttribute](#)

Required: No

DBClusterSnapshotIdentifier

L'identificatore dello snapshot del cluster a cui si applicano gli attributi.

Tipo: string

Required: No

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [AWS SDK per Java V2](#)
- [SDK AWS per Ruby V3](#)

DBEngineVersion

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Informazioni dettagliate su una versione del motore.

Indice

Note

Nell'elenco seguente, i parametri richiesti vengono descritti per primi.

DBEngineDescription

La descrizione del motore di database.

Tipo: string

Campo obbligatorio: no

DBEngineVersionDescription

La descrizione della versione del motore di database.

Tipo: string

Campo obbligatorio: no

DBParameterGroupFamily

Il nome della famiglia di gruppi di parametri per il motore di database.

Tipo: string

Campo obbligatorio: no

Engine

Il nome del motore di database.

Tipo: string

Campo obbligatorio: no

EngineVersion

Il numero di versione del motore di database.

Tipo: string

Campo obbligatorio: no

ExportableLogTypes.member.N

I tipi di log che il motore di database ha a disposizione per l'esportazione in Amazon CloudWatch Logs.

Tipo: matrice di stringhe

Campo obbligatorio: no

SupportedCACertificateIdentifiers.member.N

Un elenco degli identificatori di certificato CA supportati.

Per ulteriori informazioni, consulta [Updating your Amazon DocumentDB TLS Certificates](#) and [Encrypting Data in Transit nella](#) Amazon DocumentDB Developer Guide.

Tipo: matrice di stringhe

Campo obbligatorio: no

SupportsCertificateRotationWithoutRestart

Indica se la versione del motore supporta la rotazione del certificato del server senza riavviare l'istanza DB.

Tipo: Booleano

Campo obbligatorio: no

SupportsLogExportsToCloudwatchLogs

Un valore che indica se la versione del motore supporta l'esportazione dei tipi di log specificati da `ExportableLogTypes` CloudWatch

Tipo: Booleano

Campo obbligatorio: no

ValidUpgradeTarget.UpgradeTarget.N

Un elenco di versioni dei motori alle quali questa versione del motore di database può essere aggiornata.

Tipo: matrice di oggetti [UpgradeTarget](#)

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [AWS SDK per Java V2](#)
- [SDK AWS per Ruby V3](#)

DBInstance

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Informazioni dettagliate su un'istanza.

Indice

Note

Nell'elenco seguente, i parametri richiesti vengono descritti per primi.

AutoMinorVersionUpgrade

Non si applica. Questo parametro non si applica ad Amazon DocumentDB. Amazon DocumentDB non esegue aggiornamenti di versione secondari indipendentemente dal valore impostato.

Tipo: Booleano

Campo obbligatorio: no

AvailabilityZone

Specifica il nome della zona di disponibilità in cui si trova l'istanza.

Tipo: string

Campo obbligatorio: no

BackupRetentionPeriod

Specifica il numero di giorni per i quali vengono conservate le istantanee automatiche.

Tipo: integer

Campo obbligatorio: no

CACertificateIdentifier

Identificatore del certificato CA per questa istanza database.

Tipo: string

Campo obbligatorio: no

CertificateDetails

I dettagli del certificato del server dell'istanza DB.

Tipo: [CertificateDetails](#) oggetto

Campo obbligatorio: no

CopyTagsToSnapshot

Un valore che indica se copiare i tag dall'istanza database sugli snapshot dell'istanza database. Per impostazione predefinita i tag non vengono copiati.

Tipo: Booleano

Campo obbligatorio: no

DBClusterIdentifier

Contiene il nome del cluster di cui l'istanza fa parte se l'istanza è membro di un cluster.

Tipo: string

Campo obbligatorio: no

DBInstanceArn

Il nome della risorsa Amazon (ARN) per l'istanza.

Tipo: string

Campo obbligatorio: no

DBInstanceClass

Contiene il nome della classe di capacità di calcolo e memoria dell'istanza.

Tipo: string

Campo obbligatorio: no

DBInstanceIdentifier

Contiene un identificatore di database fornito dall'utente. Questo identificatore è la chiave univoca che identifica un'istanza.

Tipo: string

Campo obbligatorio: no

DBInstanceStatus

Specifica lo stato corrente di questo database.

Tipo: string

Campo obbligatorio: no

DbiResourceId

L'identificatore Regione AWS -unique e immutabile dell'istanza. Questo identificatore si trova nelle voci di AWS CloudTrail registro ogni volta che si accede alla AWS KMS chiave dell'istanza.

Tipo: string

Campo obbligatorio: no

DBSubnetGroup

Specifica le informazioni sul gruppo di sottoreti associato all'istanza, inclusi il nome, la descrizione e le sottoreti del gruppo di sottoreti.

Tipo: [DBSubnetGroup](#) oggetto

Campo obbligatorio: no

EnabledCloudwatchLogsExports.member.N

Un elenco di tipi di log che questa istanza è configurata per esportare in Logs. CloudWatch

Tipo: matrice di stringhe

Campo obbligatorio: no

Endpoint

Specifica l'endpoint di connessione.

Tipo: [Endpoint](#) oggetto

Campo obbligatorio: no

Engine

Fornisce il nome del motore di database da utilizzare per questa istanza.

Tipo: string

Campo obbligatorio: no

EngineVersion

Indica la versione del motore di database.

Tipo: string

Campo obbligatorio: no

InstanceCreateTime

Fornisce la data e l'ora di creazione dell'istanza.

Tipo: Timestamp

Campo obbligatorio: no

KmsKeyId

In caso `StorageEncrypted true` affermativo, l'identificatore della AWS KMS chiave per l'istanza crittografata.

Tipo: string

Campo obbligatorio: no

LatestRestorableTime

Specifica l'ora più recente in cui un database può essere ripristinato con point-in-time restore.

Tipo: Timestamp

Campo obbligatorio: no

PendingModifiedValues

Specifica che le modifiche all'istanza sono in sospeso. Questo elemento è incluso solo quando le modifiche sono in sospeso. Le modifiche specifiche sono identificate dagli elementi secondari.

Tipo: [PendingModifiedValues](#) oggetto

Campo obbligatorio: no

PreferredBackupWindow

Specifica l'intervallo di tempo giornaliero in cui vengono creati i backup automatici se questi sono abilitati, come determinato da `BackupRetentionPeriod`.

Tipo: string

Campo obbligatorio: no

PreferredMaintenanceWindow

Specifica un intervallo temporale settimanale nel fuso orario UTC (Universal Coordinated Time) durante il quale può verificarsi la manutenzione dei sistemi.

Tipo: string

Campo obbligatorio: no

PromotionTier

Un valore che specifica l'ordine in cui una replica di Amazon DocumentDB viene promossa all'istanza principale dopo un errore dell'istanza primaria esistente.

Tipo: integer

Campo obbligatorio: no

PubliclyAccessible

Non supportato. Amazon DocumentDB attualmente non supporta endpoint pubblici. Il valore di `PubliclyAccessible` è sempre `false`

Tipo: Booleano

Campo obbligatorio: no

StatusInfos.DBInstanceStatusInfo.N

Lo stato di una replica letta. Se l'istanza non è una replica letta, questo campo è vuoto.

Tipo: matrice di oggetti [DBInstanceStatusInfo](#)

Campo obbligatorio: no

StorageEncrypted

Specifica se l'istanza è crittografata o meno.

Tipo: Booleano

Campo obbligatorio: no

VpcSecurityGroups.VpcSecurityGroupMembership.N

Fornisce un elenco di elementi del gruppo di sicurezza VPC a cui appartiene l'istanza.

Tipo: matrice di oggetti [VpcSecurityGroupMembership](#)

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [AWS SDK per Java V2](#)
- [SDK AWS per Ruby V3](#)

DBInstanceStatusInfo

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Fornisce un elenco di informazioni sullo stato di un'istanza.

Indice

Note

Nell'elenco seguente, i parametri richiesti vengono descritti per primi.

Message

Dettagli dell'errore in caso di errore per l'istanza. Se l'istanza non è in stato di errore, il valore è vuoto.

Tipo: string

Required: No

Normal

Un valore booleano che indica `true` se l'istanza funziona normalmente o `false` se l'istanza è in uno stato di errore.

Tipo: Booleano

Required: No

Status

Stato dell'istanza. Per `StatusType` una replica non letta, i valori possono essere `replicating`, `stopped`, `error` o `terminated`.

Tipo: string

Required: No

StatusType

Questo valore è attualmente `»read_replication`.

Tipo: string

Required: No

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [AWS SDK per Java V2](#)
- [SDK AWS per Ruby V3](#)

DBSubnetGroup

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Informazioni dettagliate su un gruppo di sottoreti.

Indice

Note

Nell'elenco seguente, i parametri richiesti vengono descritti per primi.

DBSubnetGroupArn

Amazon Resource Name (ARN) per il gruppo di sottoreti di database.

Tipo: string

Required: No

DBSubnetGroupDescription

Fornisce la descrizione del gruppo di sottoreti.

Tipo: string

Required: No

DBSubnetGroupName

Il nome del gruppo di sottoreti.

Tipo: string

Required: No

SubnetGroupStatus

Fornisce lo stato del gruppo di sottoreti.

Tipo: string

Required: No

Subnets.Subnet.N

Informazioni dettagliate su una o più sottoreti all'interno di un gruppo di sottoreti.

Tipo: matrice di oggetti [Subnet](#)

Required: No

VpcId

L'ID al cloud privato virtuale (VPC).

Tipo: string

Required: No

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [AWS SDK per Java V2](#)
- [SDK AWS per Ruby V3](#)

Endpoint

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Informazioni di rete per accedere a un cluster o a un'istanza. I programmi client devono specificare un endpoint valido per accedere a queste risorse Amazon DocumentDB.

Indice

Note

Nell'elenco seguente, i parametri richiesti vengono descritti per primi.

Address

Specifica l'indirizzo DNS dell'istanza.

Tipo: string

Required: No

HostedZoneId

Specifica l'ID che Amazon Route 53 assegna al momento della creazione di una zona ospitata.

Tipo: string

Required: No

Port

Specifica la porta su cui è in ascolto il motore di database.

Tipo: integer

Required: No

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [SDK AWS per C++](#)

- [SDK AWS per Go](#)
- [AWS SDK per Java V2](#)
- [SDK AWS per Ruby V3](#)

EngineDefaults

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Contiene il risultato di una chiamata riuscita dell'operazione `DescribeEngineDefaultClusterParameters`.

Indice

Note

Nell'elenco seguente, i parametri richiesti vengono descritti per primi.

DBParameterGroupFamily

Il nome della famiglia del gruppo di parametri del cluster per cui è possibile restituire le informazioni sui parametri del motore.

Tipo: string

Required: No

Marker

Token di paginazione opzionale fornito da una richiesta precedente. Se questo parametro viene specificato, la risposta include solo i record oltre il contrassegno, fino al valore specificato da `MaxRecords`.

Tipo: string

Required: No

Parameters.Parameter.N

I parametri di una particolare famiglia di gruppi di parametri del cluster.

Tipo: matrice di oggetti [Parameter](#)

Required: No

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [AWS SDK per Java V2](#)
- [SDK AWS per Ruby V3](#)

Event

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Informazioni su informazioni su una serie di evento.

Indice

Note

Nell'elenco seguente, i parametri richiesti vengono descritti per primi.

Date

Specifica la data e l'ora dell'evento.

Tipo: Timestamp

Required: No

EventCategories.EventCategory.N

Specifica la categoria per l'evento.

Tipo: matrice di stringhe

Required: No

Message

Fornisce il testo di questo evento.

Tipo: string

Required: No

SourceArn

L'Amazon Resource Name (ARN) per l'evento.

Tipo: string

Required: No

SourceIdentifier

Fornisce l'identificatore per l'origine dell'evento.

Tipo: string

Required: No

SourceType

Specifica il tipo di origine per questo evento.

Tipo: String

Valori validi: `db-instance` | `db-parameter-group` | `db-security-group` | `db-snapshot` | `db-cluster` | `db-cluster-snapshot`

Required: No

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [AWS SDK per Java V2](#)
- [SDK AWS per Ruby V3](#)

EventCategoriesMap

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Un tipo di origine dell'evento, accompagnato da uno o più nomi di categorie di eventi.

Indice

Note

Nell'elenco seguente, i parametri richiesti vengono descritti per primi.

EventCategories.EventCategory.N

Le categorie di eventi per il tipo di origine specificato.

Tipo: matrice di stringhe

Required: No

SourceType

Il tipo di origine a cui appartengono le categorie restituite.

Tipo: string

Required: No

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [AWS SDK per Java V2](#)
- [SDK AWS per Ruby V3](#)

EventSubscription

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Informazioni dettagliate su un evento al quale si dispone della sottoscrizione.

Indice

Note

Nell'elenco seguente, i parametri richiesti vengono descritti per primi.

CustomerAwsId

L'accountAWS cliente associato all'abbonamento per la notifica degli eventi di Amazon DocumentDB.

Tipo: string

Required: No

CustSubscriptionId

L'ID di sottoscrizione per la notifica degli eventi di Amazon DocumentDB.

Tipo: string

Required: No

Enabled

Un valore booleano che indica se la sottoscrizione è abilitata. Il valore `true` indica che è abilitato l'abbonamento.

Tipo: Booleano

Required: No

EventCategoriesList.EventCategory.N

Un elenco di categorie di eventi per la sottoscrizione alle notifiche degli degli eventi Amazon DocumentDB.

Tipo: matrice di stringhe

Required: No

EventSubscriptionArn

L'Amazon Resource Name (ARN) per la sottoscrizione all'evento.

Tipo: string

Required: No

SnsTopicArn

L'argomento ARN dell'abbonamento per la notifica degli eventi di Amazon DocumentDB.

Tipo: string

Required: No

SourceIdsList.SourceId.N

Un elenco di ID di origine per l'abbonamento di notifica degli eventi di Amazon DocumentDB.

Tipo: matrice di stringhe

Required: No

SourceType

Il tipo di origine per la sottoscrizione per la notifica degli eventi di Amazon DocumentDB.

Tipo: string

Required: No

Status

Lo stato della sottoscrizione alle notifiche degli eventi Amazon DocumentDB.

Vincoli:

Può essere uno dei seguenti: `creating`, `modifying`, `deleting`, `active`, `no-permission`, `topic-not-exist`

Lo `no-permission` stato indica che Amazon DocumentDB non dispone più dell'autorizzazione per pubblicare nell'argomento SNS. Lo `topic-not-exist` stato indica che l'argomento è stato eliminato dopo la creazione dell'abbonamento.

Tipo: string

Required: No

SubscriptionCreationTime

L'ora in cui è stato creato l'abbonamento alle notifiche degli eventi Amazon DocumentDB.

Tipo: string

Required: No

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [AWS SDK per Java V2](#)
- [SDK AWS per Ruby V3](#)

Filter

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Un insieme denominato di valori di filtro, utilizzato per restituire un elenco di risultati più specifico. È possibile utilizzare un filtro per abbinare un set di risorse in base a criteri specifici, ad esempio gli ID.

I caratteri jolly non sono supportati nei filtri.

Indice

Note

Nell'elenco seguente, i parametri richiesti vengono descritti per primi.

Name

Il nome del filtro. I nomi dei filtri prevedono una distinzione tra lettere tra lettere

Tipo: String

Campo obbligatorio: sì

Values.Value.N

Uno o più valori di filtro. I valori di filtro fanno distinzione tra maiuscole e minuscole.

Tipo: matrice di stringhe

Campo obbligatorio: sì

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [AWS SDK per Java V2](#)
- [SDK AWS per Ruby V3](#)

GlobalCluster

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Un tipo di dati che rappresenta un cluster globale Amazon DocumentDB.

Indice

Note

Nell'elenco seguente, i parametri richiesti vengono descritti per primi.

DatabaseName

Il nome del database predefinito all'interno del nuovo cluster globale.

Tipo: string

Required: No

DeletionProtection

L'impostazione della protezione contro l'eliminazione per il nuovo cluster globale.

Tipo: Booleano

Required: No

Engine

Il motore di database Amazon DocumentDB utilizzato dal cluster globale.

Tipo: string

Required: No

EngineVersion

Indica la versione del motore di database.

Tipo: string

Required: No

GlobalClusterArn

L'Amazon Resource Name (ARN) per il cluster globale.

Tipo: string

Required: No

GlobalClusterIdentifier

Contiene un identificativo del cluster globale fornito dall'utente. Questo identificativo è la chiave univoca che identifica un cluster globale.

Tipo: String

Limitazioni di lunghezza: lunghezza minima di 1. Lunghezza massima di 255.

Modello: [A-Za-z][0-9A-Za-z-:._]*

Required: No

GlobalClusterMembers.GlobalClusterMember.N

L'elenco degli ID di cluster per i cluster secondari all'interno del cluster globale. Attualmente limitato a un articolo.

Tipo: matrice di oggetti [GlobalClusterMember](#)

Required: No

GlobalClusterResourceId

L'identificativo Regione AWS univoco e non modificabile della per il cluster database globale. Questo identificativo è disponibile nelle voci di AWS CloudTrail log ogni volta che si accede alla chiave master AWS KMS del cliente (CMK) per il cluster.

Tipo: string

Required: No

Status

Specifica lo stato corrente di questo cluster globale.

Tipo: string

Required: No

StorageEncrypted

L'impostazione della crittografia di storage per il cluster globale.

Tipo: Booleano

Required: No

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [AWS SDK per Java V2](#)
- [SDK AWS per Ruby V3](#)

GlobalClusterMember

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Una struttura di dati con informazioni su tutti i cluster primari e secondari associati a un cluster globale Amazon DocumentDB.

Indice

Note

Nell'elenco seguente, i parametri richiesti vengono descritti per primi.

DBClusterArn

L'Amazon Resource Name (ARN) per ogni cluster Amazon DocumentDB.

Tipo: string

Required: No

IsWriter

Specifica se il cluster Amazon DocumentDB è il cluster principale (ovvero dotato di capacità di lettura-scrittura) per il cluster globale Amazon DocumentDB a cui è associato.

Tipo: Booleano

Required: No

Readers.member.N

L'Amazon Resource Name (ARN) per ogni cluster secondario di sola lettura associato al cluster Aurora globale.

Tipo: matrice di stringhe

Required: No

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [AWS SDK per Java V2](#)
- [SDK AWS per Ruby V3](#)

OrderableDBInstanceOption

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Le opzioni disponibili per un'istanza.

Indice

Note

Nell'elenco seguente, i parametri richiesti vengono descritti per primi.

AvailabilityZones.AvailabilityZone.N

Elenco delle zone di disponibilità per un'istanza.

Tipo: matrice di oggetti [AvailabilityZone](#)

Required: No

DBInstanceClass

La classe di istanza per un'istanza.

Tipo: string

Required: No

Engine

Il tipo di motore di un'istanza.

Tipo: string

Required: No

EngineVersion

La versione del motore di un'istanza.

Tipo: string

Required: No

LicenseModel

Il modello di licenza per un'istanza.

Tipo: string

Required: No

Vpc

Indica se un'istanza si trova in un cloud privato virtuale (VPC, Virtual Private Cloud).

Tipo: Booleano

Required: No

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [AWS SDK per Java V2](#)
- [SDK AWS per Ruby V3](#)

Parameter

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Informazioni dettagliate su un singolo parametro.

Indice

Note

Nell'elenco seguente, i parametri richiesti vengono descritti per primi.

AllowedValues

Specifica l'intervallo valido di valori per il parametro.

Tipo: string

Required: No

ApplyMethod

Indica quando applicare gli aggiornamenti dei parametri.

Tipo: String

Valori validi: `immediate` | `pending-reboot`

Required: No

ApplyType

Specifica il tipo di parametri specifici per il motore.

Tipo: string

Required: No

DataType

Specifica il tipo di dati valido per il parametro.

Tipo: string

Required: No

Description

Fornisce una descrizione del parametro.

Tipo: string

Required: No

IsModifiable

Indica se il parametro può essere modificato (`true`) o meno (`false`). Alcuni parametri presentano implicazioni operative o di sicurezza che evitano la loro modifica.

Tipo: Booleano

Required: No

MinimumEngineVersion

La prima versione del motore sulla quale si può applicare il parametro.

Tipo: string

Required: No

ParameterName

Specifica il nome del parametro.

Tipo: string

Required: No

ParameterValue

Specifica il valore del parametro.

Tipo: string

Required: No

Source

Indica l'origine del valore del parametro.

Tipo: string

Required: No

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [AWS SDK per Java V2](#)
- [SDK AWS per Ruby V3](#)

PendingCloudwatchLogsExports

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Elenco dei tipi di log la cui configurazione è ancora in sospeso. Questi tipi di log è in fase di eliminazione.

Indice

Note

Nell'elenco seguente, i parametri richiesti vengono descritti per primi.

LogTypesToDisable.member.N

Tipi di log in fase di abilitazione. Dopo essere stati abilitati, questi tipi di log vengono esportati in Amazon CloudWatch Logs.

Tipo: matrice di stringhe

Required: No

LogTypesToEnable.member.N

Tipi di log in fase di disattivazione. Dopo essere stati disattivati, questi tipi di registro non vengono esportati CloudWatch nei registri.

Tipo: matrice di stringhe

Required: No

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [AWS SDK per Java V2](#)
- [SDK AWS per Ruby V3](#)

PendingMaintenanceAction

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Fornisce informazioni su un'operazione di manutenzione in sospeso per una risorsa.

Indice

Note

Nell'elenco seguente, i parametri richiesti vengono descritti per primi.

Action

Il tipo di operazione di manutenzione in sospeso che è disponibile per la risorsa.

Tipo: string

Required: No

AutoAppliedAfterDate

La data della finestra di manutenzione quando l'operazione viene applicata. L'operazione di manutenzione viene applicata alla risorsa durante la prima finestra di manutenzione dopo questa data. Se questa data è specificata, qualsiasi richiesta di consenso esplicito `next-maintenance` viene ignorata.

Tipo: Timestamp

Required: No

CurrentApplyDate

La data di validità quando l'operazione di manutenzione in sospeso viene applicata alla risorsa.

Tipo: Timestamp

Required: No

Description

Una descrizione che fornisce dettagli sull'operazione di manutenzione.

Tipo: string

Required: No

ForcedApplyDate

La data quando l'operazione di manutenzione viene applicata automaticamente. L'operazione di manutenzione viene applicata alla risorsa in questa data indipendentemente dalla finestra di manutenzione per la risorsa. Se questa data è specificata, qualsiasi richiesta di consenso esplicito immediata viene ignorata.

Tipo: Timestamp

Required: No

OptInStatus

Indica il tipo di richiesta di consenso esplicito che è stata ricevuta per la risorsa.

Tipo: string

Required: No

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [AWS SDK per Java V2](#)
- [SDK AWS per Ruby V3](#)

PendingModifiedValues

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Una o più impostazioni modificate per un'istanza. Queste impostazioni modificate sono state richieste, ma non sono state ancora applicate.

Indice

Note

Nell'elenco seguente, i parametri richiesti vengono descritti per primi.

AllocatedStorage

Contiene la nuova `AllocatedStorage` dimensione per l'istanza che verrà applicata o è attualmente applicata.

Tipo: integer

Required: No

BackupRetentionPeriod

Specifica il numero di giorni in sospeso durante i quali vengono conservati i backup automatici.

Tipo: integer

Required: No

CACertificateIdentifier

Specifica l'identificatore del certificato dell'autorità di certificazione (CA) per l'istanza database.

Tipo: string

Required: No

DBInstanceClass

Contiene il nuovo `DBInstanceClass` per l'istanza che verrà applicato o è attualmente applicato.

Tipo: string

Required: No

DBInstanceIdentifier

Contiene il nuovo `DBInstanceIdentifier` per l'istanza che verrà applicato o è attualmente applicato.

Tipo: string

Required: No

DBSubnetGroupName

Il nuovo gruppo di sottoreti per l'istanza.

Tipo: string

Required: No

EngineVersion

Indica la versione del motore di database.

Tipo: string

Required: No

Iops

Specifica il nuovo valore Provisioned IOPS per l'istanza che verrà applicata o è attualmente applicata.

Tipo: integer

Required: No

LicenseModel

Il modello di licenza per l'istanza.

Valori validi: `license-included`, `bring-your-own-license`, `general-public-license`

Tipo: string

Required: No

MasterUserPassword

Contiene la modifica in sospeso o attualmente in corso delle credenziali master dell'istanza.

Tipo: string

Required: No

MultiAZ

Indica che l'istanza AZ singola deve essere implementazione AZ.

Tipo: Booleano

Required: No

PendingCloudwatchLogsExports

Elenco dei tipi di log la cui configurazione è ancora in sospeso. Questi tipi di log sono in corso di implementazione o disattivazione.

Tipo: [PendingCloudwatchLogsExports](#) oggetto

Required: No

Port

Specifica la porta in sospeso per l'istanza.

Tipo: integer

Required: No

StorageType

Specifica il tipo di archiviazione da associare all'istanza.

Tipo: string

Required: No

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [SDK AWS per C++](#)
- [SDK AWS per Go](#)

- [AWS SDK per Java V2](#)
- [SDK AWS per Ruby V3](#)

ResourcePendingMaintenanceActions

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Rappresenta l'output di [ApplyPendingMaintenanceAction](#).

Indice

Note

Nell'elenco seguente, i parametri richiesti vengono descritti per primi.

PendingMaintenanceActionDetails.PendingMaintenanceAction.N

Un elenco che fornisce i dettagli sulle operazioni di manutenzione in sospeso per la risorsa.

Tipo: matrice di oggetti [PendingMaintenanceAction](#)

Required: No

ResourceIdentifier

L'Amazon Resource Name (ARN) della risorsa con azioni di manutenzione in sospeso.

Tipo: string

Required: No

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [AWS SDK per Java V2](#)
- [SDK AWS per Ruby V3](#)

Subnet

Servizio: Amazon DocumentDB (with MongoDB compatibility)

informazioni informazioni informazioni informazioni informazioni informazioni informazioni
informazioni informazioni informazioni informazioni informazioni informazioni informazioni
informazioni

Indice

Note

Nell'elenco seguente, i parametri richiesti vengono descritti per primi.

SubnetAvailabilityZone

Specifica la zona di disponibilità per la sottorete.

Tipo: [AvailabilityZone](#) oggetto

Required: No

SubnetIdentifier

Specifica l'identificatore della sottorete.

Tipo: string

Required: No

SubnetStatus

Specifica lo stato della sottorete.

Tipo: string

Required: No

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [AWS SDK per Java V2](#)
- [SDK AWS per Ruby V3](#)

- [AWS SDK per Java V2](#)
- [SDK AWS per Ruby V3](#)

UpgradeTarget

Servizio: Amazon DocumentDB (with MongoDB compatibility)

La versione del motore di database a cui è possibile aggiornare un'istanza.

Indice

Note

Nell'elenco seguente, i parametri richiesti vengono descritti per primi.

AutoUpgrade

Un valore che indica se la versione di destinazione è applicata a qualsiasi istanza DB di origineAutoMinorVersionUpgrade impostata su true.

Tipo: Booleano

Required: No

Description

La versione del motore di database a cui è possibile aggiornare un'istanza.

Tipo: string

Required: No

Engine

Il nome del motore di database di destinazione di aggiornamento.

Tipo: string

Required: No

EngineVersion

Il numero di versione del motore di database di destinazione di aggiornamento.

Tipo: string

Required: No

IsMajorVersionUpgrade

Un valore che indica se un motore di database viene aggiornato a una versione principale.

Tipo: Booleano

Required: No

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [AWS SDK per Java V2](#)
- [SDK AWS per Ruby V3](#)

VpcSecurityGroupMembership

Servizio: Amazon DocumentDB (with MongoDB compatibility)

Utilizzato come elemento di risposta per le interrogazioni sull'appartenenza al gruppo di sicurezza Virtual Private Cloud (VPC).

Indice

Note

Nell'elenco seguente, i parametri richiesti vengono descritti per primi.

Status

Stato del gruppo di sicurezza VPC.

Tipo: string

Required: No

VpcSecurityGroupId

Nome del gruppo di sicurezza VPC.

Tipo: string

Required: No

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [AWS SDK per Java V2](#)
- [SDK AWS per Ruby V3](#)

Cluster elastici Amazon DocumentDB

I seguenti tipi di dati sono supportati da Amazon DocumentDB Elastic Clusters:

- [Cluster](#)
- [ClusterInList](#)
- [ClusterSnapshot](#)
- [ClusterSnapshotInList](#)
- [Shard](#)
- [ValidationExceptionField](#)

Cluster

Servizio: Amazon DocumentDB Elastic Clusters

Restituisce informazioni su un cluster elastico specifico.

Indice

Note

Nell'elenco seguente, i parametri richiesti vengono descritti per primi.

adminUserName

Il nome dell'amministratore del cluster elastico.

Tipo: stringa

Campo obbligatorio: sì

authType

Il tipo di autenticazione per il cluster elastico.

Tipo: stringa

Valori validi: PLAIN_TEXT | SECRET_ARN

Campo obbligatorio: sì

clusterArn

L'identificatore ARN del cluster elastico.

Tipo: stringa

Campo obbligatorio: sì

clusterEndpoint

L'URL utilizzato per connettersi al cluster elastico.

Tipo: stringa

Campo obbligatorio: sì

clusterName

Il nome del cluster elastico.

Tipo: stringa

Campo obbligatorio: sì

createTime

L'ora in cui il cluster elastico è stato creato in UTC (Universal Coordinated Time).

Tipo: stringa

Campo obbligatorio: sì

kmsKeyId

L'identificatore della chiave KMS da utilizzare per crittografare il cluster elastico.

Tipo: stringa

Campo obbligatorio: sì

preferredMaintenanceWindow

Intervallo temporale settimanale nel fuso orario UTC (Universal Coordinated Time) durante il quale può verificarsi la manutenzione dei sistemi.

Format: ddd:hh24:mi-ddd:hh24:mi

Tipo: stringa

Campo obbligatorio: sì

shardCapacity

Il numero di vCPU assegnate a ogni shard di cluster elastico. Il massimo è 64. I valori consentiti sono 2, 4, 8, 16, 32, 64.

Tipo: integer

Campo obbligatorio: sì

shardCount

Il numero di shard assegnati al cluster elastico. Il massimo è 32.

Tipo: integer

Campo obbligatorio: sì

status

Lo stato del cluster elastico.

Tipo: stringa

Valori validi: CREATING | ACTIVE | DELETING | UPDATING |
VPC_ENDPOINT_LIMIT_EXCEEDED | IP_ADDRESS_LIMIT_EXCEEDED
| INVALID_SECURITY_GROUP_ID | INVALID_SUBNET_ID |
INACCESSIBLE_ENCRYPTION_CREDS | INACCESSIBLE_SECRET_ARN |
INACCESSIBLE_VPC_ENDPOINT | INCOMPATIBLE_NETWORK | MERGING | MODIFYING |
SPLITTING | COPYING | STARTING | STOPPING | STOPPED

Campo obbligatorio: sì

subnetIds

Gli ID di sottorete Amazon EC2 per il cluster elastico.

Tipo: matrice di stringhe

Campo obbligatorio: sì

vpcSecurityGroupIds

Un elenco di gruppi di sicurezza VPC EC2 associati a questo cluster elastico.

Tipo: matrice di stringhe

Campo obbligatorio: sì

backupRetentionPeriod

Il numero di giorni per i quali vengono conservate le istantanee automatiche.

Tipo: integer

Campo obbligatorio: no

preferredBackupWindow

L'intervallo di tempo giornaliero durante il quale vengono creati i backup automatici, se i backup automatici sono abilitati, come determinato da `backupRetentionPeriod`

Tipo: string

Campo obbligatorio: no

shardInstanceCount

Il numero di istanze di replica applicabili a tutti gli shard del cluster. `shardInstanceCount`Il valore 1 indica che esiste un'istanza di writer e tutte le istanze aggiuntive sono repliche che possono essere utilizzate per le letture e per migliorare la disponibilità.

Tipo: integer

Campo obbligatorio: no

shards

Il numero totale di shard nel cluster.

Tipo: matrice di oggetti [Shard](#)

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- [AWS SDK per C++](#)
- [AWS SDK for Go](#)
- [AWS SDK per Java V2](#)
- [AWS SDK per Ruby V3](#)

ClusterInList

Servizio: Amazon DocumentDB Elastic Clusters

Un elenco di cluster elastici di Amazon DocumentDB.

Indice

Note

Nell'elenco seguente, i parametri richiesti vengono descritti per primi.

clusterArn

L'identificatore ARN del cluster elastico.

Tipo: stringa

Campo obbligatorio: sì

clusterName

Il nome del cluster elastico.

Tipo: stringa

Campo obbligatorio: sì

status

Lo stato del cluster elastico.

Tipo: stringa

Valori validi: CREATING | ACTIVE | DELETING | UPDATING |
VPC_ENDPOINT_LIMIT_EXCEEDED | IP_ADDRESS_LIMIT_EXCEEDED
| INVALID_SECURITY_GROUP_ID | INVALID_SUBNET_ID |
INACCESSIBLE_ENCRYPTION_CREDS | INACCESSIBLE_SECRET_ARN |
INACCESSIBLE_VPC_ENDPOINT | INCOMPATIBLE_NETWORK | MERGING | MODIFYING |
SPLITTING | COPYING | STARTING | STOPPING | STOPPED

Campo obbligatorio: sì

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- [AWS SDK per C++](#)
- [AWS SDK for Go](#)
- [AWS SDK per Java V2](#)
- [AWS SDK per Ruby V3](#)

ClusterSnapshot

Servizio: Amazon DocumentDB Elastic Clusters

Restituisce informazioni su uno specifico snapshot del cluster elastico.

Indice

Note

Nell'elenco seguente, i parametri richiesti vengono descritti per primi.

`adminUserName`

Il nome dell'amministratore del cluster elastico.

Tipo: stringa

Campo obbligatorio: sì

`clusterArn`

L'identificatore ARN del cluster elastico.

Tipo: stringa

Campo obbligatorio: sì

`clusterCreationTime`

L'ora in cui il cluster elastico è stato creato in UTC (Universal Coordinated Time).

Tipo: stringa

Campo obbligatorio: sì

`kmsKeyId`

L'identificatore della chiave KMS è l'Amazon Resource Name (ARN) per la chiave di crittografia KMS. Se stai creando un cluster utilizzando lo stesso account Amazon che possiede questa chiave di crittografia KMS, puoi utilizzare l'alias della chiave KMS anziché l'ARN come chiave di crittografia KMS. Se non viene specificata una chiave di crittografia qui, Amazon DocumentDB utilizza la chiave di crittografia predefinita creata da KMS per il tuo account. Il tuo account ha una chiave di crittografia predefinita diversa per ogni regione Amazon.

Tipo: stringa

Campo obbligatorio: sì

snapshotArn

L'identificatore ARN dello snapshot del cluster elastico.

Tipo: stringa

Campo obbligatorio: sì

snapshotCreationTime

L'ora in cui lo snapshot del cluster elastico è stato creato in UTC (Universal Coordinated Time).

Tipo: stringa

Campo obbligatorio: sì

snapshotName

Il nome dello snapshot del cluster elastico.

Tipo: stringa

Campo obbligatorio: sì

status

Lo stato dello snapshot del cluster elastico.

Tipo: stringa

Valori validi: CREATING | ACTIVE | DELETING | UPDATING |
VPC_ENDPOINT_LIMIT_EXCEEDED | IP_ADDRESS_LIMIT_EXCEEDED
| INVALID_SECURITY_GROUP_ID | INVALID_SUBNET_ID |
INACCESSIBLE_ENCRYPTION_CREDS | INACCESSIBLE_SECRET_ARN |
INACCESSIBLE_VPC_ENDPOINT | INCOMPATIBLE_NETWORK | MERGING | MODIFYING |
SPLITTING | COPYING | STARTING | STOPPING | STOPPED

Campo obbligatorio: sì

subnetIds

Gli ID di sottorete Amazon EC2 per il cluster elastico.

Tipo: matrice di stringhe

Campo obbligatorio: sì

vpcSecurityGroupIds

Un elenco di gruppi di sicurezza VPC EC2 da associare al cluster elastico.

Tipo: matrice di stringhe

Campo obbligatorio: sì

snapshotType

Il tipo di istantanee del cluster da restituire. È possibile specificare uno dei seguenti valori:

- `automated`- Restituisci tutte le istantanee del cluster che Amazon DocumentDB ha creato automaticamente per AWS il tuo account.
- `manual`- Restituisci tutte le istantanee del cluster che hai creato manualmente per il tuo account. AWS

Tipo: stringa

Valori validi: `MANUAL` | `AUTOMATED`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- [AWS SDK per C++](#)
- [AWS SDK for Go](#)
- [AWS SDK per Java V2](#)
- [AWS SDK per Ruby V3](#)

ClusterSnapshotInList

Servizio: Amazon DocumentDB Elastic Clusters

Un elenco di istantanee di cluster elastici.

Indice

Note

Nell'elenco seguente, i parametri richiesti vengono descritti per primi.

clusterArn

L'identificatore ARN del cluster elastico.

Tipo: stringa

Campo obbligatorio: sì

snapshotArn

L'identificatore ARN dello snapshot del cluster elastico.

Tipo: stringa

Campo obbligatorio: sì

snapshotCreationTime

L'ora in cui lo snapshot del cluster elastico è stato creato in UTC (Universal Coordinated Time).

Tipo: stringa

Campo obbligatorio: sì

snapshotName

Il nome dello snapshot del cluster elastico.

Tipo: stringa

Campo obbligatorio: sì

status

Lo stato dello snapshot del cluster elastico.

Tipo: stringa

Valori validi: CREATING | ACTIVE | DELETING | UPDATING |
VPC_ENDPOINT_LIMIT_EXCEEDED | IP_ADDRESS_LIMIT_EXCEEDED
| INVALID_SECURITY_GROUP_ID | INVALID_SUBNET_ID |
INACCESSIBLE_ENCRYPTION_CREDS | INACCESSIBLE_SECRET_ARN |
INACCESSIBLE_VPC_ENDPOINT | INCOMPATIBLE_NETWORK | MERGING | MODIFYING |
SPLITTING | COPYING | STARTING | STOPPING | STOPPED

Campo obbligatorio: sì

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- [AWS SDK per C++](#)
- [AWS SDK for Go](#)
- [AWS SDK per Java V2](#)
- [AWS SDK per Ruby V3](#)

Shard

Servizio: Amazon DocumentDB Elastic Clusters

Il nome del frammento.

Indice

Note

Nell'elenco seguente, i parametri richiesti vengono descritti per primi.

`createTime`

L'ora in cui lo shard è stato creato in UTC (Universal Coordinated Time).

Tipo: stringa

Campo obbligatorio: sì

`shardId`

L'ID dello shard.

Tipo: stringa

Campo obbligatorio: sì

`status`

Lo stato attuale dello shard.

Tipo: stringa

Valori validi: CREATING | ACTIVE | DELETING | UPDATING |
VPC_ENDPOINT_LIMIT_EXCEEDED | IP_ADDRESS_LIMIT_EXCEEDED
| INVALID_SECURITY_GROUP_ID | INVALID_SUBNET_ID |
INACCESSIBLE_ENCRYPTION_CREDS | INACCESSIBLE_SECRET_ARN |
INACCESSIBLE_VPC_ENDPOINT | INCOMPATIBLE_NETWORK | MERGING | MODIFYING |
SPLITTING | COPYING | STARTING | STOPPING | STOPPED

Campo obbligatorio: sì

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- [AWS SDK per C++](#)
- [AWS SDK for Go](#)
- [AWS SDK per Java V2](#)
- [AWS SDK per Ruby V3](#)

ValidationExceptionField

Servizio: Amazon DocumentDB Elastic Clusters

Un campo specifico in cui si è verificata una determinata eccezione di convalida.

Indice

Note

Nell'elenco seguente, i parametri richiesti vengono descritti per primi.

message

Un messaggio di errore che descrive l'eccezione di convalida in questo campo.

Tipo: String

Campo obbligatorio: sì

name

Il nome del campo in cui si è verificata l'eccezione di convalida.

Tipo: String

Campo obbligatorio: sì

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- [SDK AWS per C++](#)
- [SDK AWS per Go](#)
- [AWS SDK per Java V2](#)
- [SDK AWS per Ruby V3](#)

Errori comuni

In questa sezione sono riportati gli errori comuni delle azioni API per tutti i servizi AWS. Per gli errori specifici di un'azione API per questo servizio, consulta l'argomento per quell'azione API.

AccessDeniedException

Non disponi dell'autorizzazione di accesso sufficiente per eseguire questa operazione.

Codice di stato HTTP: 400

IncompleteSignature

La firma della richiesta non è conforme agli standard AWS.

Codice di stato HTTP: 400

InternalFailure

L'elaborazione della richiesta non è riuscita a causa di un errore, un'eccezione o un guasto interno sconosciuto.

Codice di stato HTTP: 500

InvalidAction

L'azione o l'operazione richiesta non è valida. Verifica che l'operazione sia digitata correttamente.

Codice di stato HTTP: 400

InvalidClientTokenId

Il certificato X.509 o l'ID chiave di accesso AWS forniti non sono presenti nei nostri record.

Codice di stato HTTP: 403

NotAuthorized

Non disponi delle autorizzazioni per eseguire questa azione.

Codice di stato HTTP: 400

OptInRequired

L'ID chiave di accesso AWS necessita di una sottoscrizione al servizio.

Codice di stato HTTP: 403

RequestExpired

La richiesta ha raggiunto il servizio più di 15 minuti dopo il date stamp della richiesta o più di 15 minuti dopo la data di scadenza della richiesta (ad esempio per URL prefirmati) oppure il date stamp della richiesta è più di 15 minuti nel futuro.

Codice di stato HTTP: 400

ServiceUnavailable

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 503

ThrottlingException

La richiesta è stata negata a causa del throttling della richiesta.

Codice di stato HTTP: 400

ValidationError

L'input non riesce a soddisfare i vincoli specificati da un servizio AWS.

Codice di stato HTTP: 400

Parametri comuni

L'elenco seguente contiene i parametri utilizzati da tutte le azioni per firmare le richieste di Signature Version 4 con una stringa di query. Qualsiasi parametro specifico di un'operazione è riportato nell'argomento relativo all'operazione. Per ulteriori informazioni sulla versione 4 della firma, consulta [le richieste diAWS API per la firma](#) nella Guida per l'utente IAM.

Action

azione da eseguire.

Tipo: stringa

Campo obbligatorio: sì

Version

Versione dell'API per cui è scritta la richiesta, espressa nel formato AAAA-MM-GG.

Tipo: stringa

Campo obbligatorio: sì

X-Amz-Algorithm

Algoritmo hash utilizzato per creare la firma della richiesta.

Condition: specifica questo parametro quando includi le informazioni di autenticazione in una stringa di query anziché nell'intestazione di autorizzazione HTTP.

Tipo: stringa

Valori validi: AWS4-HMAC-SHA256

Obbligatorio: condizionale

X-Amz-Credential

Il valore dell'ambito delle credenziali, che è una stringa che include la chiave di accesso, la data, la regione di destinazione, il servizio richiesto e una stringa di terminazione ("aws4_request").

Il valore viene espresso nel seguente formato: chiave_accesso/AAAAMMGG/regione/servizio/aws4_request.

Per ulteriori informazioni, consulta [Creare una richiesta AWS API firmata](#) nella Guida per l'utente IAM.

Condition: specifica questo parametro quando includi le informazioni di autenticazione in una stringa di query anziché nell'intestazione di autorizzazione HTTP.

Tipo: stringa

Obbligatorio: condizionale

X-Amz-Date

La data utilizzata per creare la firma. Il formato deve essere il formato di base ISO 8601 (YYYYMMDD'T'HHMMSS'Z'). Ad esempio, la seguente combinazione data/ora è un valore X-Amz-Date valido: 20120325T120000Z.

Condition: X-Amz-Date è facoltativo per tutte le richieste; può essere utilizzato per sovrascrivere la data utilizzata per firmare le richieste. Se l'intestazione Date è specificata nel formato base ISO 8601, X-Amz-Date non è richiesto. Quando utilizzi X-Amz-Date, sostituisce sempre il valore

dell'intestazione Date. Per ulteriori informazioni, consulta [Elements of an AWS API request signature](#) nella IAM User Guide.

Tipo: stringa

Obbligatorio: condizionale

X-Amz-Security-Token

Il token di sicurezza provvisorio ottenuto tramite una chiamata ad AWS Security Token Service (AWS STS). [Per un elenco di servizi che supportano le credenziali di sicurezza temporanee da AWS STS, vai Servizi AWS a Guida per l'utente di IAM.](#)

Condition: se utilizzi le credenziali di sicurezza temporanee da AWS STS, devi includere il token di sicurezza.

Tipo: stringa

Obbligatorio: condizionale

X-Amz-Signature

Specifica la firma con codifica esadecimale calcolata dalla stringa da firmare e dalla chiave di firma derivata.

Condition: specifica questo parametro quando includi le informazioni di autenticazione in una stringa di query anziché nell'intestazione di autorizzazione HTTP.

Tipo: stringa

Obbligatorio: condizionale

X-Amz-SignedHeaders

Specifica tutte le intestazioni HTTP incluse come parte della richiesta canonica. Per ulteriori informazioni sulla definizione delle intestazioni firmate, consulta [Creare una richiesta AWS API firmata](#) nella Guida per l'utente IAM.

Condition: specifica questo parametro quando includi le informazioni di autenticazione in una stringa di query anziché nell'intestazione di autorizzazione HTTP.

Tipo: stringa

Obbligatorio: condizionale

Note di rilascio

Queste note di rilascio descrivono le funzionalità, i miglioramenti e le correzioni di bug di Amazon DocumentDB in base alla data di rilascio. Le note di rilascio includono aggiornamenti per tutte le versioni del motore Amazon DocumentDB man mano che vengono rilasciate.

Puoi determinare la versione corrente della patch del motore Amazon DocumentDB eseguendo il seguente comando:

```
db.runCommand({getEngineVersion: 1})
```

Se il cluster non utilizza la versione più recente del motore, è probabile che sia disponibile una manutenzione in sospeso che consentirà di aggiornare il motore. Per ulteriori informazioni, consulta [Manutenzione di Amazon DocumentDB](#) la Guida per gli sviluppatori.

Argomenti

- [3 aprile 2024](#)
- [22 febbraio 2024](#)
- [30 gennaio 2024](#)
- [10 gennaio 2024](#)
- [20 dicembre 2023](#)
- [13 dicembre 2023](#)
- [29 novembre 2023](#)
- [21 novembre 2023](#)
- [17 novembre 2023](#)
- [6 novembre 2023](#)
- [20 ottobre 2023](#)
- [25 settembre 2023](#)
- [20 settembre 2023](#)
- [15 settembre 2023](#)
- [11 settembre 2023](#)
- [3 agosto 2023](#)
- [13 luglio 2023](#)

- [7 giugno 2023](#)
- [10 maggio 2023](#)
- [4 aprile 2023](#)
- [22 marzo 2023](#)
- [1 marzo 2023](#)
- [27 febbraio 2023](#)
- [2 febbraio 2023](#)
- [30 novembre 2022](#)
- [9 agosto 2022](#)
- [25 luglio 2022](#)
- [27 giugno 2022](#)
- [29 aprile 2022](#)
- [7 aprile 2022](#)
- [16 marzo 2022](#)
- [8 febbraio 2022](#)
- [24 gennaio 2022](#)
- [21 gennaio 2022](#)
- [25 ottobre 2021](#)
- [24 giugno 2021](#)
- [4 maggio 2021](#)
- [15 gennaio 2021](#)
- [9 novembre 2020](#)
- [30 ottobre 2020](#)
- [22 settembre 2020](#)
- [10 luglio 2020](#)
- [30 giugno 2020](#)

3 aprile 2024

Amazon DocumentDB è ora disponibile nella regione del Medio Oriente (Emirati Arabi Uniti). Per ulteriori informazioni, consulta questo [post di blog](#).

Note

La seguente patch del motore di Amazon DocumentDB verrà distribuita a tutte le regioni di Amazon DocumentDB nelle prossime settimane. Quando questa patch per il motore sarà disponibile nella tua regione, riceverai una notifica della patch di servizio tramite AWS Health Dashboard (AHD) AWS Management Console e tramite e-mail all'indirizzo e-mail dell'utente root del tuo AWS account.

Questa patch per il motore include le seguenti nuove funzionalità e correzioni di bug. Tieni presente che l'elenco seguente, insieme alla documentazione di supporto pertinente, potrebbe essere aggiornato per includere annunci di funzionalità aggiuntive una volta che la patch del motore sarà disponibile in tutte le regioni.

Nuove funzionalità

Amazon DocumentDB 5.0 (patch del motore versione 3.0.5721)

- Aggiunto supporto `bypassDocumentValidation` e messaggio di errore granulare per `$jsonSchema`
- È stato aggiunto il supporto di `$expr`
- È stato aggiunto il supporto per `Uncorrelated Joins` in `$lookup`
- È stato aggiunto il supporto per mantenere le regole di convalida in fase di aggregazione. `$out`

Amazon DocumentDB 4.0 (patch del motore versione 2.0.10392)

- Aggiunto supporto e messaggio di errore granulare per `bypassDocumentValidation`. `$jsonSchema`
- È stato aggiunto il supporto di `$expr`
- È stato aggiunto il supporto per `Uncorrelated Joins` in `$lookup`
- È stato aggiunto il supporto per mantenere le regole di convalida in fase di aggregazione. `$out`

Correzioni di bug e altre modifiche

- Risolto un errore durante l'invocazione `db.coll.stats()` su mongo shell versione 1.7 e successive.

- È stato risolto un problema di perdita di memoria per le query Change Stream che contenevano `$regex` come parte della stessa pipeline di aggregazione.

22 febbraio 2024

Nuove funzionalità

Cluster elastici Amazon DocumentDB

I cluster elastici di Amazon DocumentDB ora supportano le seguenti funzionalità:

- Repliche di istanze shard secondarie leggibili: per ulteriori informazioni, consulta il passaggio 5b di [Fase 1: Creare un cluster elastico](#)
- Avvia/interrompi il cluster: per ulteriori informazioni, vedere [Arresto e avvio di un cluster elastico Amazon DocumentDB](#)
- Istanze shard configurabili: per ulteriori informazioni, vedere il passaggio 5b di [Fase 1: Creare un cluster elastico](#)
- Backup automatici per le istantanee: per ulteriori informazioni, consulta [Gestione di un backup automatico di snapshot del cluster elastico](#)
- Copia istantanea: per ulteriori informazioni, consulta [Copia di un'istantanea del cluster elastico](#)

30 gennaio 2024

Nuove funzionalità

Cluster elastici Amazon DocumentDB

I cluster elastici di Amazon DocumentDB sono ora disponibili nelle seguenti regioni:

- Asia Pacifico (Mumbai)
- Asia Pacifico (Seul)
- Sud America (San Paolo)
- Europa (Londra)

Per ulteriori informazioni, consulta [Disponibilità della regione e della versione del cluster elastico](#).

Cluster globali Amazon DocumentDB

I cluster globali sono ora disponibili in entrambe le AWS GovCloud (US) regioni: AWS GovCloud (Stati Uniti orientali) e AWS GovCloud (Stati Uniti occidentali).

10 gennaio 2024

Nuove funzionalità

Amazon DocumentDB 5.0 (versioni delle patch del motore 3.0.4574, 3.0.4780, 3.0.4960)

- È stato aggiunto il supporto per gli indici vettoriali HNSW. Per ulteriori informazioni, consulta [Ricerca vettoriale per Amazon DocumentDB](#).
- Aggiunto il supporto per gli indici parziali. Per ulteriori informazioni, consulta [Indice parziale](#).
- Aggiunto un supporto per il runtime GC su una raccolta all'interno del comando. `currentOp`
- È stato aggiunto il supporto dell'indice di testo per la ricerca di testo nativa su Amazon DocumentDB. Per ulteriori informazioni, consulta [Esecuzione di ricerche di testo con Amazon DocumentDB](#).
- È stato aggiunto il supporto per le parole chiave `$jsonSchema` dello schema type `allOf` `oneOf` `anyOf` `not`, `maxItems`, `minItems`, `maxProperties`, `minProperties`, `pattern`, `patternProperties`, `multipleOf` `dependencies`, `uniqueItems`.

Per ulteriori informazioni, consulta [Utilizzo della convalida dello schema JSON](#).

- È stato aggiunto il supporto per gli operatori aritmetici `$ceil`, `$floor`, `$ln`, `$log` `$log10`, `$sqrt` e `$exp`

Per ulteriori informazioni, consulta [Operatori aritmetici](#).

- È stato aggiunto il supporto per le build di indici IVFFLAT vettoriali paralleli. La documentazione è stata aggiornata rimuovendo la limitazione delle build dell'indice IVFFLAT vettoriale parallelo dalla guida per sviluppatori.

Amazon DocumentDB 4.0 (patch del motore versioni 2.0.10124, 2.0.10179, 2.0.10221)

- È stato aggiunto un supporto per il runtime GC su una raccolta all'interno del comando. `currentOp`

- È stato aggiunto il supporto per le parole chiave `$jsonSchema` dello schema type `allOf` `oneOf` `anyOf` `not`, `maxItems`, `minItems`, `maxProperties`, `minProperties`, `pattern`, `patternProperties`, `multipleOf` `dependencies`, `euniqueItems`.

Per ulteriori informazioni, consulta [Utilizzo della convalida dello schema JSON](#).

- È stato aggiunto il supporto per gli operatori aritmetici `$ceil`, `$floor`, `$ln`, `$log` `$log10`, `$sqrt` e `$exp`

Per ulteriori informazioni, consulta [Operatori aritmetici](#).

Correzioni di bug e altre modifiche

- Aggiunta funzionalità di invocazione senza distinzione tra maiuscole e minuscole. `db.runCommand("dbstats")` I clienti di Amazon DocumentDB 5.0 e 4.0 con versioni di patch per i motori precedenti alla 3.0.4960 o alla 2.0.10221 devono applicare queste ultime patch al motore.
- È stato corretto un errore durante l'invocazione `db.coll.stats()` su mongo shell versione 1.7 e successive. La documentazione è stata aggiornata rimuovendo il suggerimento per la `db.coll.stats()` risoluzione dei problemi di mongo shell dalla guida per sviluppatori.

20 dicembre 2023

Altre modifiche

Supporto abilitato per l'aggiornamento immediato delle versioni principali in Amazon DocumentDB 3.6 e 4.0. Per ulteriori informazioni, consulta [Aggiornamento immediato della versione principale di Amazon DocumentDB](#).

13 dicembre 2023

Nuove funzionalità

È stato aggiunto il supporto per la connettività EC2 con 1 clic. Per ulteriori informazioni, consulta [Connect tramite Amazon EC2](#).

29 novembre 2023

Amazon DocumentDB 5.0 (patch del motore versione 3.0.3727)

Nuove funzionalità

È stato aggiunto il supporto per la ricerca vettoriale. Per ulteriori informazioni, consulta questo [post di blog](#) e [Ricerca vettoriale per Amazon DocumentDB](#) consulta la Amazon DocumentDB Developer Guide.

21 novembre 2023

Amazon DocumentDB 5.0 (patch del motore versione 3.0.3727)

Nuove funzionalità

È stato aggiunto il supporto per lo storage ottimizzato per l'I/O. Per ulteriori informazioni, consulta [Configurazioni di storage in cluster Amazon DocumentDB](#) la Amazon DocumentDB Developer Guide.

È stata aggiunta l'integrazione per l'apprendimento automatico senza codice con SageMaker Canvas. Per ulteriori informazioni, consulta [Apprendimento automatico senza codice con Amazon Canvas SageMaker](#) la Amazon DocumentDB Developer Guide.

17 novembre 2023

Nuove funzionalità

Amazon DocumentDB è ora disponibile nella regione AWS GovCloud (Stati Uniti orientali). Per ulteriori informazioni, consulta questo [post di blog](#).

Correzioni di bug e altre modifiche

Amazon DocumentDB 3.6 (patch del motore versione 1.0.208570)

I nomi delle variabili locali definiti dall'utente ora supportano «_» (trattino basso) per gli operatori di proiezione come e. `$let $filter`

6 novembre 2023

Amazon DocumentDB 5.0 (patch del motore versione 3.0.3727) e 4.0 (patch del motore versione 2.0.9876)

Nuove funzionalità

- È stato aggiunto il supporto per le parole chiave `$jsonSchema` dello `schemamaxLength,,,minLength, emaximum. minimum exclusiveMaximum exclusiveMinimum items additionalItems`

Tieni presente che la convalida dello schema JSON è supportata solo nei cluster basati su istanze.

- È stato aggiunto il supporto per l'operatore `$convert` di pipeline di aggregazione e i suoi operatori `$toBool` derivati abbreviati,,,,, e. `$toInt $toLong $toDouble $toString $toDecimal $toObjectId $toDate`
- È stato aggiunto il supporto per gli operatori `$setDifference` di espressione di set e. `$anyElementTrue $allElementTrue`

Correzioni di bug e altre modifiche

Problema risolto per cui non NaN veniva visualizzato un aggiornamento del flusso di modifiche da - NaN a.

20 ottobre 2023

Altre modifiche

Amazon DocumentDB ha identificato un problema e non consente temporaneamente gli aggiornamenti delle versioni principali (MVU) in tutte le regioni. Abbiamo identificato la causa principale del problema e abbiamo sviluppato una correzione che è attualmente in fase di test. Prevediamo che questa correzione verrà implementata in tutte le regioni entro la fine del quarto trimestre 2023. MVU rimarrà disabilitato fino a quando la correzione non verrà distribuita in tutte le regioni. Consulta questa pagina della nota di rilascio per ulteriori aggiornamenti sulla disponibilità delle funzionalità MVU.

Nel frattempo, puoi AWS DMS eseguire aggiornamenti di versione principali migrando il database Amazon DocumentDB da un cluster di versioni precedenti a una versione superiore. Segui i passaggi

indicati per eseguire l'upgrade utilizzando. [Aggiornamento del cluster Amazon DocumentDB tramite AWS Database Migration Service](#) AWS DMS Puoi anche fare riferimento a questo [post del blog](#) per ulteriori informazioni sulle migliori pratiche da seguire durante l'aggiornamento tramite AWS DMS

25 settembre 2023

Nuove funzionalità

Amazon DocumentDB è ora disponibile nella regione Asia Pacifico (Hong Kong). Per ulteriori informazioni, consulta questo [post del blog](#).

20 settembre 2023

Nuove funzionalità

È stato aggiunto il supporto per gli aggiornamenti delle versioni principali in Amazon DocumentDB 3.6 e 4.0. Per ulteriori informazioni, consulta [Aggiornamento immediato della versione principale di Amazon DocumentDB](#).

15 settembre 2023

Nuove funzionalità

Amazon DocumentDB 5.0 (patch del motore versione 3.0.3140) e 4.0 (patch del motore versione 2.0.9686)

- È stato aggiunto il supporto per il validatore dello schema \$JsonSchema solo nei cluster basati su istanze.

Per ulteriori informazioni, consulta [Utilizzo della convalida dello schema JSON](#).

11 settembre 2023

Nuove funzionalità

Amazon DocumentDB è ora disponibile nella regione Asia Pacifico (Hyderabad). [Per ulteriori informazioni, consulta questo post del blog](#).

3 agosto 2023

Nuove funzionalità

Cluster elastici Amazon DocumentDB

- I cluster Amazon DocumentDB Elastic ora supportano le seguenti operazioni:
 - `top`
 - `collStats`
 - `hint`
 - `dataSize`

Consulta [API, operazioni e tipi di dati di MongoDB supportati](#) l'elenco completo dei comandi e delle operazioni supportati.

- Gli indici Time to Live (TTL) sono ora supportati.
- `hints` Gli indici sono ora supportati con le espressioni di indice.

13 luglio 2023

Nuove funzionalità

Amazon DocumentDB 5.0 (patch del motore versione 3.0.1948)

- È stato aggiunto il supporto per la compressione dei documenti.
- È stato aggiunto il supporto per le build di indici paralleli.
- È stato aggiunto il supporto per lo stato di creazione dell'indice.

Amazon DocumentDB 4.0 (patch del motore versione 2.0.9259)

- È stato aggiunto il supporto per le build di indici paralleli.

Correzioni di bug e altre modifiche

Amazon DocumentDB 5.0 (patch del motore versione 3.0.1948)

- È stato risolto il problema di autenticazione `createCollection` relativo ai cluster elastici di Amazon DocumentDB quando gli utenti non hanno accesso alle raccolte di sistema.
- Problema risolto per cui le istanze della regione secondaria non potevano utilizzare gli stessi nomi di istanze della regione primaria.

Amazon DocumentDB 4.0 (patch del motore versione 2.0.9259)

- È stata interrotta l'aggiunta di query di monitoraggio interne ai log di controllo.

7 giugno 2023

Correzioni di bug e altre modifiche

Amazon DocumentDB 5.0

- Le istanze `r5` e `t3.medium` sono ora supportate in Amazon DocumentDB 5.0.
- `engineVersion` l'opzione predefinita è `5.0.0` in AWS SDK e. AWS CLI AWS CloudFormation

10 maggio 2023

Correzioni di bug e altre modifiche

Amazon DocumentDB 5.0 (patch del motore versione 3.0.1361)

- È stato aggiunto il supporto per `ignoreunknownindexoptions` nel comando. `createIndex`
- È stata interrotta l'aggiunta di interrogazioni di monitoraggio interne ai registri di controllo.
- I nomi delle variabili locali definiti dall'utente ora supportano «`_`» (trattino basso) per gli operatori di proiezione come e. `$let $filter`

4 aprile 2023

Correzioni di bug e altre modifiche

Amazon DocumentDB 4.0 (patch del motore versione 2.0.8934)

- È stato risolto il problema relativo al controllo DML quando è abilitato durante un carico di lavoro in corso.
- È stato risolto il problema relativo al controllo DML quando ai comandi aggregati con hint viene passato un valore di stringa.
- È stato risolto il problema relativo al mancato funzionamento del `listCollections` comando quando gli utenti con ruolo `readwriteanydatabase` avevano entrambe le opzioni `AuthorizedCollections` e `NameOnly` impostate su `true`.
- Problema risolto relativo all'analisi corretta della stringa numerica in un nome di campo.
- Annulla i cursori a lunga durata quando influiscono sulla raccolta dei rifiuti.
- I nomi delle variabili locali definiti dall'utente ora supportano «`_`» (trattino basso) per gli operatori di proiezione come e. `$let $filter`

22 marzo 2023

Nuove funzionalità

I cluster elastici di Amazon DocumentDB sono ora disponibili nelle regioni Asia Pacifico (Singapore), Asia Pacifico (Sydney) e Asia Pacifico (Tokyo). Per ulteriori informazioni, consulta [Disponibilità della regione e della versione del cluster elastico](#).

1 marzo 2023

Nuove funzionalità

Amazon DocumentDB 5.0 (patch del motore versione 3.0.775)

- Presentato Amazon DocumentDB 5.0
 - Compatibilità con MongoDB 5.0 (supporto per i driver API MongoDB 5.0)
 - Support per la crittografia a livello di campo (FLE) lato client. Ora puoi crittografare i campi sul lato client prima di scrivere i dati nel cluster Amazon DocumentDB. [Per ulteriori informazioni, consulta Crittografia a livello di campo lato client](#)
 - Nuovi operatori di aggregazione: `$dateAdd` `$dateSubtract`
- Limite di storage aumentato a 128 TiB per tutti i cluster Amazon DocumentDB basati su istanze e i cluster elastici basati su shard.

- Amazon DocumentDB 5.0 ora supporta la scansione dell'indice con l'`$elemMatch` operatore nel primo livello di nesting. Le scansioni degli indici sono supportate quando la query ha un solo livello di `$elemMatch` filtro e la `$elemMatch` query annidata non supporta la scansione dell'indice.

Forma di interrogazione che supporta la scansione dell'indice:

```
db.foo.find( { "a": { $elemMatch: { "b": "xyz", "c": "abc" } } })
```

Forma di interrogazione che non supporta la scansione dell'indice:

```
db.foo.find( { "a": { $elemMatch: { "b": { $elemMatch: { "d": "xyz", "e": "abc" } } } } })
```

27 febbraio 2023

Correzioni di bug e altre modifiche

Amazon DocumentDB 4.0

È stato aggiunto il supporto per AWS Lambda. Per ulteriori informazioni, consulta [Using AWS Lambda with Change Streams](#).

2 febbraio 2023

Correzioni di bug e altre modifiche

Amazon DocumentDB 3.6 (patch del motore versione 1.0.208432)

- È stato risolto il problema relativo al controllo DML quando è abilitato durante un carico di lavoro in corso.
- È stato risolto il problema relativo al controllo DML quando ai comandi aggregati con hint viene passato un valore di stringa.
- È stato risolto il problema relativo al mancato funzionamento del `listCollections` comando quando gli utenti con ruolo `readwriteanydatabase` avevano entrambe le opzioni `AuthorizedCollections` e `NameOnly` impostate su `true`.
- Problema risolto relativo all'analisi corretta della stringa numerica in un nome di campo.

- Annulla i cursori a lunga durata quando influiscono sulla raccolta dei rifiuti.

30 novembre 2022

Nuove funzionalità

Cluster elastici Amazon DocumentDB

I cluster elastici di Amazon DocumentDB sono un nuovo tipo di cluster Amazon DocumentDB che consente agli utenti di sfruttare le API di sharding MongoDB per scalare orizzontalmente il proprio cluster. I cluster elastici gestiscono praticamente qualsiasi numero di letture e scritture con petabyte di capacità di storage distribuendo i dati e l'elaborazione su più istanze e volumi di calcolo sottostanti. Per ulteriori informazioni, consulta [Utilizzo dei cluster elastici di Amazon DocumentDB](#).

9 agosto 2022

Nuove funzionalità

Amazon DocumentDB 3.6 (patch del motore versione 1.0.208152) e 4.0

- È stato aggiunto il supporto per il tipo di dati Decimal128. Decimal128 è un tipo di dati BSON supportato in tutte le regioni in cui è disponibile DocumentDB.

Per ulteriori informazioni, consulta la sezione relativa ai [tipi di dati](#).

- È stato aggiunto il supporto per il controllo delle query DML con Amazon CloudWatch Logs. Ora Amazon DocumentDB può registrare eventi DML (Data Manipulation Language) ed eventi DDL (Data Definition Language) su Amazon Logs. CloudWatch

[Per ulteriori informazioni, consulta questo post di blog.](#)

Correzioni di bug e altre modifiche

Amazon DocumentDB 3.6 (patch del motore versione 1.0.208152) e 4.0

- È ora possibile modificare la propria password con una propria password con privilegi. `changeOwnPassword`

25 luglio 2022

Nuove funzionalità

Amazon DocumentDB 4.0

Ora è possibile creare cluster più velocemente grazie alla possibilità di creare cloni che utilizzano lo stesso volume del cluster DocumentDB e contengono gli stessi dati del cluster originale. Per i dettagli, consulta [Managing Amazon DocumentDB Clusters](#).

27 giugno 2022

Nuove funzionalità

Amazon DocumentDB 4.0 (patch del motore versione 2.0.7509)

Amazon DocumentDB ridimensiona dinamicamente il database in base ai modelli di utilizzo. L'aggiunta di altri dati aumenta lo spazio fino a 64 Tebibyte (TiB) e l'eliminazione dei dati riduce lo spazio assegnato.

29 aprile 2022

Nuove funzionalità

Amazon DocumentDB è ora disponibile nella regione Cina (Pechino). Per ulteriori informazioni, consulta questo [post di blog](#).

7 aprile 2022

Nuove funzionalità

Amazon DocumentDB 3.6 (versioni delle patch del motore 1.0.207836 e 1.0.208015) e 4.0 (versioni delle patch del motore 2.0.6142 e 2.0.6948)

Amazon DocumentDB Performance Insights è ora disponibile in anteprima. Ora puoi archiviare sette giorni di cronologia delle prestazioni in una finestra scorrevole senza costi aggiuntivi. Per ulteriori informazioni, consulta [Monitoring with Performance Insights](#).

16 marzo 2022

Nuove funzionalità

Amazon DocumentDB è ora disponibile nella regione Europa (Milano). Per ulteriori informazioni, consulta questo [post di blog](#).

8 febbraio 2022

Nuove funzionalità

Le istanze Amazon DocumentDB R6g e T4g sono ora disponibili in Asia Pacifico, Sud America ed Europa. [Per ulteriori informazioni, consulta questo post di blog](#).

24 gennaio 2022

Nuove funzionalità

Amazon DocumentDB 3.6 (patch del motore versione 1.0.207684) e 4.0 (patch del motore versione 2.0.5170)

- DocDB; ora offre una versione di prova gratuita. Per i dettagli, consulta la pagina di [prova gratuita di Amazon DocumentDB](#).
- Ora puoi utilizzare funzionalità avanzate con Geospatial Query, incluse le seguenti API:
 - `$geoWithin`
 - `$geoIntersects`
- È stato aggiunto il supporto per i seguenti operatori MongoDB:
 - `$mergeObjects`
 - `$reduce`

Per ulteriori informazioni, consulta la sezione [Interrogazione di dati geospaziali con Amazon DocumentDB](#).

21 gennaio 2022

Nuove funzionalità

Amazon DocumentDB 4.0 (patch del motore versione 2.0.5706)

- Le istanze Amazon DocumentDB Graviton2 (r6g.large, r6g.2xlarge, r6g.4xlarge, r6g.8xlarge, r6g.12xlarge, r6g.16xlarge e t4g.medium) sono ora supportate

Amazon DocumentDB 3.6 (patch del motore versione 1.0.207781) e 4.0 (patch del motore versione 2.0.5706)

- È stato aggiunto il supporto per le seguenti API MongoDB:
 - `$reduce`
 - `$mergeObjects`
 - `$geoWithin`
 - `$geoIntersects`

25 ottobre 2021

Nuove funzionalità

Amazon DocumentDB 3.6 (patch del motore versione 1.0.207780) e 4.0 (patch del motore versione 2.0.5704)

- Aggiunto il supporto per le seguenti API MongoDB
 - `$literal`
 - `$map`
 - `$$ROOT`
- Support per le funzionalità di GeoSpatial interrogazione. Leggi questo [post del blog](#) per maggiori dettagli
- Support per il controllo degli accessi con ruoli definiti dall'utente. Leggi questo [post sul blog](#) per maggiori dettagli
- Amazon DocumentDB JDBC Driver per abilitare la connettività da strumenti di BI come Tableau e strumenti di query come SQL Workbench

Correzioni di bug e altre modifiche

Amazon DocumentDB 3.6 (patch del motore versione 1.0.207780) e 4.0 (patch del motore versione 2.0.5704)

- Correzione di bug che impediva l'ordinamento corretto quando è presente un elemento esplicito `$natural` insieme a `.sort()` `$natural`
- Correzione di bug per il change stream con cui lavorare `$redact`
- Correzione di bug `$ifNull` per lavorare con un array vuoto
- Correzione di bug per un consumo eccessivo di risorse/arresto anomalo del server quando un utente attualmente connesso viene eliminato o il privilegio di quell'utente per un'attività in corso viene revocato
- Correzione dei bug e controllo dei privilegi `listDatabase` `listCollection`
- Bug Fix: logica di deduplicazione per elementi a più chiavi

24 giugno 2021

Nuove funzionalità

Amazon DocumentDB 3.6 (patch del motore versione 1.0.207117) e 4.0 (patch del motore versione 2.0.3371)

- Le istanze `r5.8xlarge` e `r5.16xlarge` sono ora supportate. Scopri di più nel post del blog [Amazon DocumentDB ora supporta le istanze r5.8xlarge e r5.16xlarge](#).
- [I cluster globali](#) sono ora supportati per fornire il disaster recovery da interruzioni a livello regionale e consentire letture globali a bassa latenza consentendo le letture dal cluster Amazon DocumentDB più vicino.

4 maggio 2021

Nuove funzionalità

[Scopri tutte le nuove funzionalità in questo post del blog.](#)

Amazon DocumentDB 3.6 (patch del motore versione 1.0.207117) e 4.0 (patch del motore versione 2.0.3371)

- `renameCollection`
- `$zip`
- `$indexOfArray`
- `$reverseArray`
- `$natural`
- `$hint` supporto per l'aggiornamento
- Scansione dell'indice per `distinct`

Correzioni di bug e altre modifiche

Amazon DocumentDB 3.6 (patch del motore versione 1.0.207117) e 4.0 (patch del motore versione 2.0.3371)

- Utilizzo `$in` ridotto della memoria per le query
- È stata corretta una perdita di memoria negli indici a più chiavi
- Risolto il problema del piano di spiegazione e dell'output del profiler per `$out`
- È stato aggiunto un timeout per le operazioni dal sistema di monitoraggio interno per migliorare l'affidabilità
- È stato corretto un difetto che influiva sui predicati di interrogazione passati agli indici a più chiavi

15 gennaio 2021

Nuove funzionalità

Amazon DocumentDB 4.0 (patch del motore versione 2.0.722)

- Nessuno

Amazon DocumentDB 3.6 (patch del motore versione 1.0.206295)

- Capacità di utilizzare un indice con la fase di aggregazione `$lookup`
- `find()` le interrogazioni con proiezioni possono essere indirizzate da un indice (interrogazione coperta)
- Possibilità di utilizzare `hint()` con `findAndModify`

- Ottimizzazioni delle prestazioni per l'operatore `$addToSet`
- Miglioramenti per ridurre le dimensioni complessive dell'indice
- Nuovi operatori di aggregazione: `$ifNull$replaceRoot`, `$setIsSubset`, `$setIntersection`, `$setUnion`, e `$setEquals`
- Gli utenti possono anche terminare i propri cursori senza richiedere il ruolo `KillCursor`

9 novembre 2020

Nuove funzionalità

Scopri tutte le nuove funzionalità in questo [post del blog](#).

Amazon DocumentDB 4.0 (patch del motore versione 2.0.722)

- Compatibilità con MongoDB 4.0
- Transazioni ACID
- Support per `cluster(client.watch() or mongo.watch())` e i flussi di `(db.watch())` modifica a livello di database
- Possibilità di avviare o riprendere un flusso di modifiche utilizzando `startAtOperationTime`
- Estendi il periodo di conservazione del flusso di modifiche a 7 giorni (in precedenza 24 ore)
- AWS DMS destinazione per Amazon DocumentDB 4.0
- CloudWatch metriche: `TransactionsOpen`, `TransactionsOpenMaxTransactionsAborted`, e `TransactionsStarted` `TransactionsCommitted`
- Nuovi campi per le transazioni in `currentOpServerStatus`, e `profiler`.
- Capacità di utilizzare un indice con la fase di `$lookup` aggregazione
- `find()` le interrogazioni con proiezioni possono essere indirizzate da un indice (interrogazione coperta)
- Possibilità di utilizzare `hint()` con `findAndModify`
- Ottimizzazioni delle prestazioni per l'operatore `$addToSet`
- Miglioramenti per ridurre le dimensioni complessive dell'indice.
- Nuovi operatori di aggregazione: `$ifNull$replaceRoot`, `$setIsSubset`, `$setIntersection`, `$setUnion`, e `$setEquals`

- Con i `ListDatabase` comandi `ListCollection` and, ora è possibile utilizzare facoltativamente i `authorizedDatabases` parametri `authorizedCollections` and per consentire agli utenti di elencare le raccolte e i database a cui hanno l'autorizzazione ad accedere senza richiedere rispettivamente i `listDatabase` ruoli `listCollections` e
- Gli utenti possono inoltre terminare i propri cursori senza richiedere il ruolo `KillCursor`
- Il confronto dei tipi numerici di documenti secondari è ora coerente con il confronto dei tipi numerici di documenti di primo livello. Il comportamento di Amazon DocumentDB 4.0 è ora compatibile con MongoDB.

Amazon DocumentDB 3.6 (patch del motore versione 1.0.206295)

- Nessuno

Correzioni di bug e altre modifiche

Amazon DocumentDB 4.0 (patch del motore versione 2.0.722)

- `$setOnInsert` non consente più aggiornamenti quando si utilizza l'operatore posizionale. \$ Il comportamento di Amazon DocumentDB 4.0 è ora compatibile con MongoDB.
- Problema risolto e impostato `$createCollection` `autoIndexId`
- Proiezione per documenti annidati
- Modificata l'impostazione predefinita per la memoria di lavoro in modo da adattarla alla dimensione della memoria dell'istanza
- Miglioramenti alla raccolta dei rifiuti
- Ricerca con chiave vuota nel percorso, differenza di comportamento con mongo
- Risolto un `dateToString` bug nel comportamento del fuso orario
- Risolto `$push` (aggregazione) per rispettare l'ordinamento
- Risolto un bug relativo all'`$currentOp` aggregato
- Risolto il problema relativo al `readPreference` secondario
- È stato risolto il problema relativo alla convalida dello stesso database in cui `$createIndex` è stato emesso il comando
- Risolto il problema del comportamento incoerente in caso di errore di `minKey` ricerca `maxKey`
- È stato risolto il problema che `$size` impediva all'operatore di utilizzare un array composito

- Risolto il problema con la negazione di `$in` con regex
- Risolto il problema con `$distinct` il comando eseguito su una vista
- È stato risolto il problema relativo alle aggregazioni e ai comandi di ricerca che ordinavano i campi mancanti in modo diverso
- Risolto `$eq` il problema che le espressioni regolari non controllavano il tipo
- Risolto `$currentDate` un bug nel comportamento della posizione ordinale del timestamp
- Granularità fissa in millisecondi per `$currentDate`

Amazon DocumentDB 3.6 (patch del motore versione 1.0.206295)

- Nessuno

30 ottobre 2020

Nuove funzionalità

[Scopri tutte le nuove funzionalità in questo post del blog.](#)

Amazon DocumentDB 3.6 (patch del motore versione 1.0.206295)

- È stata aggiunta la possibilità di aprire un cursore del flusso di modifica a livello di cluster o del database (`client.watch()` `mongo.watch()`) (`db.watch()`)
- Possibilità di aumentare il periodo di conservazione del flusso di modifiche a 7 giorni (in precedenza 24 ore)

Correzioni di bug e altre modifiche

Amazon DocumentDB 3.6 (patch del motore versione 1.0.206295)

- Vari miglioramenti generali delle prestazioni dei casi
- Un miglioramento mirato della sicurezza
- È stato risolto un problema con skip sort sul secondo campo di un indice composto
- Abilita l'indice regolare per l'uguaglianza su un singolo campo di un indice a più chiavi (non composto)
- Condizione di gara di autenticazione fissa

- È stato risolto il problema che causava un raro arresto anomalo della raccolta dei rifiuti
- Miglioramento della sicurezza RBAC
- Metrica aggiunta `databaseConnectionsMax`
- Miglioramenti delle prestazioni per determinati carichi di lavoro su istanze `r5.24xlarge`

22 settembre 2020

Nuove funzionalità

Scopri tutte le nuove funzionalità in questo [post del blog](#).

Amazon DocumentDB 3.6 (patch del motore versione 1.0.206295)

- \$outfase di aggregazione
- Il numero massimo di connessioni e cursore per istanza è stato aumentato fino a 10 volte

Correzioni di bug e altre modifiche

Amazon DocumentDB 3.6 (patch del motore versione 1.0.206295)

- Nessuno

10 luglio 2020

Nuove funzionalità

[Scopri tutte le nuove funzionalità in questo post del blog](#).

Amazon DocumentDB 3.6 (patch del motore versione 1.0.206295)

- Copia di snapshot interregionali

Correzioni di bug e altre modifiche

Amazon DocumentDB 3.6 (patch del motore versione 1.0.206295)

- Nessuno

30 giugno 2020

Nuove funzionalità

[Scopri tutte le nuove funzionalità in questo post del blog.](#)

Amazon DocumentDB 3.6 (patch del motore versione 1.0.206295)

- Istanze medie T3

Correzioni di bug e altre modifiche

Amazon DocumentDB 3.6 (patch del motore versione 1.0.206295)

- Recupero della memoria inattiva per le istanze t3
- Miglioramenti dell'autenticazione
- Prestazioni di autenticazione SASL migliorate
- `currentOpProblema` risolto che si verificava quando si superava il numero massimo di operazioni possibili
- `killOpsProblema` risolto per l'aggiornamento e l'eliminazione in blocco
- Miglioramenti `$sample` delle prestazioni con `$match`
- Supporto fisso per `$$` in cond case in fase di redazione
- Risolte varie cause ricorrenti di crash root
- Miglioramenti allo sweeping TTL per ridurre iOS e la latenza
- Utilizzo ottimizzato della memoria per `$unwind`
- Raccolta fissa, statistiche, condizioni di gara con indice di calo
- Condizione di gara fissa durante la creazione simultanea dell'indice
- Risolto un raro crash nell'indice `hash_search`

Cronologia dei documenti per la Amazon DocumentDB Developer Guide

- Versione API: 31-10-2014
- Ultimo aggiornamento della documentazione: 2 giugno 2023

La tabella seguente descrive la documentazione per questa versione della Amazon DocumentDB Developer Guide.

Modifica	Descrizione	Data
AWS aggiornamento gestito della politica: modifica della politica	Amazon DocumentDB aggiorna le policy di accesso completo per i cluster elastici.	21 febbraio 2024
AWS aggiornamento gestito della politica: modifica della politica	Amazon DocumentDB aggiorna le policy di sola lettura e di accesso completo per i cluster elastici.	21 giugno 2023
AWS aggiornamento gestito della politica: nuova politica	Amazon DocumentDB introduce una nuova policy di sola lettura per i cluster elastici.	8 giugno 2023
AWS aggiornamento gestito della politica: nuova politica	Amazon DocumentDB introduce una nuova policy di accesso completo per i cluster elastici.	5 giugno 2023
Compatibilità con MongoDB 5.0	Amazon DocumentDB è ora compatibile con la versione 5.0 di MongoDB.	1 marzo 2023
Aggiornamento della politica	Per supportare la funzionalità di cluster elastico di Amazon	30 novembre 2022

	AmazonDoc DocumentDB, la ConsoleFullAccess policy del database viene aggiornata e ElasticServiceRolePolicy viene introdotto il AmazonDoc DB-.	
Cluster elastici	È stata aggiunta una nuova funzionalità Elastic Cluster che supporta il partizionamento (sharding) basato su hash dei dati nel sistema di storage distribuito di Amazon DocumentDB.	30 novembre 2022
Cluster globali	È stata aggiunta documentazione su come utilizzare Global Clusters.	2 giugno 2021
Sottoscrizioni agli eventi	È stata aggiunta la documentazione relativa all'abbonamento agli eventi.	26 marzo 2021
Aggiornamenti alla versione 3.6	Miglioramenti documentati alla versione 3.6 nei controlli di accesso basati sui ruoli, negli operatori di aggregazione e nelle prestazioni.	15 gennaio 2021
Compatibilità con MongoDB 4.0	Amazon DocumentDB è ora compatibile con la versione 4.0 di MongoDB.	9 novembre 2020
Guide introduttive	Nuove guide introduttive per iniziare a usare Amazon DocumentDB utilizzando Amazon EC2 AWS Cloud9, Robo3T o Studio3T.	15 agosto 2020

Zone di disponibilità aggiuntive supportate	Amazon DocumentDB ha aggiunto il supporto per una zona di disponibilità aggiuntiva in Asia Pacifico (Seoul) (ap-northeast-2).	14 luglio 2020
È stato aggiunto il supporto per la copia di istantanee tra regioni.	Amazon DocumentDB ha aggiunto il supporto per la copia di istantanee di cluster su più file. Regioni AWS Per ulteriori informazioni, consulta Copiare istantanee tra regioni.	10 luglio 2020
È stato aggiunto il supporto per la classe di istanze T3.	È stato aggiunto il supporto per i tipi di istanze T3 in tutte le regioni che supportano Amazon DocumentDB. Per ulteriori informazioni, consulta Classi di istanze supportate per regione e Specifiche delle classi di istanza .	30 giugno 2020
È stato aggiunto il supporto per AWS GovCloud (US).	Amazon DocumentDB è ora disponibile nella AWS GovCloud (US) regione (us-gov-west-1).	29 giugno 2020
Aggiunte 16 nuove CloudWatch metriche.	Amazon DocumentDB ha aggiunto il supporto per 16 nuovi parametri Amazon CloudWatch . Per ulteriori informazioni, consulta Monitoring Amazon DocumentDB with. CloudWatch	23 giugno 2020

[È stato aggiunto il supporto per i caratteri null e l'operatore \\$regex.](#)

Amazon DocumentDB ha aggiunto il supporto per i caratteri null nelle stringhe e la possibilità di utilizzare un indice per \$regex. [Per visualizzare le API MongoDB supportate e le funzionalità della pipeline di aggregazione per Amazon DocumentDB, consulta Differenze funzionali con MongoDB.](#)

22 giugno 2020

[È stato aggiunto il supporto per funzionalità di indicizzazione a più chiavi migliorate.](#)

Amazon DocumentDB ha aggiunto il supporto per funzionalità di indicizzazione a più chiavi migliorate e che includono l'indicizzazione di array di dimensioni superiori a 2.048 byte e la possibilità di creare un indice composto a più chiavi con più chiavi nello stesso array. Per ulteriori informazioni, consulta [Differenze funzionali con MongoDB.](#)

23 aprile 2020

[È stato aggiunto il supporto per la protezione da eliminazione per uno stack Amazon DocumentDB. AWS CloudFormation](#)

Amazon DocumentDB ha aggiunto il supporto per abilitare la protezione da eliminazione durante la creazione di uno stack Amazon AWS CloudFormation DocumentDB.

20 aprile 2020

<u>È stato aggiunto il supporto per il controllo degli accessi basato sui ruoli.</u>	Amazon DocumentDB ha aggiunto il supporto per il controllo degli accessi basato sui ruoli utilizzando ruoli integrati.	26 marzo 2020
<u>È stato aggiunto il supporto per una zona di disponibilità aggiuntiva in Canada (Central) (ca-central-1).</u>	Amazon DocumentDB è ora disponibile nella regione Canada (Centrale) (ca-central-1) con istanze di classe R5 e 3 zone di disponibilità.	26 marzo 2020
<u>È stato aggiunto il supporto per due API MongoDB aggiuntive.</u>	Amazon DocumentDB ha aggiunto il supporto per le API <code>\$dateFromString</code> e <code>MongoDBexecutionStats</code> .	23 marzo 2020
<u>È stato aggiunto il supporto per cinque API MongoDB aggiuntive.</u>	Amazon DocumentDB ha aggiunto il supporto per <code>\$objectToArray</code> , <code>\$arrayToObject</code> , <code>\$slice\$mod</code> , e le API <code>MongoDB\$range</code> .	6 febbraio 2020
<u>È stato aggiunto il supporto per Canada (Central).</u>	Amazon DocumentDB è ora disponibile nella regione Canada (Central) (ca-central-1) con istanze di classe R5.	11 dicembre 2019
<u>ChangeStreamLogSizeÈ stato aggiunto il supporto per.</u>	Amazon DocumentDB ha aggiunto il supporto <code>ChangeStreamLogSize</code> per i parametri di Cloudwatch.	22 novembre 2019
<u>È stato aggiunto il supporto per la regione Europa (Parigi)</u>	Amazon DocumentDB è ora disponibile nella regione Europa (Parigi) (eu-west-3) con istanze di classe R5.	30 ottobre 2019

È stato aggiunto il supporto per la regione Asia Pacifico (Mumbai)	Amazon DocumentDB è ora disponibile nella regione Asia Pacifico (Mumbai) (ap-south-1) con istanze di classe R5.	17 ottobre 2019
Aggiunto il supporto per tre API MongoDB aggiuntive	Amazon DocumentDB ha aggiunto il supporto per le <code>\$addField</code> s <code>\$concatArrays</code> , e le API <code>MongoDB\$lookup</code> .	16 ottobre 2019
È stato aggiunto il supporto per la regione Asia Pacifico (Singapore)	Amazon DocumentDB è ora disponibile nella regione Asia Pacifico (Singapore) (ap-south-east-1) con istanze di classe R5.	14 ottobre 2019
Aggiunto un nuovo documento per l'aggiornamento dei certificati TLS	Sono state aggiunte istruzioni per l'aggiornamento dei certificati CA per utilizzare il nuovo certificato CA per creare connessioni TLS.	2 ottobre 2019
Aggiunto il supporto API per i certificati	Amazon DocumentDB è un nuovo tipo di dati Certificate per le istanze. Per ulteriori informazioni, consulta DBInstance .	1 ottobre 2019
Support per la profilazione delle query	Amazon DocumentDB ha aggiunto la possibilità di profilare le operazioni supportate sulle istanze e sui database del cluster.	19 agosto 2019

È stata aggiunta una terza AZ in Asia Pacifico (Tokyo)	Amazon DocumentDB ha aggiunto una terza zona di disponibilità (AZ) per le istanze di calcolo in Asia Pacifico (Tokyo).	9 agosto 2019
Support per API Mongo aggiuntive	È stato aggiunto il supporto per funzionalità aggiuntive della pipeline di aggregazione che includono gli operatori <code>\$in</code> , <code>\$isoWeek</code> <code>\$isoWeekYear</code> <code>\$isoDayOfWeek</code> , e di aggregazione e la fase di <code>\$dateToString</code> aggregazione. <code>\$addToSet</code> Amazon DocumentDB ha inoltre aggiunto il supporto per il <code>top()</code> comando per la diagnostica a livello di raccolta e la possibilità di modificare il <code>expireAfterSeconds</code> parametro per gli indici TTL utilizzando il comando. <code>collMod()</code>	31 luglio 2019
È stato aggiunto il supporto per l'Europa (Londra)	Amazon DocumentDB è ora disponibile in Europa (Londra) (eu-west-2) con istanze di classe R5.	18 luglio 2019
Sono stati aggiunti esempi di codice	Sono stati aggiunti esempi di codice in R e Ruby per la connessione programmatica ad Amazon DocumentDB.	17 luglio 2019

Sono state aggiunte le migliori pratiche	È stata aggiunta una best practice per aiutarti a gestire i costi di Amazon DocumentDB.	17 luglio 2019
Support per l'arresto e l'avvio di un cluster	Amazon DocumentDB ha aggiunto il supporto per l'arresto e l'avvio dei cluster per gestire i costi per gli ambienti di sviluppo e test.	1 luglio 2019
Support per la protezione dall'eliminazione dei cluster	Per proteggere i cluster dall'eliminazione accidentale, Amazon DocumentDB ha aggiunto la protezione dall'eliminazione. Per ulteriori informazioni, consulta i seguenti argomenti: Creazione di un cluster Amazon DocumentDB, Modifica di un cluster Amazon DocumentDB, Eliminazione di un cluster Amazon DocumentDB e nell'argomento API DBCluster. DeletionProtection	1 luglio 2019
Aggiornamento delle differenze funzionali	Aggiunte le transazioni implicite alle differenze funzionali.	26 giugno 2019
Aggiunta di differenze funzionali	È stata aggiunta una nota relativa allo storage e alla compressione degli indici in Amazon DocumentDB.	13 giugno 2019

Regione aggiuntiva supportata	Amazon DocumentDB è ora disponibile in Asia Pacifico (Sydney) (ap-southeast-2) con istanze di classe R5.	5 giugno 2019
Classe di istanza R5 supportata in altre regioni	Aggiunto il supporto per la classe di istanza R5 per 4 altre regioni: Stati Uniti orientali (Ohio), Stati Uniti orientali (Virginia settentrionale), Stati Uniti occidentali (Oregon) e UE (Irlanda). Con questa modifica, le istanze R5 sono supportate in tutte le regioni che supportano Amazon DocumentDB.	17 maggio 2019
Regioni aggiuntive supportate	È stato aggiunto il supporto per 2 regioni aggiuntive, Asia Pacifico (Tokyo) (ap-north-east-1) e Asia Pacifico (Seoul) (ap-northeast-2) con classi di istanze R5. Per ulteriori informazioni, consultare Classi di istanze supportate in base alle regioni e Specifiche delle classi delle istanze .	8 maggio 2019
Sono stati aggiunti altri esempi di codici di connessione	Sono stati aggiunti esempi di codice in Java e C# per la connessione ad Amazon DocumentDB.	24 aprile 2019

[Supporto aggiuntivo per l'API Mongo](#)

Aggiunto il supporto per sette operatori di stringa di aggregazione (`$indexOfBytes` , `$indexOfCP` , `$strLenBytes` , `$strLenCP` , `$toLowerCase` , `$toUpperCase` , `$split`), nove operatori data-ora (`$dayOfYear` , `$dayOfMonth` , `$dayOfWeek` , `$year` , `$month` , `$hour` , `$minute` , `$second` , `$millisecond`) e la fase `$sample` della pipeline di aggregazione.

4 aprile 2019

[Aggiunti esempi di codice di connessione](#)

Sono stati aggiunti esempi di codice in Python, Node.js, PHP e Go per la connessione ad Amazon DocumentDB.

21 marzo 2019

[Support per la regione di Francoforte e le istanze R5](#)

È stato aggiunto il supporto per la regione Europa (Francoforte) (eu-central-1) con classi di istanze R5. Per ulteriori informazioni, consultare [Classi di istanze supportate in base alle regioni](#) e [Specifiche e delle classi delle istanze](#).

13 marzo 2019

[Supporto per gli operatori di pipeline di aggregazione](#)

Aggiunto il supporto per i nuovi operatori di stringa di aggregazione (`$concat`, `$substr`, `$substrBytes`, `$substrCP`, `$strcasecmp`), un operatore di aggregazione di array (`$size`), un operatore accumulatore per gruppo di aggregazione (`$push`) e fasi di aggregazione (`$redact` e `$indexStats`). Aggiunto anche il supporto per gli operatori di array posizionali (`$[]` e `$[<identifier>]`) e `hint()`.

28 febbraio 2019

[Aggiornamenti del motore](#)

Aggiunta la documentazione per determinare le modifiche del cluster in sospeso e per aggiornare la versione del motore del cluster.

15 febbraio 2019

[Eventi di controllo](#)

È stato aggiunto il supporto per il controllo degli eventi del database con Amazon CloudWatch Logs.

12 febbraio 2019

[Quick Start](#)

È stato aggiunto un argomento Quick Start per aiutarti a iniziare facilmente a usare Amazon DocumentDB. AWS CloudFormation

11 gennaio 2019

[Rilascio pubblico](#)

Questa è la versione pubblica iniziale di Amazon DocumentDB (con compatibilità con MongoDB). Questa release include la [guida per gli sviluppatori](#) e la [documentazione integrata di riferimento sulle API per la gestione delle risorse](#).

9 gennaio 2019

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.